European Investigations Guide

2024

With contributions from:

A&L Goodbody
ASTERS
Babić & Partners
BORENIUS
Camilleri Preziosi
Cerrahoğlu
Chrysses Demetriades
COBALT
Ellex
Gasser Partner
HAVEL & PARTNERS
Hogan Lovells
Kalo & Associates
Kambourov & Partners
KINSTELLAR
KNOETZL
Kromann Reumert
Lutgen + Associés
Mareş & Mareş
NORDIA
Ovvadias S. Namias
SENICA
taormina
Uría Menéndez
Wikborg Rein

European Investigations Guide 2024

Published by

Hogan Lovells International LLP

Karl-Scharnagl-Ring 5

80539 Munich

Germany

Fourth Edition
Printing 2024

Contributing editors

Dr. Sebastian Lach, Hogan Lovells

Dr. Lukas Ritzenhoff, Hogan Lovells

Carolin Binder, Hogan Lovells

Angeliki Lampousi, Hogan Lovells

Silvia Gardini, Hogan Lovells

Editorial assistants

Stephanie Küppers, Hogan Lovells

Lorena Zagari, Hogan Lovells

Contents

Preface

Dear Reader,

On behalf of all colleagues and experts involved, we are proud to publish the fourth and updated edition of the European Investigations Guide. This guide continues to be designed to provide you with a quick reference to some of the most pressing questions and trends relating to internal investigations in European countries.

Although it is important to note that this guide cannot, and is not intended to, replace any kind of legal advice in individual cases, it will help the compliance expert to identify the risks arising and the right questions to ask to address those risks. To that end, leading practitioners from various European countries have provided their expert input on such issues in their jurisdiction. As this guide presents the view of experts on legal issues, we can, of course, not exclude that courts, authorities, and other third parties might hold or take different views.

We hope that you will find the European Investigations Guide helpful and would like to thank you for your interest in this publication.

Dr. Sebastian Lach

Partner
Hogan Lovells

Cross-Border Investigations

INTRODUCTION

The more countries and jurisdictions are involved, the harder it becomes to run and complete an investigation quickly, efficiently, and comprehensively. Various issues arise like language barriers, different cultural perceptions, local laws, data privacy provisions, and blocking statutes. All of those have to be coordinated at the same time. Such investigations are, therefore, not only difficult to complete but also bear the risk that the investigation itself may lead to cases of non-compliance. As a consequence, those in charge of such investigations have to be mindful to avoid generating such risks – also for themselves personally.

While it is no substitute for individually tailored legal advice, this Guide aims to reduce those very risks. It provides a general overview of investigations on the European continent to help orient those leading or involved with such investigations. The following article provides an overview of the most important questions and considerations that arise during the various stages of an investigation – from the beginning to the end.

INVESTIGATING COMPLIANCE HOTLINE REPORTS

All around the world, employees are more and more encouraged to raise concerns and report violations of legal, compliance, or ethical topics. In Europe, companies continuously need to monitor legal developments in that regard, in particular, the implementation of the EU Whistleblower Protection Directive (EU) 2019/1937.

The EU Whistleblower Protection Directive aims to provide common minimum standards of protection to whistleblowers who report breaches of EU law from their employer. It contains requirements particularly on the reporting channels to be set up, the communication with reporters, and the responsibilities for investigating the compliance reports. In addition, the EU Whistleblower Protection Directive compels the member states to provide effective penalties, for example, for hindering whistleblower reports.

Even though the implementation deadline expired by 17 December 2021, not all EU member states have yet implemented the directive. This is why, on 27 January 2022, the European Commission initiated infringement proceedings against a total of 24 European countries. The European Commission has thereby set an ultimatum to implement the directive into national law. In 2023, the Commission took Germany, Italy and six other countries to the European Court of Justice and demanded monetary sanctions with the cases still pending. At the beginning of 2024, only Poland and Estonia had still not transposed the directive into national law.

The extent to which the directive has so far been implemented varies from one member state to another. In some member states, the law only meets the directive's minimum requirements. In contrast, other countries broadened the scope and focused on stronger protection of whistleblowers. Therefore, the various adoptions and reforms as well as administrative guidelines regarding the EU Whistleblower Protection Directive in each member state's national law need to be monitored.

START OF A CROSS-BORDER INVESTIGATION

After an initial assessment of which countries are implicated in the investigation, various issues have to be considered

The first question is often whether local support is needed. The answer will often be yes. Mostly, local in-house legal capabilities will be sufficient. However, outside counsel or other external resources will sometimes have to be consulted. In this regard, it has to be noted that it may prove difficult to find the right experts in certain countries. In many locations, there is seldom an abundance of white collar crime or compliance experts. Therefore, it is advisable to build and maintain a network of experts in the most important countries, even before an investigation starts. In crisis situations (like dawn raids or cyber-attacks), there may not be time to search for local support. Even if there is time, if competitors or other companies are faced with the same problem, the best counsel may already have been taken or may already be conflicted once they are approached. Working with non-expert counsel, especially in smaller legal markets, can bear risks and create inefficiencies.

Once the team has been assembled, the next question is whether one is even allowed to investigate in the respective country. This question must be answered with the help of dedicated local counsel. In this regard, one has to differentiate between blocking statutes and data privacy considerations. A blocking statute will often mean that all or certain investigative measures may not be allowed or only with special permission. Data privacy concerns relate to the treatment of data containing personal information, but they rarely present an absolute obstacle to any investigative step. To provide a simple example: A blocking statute may prevent an interview, while data privacy laws may simply limit the use of information gathered from an interview or call for special measures for the collection and treatment of that data.

Once the question of blocking statutes has been addressed, one may have to clarify whether specific bodies like trade unions, works councils, corporate supervisory boards, financial stakeholders and shareholders have to be informed of the start of the investigation or the information that led to the investigation. Some local laws have very rigid and detailed disclosure requirements. The violation of any such requirements might hinder the investigation or even lead to civil or criminal liability of the company or the individual actors.

In addition, it must be carefully assessed whether early disclosures to local law enforcement agencies are necessary or would be helpful from a strategic standpoint. In some countries, certain situations call for such disclosure under the applicable local laws. In other countries, it is culturally necessary to involve the authorities to maintain a cooperative atmosphere. In other countries, however, such disclosures are uncommon and may create more problems than they solve. In cross-border cases, where many authorities may be involved, there may be a strategic advantage to disclosing information in a certain order or having one authority take the lead. Especially at this stage, local expertise – legally and culturally – is very helpful to avoid making the wrong decisions.

THE INVESTIGATIVE PHASE

Once all obstacles that may hinder the start of an investigation have been cleared, the company can start the investigation.

An investigation often begins with so-called immediate measures. Normally, the first task is to ensure that any potentially ongoing criminal or unlawful conduct is stopped. This frequently means monitoring certain payment streams or putting specific individuals at least under close monitoring to make sure that all their actions are appropriate going forward. It may also mean checking whether certain products can still be sold on the market.

Another early step is to ensure that all data potentially relevant to the investigation is preserved. This may entail a wide range of measures, from issuing a data hold to suspending auto-delete functions to immediately imaging data carriers. These measures play an important role in dissuading local prosecutors from performing dawn raids. If one can demonstrate that all relevant data has been stored securely, it may even be disproportionate for prosecutors to raid companies.

The investigation team then has to decide who will formally lead the investigation. The question often comes down to whether this is done by in-house counsel or external lawyers. In this regard, the sensitivity of the matter and privilege protection will often be decisive factors. The rule of thumb is that countries in Continental Europe often award very little privilege protection to in-house counsel. This can even mean that work product of outside counsel in the custody of the company's in-house counsel could be seized and reviewed by the authorities in some jurisdictions. Therefore, the decision is not only who runs the investigation but also where to generate and store sensitive work products.

In particular when communicating with reporters, performing interviews, collecting and reviewing information, data privacy laws have to be considered. The good news is that a uniform European Data Privacy Regulation came into force in 2018. This reduced the impact of local law specifics. On the other hand, local law specifics are not entirely abolished. For example, certain labour laws or criminal laws may contain stricter provisions on data handling. In addition, potential penalties substantially increased, and rules became more stringent. Given the potential legal exposure and the complexity of the issue, it is strongly recommended that expert data privacy counsel be part of any cross-border investigation team in all phases. Another specific issue in cross-border cases is the "export" of data to other countries. This can be particularly problematic if such countries do not have an equivalent level of data privacy protection compared to the European Union. This may necessitate a case-by-case analysis and may also call for additional protective measures like reducing data amounts or redacting personal information before any data transfer.

The right of participation of works councils and/or trade unions during an investigation may also need to be considered. Local laws will have different views in this regard. A mistake in this area can have serious consequences. It cannot only damage the relationship between the company and its employees, but it can also lead to the end or at least to an interruption of the investigation itself. Disregarding the rights of a works council may allow this body to obtain a cease-and-desist order against the investigation.

Interviews often also raise various legal issues, such as the need for data privacy waivers and the need for special instructions on the right to not self-incriminate or the right to legal counsel. Each jurisdiction has its own rules and best practices in this regard. If an interviewee is not adequately instructed or the interview is otherwise not done correctly, these issues can lead to evidence being deemed inadmissible down the road.

THE END OF THE INVESTIGATION

Questions arising at the end of an investigation may also vary from one jurisdiction to the other. However, some issues are frequently in focus in many countries.

The first question, which comes up rather frequently, is whether a detailed investigation report should be produced or not. This is, again, linked to the question of privilege. If in-house counsel produces an investigation report, this report may not be privileged in many countries on the European continent. Even if outside counsel produces the report, it may have only limited protection if it enters into the custody of the company. In some countries, authorities may view the waiver of privilege and production of the report as necessary to demonstrate good faith and cooperation. There may then be pressure to produce such a report.

Another step at the end of the life cycle of an investigation is remediation. Firstly, this may make an update of internal processes necessary. What is legally possible and state of the art with respect to internal guidelines may differ greatly, especially throughout Europe. For companies operating in multiple jurisdictions, it may be necessary to conform worldwide internal guidelines to the higher legal standard in the home jurisdiction, even though a lower standard may be permissible in local jurisdictions. In the end, it is often in the home jurisdiction where the biggest risks lie.

Secondly, personnel measures like warning letters, training and terminations will play an important role in any remediation. In this regard, it is important to note that countries may have different deadlines for implementing personnel measures. If the deadlines are missed, personnel measures may not be taken for that reason alone. Furthermore, it may be necessary to involve works councils or trade unions in such processes. The prerequisites for termination will also differ greatly among countries. For example, it may be much easier to terminate an employee in the United Kingdom than in France or Germany.

Finally, a step that is sometimes missed at the end of an investigation is recovery. In many countries, board members are responsible for compliance in companies. If a major compliance failure arises, board members may be liable to the company if they had knowledge of the conduct or if they had responsibility for the respective compliance topic and failed to implement an appropriate compliance system. The company may then even be under a duty to assess such claims against its own board members and – if there is substance to such claims – pursue them. This may even mean that if the company or its management fails to assess and pursue such claims, those responsible for the assessment may themselves be liable for the omission. In Germany, for example, this can even lead to the criminal liability of the supervisory board for breach of fiduciary duties.

CONCLUSION

When doing a cross-border investigation in or involving Europe, many steps have to be kept in mind. Issues can arise at every stage in the life cycle of an investigation. It is not necessary to know all the answers from the beginning, but important to ask the right questions. Once a potential issue has been identified, the investigative process can be set up and managed in a way that minimises risks.

AUTHORS

Dr. Sebastian Lach

Partner
Hogan Lovells Munich
T +49 69 96236 308
E sebastian.lach@hoganlovells.com

Sebastian Lach leads the German Compliance and Investigations practice and is co-CEO of ELTEMATE – the Hogan Lovells technology company.

Sebastian has successfully advised on a wide range of criminal investigations relating to more than 50 countries, including FCPA, SEC/DOJ implications. He is therefore familiar with appropriate use cases for all major eDiscovery platforms and tools as well as databases. Most of his investigations for Fortune 500 and DAX 40 clients included vast technology-driven data forensics, including data collection, data processing and data review. With his understanding of technology in the legal industry, he was instrumental in developing the firm's legal tech strategy. In his role as Co-CEO of ELTEMATE, he leads a market-leading team of AI experts, data scientists, software engineers and data analytics professionals focused on developing innovative AI solutions, particularly in the area of generative AI.

Sebastian Lach utilises his extensive experience of over 15 years working at the intersection of technology and legal practice to advise clients on the selection and implementation of cutting-edge legal tech solutions.

Désirée Maier

Partner
Hogan Lovells Munich
T +49 89 29012 340
E desiree.maier@hoganlovells.com

Désirée Maier advises clients on issues relating to white-collar criminal law and compliance. She has particular expertise in the life sciences and health care sector.

One focus of her work lies on setting up and conducting cross-border investigations and in the defence against allegations of a criminal nature. She has extensive experience in advising during dawn raids, coordinating compliance of investigations with requirements under German, local law, U.S. and UK law as well as communicating with law enforcement authorities.

Désirée also regularly advises on the establishment and implementation of global compliance systems, including the performance of compliance audits. In addition, she has expertise in connection with civil law claims arising from compliance matters.

Désirée worked in the legal department of a U.S. Fortune 500 company with global responsibility for internal investigations and is head of the compliance working group of the German Mergers & Acquisitions Association.

Dr. Lukas Ritzenhoff

Partner
Hogan Lovells Berlin
T +49 30 800 9300 60
E lukas.ritzenhoff@hoganlovells.com

Lukas Ritzenhoff advises clients from various industries on white collar criminal law issues, compliance and internal investigations. He is particularly experienced in highly regulated industries.

Lukas has extensive experience in assisting with dawn raids and cross-border regulatory investigations, conducting internal investigations and compliance audits. He also advises on the development and implementation of global compliance management systems. One of his main areas of focus is the implementation of legal tech tools and the use of artificial intelligence.

He was listed as one of the most renowned lawyers for compliance by WirtschaftsWoche in 2023 and 2019 and was named by Legal 500 Germany as a "Rising Star" in the field of compliance for 2024.

Data Privacy in Investigations

*Companies must observe strict data protection law requirements when conducting an internal investigation. The European General Data Protection Regulation (EU) 2016/679 ("**GDPR**") provides a uniform set of rules for data processing throughout the European Union, which replaced the existing patchwork of national laws governing how personal data is handled. The GDPR imposes strict and detailed obligations for companies processing personal data, including extensive accountability obligations. Failure to demonstrate compliance with these rules could lead to claims for damages as well as administrative sanctions and high fines from the competent data protection authorities. In addition, despite harmonisation on the European level, national differences must be taken into account, such as specific national law provisions in the area of processing of employee data that can have a substantial impact on how internal investigations can effectively be conducted.*

The following sections shall provide a general overview of the requirements and conditions for internal investigations under the GDPR. The text also highlights relevant case law and potential consequences of unlawful processing.

WHAT IS THE LEGAL BASIS FOR PERFORMING INTERNAL INVESTIGATIONS UNDER THE GDPR?

Companies may only perform internal investigations if they can rely on a valid legal basis for the intended data processing operations. The appropriate legal basis depends on the purpose of the investigation, the categories of data subjects affected, and the nature of the data concerned.

- **Legal obligation to perform investigation:** Under certain conditions, companies may be legally obliged to perform an internal investigation. In this case, the company may legitimise the data processing based on Article 6(1) lit. c GDPR. However, such cases will likely remain an exception in practice.
- **Data processing due to legitimate interests:** Companies may further justify the data processing to the extent the processing is necessary for legitimate interests pursued by the company or a third party (Article 6(1) lit. f GDPR), provided that the legitimate interests of the affected data subjects do not supersede. This legal basis (which in practice will often form the only available legal ground) requires a thorough balancing of interests, taking into account all circumstances of the individual case, including the extent of the investigation, the nature of the data processed, the reasonable expectations of the data subjects and the potential consequences for their rights and freedoms. The envisaged processing activities are not admissible if there are less intrusive measures to achieve the purposes of the investigation. A key aspect of the balancing of interests will be the implementation of safeguards to reduce the impact on the data subject and to ensure a proportionate approach in compliance with the data protection principles (see below). The legitimate interest assessment ("**LIA**") should be thoroughly documented.
- **Consent of data subject:** The GDPR stipulates strict requirements for obtaining valid consent, including, in particular, that consent must be freely given. This means that data subjects must have a real choice to agree to the related processing of their personal data or not, and also to withdraw any consent given at any time. Therefore, consent is not advisable as a general legal basis for permitting an internal investigation. Particularly within an employment context, due to the imbalance between the employee and the employer, consent will likely not be considered voluntary. This may potentially be different where the processing implies any legal or economic advantage for the employee or the employer and employee pursue similar interests, such as in limited scenarios for certain types of custodians or whistleblowers who are free to provide their consent or not.
- **Collective agreements:** Collective agreements (in particular works council agreements) may – to some extent – also form a legal basis (or at least additional safeguard) for internal investigations. However, collective agreements intended to legitimise data processing must comply with the specific requirements of Article 88 GDPR and potential national implementations laws (see below).

If the internal investigation also involves special categories of personal data within the meaning of Article 9(1) GDPR (e.g. race, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation, health data)

additional restrictions apply. Companies may only process sensitive data if they can rely on one of the exemptions stated in Article 9(2) GDPR, in addition to a legal basis under Article 6(1) GDPR as set out above. In particular, companies may process sensitive data to the extent necessary for the establishment, exercise or defence of legal claims (Article 9(2) lit. g GDPR). On the other hand, companies cannot legitimise the processing of sensitive data merely on the basis of their legitimate interests.

WHAT OTHER REQUIREMENTS DO COMPANIES HAVE TO CONSIDER?

The GDPR and national implementation laws, where applicable, provide for additional requirements and conditions for internal investigations.

- **Compliance with data protection principles:** When performing internal investigations, companies have to comply with the general principles of data processing set out in Article 5 GDPR (i.e. lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity, and confidentiality). In particular, companies should carefully assess whether the intended processing of personal data is limited to what is necessary and whether all data is in fact adequate and relevant for the investigation. Where possible, companies should only process anonymised or pseudonymised data. Proportionality is a key aspect and may require, among other things, a thorough definition of search terms, a limitation of the group of data subjects concerned, the use of automated filtering, the implementation of pseudonymisation, and other safeguards.
- **Considering national implementation laws:** National laws implemented under the GDPR and other legal national particularities may provide for additional requirements for internal investigations. As an example, the German Federal Data Protection Act ("**BDSG**") and principles established by national court law impose strict requirements on companies willing to perform internal investigations in the employment context. In addition, the German law provisions implementing the European e-privacy rules are interpreted to impose strict limitations on the possibilities of an employer to access and review electronic communications of its employees, such as emails, where private use of the employer's IT and communication systems is permitted (with potential liability under criminal law). Also, the specific (and differing) national laws transposing the EU Whistleblower Directive can impact data protection law aspects in the context of internal investigations triggered by whistleblowers. For example, the German Whistleblower Protection Act ("**HinSchG**") provides for a separate legal basis for processing of personal data in the context of the operation of a whistleblower system, and leads to certain modifications of the principles established under the GDPR (such as by stipulating specific confidentiality restrictions in respect of information and access rights).
- **Accountability obligations:** The GDPR imposes strict accountability and documentation obligations (Article 5(2), Article 24(1) GDPR). In particular, companies must not only take all necessary measures to ensure compliance with data protection laws but also be able to prove, such as in the case of enquiries from the data protection authorities, that they have performed the internal investigation in accordance with the GDPR. To comply with these obligations, companies should establish a documented data protection concept and investigation plan setting out the legal considerations and all technical and organisational safeguards implemented for conducting the internal investigation and should comprehensively document every step taken.
- **Information of data subjects:** In general, companies must inform affected data subjects about the processing of their personal data in advance (Articles 12 *et seq*. GDPR). This applies, in principle, also in the case of internal investigations. However, the success of the investigation might be at risk if the suspect is informed about the envisaged data processing in advance. The GDPR does not provide for explicit exceptions to the notification requirements for such cases. The national implementation laws, however, may include respective provisions. For instance, under German law, companies do not have to inform data subjects in certain scenarios where the information would impair the establishment, exercise or defence of legal claims. However, there is no uniform implementation on national level across Europe. Therefore, companies should carefully assess in each case to what extent national exceptions can be relied upon. Whenever possible, companies should inform affected data subjects prior to the investigation.

- **Data transfer to third parties:** It might be necessary for companies to transfer personal data to third parties outside the company, either to analyse the information with the help of external advisors or to share the results of an investigation with third parties, such as in case of disclosures to courts or law enforcement authorities. Such data transfers must also comply with the requirements of the GDPR. Where external service providers are involved, acting only as processors on behalf and in accordance with the instructions of the company conducting the investigation, the data can likely be shared if an appropriate data processing agreement is entered into, which reflects the requirements under Article 28 GDPR. In other data transfer scenarios to controllers, companies will have to thoroughly assess whether and on which legal basis the data can be shared and what safeguards need to be implemented to protect the personal data. Where cross-border transfers are made, the authorities require companies to take a layered approach to reduce the impact on the rights and freedoms of data subjects, requiring in some cases to limit the transfer at least initially to only anonymised or pseudonymised data. In addition, the transfer of personal data to recipients in third countries outside the European Economic Area is only permitted where the strict requirements for international data transfers according to Articles 44 *et seq*. GDPR are met. In its 2021 decision (*Schrems II*), the Court of Justice in the European Union (CJEU) has stipulated strict requirements for the necessary assessment to be carried out by data exporters transferring personal data to recipients in third countries not benefitting from an adequacy decision. In many cases, specific safeguards need to be implemented to ensure an adequate protection of personal data, such as by entering into additional agreements with the recipients outside the European Economic Area and by implementing additional supplementary technical and organisational safeguards to ensure that the legal regime in the third country does not impinge upon the effectiveness of the selected transfer mechanism. Appropriate documentation needs to be in place to demonstrate compliance with these requirements. In 2023, the European Commission recognised an adequate level of data protection for transfers to U.S. recipients participating in the EU–U.S. Data Privacy Framework which substantially reduces (but does not fully exclude) obligations for companies exporting data to the U.S.
- **Data protection impact assessment ("DPIA"):** A DPIA must be performed if the envisaged data processing is likely to result in a high risk to the freedom and rights of data subjects (Article 35 GDPR). In certain cases, particularly cases involving the automated processing of large data sets, including sensitive information, internal investigations can have such a potential impact on the rights and freedoms of the affected data subjects. To avoid legal risks, companies should generally perform and document a full DPIA, or at least a reasonably detailed privacy risk assessment, prior to any investigation.
- **General data protection law requirements:** As for any other processing of personal data, the general requirements under the GDPR must be complied with, such as establishing appropriate records of processing activities (Article 30 GDPR), ensuring compliance with the principles of data protection by design and by default (Article 25 GDPR), and implementing appropriate technical and organisational security measures appropriate to the risks for the protection of personal data (Article 32 GDPR).
- **Co-determinations rights of works council:** In some countries, it may be necessary to involve the local works council in advance. Investigation measures the works council did not consent to might be invalid. In addition, the works council might seek a preliminary injunction to ban the employer from performing the investigation.

WHAT MAY BE THE CONSEQUENCES OF UNLAWFUL PROCESSING?

Companies that do not consider the aforementioned requirements and conditions may face high legal risks when processing personal data in the course of internal investigations.

- **Administrative fines/criminal liability:** Companies that do not comply with the strict requirements of the GDPR may face administrative fines up to €20 million or four percent of their total global turnover for the previous year, whichever is higher. In the case of company groups, there is the risk that data protection authorities will calculate fines on the basis of the consolidated revenue of the group. Additionally, national implementation laws and national criminal codes may provide for criminal liability in case of unlawful processing.

- **Exclusion of evidence:** In case of unlawful processing, the company may not be able to use the findings of the internal investigation in court. This aspect is particularly important if the company has imposed sanctions (e.g. a dismissal) against an employee due to the findings of the internal investigation. If the employee challenges the lawfulness of the dismissal in court, the company has to show that it has performed the respective data processing in accordance with applicable data protection laws. If the court deems the data processing unlawful, the findings may be excluded as evidence and a dismissal might be invalidated.
- **Claim for damages by affected data subjects:** Data subjects whose personal data have not been processed in accordance with the GDPR may claim damages from the company. Those claims may refer to material and non-material losses due to the infringement.

WHICH CASE LAW IS RELEVANT FOR INTERNAL INVESTIGATIONS?

In January 2016, the European Court of Human Rights ("**ECHR**") rendered an important decision regarding the secret monitoring of employee communication (application No. 61496/08). In the "Bărbulescu" case, the ECHR ruled that employers violate the employees' fundamental right to respect for private life and communication (Article 8 European Convention of Human Rights) if they secretly monitor their employees' messenger communication without implementing appropriate safeguards to preserve the employees' legitimate interests.

According to the ECHR, employers are generally allowed to monitor their employees' communication to a certain degree. Such monitoring measures, however, must be accompanied by adequate and sufficient safeguards to preserve the employees' right to privacy. In particular, employers must generally inform their employees about the envisaged monitoring in advance. This notification must include detailed information on the nature, the extent of the monitoring and the degree of intrusion. In addition, employers need to provide legitimate reasons to justify the monitoring of employee communication. In this context, the ECHR particularly refers to the principle of data minimisation. The employers must prove that there is no less intrusive measure to reach the envisaged purposes.

The criteria established for the monitoring of employees were further refined in a decision of the ECHR in the Ribalda case (applications Nos. 1874/13 and 8567/13) in October 2019. The court ruled that covert video surveillance of employees does not violate the employees' fundamental rights for private life and communication (Article 8 European Convention of Human Rights). Thus, the knowledge gained by the employer may be used as justification for the dismissal.

The case revolved around the fact that in a Spanish supermarket, merchandise worth between €8,000 and €25,000 per month disappeared over a period of several months – with increasing tendency. The employer used covert video surveillance to identify the guilty parties (a group of cashiers and sales assistants), who were later dismissed. The Grand Chamber decided that – while covert video surveillance is not justified for every slightest suspicion of misappropriation or wrongdoing – the video surveillance in the specific case was lawful even though the employees had not been informed in advance about the monitoring by the employer. The case is different from the Bărbulescu case (where also no prior information was given) because the Bărbulescu case concerned the general monitoring of an employee's activities during working hours. In the Ribalda case, however, there was concrete suspicion of a crime causing considerable damage.

The ECHR weighed the protection of the privacy of employees against the protection of the employer's property and business operations. The court considered that there was a legitimate aim because of concrete and reasonable suspicion of serious misconduct causing a substantial extent of losses and endangering the smooth function of the company. Also, the employees' expectation as to the protection of their private life was limited since the employees were not monitored in very private areas (e.g. toilets, locker rooms, or closed working areas) but in areas open to the public (such as checkout counters). In these public areas, the employees' privacy was restricted by the permanent contact with customers, and the activities filmed were not of an intimate or private nature. The court further considered that the duration had not exceeded what was necessary to confirm the suspicions of theft. The measures were thus appropriate and proportionate as there were no other less intrusive means to achieve the legitimate aim.

While the court stressed the importance of appropriate prior information, the lack of information in the specific case was considered just one of the criteria to be taken into account in order to assess the proportionality of the measures taken. Also, other safeguards were sufficient to justify the overall balancing in favour of the employer.

Although the Bărbulescu and Ribalda decisions did not directly refer to the GDPR, the decisions are generally understood to interpret the accepted principles under the European Convention that remain applicable under the GDPR. Therefore, companies are well advised to consider the criteria established by the ECHR when conducting international investigations.

In addition, on national level, there is a rising number of specific court cases (and decisions by the competent data protection authorities) relating to employee monitoring and investigations under the GDPR. These cases further refine the principles that need to be taken into account in order to ensure compliance with national law requirements.

CONCLUSION

The GDPR and national implementation laws, if applicable, set strict limits for conducting internal investigations. Companies have to deal with a variety of requirements and obligations. To ensure compliance with data protection laws, companies should carefully assess the individual circumstances and legal requirements for each investigation. Companies are well advised to establish a professional data protection concept and investigation plan, including appropriate internal procedures and technical and organisational safeguards, enabling the company to effectively manage the internal investigation in line with legal requirements. The steps taken should be documented in an appropriate privacy risk assessment in order to be able to demonstrate compliance with the GDPR. Otherwise, companies may face serious sanctions, data subject damage claims, reputational damage and exclusion of evidence due to unlawful processing.

AUTHOR

Dr. Martin Pflüger

Partner
Hogan Lovells Munich
T +49 89 29012 241
E martin.pflueger@hoganlovells.com

Since the early days of his career, Martin Pflüger has been focusing his practice on advice in the area of information technology, Internet, e-commerce and data protection law, with a focus on the technology, automotive and life sciences industry. Not only from his various secondments with clients in the technology and pharmaceutical sector, including as European privacy counsel for a worldwide leading cloud computing service provider, Martin brings extensive experience in drafting and negotiating IT agreements, evaluating new technologies and business models as well as advising clients on all aspects of European and German data protection law, including data security and cybersecurity.

Martin is recognised for having a deep understanding of the expectations and legal challenges clients are facing in connection with complex technology or outsourcing projects, the implementation of business processes in the field of deep digital transformation, and the handling of personal and non-personal data. He regularly advises clients on IT/IP related aspects in various commercial and corporate transactions. Martin's privacy practice covers all aspects of European and German data protection law, including the coordination of multi-jurisdictional projects on European and international level – whether you are looking at setting-up your cross-border transfers of personal data (including implementing Binding Corporate Rules), at managing your internal investigations or compliance systems, or at dealing with the particularities for the processing of employee or health data, whether you need assistance with the drafting of privacy policies or data transfer agreements, or whether you seek advice on topics such as artificial intelligence, data governance, big data, connected cars or the Internet of Things. He regularly assists companies in relation to GDPR compliance audits and implementation projects. Martin further regularly represents companies in data protection law proceedings with the data protection authorities or German courts, including handling civil law proceedings relating to (mass)-claims for damages.

Legal Framework for Money Laundering in Europe

INTRODUCTION

An estimated two to five percent of the Global Gross Domestic Product ("**GDP**") in one year is the result of money laundering. Money launderers prefer countries with solid financial markets and financial services, high GDP, high exports and imports, and a rather lax anti-money laundering regime and low fines.

Europol has estimated that around one percent of the EU's annual GDP is "detected as being involved in suspect financial activity". According to a study from the European Parliament dated 2017, this issue poses a particular threat to large European countries. The United Kingdom tops the list with an estimated total of €282 billion laundered annually, followed by France, Belgium, Germany, Luxembourg, the Netherlands, and Austria. Compared to their GDP, the Baltic States, Luxembourg and Cyprus have a disproportionate volume of money laundering. According to Europol's European Financial and Economic Crime Threat Assessment for 2023, money laundering is a crucial activity for organised crime, enabled by globalisation and the digitalisation of the financial sector. Almost 70 percent of criminal networks acting in the European Union perform basic money laundering techniques, and about 30 percent operate with highly developed money laundering networks and/or underground banking systems.

In recent years, the competent local authorities have published general guidelines to inform the obliged entities about the applicable due diligence and organisational requirements. As a further step, several thousand audits have been performed in the member states to evaluate the status quo and pave the way for further action against those who do not comply with the requirements of the AML laws. The most recent reports demonstrate that administrative fines have been levied against traders in goods. The most common reasons have been:

- The official identification document was not fully copied during the customer identification process.
- The obliged entity cannot prove that it has obtained appropriate confirmation whether or not the contracting party is acting on behalf of a beneficial owner.
- The obliged entity cannot prove that it has verified the obtained customer data on the basis of an appropriate official identification document.
- The obliged entity has not submitted the suspicious activity report completely, correctly and in due course.

Following a number of prominent cases of alleged money laundering taking place at EU credit institutions, the European Commission adopted a set of documents in July 2019 analysing the effectiveness and efficiency of the EU Anti-Money Laundering/Countering the Financing of Terrorism ("**AML/CFT**") regime as it stood at that time, and concluding that reforms were necessary.

On 7 May 2020, the European Commission presented an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing and defined six priorities or pillars in order to strengthen the EU's rules on combating money laundering and terrorist financing:

- Ensuring effective implementation of the existing EU AML/CFT framework;
- Establishing an EU single rulebook on AML/CFT;
- Bringing about EU-level AML/CFT supervision;
- Establishing a support and cooperation mechanism for Financial Intelligence Units ("**FIUs**");
- Enforcing EU-level criminal law provisions and information exchange;
- Strengthening the international dimension of the EU AML/CTF framework.

THE AML PACKAGE 2021

On 20 July 2021, the European Commission introduced its Anti-Money Laundering Package ("**AML Package**"; https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en) that includes the following legislative proposals:

- A Regulation on AML/CFT ("**AMLR**"), containing directly-applicable rules, for example in the areas of Customer Due Diligence and Beneficial Ownership;
- A sixth Directive on AML/CFT ("**AMLD6**"), replacing the existing Directive 2015/849/EU (AMLD4 as amended by AMLD5), containing provisions that will be transposed into national law, such as rules on national supervisors and Financial Intelligence Units in member states;
- A Regulation establishing a new EU AML/CFT Authority ("**AMLA**") in the form of a decentralised EU regulatory agency; and
- A revision of the 2015 Regulation on Transfers of Funds to trace transfers of crypto-assets (Regulation 2015/847/EU).

The AML package is being discussed by the European Parliament and Council. The European Commission stated that it looks forward to a speedy legislative process. Following announcement dated 18 January 2024 that the European Parliament and Council had reached provisional political agreement on the texts of the new AMLR and AMLD6, the final compromise texts were released on 12 February 2024. The Council and the Parliament will now have to formally adopt the texts before they are published in the EU's Official Journal and enter into force.

OBLIGED ENTITIES UNDER AML LAWS

It is a widespread misconception that only financial institutions and the related industry must undertake appropriate measures in the European Union to comply with AML laws. So-called traders in goods are subject to the same legal requirements if these persons are dealing in luxury goods such as precious metals, precious stones, jewellers, horologists and goldsmiths and other high value goods, where such trading is either a regular or a principal professional activity. The term "value goods" has been expanded to motor vehicles, watercrafts and aircrafts in the higher market segments given their high value and transportability. Therefore, traders of such goods should be subject to AML/CFT requirements.

Other affected parties are lawyers, auditors, tax advisors, real estate agents (including when acting as intermediaries in the letting of immovable property), casinos, art traders (i.e. persons storing, trading or acting as intermediaries in the trade of works of art), operators and brokers of online gambling platforms, custodian wallet providers, and virtual currency exchange service providers.

Additionally, professional football clubs and agents shall become obliged entities under the AMLR. These rules shall apply after five years upon entry into force, as opposed to three years for the other obliged entities.

CASH PAYMENTS

AMLR sets a EU-wide limit to large cash payments of €10,000. Member states should be able to adopt lower thresholds and further stricter provisions to the extent that they pursue legitimate objectives in the public interest. Given that the AML/CFT framework is based on the regulation of the business economy, the limit should not apply to payments between natural persons who are not acting in a professional function. To ensure that the measures are proportionate with the risks posed by transactions of a value lower than €10,000, such measures should be limited to the identification and verification of the customer and the beneficial owner when carrying out occasional transactions in cash of at least €3,000. This provision does not relieve the obliged entity from conducting all customer due diligence measures whenever there is a suspicion of money laundering or terrorist financing, or from reporting suspicious transactions to the FIU.

CRIMINAL AND ADMINISTRATIVE LIABILITY

The member states must ensure that obliged entities can be held liable for breaches of AML laws. Furthermore, the member states have the right to provide for and impose penalties under criminal law and must lay down rules on administrative measures to ensure that their competent authorities may enforce AML rules and regulations. In addition,

member states must ensure that their competent authorities promptly report any identified criminal offences to their law enforcement authorities.

With regard to criminal liability, some member states previously excluded "self-laundering" from money laundering as a criminal offence. The reason for the previous exclusion was that if, for example, a person stole money and was prosecuted for both theft and money laundering, this was seen as an inadmissible double punishment. However, under strong pressure from the Financial Action Task Force on Money Laundering ("**FATF**"), all countries have meanwhile amended their laws, declaring self-laundering a money laundering crime. Germany was the last country to amend its laws accordingly in November 2015.

Administrative sanctions and measures apply to breaches on the part of obliged entities that are serious, repeated, systematic, or a combination thereof of the requirements for:

- Customer due diligence;
- Suspicious transaction reporting;
- Record-keeping; and
- Internal control measures.

Member states must ensure that in these cases, the administrative sanctions and measures include at least:

- A public statement which identifies the natural or legal person and the nature of the breach;
- An order requiring the natural or legal person to cease the conduct and to desist from repeating that conduct;
- Withdrawal or suspension of the authorisation where an obliged entity is subject to an authorisation;
- A temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person, held responsible for the breach, from exercising managerial functions in obliged entities;
- Maximum administrative fines of at least twice the amount of the benefit derived from the breach where that benefit can be determined, or at least €1 million.

SUPERVISION OF AML LAWS AND AMLA

Member states are required to appoint competent authorities to supervise obliged entities effectively and, in particular, to monitor the adherence and take the measures necessary to ensure compliance with the AML laws. In this context, it is important that member states provide the competent authorities with adequate powers of enforcement, including the power to demand any information relevant to monitoring compliance and performing external audits.

More specifically, the standard under European AML rules requires that the competent authorities have on-site and off-site access to all relevant information on particular domestic and international risks associated with customers, products, and services of the obliged entities. Regarding the frequency and intensity of on-site and off-site supervision, competent authorities will consider the individual risk profile of obliged entities and the risks of money laundering and terrorist financing in the respective member state.

Moving forward, AMLA will directly supervise up to 40 financial institutions deemed to pose the biggest risk of money laundering or terrorist financing. This shall include at least one institution from each member state of the European Union. AMLA will define the selection criteria for the direct supervision of financial entities separately. Direct supervision will be conducted by so called joint supervisory teams led by AMLA and including staff from national AML authorities. AMLA will coordinate and assist national supervisory authorities to increase their effectiveness in enforcing the single rulebook and ensuring homogeneous, high-quality supervisory standards, approaches and risk assessment methodologies. Moreover, AMLA will provide stable hosting of the FIU.net platform and enable, *inter alia*, a development of common reporting templates and standards to be used by EU FIUs. Moreover, AMLA will be entrusted to adopt regulatory technical standards and implement technical standards and issue guidelines or recommendations addressed to obliged entities, national supervisors or FIUs.

In addition, all existing FIUs shall be increasingly involved in the fight against money laundering. Under AMLD6 FIUs shall have immediate and direct access to financial, administrative and law enforcement information.

According to the announcement of 22 February 2024, Frankfurt has been chosen by Parliament and Council as the seat of AMLA. AMLA is expected to begin operations mid-2025 with over 400 staff members and to start direct supervision a little later, once AMLD6 is implemented and the new legal framework enters into force.

OBLIGATIONS UNDER AML LAWS

Compliance with the requirements of the AML laws mainly consists of satisfying two high-level obligations:

- Organisational requirements and
- Customer due diligence requirements.

RISK ANALYSIS

Obliged entities are required to rate individual business relationships and transactions in light of their respective money laundering risk (risk-based approach). The results of the risk assessment must be documented. It should describe the potential risks associated with the business of the obliged entity, which can be divided into the following categories:

- Company risks;
- Customer risks;
- Product risks;
- Transactional risk; and
- Geographic risks.

The risk factors will be set out in Annexes II and III of the AMLR. As soon as the potential risks have been determined and described, it is the task of the obliged entity to determine to what extent they may actually materialise. Depending on the risk levels (i.e. risk-based approach), preventive measures and safeguards may be implemented. The risk assessment must also be updated at least once a year in order to ensure the effectiveness of the preventive measures and safeguards. By two years after the date of application of AMLR, AMLA shall issue guidelines on risk factors to be taken into account by obliged entities when entering into business relationships or carrying out occasional transactions.

COMPLIANCE MANAGER AND COMPLIANCE OFFICER

The essential element of compliance with AML laws is an appropriate internal organisation. Even if this is only required for certain entities (where appropriate with regard to the size and nature of the business), the appointment of a compliance manager (one member of the management body in its management function who shall be responsible to ensure compliance with AMLR and AMLD6) and a compliance officer is required to bear responsibility for the development of internal policies, procedures, and controls. These include risk analysis and risk management measures, customer due diligence, reporting, record keeping, internal control, and employee screening. The MLRO is also entitled to report suspicious events to the FIU. The compliance officer shall be appointed by the management body in its management function and with sufficiently high hierarchical standing, who shall be responsible for the policies, procedures and controls in the day-to-day operation of the obliged entity's AML rules, including in relation to the implementation of targeted financial sanctions, and shall be a contact point for competent authorities. The compliance officer shall also be responsible for reporting suspicious transactions to the FIU. The fulfilment of their duties may not lead to any disadvantages in the employment relationship. The clear organisational responsibility for this task is the foundation for compliance with the AML laws.

AML MANUAL

With the confidential risk assessment in place, the next element of the compliance structure – the AML manual – can be drafted and implemented. The AML manual describes the internal processes and activities to be implemented by the company to ensure compliance with legal requirements. Amongst other matters, the manual includes regulations for customer identification, the document or software system to be used, the escalation process for onboarding politically exposed persons, as well as record keeping and retention requirements and the internal procedure to report suspicious activities to the MLRO and other corporate governance provisions.

AML POLICY

Each obliged entity must implement appropriate processes and train employees on the types and current methods of money laundering and terrorist financing. This requirement can be met through an AML policy where each employee receives general information on money laundering and appropriate obligations. The training should be repeated at regular intervals depending on the respective AML risk of the obliged entity; the market standard is an interval of two years. It is also important to document all employees' attendance at the training sessions to ensure compliance with the AML provisions.

INTERNAL CONTROLS

With the AML manual and the AML policy in place, the company and all employees must implement the internal requirements in practice. One of the central tasks is the performance of customer due diligence. More generally, it is important to monitor the business activities and effectiveness of the implemented preventive measures and safeguards.

CENTRAL REGISTER OF BENEFICIAL OWNERS

All member states are required to set up a central register of beneficial owners to obtain and store information on beneficial owners. All legal persons under private law and all registered partnerships must collect, hold, and provide beneficial ownership information and communicate this information to the central register. The requirements for beneficial ownership will be streamlined by AMLR. Rules to identify the beneficial owner(s) of corporate and other legal entities will be more detailed and will, therefore, trigger a substantial amount of implantation work for the obliged entities. Beneficial ownership will be defined as "any natural person who ultimately owns or controls a legal entity or express trust or similar legal arrangement, as well as any natural person on whose behalf or for the benefit of whom a transaction or activity is being conducted". According to AMLR "control through an ownership interest" shall mean an ownership of 25 percent plus one of the shares or voting rights or other ownership interest in the corporate entity, including through bearer shareholdings, on every level of ownership. According to the current legal framework of Directive (EU) 2015/849 (AMLD), this threshold only applies at the first level of participation, while a majority of shares or voting rights is generally required at the second or higher level of participation.

Under AMLD6 member states shall ensure that the beneficial ownership information of legal entities and legal arrangements, information on nominee arrangements and information on foreign legal entities and foreign legal arrangements are held in a central register. To ensure that the registers of beneficial ownership information are easily accessible and contain high-quality data, consistent rules on the collection and storing of this information by the registers will be introduced by the member states. Such registers will be required to screen the beneficial ownership information they hold against designations in relation to targeted financial sanctions, both immediately upon such designation and regularly thereafter, in order to detect whether changes in the ownership or control structure of the legal entity or legal arrangement are conducive to risks of evasion of targeted financial sanctions. Entities that are associated or affiliated with persons or entities that are subject to targeted financial sanctions shall be flagged. The entities in charge of the register shall be granted the power to carry out inspections at the institutions, if there are doubts regarding the accuracy of the information made available. There is no need to demonstrate a legitimate interest to access the central register. Public access to beneficial ownership information allows greater scrutiny of information by civil society, including the press or civil society organisations, and contributes to preserving trust in the integrity of business transactions and of the financial system.

CRIMINAL LIABILTY

A directive on combating money laundering by criminal law was adopted on 23 October 2018. It lays down minimum rules on criminal liability for money laundering. In particular, the directive harmonises the definitions of money laundering and predicate offences, lays down minimum sanctions, and extends criminal liability to legal persons. As those concepts are now clarified in Union criminal law, it is no longer needed for the Union's AML rules to define money laundering, its predicate offences or terrorist financing. Instead, the AML laws will be fully coherent with the Union's criminal law framework.

CONCLUSION

In practice, entities must produce three documents based on the market standard to meet AML compliance: a risk analysis, an AML manual, and an AML policy. All three documents must be tailored to their respective business model and the entailing AML risks. The risk-based approach allows an individual set of measures depending on the respective level of risk, i.e. fewer measures in case of lower risks. Most importantly, the documentation provides protection against reputational harm and external challenges by supervisory authorities.

The new AMLR and AMLD6 will, for the first time, exhaustively harmonise rules throughout the EU, closing possible loopholes used by criminals to launder illicit proceeds or finance terrorist activities through the financial system. This will also be relevant for the obliged non-financial entities which will be subject of publication of AMLA aiming to harmonise the applicable AML rules going forward. The new AML rules will trigger implementation projects for all obliged entities, which will comprise a GAP analysis and a programme to close any identified gaps.

AUTHORS

Dr. Richard Reimer
Partner
Hogan Lovells Frankfurt
T +49 69 962 36 414
E richard.reimer@hoganlovells.com

Richard Reimer advises financial institutions, FinTechs and other companies on all aspects of financial regulation and compliance, with a particular focus on payments law. Furthermore, Richard advises on regulatory aspects of M&A transactions involving financial institutions (e.g. ownership control proceedings). He has dealt with major investigations in the financial sector and handled the relationship with the financial supervisory authority (BaFin). He is trusted advisor of the Federal Association of Payment and E-Money Institutions and as such involved in all relevant legislative procedures. He is part of the investment fund team and contributes to all regulatory aspects in structuring investments in Germany. Richard leads a team which primarily advises on banking licence proceedings, own funds requirements and compliance projects including whistleblowing systems, anti-money laundering compliance and financial sanctions.

Dr. Sarah Wrage, LL.M.
Partner
Hogan Lovells Frankfurt
T +49 69 962 36 421
E sarah.wrage@hoganlovells.com

Sarah Wrage advises German and international banks and financial services institutions as well as other companies on all aspects relating to banking regulatory law, payment services law and investment law. The main focus of her work is to give advice on licensing, capital requirements, duty of care and organisational requirements, compliance, and regulatory implications of transactions. Furthermore, Sarah assists her clients in the implementation of new financial products, particularly in the payment area.

In investment law, Sarah primarily offers advice and support to asset management companies, investment fund managers and investors regarding the structuring and setting up of investment funds as well as the permissibility of investments and the distribution of funds.

Matter Specific Investigations

Cartel Investigations

NEW TRENDS IN CARTEL ENFORCEMENT

Competition law has proven to be a high-risk area for companies in many different industries all over the world. Multi-jurisdictional cartel investigations are of increasing importance to businesses around the globe, with legal and compliance departments investing heavily in competition expertise. This is also true for the European Union, where both the European Commission ("**Commission**") and National Competition Authorities ("**NCA**") are taking a clear stance on competition law violations.

After a slowdown in dawn raids by competition authorities across Europe during the pandemic years, enforcement activity has increased since 2022. Several dawn raids were carried out across Europe in 2023. The Commission has also updated its enforcement tools, by setting up a whistleblower hotline and investing in digital investigation intelligence, such as a newly established data analysis unit, which enables the Commission to open investigations on its own initiative.

In recent years, the Commission has expanded its enforcement focus on industries, not in the spotlight in the recent past, like the life sciences and the financial services sector. Specifically in 2023, we have seen dawn raid activity e.g. in construction chemicals, fashion, fragrances and online food delivery. Similarly, recent years have witnessed investigations in some rather atypical cartel cases which are based on somewhat novel theories of harm, including those focusing on labour markets and sustainability objectives. This adds further uncertainty to the cartel proceedings. We expect to see a further rise in antitrust investigations in this regard, both on an EU level as well as on a national level.

When it comes to cartel investigations, being prepared is key in order to react appropriately during a dawn raid and master the subsequent proceedings in the best possible way for the company. In the following paragraphs we will provide an overview of the legal framework, the relevant institutions, and the different stages of a typical Commission cartel investigation.

LEGAL FRAMEWORK AND RELEVANT INSTITUTIONS

The Treaty on the Functioning of the European Union ("**TFEU**") provides the rules to implement a system of undistorted competition, substantially unchanged for decades. Investigations into alleged cartels or other forms of anti-competitive agreements between companies (Article 101 TFEU) and unilateral measures by market-dominant companies (Article 102 TFEU) constitute an important pillar of European competition law enforcement. Both provisions are directly applicable in all EU Member States and can be enforced by the Commission as well as by NCAs.

Council Regulation (EC) No. 1/2003 ("**Regulation 1/2003**") sets out the Commission's powers during the different stages of an investigation. The Commission has published best practice guidelines as well as an internal manual of procedures which provide useful information on how the Directorate General for Competition ("**DG Competition**") runs investigations.

The Commission acts as the European competition law enforcer. Regulation 1/2003 grants considerable powers to the European Union's executive body to ensure that the Commission can effectively guard the adherence to competition law rules in the Treaty. Within the Commission, there are generally two hearing officers responsible for ensuring the rights of accused undertakings, especially impartiality and objectivity of competition proceedings.

The Commission also takes a central role in the European Competition Network ("**ECN**"). The ECN consists of the Commission and the NCAs in the EU Member States. The ECN provides means to ensure an effective and coherent cross-border application and enforcement of competition law within the European Union.

Upon appeal, Commission decisions in cartel cases are subject to examination by the General Court (formerly referred to as Court of First Instance). Ultimately, the Court of Justice of the European Union ("**CJEU**") is responsible for appeals on the point of law against General Court decisions.

Considering the complexity of EU level cartel investigations and the authorities involved, cartel cases may last many years, starting from the authorities' first investigative steps to a final potential decision by the CJEU.

OVERVIEW OF A TYPICAL EUROPEAN COMMISSION CARTEL INVESTIGATION

Initiation of Proceedings

The Commission can start proceedings either on its own initiative, on the basis of a third-party complaint, or via a leniency applicant blowing the whistle on a cartel conspiracy. While third-party complaints usually mark the beginning of an abuse of dominance-probe, cartel cases are often triggered by leniency applications that are followed by dawn raids. The Commission stated that it has significantly increased the number of cartel investigations opened at the Commission's own initiative to 25 percent of the currently launched investigations. This mainly results from the Commission's investments into digital investigation intelligence, the whistleblower hotline, and its newly established data analysis unit, which uses data-mining and algorithms to scour information for specific patterns indicating collusion.

a) Leniency Applications

Leniency applications mark the typical start of a Commission investigation into an alleged cartel. Full immunity from an eventual fine may be granted to the first cartel participant that applies for leniency and provides sufficient information for the Commission's investigation. In order to win the race for leniency, an undertaking can set a "marker" with DG Competition, i.e. file an abridged application for a reduction of fines and submit detailed information within a certain period of time thereafter in order to secure its rank under the Leniency Programme. Substantial fine reductions may be granted for subsequent applications by other cartel participants. The different cooperation scenarios are laid out in the Commission Notice on Immunity from fines and reduction of fines in cartel cases ("**Leniency Notice**").

b) Dawn Raids

DG Competition has extensive powers to conduct unannounced inspections ("**dawn raids**") when there is an early suspicion of competition law infringements. As long as the scope of the inspection is limited to business premises, no local court search warrant is needed. Commission inspectors – usually supported by national inspectors – make use of their extensive rights. Undertakings are liable for obstructions of these inspections, such as destroying or withholding evidence with potential fines of up to one percent of the undertaking's annual turnover. On site, the Commission is empowered to examine books and business records both in digital and hard copy format, take copies, seal particular objects, and interview employees at all levels (Article 20 Regulation 1/2003).

In recent years, the Commission's focus has shifted towards e-dawn raids. The Commission requests large amounts of electronic data that it then reviews on its own mobile servers at the undertaking's premises.

Dawn raids hit companies rather unexpectedly and are often disturbing for the operational business. As mistakes during the dawn raid can be very costly and may jeopardise the companies' and employees' defence position, dawn raid preparation is key. It is highly advisable to have a specific process for Commission dawn raids with designated antitrust advisors established, to regularly train the in-house dawn raid team, and to have IT system administrators trained and prepared to provide the inspectors with easy access to the IT infrastructure.

A very sensitive and important topic throughout the entire investigation and specifically during a dawn raid is the protection of legally privileged documents. Generally speaking, only communication with or prepared for external lawyers, which has taken place after the initiation of the administrative proceedings, can be legally privileged under EU law and can therefore be withheld from inspection. Prior communications can only be regarded as privileged where they relate to the subject matter of the procedure. Other documents and data need to be provided upon request as long as they fall within the scope of the investigation.

The duration of such inspections depends – amongst other factors – on the scope of the investigation, the company's size, and the amount of data requested by the Commission. Inspections at the companies' premises can last several days and be continued at DG Competition's offices in Brussels if the data volume to be reviewed by the officials is very large.

Additional Investigative Powers

Before the Commission initiates formal proceedings, it gathers information relevant to the specific sectors in order to uncover competition law infringements and to collect evidence of such alleged violations. The Commission is under a duty to investigate all facts relevant to the case diligently and impartially. In addition to the powerful investigative tool of dawn raids, Regulation 1/2003 equips the Commission with a range of additional powers typically applied by DG Competition in cartel investigations:

- **Requests for information:** In order to carry out its duties under Regulation 1/2003, the Commission may issue a Request for Information (Article 18 Regulation 1/2003). The submission of incorrect or misleading information can be fined up to one percent of the undertaking's total annual turnover (Article 23(1)(a) Regulation 1/2003).
- **Power to take statements:** Further, the Commission has the power to take statements and may interview any natural or legal person for the purpose of collecting information relating to the subject-matter of the investigation (Article 19 Regulation 1/2003).

Initiation of Formal Proceedings, Statement of Objections and Oral Hearing

The opening of proceedings is a formal act by the Commission that is notified to the parties and usually also to the public. The Commission can formally open the proceedings in different ways. Typically, DG Competition opens formal proceedings by issuing a so-called Statement of Objections ("**SO**") to the companies under investigation. The SO lays out the Commission's position and must contain all facts and evidence necessary for the final decision.

The main purpose of the SO is to inform the undertakings about the concrete competition law charges against them and to enable them to exercise their rights of defence. Informal meetings could be held before the SO is issued, helping the companies to understand the Commission's views on the status of the case. The cover letter to the SO explains the rights of the addressees and sets a deadline for the reply of at least four weeks.

The issuing of the SO usually also marks the point in time where the companies under investigation receive access to the Commission's file. Access to the file is part of the companies' right to be heard and constitutes a very important element in the companies' defence strategy: It provides the opportunity to inspect any potential leniency application and consecutive statements of other cooperating parties involved in the investigation. Depending on the scope and complexity of the SO and the size of the Commission's file, companies are usually granted a period of six to 10 weeks to file their reply to the SO ("**Reply**").

Where documents are submitted as part of the Reply, confidentiality should be claimed for those documents containing business secrets and other confidential information to prevent them from being disclosed to other parties.

In case one of the companies involved requests an Oral Hearing, this will usually take place following the Commission's receipt of the Replies. The Oral Hearing is held by the Hearing Officer and provides the Commission as well as the companies involved with a forum to discuss their case and exchange arguments on the facts and legal analysis.

Decision and Settlement

The procedure generally comes to a close with the Commission adopting its final decision in which it can impose substantial fines. In most cases, the publication of the decision is preceded by a State of Play meeting. In this meeting, the Commission presents its conclusions to the company.

Only when the Commission is convinced of a competition law infringement based on meaningful and consistent evidence it can adopt a decision and impose fines. Fines for infringements of Articles 101 and 102 TFEU can go up to 10 percent of the company's total annual turnover. In setting the fine, the Commission weighs different factors such as gravity and duration of the infringement as well as the role of the undertaking in the infringement. The details on the fining method are laid out in the Commission's Guidelines on the method of setting fines. After years of very significant cartel fines

(€3.7 billion in 2016; €1.9 billion in 2017), over the last five years, the Commission imposed accumulated fines of €3.8 billion. However, the described increased dawn raid activity will lead to new cartel proceedings.

In recent years, many cartel cases have been settled between the Commission and the companies under investigation. Such settlements usually take place before the submission of the SO. However, recent cases have also shown that even after the submission of the SO, and even after the companies under investigation have filed their Reply to the SO, a slot for settlement negotiations with the Commission may open up. It is the essence of settlements that the settling companies acknowledge their misconduct and their liability and in return may receive an (additional) reduction of the fine of up to 10 percent based on the Commission Notice on the conduct of settlement procedures in cartel cases ("**Settlement Notice**"). On the part of the participating undertakings, this has the advantage that further money and resources can be saved as the procedure is expedited.

TYPICAL FOLLOW-ON: CARTEL DAMAGES CLAIMS

Since the Commission has no power to award damages to victims of a cartel, civil cartel damages litigation has increased significantly in recent years. Both the European Courts and the Commission have pushed this development and called for effective means to recover cartel damages before national civil courts.

The risks of such claims by companies who may have suffered damages, for instance, through the payment of cartel overcharges, must already be carefully considered by the companies under investigation during the Commission proceedings, e.g. when determining leniency or settlement strategies.

CONCLUSION

Cartel investigations are still on the rise and constitute a high-risk area for companies around the globe, bringing along everything companies need to avoid: Cartel cases have a very long lifecycle from dawn raids to follow-on litigation, are costly, bind a lot of resources and can damage the reputation of the companies involved.

Experience has shown that preparation is key for companies to master the dawn raid situation and the subsequent cartel proceedings in the best possible way.

AUTHORS

Dr. Christoph Wünschmann

Partner
Hogan Lovells Munich
T +49 89 29012 432
E christoph.wuenschmann@hoganlovells.com

Christoph Wünschmann is the global co-head of the Hogan Lovells Antitrust, Competition and Economic Regulation practice. Since the beginning of his career, Christoph has been advising clients with a focus on German and European antitrust, competition and merger control law. Christoph is the professional for all competition related aspects of your business. He handles all competition aspects of transactions and advises on commercial agreements and compliance issues. He regularly represents his clients before competition authorities (European Commission, Federal Cartel Office) and courts.

He also handles merger filings with the European Commission and the German Federal Cartel Office and coordinates filings worldwide. Christoph also advises on all kinds of corporate and commercial agreements (joint ventures, cooperations, distribution, R&D, technology transfer) as well as abuse of dominance issues. He represents companies in antitrust investigations and represents his clients in antitrust related court proceedings, including follow-on damages claims.

Christian Ritz, LL.M. (USYD)

Partner
Hogan Lovells Munich
T +49 89 29012 542
E christian.ritz@hoganlovells.com

Christian Ritz handles complex antitrust and competition law matters, multi-jurisdictional investigations as well as compliance matters. In particular, Christian's practice focuses on representing his clients in dawn raids and providing them with strategic guidance and legal advice in cross-border investigations, including coordination with authorities in Europe and the U.S.

Christian regularly advises on the design and implementation of global compliance systems. Christian defends his clients against litigation arising out of alleged compliance violations and represents them in cartel damages claims and broader competition litigation. He also regularly guides his clients through complex multi-jurisdictional merger control proceedings and advises on international joint venture projects and cooperation agreements between competitors.

Export / Sanctions

Due to geopolitical tensions and conflicts such as in Ukraine or the Middle East, export control and sanctions regulations keep evolving. Recent activities of in particular both, the U.S. and the EU, show that one particular focus is on combatting the circumvention of sanctions regulations.

On 22 December 2023, U.S. President Joe Biden signed an executive order (EO 14114) threatening penalties for financial institutions that help Russia circumvent sanctions. A few days earlier, the EU adopted the 12th package of sanctions against Russia that includes additional listings of Russian individuals and entities as well as new import and export bans. Moreover, the EU has introduced a quarterly reporting obligation of entities established in the EU concerning the transfer of funds exceeding €100,000 out of the EU. This reporting obligation will become effective as of 1 May 2024. It applies to EU entities in which Russians or entities established in Russia directly or indirectly hold more than 40 percent of the shares.

Furthermore, with regard to specific goods or technology, exporters shall, as of 20 March 2024, contractually prohibit re-exportation to Russia and re exportation for use in Russia if their contract partner is not from the EU or an allied third country.

Also at the level of EU Member States, a trend can be seen that aims to combat the circumvention of sanctions regulations. Germany, for example, has demonstrated a tougher stance in the enforcement of EU sanctions. This can particularly be seen from the following activities:

- Already in 2022, Germany has adopted two Sanctions Enforcement Acts (*Sanktionsdurchsetzungsgesetze*) that introduced new asset tracing and freezing powers, as well as structural improvements in, among others, the operational implementation of sanctions.
- In February 2023, German public prosecutors and customs authorities searched premises of three German companies as well as the residence of three individuals. The reason for these dawn raids was the sale, export and delivery of IT and electrical sectors goods from a German company to a Turkish company. The components were later found in the remains of Russian missiles in Ukraine which suggests that the goods had been diverted to Russia via Turkey.
- In October 2023, German police, public prosecutors and customs authorities searched the properties of an Russian Oligarch to seize assets.
- Moreover, the German Federal Government proposed a draft of the Combating Financial Crimes Act (*Finanzkriminalitätsbekämpfungsgesetz*). This draft law is part of a broad reform aiming to strengthen the fight against financial crime, in particular, money laundering and circumvention of sanctions.
- At the end of 2023, the German supervisory authorities carried out several on-site financial crime audits of licensed institutions, focusing on financial sanctions. The audit covered, among others, questions relating to the proper governance, screening measures, reporting, resources and compliance in domestic and foreign branches of the institutions.

INTERNAL INVESTIGATIONS OF A POTENTIAL EXPORT CONTROL OR SANCTIONS INFRINGEMENT

The increased activity of the authorities in conjunction with complex legal frameworks and fast-changing rules and regulations demonstrate the need to keep internal compliance programmes under review. Infringements of export control or sanctions provisions may result in heavy fines, reputational damage and criminal prosecution of individuals. As a result, internal investigations of alleged infringements – whether those may have occurred wilfully or negligently – are a crucial instrument to protect the integrity of a company and to ensure that it keeps control of the situation.

Typically, internal investigations of a potential export control or sanctions infringement are triggered by one of the following situations:

- **Internal suspicions of export control or sanctions infringements**. Often, companies themselves realise that they have erred in applying export control or sanctions provisions. Such internal suspicions can arise, for example, through reports via whistleblower channels of the company or through internal audits. In such cases, an internal investigation is required to fully assess the gravity of the infringement, potential liability of the company and the steps required to remedy the concerns.
- **Official investigations by authorities.** Internal investigations may also follow official investigations by authorities. These may either be triggered by a specific suspicion of a violation or an external review such as an external audit of the company's books without any specific suspicion of export control issues. In such a case, a company should mirror the authority's "fishing expedition" to ensure that it has clean records. Where an authority is already investigating an alleged breach of export control or sanctions laws, the company concerned may want to investigate whether any further infringements have occurred and require immediate action.
- **M&A and financing**. Finally, investigations of potential past export control and sanctions issues and, more generally, of the compliance system in this field may be caused by M&A or financing projects. In the course of preparing documents for a due diligence or for corporate finance projects, third parties may request a statement on potential legal areas of concern and a risk assessment. In this case, companies need to investigate their compliance internally with the export control and sanctions rules applicable to them.

SPECIFICS TO BE CONSIDERED IN INTERNAL INVESTIGATIONS IN THE AREA OF SANCTIONS AND EXPORT CONTROL

While an internal investigation in the area of export control and sanctions has many parallels with investigations in other legal areas, some specifics need to be considered.

- It follows from the nature of trade activities that often several jurisdictions may need to be considered in determining which law applies to a specific transaction. Therefore, before starting the internal investigation, the applicable legal regime and the competent authorities have to be determined. Thereby, it has to be taken into account that especially U.S. legislation has an extraterritorial reach. This means that, provided there is some nexus to the U.S. (e.g. payment in USD, involvement of U.S. citizens), U.S. sanctions regulations may be applicable to the company even though it is not located in the U.S. In this regard, the concept of secondary sanctions should also be taken into account. Secondary sanctions may, for example, become relevant if non-U.S. financial institutions are deemed to have conducted or facilitated significant transactions for Specifically Designated Nationals (SDNs) for operating or having operated in Russia's technology, defence, construction, aerospace or manufacturing sectors. Even if U.S. sanctions are not applicable, often financing documents involving U.S. banks contain clauses that oblige parties to treat themselves as if U.S. sanctions were applicable.
- Other member states of the EU such as Germany may even prohibit complying with certain sanctions other states imposed (anti-boycott laws). In the EU, the Blocking Statute expressly mentions certain U.S. sanctions that EU companies are not allowed to follow. It is worth noting that the U.S. also has an anti-boycott regime that is stricter than in Germany. In particular, in the U.S., a reporting obligation for boycott requests exists regardless of whether the company complied with the request. This may affect the way an investigation is structured between the EU and the U.S. For instance, German subsidiaries receiving a boycott request should make their U.S. parent entity aware of it, so that the U.S. corporation can comply with potential reporting obligations.
- Sanctions provisions can rapidly change due to political developments. This makes it challenging for companies to keep their compliance systems up-to-date. For instance, from time to time entities or individuals are added to or removed from asset-freezing lists. In other areas, newly introduced sanctions sometimes make provision for the grandfathering of existing contracts otherwise covered under the new regime. These grandfathering provisions can differ between EU and U.S. sanctions regimes and between contracts entered into in a variety of different time frames, sometimes they only apply on a temporary basis, in effect stipulating a grace period for winding up existing contracts.

- Investigations in the area of export control and sanctions generally gain high management attention. This is not only due to the risk of fines and reputational damage. Under certain legal systems in the EU, it is mandatory for companies exporting goods to have a board member take legal responsibility for export control compliance. Governmental procedures are often directed against this board member, especially if a lower-level employee that might be responsible for the alleged infringement cannot be determined. Accordingly, investigations of export control infringements require professional handling, including experience of substantive export control laws and the procedural aspects of handling an investigation to fulfil management expectations. Close coordination between compliance and trade experts is therefore fundamental to the investigation due to the specialised knowledge of foreign trade law required.
- The clarification of the relevant facts often requires a combination of several investigative measures. In general, it is useful to direct the internal investigation towards gaining an understanding of the internal (control) processes, the IT systems used, the (technical) specifications of the product or service and the actual supply chain and logistics. Therefore, unlike in other investigations, a review of email data of employees often does not contain all the relevant facts required for a risk assessment. Even interviews with the key employees involved do not ensure that all facts can be sufficiently established. Rather, many investigations in the area of export control or sanctions therefore, require an in-depth review of the company's electronic accounts in order to identify the number of shipments involved, the items shipped, and the consignees of the goods. For instance, this may originate in ERP systems tracking all orders and shipments a company handles in its day-to-day business operations. Accordingly, a thorough legal investigation goes hand in hand with the involvement of forensic experts experienced in the e-discovery of structured data.

COOPERATION WITH AUTHORITIES

The complexity of export control law and sanctions provisions and the difficulties in reviewing the vast amount of data is also a challenge for authorities. Therefore, many national (supervisory, export control or customs) authorities appreciate the cooperation of companies that investigate potential infringements internally and present the results of their review to officials (whilst observing applicable data privacy provisions).

Depending on the specific infringements in question, companies may qualify for a voluntary disclosure programme that provides companies with full immunity from fines in some jurisdictions. However, companies should seek legal advice before proactively making use of such procedure. This is because they may find themselves in a risky situation, including a criminal investigation, if the conduct is not covered by the scope of the applicable voluntary disclosure scheme, or if such a scheme is not provided for under applicable national legislation. However, even if full immunity is not available, disclosing information voluntarily is often considered a mitigating factor in determining a fine and may even lead to a termination of administrative procedures without a conviction.

INTERNAL COMPLIANCE POLICIES

Increased attention by regulators in the area of trade and sanctions compliance, as well as higher expectations at management and shareholder level, are necessarily leading to the maturing of internal compliance policies. Different authorities provide guidance on key aspects to consider. Compliance policies should cover the full range of possible export control or sanctions issues, taking into account a company's individual risk profile in this area. Robust internal policies should firstly prevent or at least help pick up possible infringements. Secondly, they should provide a structure as to how an investigation should be carried out. Thirdly, a robust internal compliance policy provides reassurance to authorities that a company not only takes this subject seriously but has the means to implement any lessons learned in the case of a genuinely mistaken infringement. This may act as a mitigating factor in determining a fine.

CONCLUSION

In times of dynamic international relations, export control and sanctions law gain importance as a political instrument. Infringements carry a high risk of fines, criminal prosecution and reputational damage for companies, their management, and their personnel. Internal investigations in this area require specialised expertise regarding the substantive legal assessment, the procedural management of the investigation, the forensic review of electronic data and the internal procedures followed at all stages of the supply chain until the export is completed.

AUTHORS

Dr. Falk Schöning
Partner
Hogan Lovells Brussels
T +32 2 505 0911
E falk.schoening@hoganlovells.com

Falk Schöning can assist you regarding all questions and problems of EU and German antitrust law, foreign investment control law and export control law. He advises in particular on international cases which require coordination between different legal systems or representation vis-à-vis several regulators. Falk is frequently called on by companies which need advice on EU or German export control law, in particular regarding procedures with the German authorities. He knows the typical pitfalls of trade and sanctions cases and regularly cooperates with European and German regulators BAFA, Bundesbank, the Federal Ministry of Economics and the customs authorities. As part of Hogan Lovells' wider European trade compliance team Falk frequently structures compliance programmes according to BAFA's guidance on Internal Compliance Programmes.

Dr. Richard Reimer
Partner
Hogan Lovells Frankfurt
T +49 69 962 36 414
E richard.reimer@hoganlovells.com

Richard Reimer advises financial institutions, FinTechs and other companies on all aspects of financial regulation and compliance, with a particular focus on payments law. Furthermore, Richard advises on regulatory aspects of M&A transactions involving financial institutions (e.g. ownership control proceedings). He has dealt with major investigations in the financial sector and handled the relationship with the financial supervisory authority (BaFin). He is trusted advisor of the Federal Association of Payment and E-Money Institutions and as such involved in all relevant legislative procedures. He is part of the investment fund team and contributes to all regulatory aspects in structuring investments in Germany. Richard leads a team which primarily advises on banking licence proceedings, own funds requirements and compliance projects including whistleblowing systems, anti-money laundering compliance and financial sanctions.

Michael Jahn
Counsel
Hogan Lovells Munich
T +49 89 29012 246
E michael.jahn@hoganlovells.com

Michael Jahn advises national and international companies, including various Fortune 500 and DAX 40 companies, on issues regarding commercial criminal law as well as on topics related to compliance and internal investigations.

As part of his practice, Michael advises in particular on the set-up and management of internal investigations, often in the context of public prosecutor investigations. In doing so, he coordinates the review of relevant data and provides the legal assessments, in particular regarding possible questions of liability of companies and their employees. Michael has extensive experience in communicating with authorities, for example in the context of dawn raids or sanction proceedings.

ESG

RISE OF ESG INVESTIGATIONS

Environment, Social and Governance ("**ESG**") will remain a key regulatory driver also in 2024. With the continuing transition from a soft law to a hard law environment, enforcement activity and investigations remain at a high level and will further increase significantly. Although investigations into ESG issues often come in a similar form than typical criminal or regulatory investigations, there are some specifics to ESG investigations that companies should be aware of to mitigate increased liability and reputational risks for companies. This development requires a new focus and adjustments to existing compliance and investigation processes.

In autumn 2023, for example, the first major greenwashing investigation was partially settled with ongoing proceedings in Germany. A banking group and its funds subsidiary settled a SEC investigation in the U.S., agreeing on a payment of US$25 million based on greenwashing allegations that financial products did not comply with the declared ESG criteria. According to the SEC, the order found that the companies failed to adopt and implement policies and procedures reasonably designed to ensure the accuracy of their public statements about the ESG integrated products.

Since the German Supply Chain Due Diligence Act (Lieferkettensorgfaltspflichtengesetz – "**LkSG**") came into effect on 1 January 2023, the Federal Office of Economics and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle – "**BAFA**") has been actively enforcing and closely examining several grievances with allegations of human rights and environment related violations. Considering the ever-increasing public scrutiny, it remains highly likely that multinational companies with widespread supply chains will remain under specific focus for future investigations into ESG topics, especially in Germany and the EU with the Corporate Sustainability Due Diligence Directive ("**CS3D**") on the horizon.

ESG TOPICS IN INVESTIGATIONS

The range of ESG topics that can become subject of investigations is broad. It can essentially be divided into the following three key areas of **E S G**:

- **Environment**: The focus under "**E**" is on compliance with environmental regulation such as air, water, soil or waste regulation. In addition, sustainability criteria set by companies, such as climate protection targets, play an important role. This includes, for example, the establishment of an ecological balance and biodiversity, air, water and soil quality, energy and water consumption, CO_2 compensation, the use of natural resources, waste management and recycling processes.
- **Social**: The focus under "**S**" is on the protection and respect for human rights, equal treatment and non-discrimination, prohibition of child and forced labour, and ensuring fair working conditions for the own workforce and worker in the supply chain. The supply chain due diligence obligations under the LkSG are a prominent regulatory reality in this regard, which will be accompanied by the CS3D and other laws in the medium term.
- **Governance**: The focus under "**G**" lies on the question of how successfully a company takes account of its environmental and social responsibility and how effectively it can prevent or at least investigate and remedy incidents through the clear allocation of areas of responsibility, the establishment of grievance mechanisms and comprehensive prevention and remediation measures. Additionally, overall governance topics play an important role under the "**G**".

GREENWASHING

In addition, so-called greenwashing allegations based on misrepresentation of the sustainability performance of a company are likely to continue to rise globally in the future considering the recent trend in legislation to heighten the requirements regarding "green claims".

Such claims may refer to:

- **The company's performance itself** and include, for example, inaccurate information on company's sustainability performance (e.g. regarding CO2 or circularity, or the protection of human rights);
- **A company's products**, e.g. to marketing statements declaring products as sustainable, environmental friendly, CO2 neutral etc.

SPECIFICS IN ESG INVESTIGATIONS

The processes of an internal investigation also apply in principle to ESG investigations. However, there are some specifics requiring attention when managing ESG (internal) investigations.

Greater variety of triggering events for an investigation

ESG investigations can be initiated by a broad variety of potential triggering events. In addition to compliance hotline reports, customer complaints and internal audit findings, in recent years it has also been non-governmental organisations and other external stakeholders including (social) media which have uncovered violations of ESG standards.

Special expertise and independence in internal investigations

ESG topics often involve complex natural science contexts data, techniques and processes that require special expertise to investigate. While companies' ESG related knowledge is steadily improving, in many cases, it will still be necessary to consult and involve external experts.

The independence of the experts taking the investigation lead is very important for an unbiased and successful investigation. Any actual or perceived conflict of interest may cast doubt on the integrity of the investigation. Thus, an internal investigation conducted by external lawyers may prove beneficial.

Complex evidence collection

Although much company-related information in the ESG area is publicly available, it is sometimes difficult to secure sufficient evidence due to the global responsibility of companies in this field and the associated complex structures.

Regarding greenwashing specifically, investigators should also not limit their view on internal documents and processes, but review also advertisement and public communication to detect possible ESG related violations.

Reputational risk

Although reputational risks are a typical concern in investigations, companies are particularly likely to be held (publicly) accountable in the ESG area given the high public scrutiny. Operational and reputational damage, financial losses and legal consequences are often the result.

While follow-on litigation and regulatory enforcement are very real risks in many investigations, ESG topics normally trigger shareholder lawsuits as well as strategic lawsuits by NGOs or other external stakeholders for ESG failures or in the interest of protecting victims.

Thus, it is even more important in ESG investigations to have a clear and early coordinated communication strategy in place to mitigate potential negative spillover effects. Before going public, companies should develop a clear and facts-based communication strategy involving all relevant internal stakeholders and external counsel (if necessary).

Specific reporting and transparency requirements

On ESG topics, companies often enter into transparency obligations, e.g. under disclosure regulations such as the EU Corporate Sustainability Reporting Directive or towards their investors. These obligations may cause conflicts with confidentiality standards or attorney-client privilege. Companies should be aware of this and not rely on the confidentiality of the data and materials secured.

Involvement of external stakeholders

Like ESG due diligence requires the involvement of external stakeholders, the same may be true for ESG investigations, e.g. including external parties such as suppliers, workers in the supply chain or affected local communities. This usually increases the complexity of investigations.

Cross-border considerations

Considering the global nature of supply chains, national peculiarities of the countries and the specifics of cross-border investigations must be diligently taken into account.

OUTLOOK

Since the number of ESG investigations will likely increase, companies should continuously align their compliance management system and investigation processes. These should reflect current developments and legislative changes accordingly through an effective ESG strategy and ESG risk management including investigation processes to mitigate both regulatory and reputational risks to the best possible extent.

Likewise, ensuring compliance with all applicable legal regulations during an ESG investigation (e.g. whistleblower protection, supply chain law, but also the UNGP and OECD Guidelines), voluntary public and contractual commitments (e.g. industry standards and health programmes) and internal company standards (e.g. internal policies and codes of conduct) will best protect the integrity of the ESG commitments.

AUTHORS

Christian Ritz, LL.M. (USYD)
Partner
Hogan Lovells Munich
T +49 89 29012 542
E christian.ritz@hoganlovells.com

Christian Ritz advises his clients on cross-border investigations and compliance matters with a focus on ESG compliance and supply chain due diligence. He regularly advises on the development, design and implementation of global risk and compliance management systems. A particular focus of his advice is on the development and implementation of compliance systems and processes to comply with global requirements in the areas of ESG and supply chain due diligence, in particular with the German Supply Chain Due Diligence Act (SCDDA), the EU Corporate Sustainability Due Diligence Directive (CS3D), and the EU Deforestation Regulation (EUDR).

Just over the past 18 months Christian has advised over 30 international and national companies on the implementation of and compliance with the German SCDDA, including representation in ongoing investigations by the competent German enforcement authority BAFA.

He is an active member of Hogan Lovells' global ESG group as well as the Business & Human Rights group.

Christian is regularly recognised by legal directories such as Legal 500 and JUVE for his work in ESG, compliance, investigations, and antitrust.

Dr. Sebastian Gräler
Partner
Hogan Lovells Dusseldorf
T +49 211 1368 394
E sebastian.graeler@hoganlovells.com

Sebastian Gräler handles compliance as well as investigation issues. He regularly represents his clients in regulatory and administrative litigation. Clients praise him as "highly committed and competent".

Sebastian is a member of the global ESG Core Team of Hogan Lovells and regularly advises on ESG and environmental compliance issues. During a five-months secondment, he worked for the legal department of Volkswagen AG.

Sebastian studied at the Westfälische Wilhelms-Universität Münster and the University of Sheffield (UK) and also worked at the German Police University. He was honored for his outstanding performance in the first and second state law examinations by the Friends of Law at the University of Münster and the State Government of North Rhine-Westphalia.

In addition to his professional activities, Sebastian is a lecturer for European and International Business Law at the University of Wuppertal.

Dr. Felix Werner
Senior Associate
Hogan Lovells Berlin
T +49 30 800930061
E felix.werner@hoganlovells.com

Felix Werner's practice focuses on legal compliance matters, internal investigations, public prosecutors' investigations including dawn raids, and corporate governance. His corporate governance practice comprises the development, structure and implementation of global compliance management systems.

In addition, he counsels clients on corporate social responsibility, including environmental, social, and corporate governance matters, and supply chain due diligence (particularly regarding the German Supply Chain Due Diligence Act) as well as whistleblower legislation and Greenwashing. Felix is an active member of Hogan Lovells' global ESG group as well as the Business & Human Rights group.

Felix studied law in Berlin and Milan. Subsequently, he wrote a dissertation on the personal liability of managers for violations of antitrust law. While completing his doctorate, Felix worked at international law firms in Berlin and Vienna and gained valuable experience in the field of antitrust law and compliance. During his legal clerkship, he worked for the Federal Ministry for Economic Affairs and Energy in Germany and at two international law firms. Before joining Hogan Lovells, Felix gained practical experience at an international law firm as an Associate.

Transgressive behaviour in the workplace: from #MeToo and harassment to discrimination and racism

INTRODUCTION

Making its debut in our European Investigation Guide is a topic in which we witnessed an undeniable increase in awareness with our clients over the past few years: Transgressive behaviour.

This can manifest itself in many forms. The #MeToo movement tried to break an age-old taboo on speaking openly about abuse of power and sexual offences. The movement and the number of cases which came to light in its wake in various countries and industries, led to a renewed interest in compliance standards to prevent them. There is also an increased societal awareness to forms of (sexual) transgressions, racism, discrimination on the basis of religion or belief, disability, age or sexual identity, bullying, and other forms of unequal treatment. For the purpose of this editorial we understand transgressive behaviour to include any form of abuse of power and authority in which professional and personal boundaries are not respected in the context of the workplace. It will specifically focus on employer obligations in this regard.

LEGAL FRAMEWORK

The legal sources on this topic are scattered: On a supranational level, provisions for the protection against unequal treatment in the workplace can be found in the Violence and Harassment Convention (2019) of the International Labour Organisation (ILO), hereafter and its recommendation R206 – Violence and Harassment Recommendation, 2019. On a European level, various Directives exist. Although these sources do not apply directly, their provisions found their way into different areas of local law. Potentially applicable local laws include in particular criminal law provisions and employer obligations.

Relevant criminal law provisions

When investigating allegations of transgressive behaviour, it is important to differentiate whether the alleged behaviour would result in violations of behavioural/moral standards, internal policies or if the case even involves criminally relevant behaviour.

Applicable criminal law provisions include in particular provisions on:

- Insult and defamation;
- Secret image or sound recordings;
- Data privacy violations; and
- Sexual harassment and rape.

Employer obligations – Example Germany

In Germany, provisions on the prevention of unequal treatment in the workplace can be found in the General Act on Equal Treatment (*Allgemeines Gleichbehandlungsgesetz*, the "**AGG**") and employment legislation.

The AGG prohibits both direct and indirect forms of unequal treatment in a work context. Sexual harassment is considered a specific category of unequal treatment (paragraph 3 under 4 AGG). The AGG (Subsection 2) requires employers to take preventive measures, investigate potential cases and take repressive measures. Paragraph 12 under 1 AGG of said subsection stipulates that employers are "**required to take measures necessary to ensure protection against unequal treatment**". This explicitly includes preventive measures. What these preventive measures entail is explained in subparagraphs 2 to 5. Key measure is to appropriately train and educate employees on the inadmissibility of unequal treatment and to ensure that it does not occur in the first place. Such training can be incorporated into employees' regular vocational training or further education. Employers also have the obligation to promote reporting channels and inform employees thereof. This may be done by putting up a notice or place information leaflets at a

suitable location, or by using the information channels normally used within the company (paragraph 12 under 5 AGG). That way, employees know when, where and who to turn to.

Paragraph 13 AGG stipulates the employee's right to report cases of unequal treatment. According to paragraph 12 under 3 and 4, the report has to be examined/investigated: The employer must take **appropriate, necessary and suitable measures to put a halt to the unequal treatment**. This is an **implicit obligation to perform an internal investigation**, since in order to decide which measures to take, one has to know the facts of the case. Examples of measures are the cautioning, moving, relocating or dismissal of the employee in question (paragraph 12 under 3 and 4 AGG). The reporter needs to be informed of the outcome of the investigation.

If a plausible report is not investigated or appropriately addressed, the employee has the right to refuse performance of work, without loss of pay, insofar as this is necessary for their protection (specifically against (sexual) harassment), while the employer risks being held liable (paragraph 15 AGG): If the offence reoccurs, the employer is considered to not have reacted appropriately to the first offence, making the employer liable for damages and compensation.

PREVENTIVE COMPLIANCE

A successful compliance strategy against unequal treatment or transgressive behaviour is threefold and focuses on 1) preventive measures; 2) the protection and prevention of the individual employee whom has been mistreated and; 3) the enforcement of measures and remedies once unequal treatment has been established. The strategy should include the training, advice and awareness-raising amongst employees; a clear Tone from the Top promoting a healthy and safe company culture, making available material clarifying which type of behaviour is appropriate and which is unacceptable, training in and promoting the Code of Conduct or other relevant policies such as the Anti-Harassment Policy, and the establishment, promotion and opening of an internal reporting point.

Not addressing reports of unequal treatment is not just against the legal provisions mentioned above, but also constitutes a reputational risk and liability for the company. These cases could be considered a signal that the work culture requires attention. Regular employee surveys may be implemented to get clarity in this regard. In addition, transgressive behaviour such as racism or sexual harassment, have a high threshold for reporting and an equally dark number of unreported cases. They require a different approach than 'classic' compliance cases, such as fraud or money-laundering.

INTERNAL INVESTIGATIONS

Special considerations for internal investigations

Internal investigations into unequal treatment and transgressive behaviour roughly follow the lines of a regular investigation. However, there are specificities to keep in mind, such as the high threshold to report, the composition of the investigative team, the interview setting, duration of the investigation, evidence-gathering, involvement of authorities and documentation:

- **Plausibility check**: The first step is the review of the plausibility of the report: Is it manifestly unfounded, pure conjecture or evidently based on rumours, or not even a compliance or company matter in the first place, but a private one?
- **The investigating team**: There is no explicit legal provision regarding the persons who should be on the investigating team. In practice, the HR department is often a logical choice, with its expertise in employment issues, and overview of the persons in and structures of the company. On the other hand, the legal or compliance department will have more experience and specific expertise in leading internal investigations and be more aware of potential overlap with other fields of law, such as criminal law. In any case, close cooperation between the two departments is advised, in a way that one might take over the case from the other in case of i.e. a conflict of interest. The composition of the team should be based on the individual professional expertise, ability to show empathy while guarding neutrality and objectivity. A small team with a high level of integrity safeguards their duty of care, facilitates communication with the person impacted by the alleged transgression, thus limiting the risk of liability and damages. An external investigator or consultant may be involved in case of limited capacity of the in-company investigation team – in particular in time sensitive cases – and when there is a high reputational risk (when the topic is sensitive and/or the accused employee is high profile). In many cases, working with mixed-gender investigations teams has proven to be helpful.

- **Guiding principles**: As described above, confidentiality and neutrality are especially important: Both parties need to be given a fair opportunity to comment on the allegations. Due to the personal and private nature of the transgressions, it is imperative that information is handled discretely and appropriately. Empathy is a must and appropriate handling of sensitive and personal information. This prevents further escalation and damages. Additionally, swift and thorough evidence-gathering is crucial. This is especially relevant for cases of harassment, since such incidents often occur in an intimate setting, with a lack of evidence to follow.
- **The Interviews**: The interviews should be conducted in an appropriate setting, preferably be carried out by a small, professionally experienced team that is committed to confidentiality. Interviewers must maintain their neutrality, at the same time have the necessary sensitivity. It should be avoided to conduct interviews twice, which could risk revictimisation. More important than in other investigations, the credibility of interviewees and interview statements needs to be assessed. Therefore, interviewers should also be experienced investigators. However, if possible it should be avoided to having to assess an allegation solely based on personal statements.
- **No standard approach**: Each case is different, especially with such personal experiences as violence and harassment. The factor time is also more important than usual here, due to the heavy reliance on personal statements/memories and lack of the usual paper trail, compared to i.e. financial and fraud internal investigations. Slow response times can significantly complicate an investigation. A long and dragging investigation prevents the affected person to find closure.

CONCLUSION - MAIN OBLIGATIONS FOR EMPLOYERS

Implementing effective compliance measures is becoming increasingly important to address corporate and management liability as companies are more frequently faced with reports on transgressive behaviour. Being prepared for this means having a solid preventive strategy from the get-go and a well-trained team that can provide a quick response the moment a report is filed, fitting for the type of transgression and individual factors of the case. Due to the subjective nature of these cases, swift and proper documentation is crucial. In any case, cultivating a healthy corporate culture is fundamental to an effective prevention strategy.

AUTHORS

Désirée Maier
Partner
Hogan Lovells Munich
T +49 89 29012 340
E desiree.maier@hoganlovells.com

Désirée Maier focuses on white collar, compliance, and internal investigations. She advises national and international clients, in particular from the life sciences industry. One focus of her work lies in the set-up and management of internal investigations. She has particular experience in advising during dawn raids and conducting cross-border investigations of potential breaches of criminal law or compliance regulations. In doing so, she is able to manage the different requirements from local law and U.S. law. She regularly communicates with German, U.S., and other enforcement authorities.

Désirée also advises clients on the establishment and enforcement of global compliance systems, including the performance of compliance audits to ensure these respond to regulators' expectations. Moreover, she has expertise in supporting clients in the defence against criminal law charges and providing advice on recovery issues in relation to claims arising from compliance matters. As part of a secondment, Désirée also worked in the U.S. legal department of a world's leading U.S. pharmaceutical company (Fortune 500) with a global responsibility for investigations.

Dr. Angelina Leder
Partner
Hogan Lovells Munich
T +49 89 29012 358
E angelina.leder@hoganlovells.com

Angelina Leder advises our clients, including numerous DAX 40 and Fortune 500 companies, on issues regarding commercial criminal law and on topics related to compliance and internal investigations.

Angelina advises national and international companies in particular on the set up and management of internal investigations. She has specific experience in accompanying dawn raids, communicating with authorities and conducting interviews.

Angelina also advises on the creation and implementation of global compliance systems. She has provided in house support as part of a secondment to the compliance department of a globally acting company from the automotive industry in Germany and the USA.

Silvia Gardini
Senior Business Lawyer
Hogan Lovells Munich
T +49 89 29012 565
E silvia.gardini@hoganlovells.com

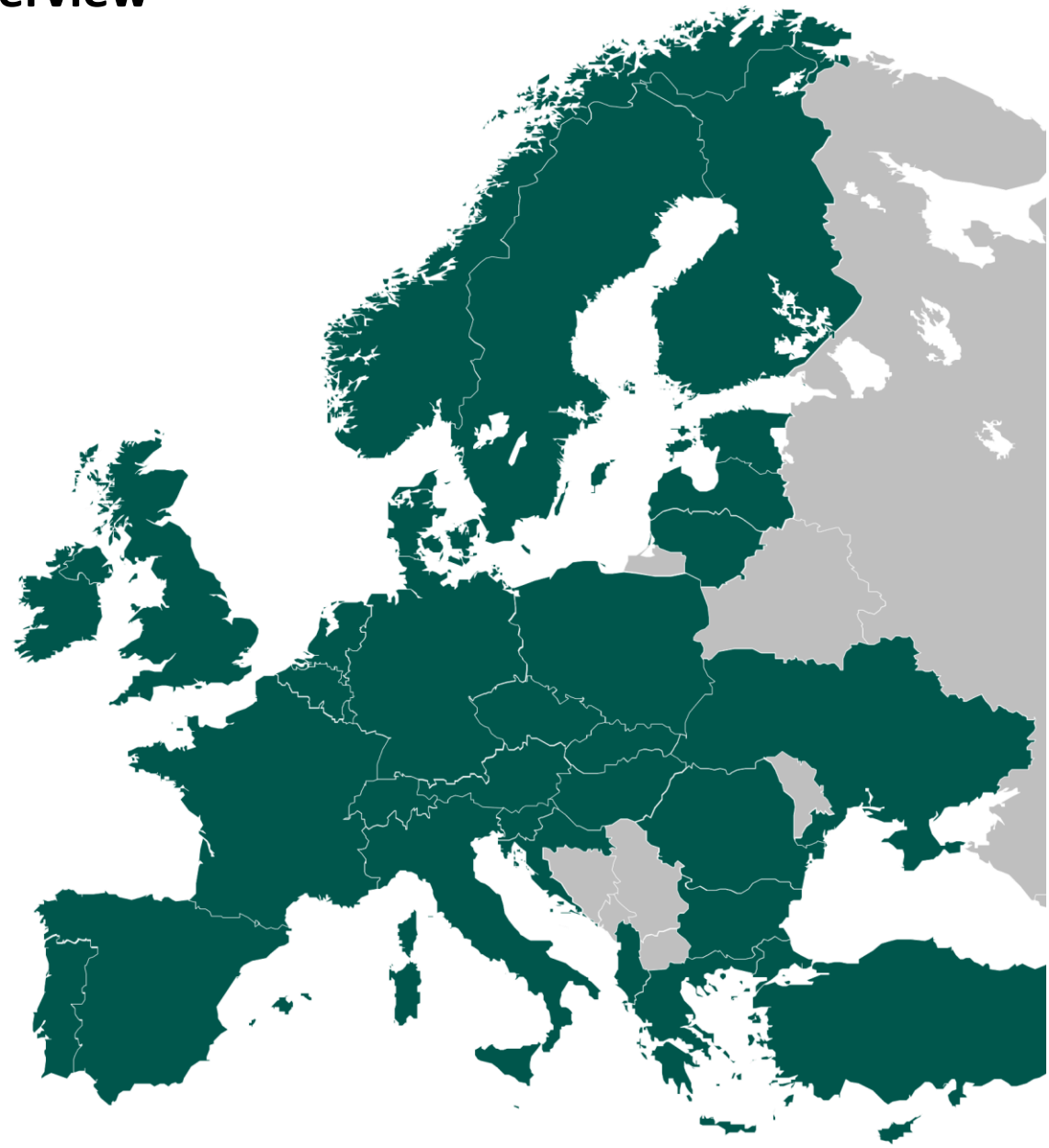
Silvia Gardini helps her clients navigate complex and highly regulated fields of law.

She does this by combining her legal background in Life Sciences with her experience in internal investigations. Her experience in assisting pharmaceutical companies with life cycle management issues and advertising and promotion questions, enables her to advise national and international companies on a broad spectrum of Compliance topics.

As part of a secondment, Silvia Gardini assisted a leading Pharmaceutical company (Fortune 500), at its Dutch branch as Legal Director a.i.

Silvia joined Hogan Lovells' Amsterdam office in 2014 and the Munich office in 2018.

Overview



The following jurisdictions are covered in this guide:

Albania
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Liechtenstein
Lithuania
Luxembourg
Malta
The Netherlands
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
Ukraine
United Kingdom

Albania

Kalo & Associates


Shirli Gorenca


Eni Kalo


Frensis Nakuçi

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X		X
No				X	

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Whistleblowing in Albania is regulated by Law No. 60/2016 ("**Whistleblowing Law**"). The law establishes mechanisms for the protection of whistleblowers and imposes obligations for public and private entities vis-à-vis whistleblowers.

According to the Whistleblowing Law, private companies and public authorities must establish an internal whistleblowing unit ("**WU**"), composed of one or more employees, which is responsible for reviewing whistleblower reports and for the protection of the whistleblowers. Although normally a whistleblower should provide their name and contact information in any report, the Whistleblowing Law permits anonymous reports, where the whistleblower can justify the need for anonymity and the report contains sufficient information to initiate an investigation.

During the investigation, the whistleblower's identity may not be disclosed to third parties without their written consent. Information relating to the report is confidential and may not be shared with, or transmitted to, internal or external third parties without the whistleblower's written consent, unless disclosure is required to fulfil a legal obligation.

Furthermore, an investigation must be, barring special circumstances, concluded within 60 days of the commencement of the investigation. The whistleblower may request information about the progress and results of the investigation, which must be provided within 30 days of receipt of the written request. In any event, the WU must notify the whistleblower about the status and, if applicable, of the results of the investigation within 30 days from the moment the report was made.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

As Albania is not member of the European Union, the Whistleblower Directive has not been implemented in Albania. Therefore, the reporting procedures are those foreseen in the Whistleblowing Law (please refer to the answer to question 1a above).

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) An employees' council is charged with representing the interests of employees and, to that end, is entitled to supervise the enforcement of laws, collective agreements, and a company's articles of association (Article 20 of Law No. 9901 of 14 April 2008). Councils have a statutory right to information and the right to make suggestions about the general policies of their companies.

However, the information rights of the employees' council likely do not apply to internal investigations. Nevertheless, an obligation to inform the employees' council may stem from an individual employment contract, a collective agreement, or another agreement between the employer and the employees' council.

Even though it is legally required for companies with at least 20 employees to establish an employees' council (Article 19 of Law No. 9901 of 14 April 2008), in practice, employees' councils are very rarely formed in Albania. This is partly due to the absence of penalties in case such a council is not formed. Therefore, no unified practice exists in this area.

b) The Whistleblowing Law provides that personal data of individuals involved in investigations must be processed in compliance with the principles and procedures provided under local data privacy laws as well as the GDPR ("**Data Protection Laws**"). Under the Data Protection Laws, the data controller (i.e. typically the employer) has the general obligation to notify the Information and Data Protection Commissioner ("**DPA**"), an independent public authority, of any data processing activities prior to the commencement of such activities. The notification is made by submitting an official notification form. In this form, the data controller must disclose, among other things, who will receive the personal data and whether the data will be transferred internationally. In principle, once the notification is filed, a controller may move forward with the processing (except when authorisation of the DPA is required, i.e. for processing sensitive data or for transfers of data to third countries).

Per the Whistleblowing Law, violations of the Data Protection Law are referred to the DPA.

c) There is no legal obligation to inform local authorities before beginning an internal investigation. However, the Whistleblowing Law provides reporting obligations, which require the internal WUs to file an annual written report with the High Inspectorate of the Declaration and Control of Resources and Conflicts of Interest ("**ILDKP**"), describing any investigations of whistleblower complaints in the preceding year.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Even though not expressly provided by applicable law, the duty to support an investigation is implied in the Whistleblowing Law, which grants the WU or the relevant state authority conducting the internal investigation (i.e. ILDKP) the right to collect statements and conduct interviews. The Whistleblowing Law also provides investigators the right to collect relevant documents from the whistleblower and third parties if it is deemed necessary by the head of the investigation.

The company may impose disciplinary measures on employees refusing to cooperate during the investigation, as it may be subject to administrative or criminal penalties for such behaviour. However, there are no legal penalties for employees who refuse to participate in the investigation.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

The duty to terminate an employee immediately or with notice is triggered when the person or body with the authority to terminate the employee becomes sufficiently aware of the conduct warranting termination. However, there is no deadline by which these sanctions must be imposed.

In practice, it is advisable to wait until the end of an investigation, or at least until a late stage, before initiating any termination procedure. In any case, under the Whistleblowing Law, an investigation must be, barring special circumstances, concluded within 60 days of commencement of the investigation.

---

5. Are there relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

In accordance with the Data Protection Law, an interviewee should be notified, ahead of the interview, if applicable, that their data is being processed. The interviewee should also be informed of the reason for the processing, who is processing the data (i.e. the data processor), and the means of processing, unless the interviewee (i.e. the data subject) is already aware of such information.

b) reviewing emails?

The reviewing/monitoring of emails is not expressly regulated by the Labour Code. The employer is allowed to collect, during the employment relationship, any information about the employee that relates to their professional capabilities or to the applicability of the employment contract. Notwithstanding this, the employees, as well as their personal items, cannot be subject to control unless this is required to protect the assets of the employer, other employees, or third parties from an illegal violation.

Employers should therefore have in place clear policies regarding the use of email, outlining under which circumstances employees may be monitored and explaining how any information gathered through monitoring may be used. Also, for the monitoring process to be lawful, it is important that the employee is aware of such activity. It is strongly advised to obtain their consent in writing.

c) collecting (electronic) documents and/or other information?

From a data privacy perspective, collecting electronic documents does not trigger any notification obligation unless such documents contain data classified as personal. Personal data is any information relating to an identified or identifiable natural person. Under the Data Protection Law, data controllers have the obligation to: (1) inform the data subjects that personal data are going to be collected; and (2) notify the DPA before starting data processing activities through the submission of an official notification form. The form should contain the name and address of the controller; the scope of the processing; the categories of data subjects and personal data; the receivers and/or categories of receivers of the personal data; whether the controller intends to transfer the personal data internationally; and a general description of the safety measures for the protection of personal data.

d) analysing accounting and/or other business databases?

To the extent the business databases do not contain personal data, they are not subject to the Data Protection Law.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no legal obligation to provide an employee with written instructions before conducting an interview.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

There is no legal obligation to inform an employee of their right to remain silent during an internal investigation. Such a requirement exists only in criminal investigations led by prosecutors.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no legal obligation to provide an employee with an Upjohn warning at the beginning of an interview.

d) be informed of their right to have their own lawyer attend the interview?

There is no legal obligation to inform an employee of their right to counsel during an internal investigation. Such a requirement exists only in criminal investigations led by prosecutors.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

As explained above, works councils are very rarely formed in Albania. Therefore, an employee does not generally have a right to have an employee representative attend their interview. Nevertheless, where there is such a council, the employee's contract should be consulted to confirm that no such right exists.

f) Be informed that data may be transferred to another country (in particular to the United States)?

As explained above, under the Data Protection Law, an interviewee should be notified, ahead of the interview, if applicable, that their data is being processed. The interviewee should also be informed of the reason for the processing, who is processing the data (i.e. the data processor), and the means of processing unless the interviewee (i.e. the data subject) is already aware of such information. Any international transfer should be disclosed to the data subject as part of this notification.

g) sign a data privacy waiver?

An individual cannot waive their rights under the Data Protection Law. However, the controller may obtain a written declaration from the data subject, in which the subject freely and knowingly consents to the collection and processing of their personal data. Consent of the data subject constitutes one of the grounds for lawful processing of personal data.

h) be informed that the information gathered might be passed on to authorities?

Under the Data Protection Law, data subjects must be informed by the controller about the recipients of their personal data.

i) be informed that written notes will be taken?

There is no legal obligation to inform an employee that written notes will be taken during their interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

The Whistleblowing Law provides that the WU must take all the necessary measures to protect evidence of wrongful conduct from disappearance or destruction. Companies that do not take such protective measures may be subject to administrative or criminal penalties.

Although the question of the admissibility of document hold notices has not been tested by court practice, in light of the obligations under the Whistleblowing Law, they may be admissible. The internal policies of the company should provide that the company may issue hold notices from time to time and that employees agree to abide by them Otherwise, they may be subject to disciplinary measures imposed by the employer.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Under Law No. 55/2018 ("**Legal Profession Law**") the attorney-client privilege extends to any facts, information, or documents that an attorney has obtained in the course of representing their client. An "attorney" is defined as an individual who is professionally licensed and registered with the tax authorities as an attorney and who practices law, whether as a solo practitioner or in cooperation with other attorneys (i.e. in a law firm). The privilege protection applies to written documents and any type of information that the attorney has obtained from the client. Unfortunately, there is little case law in Albania concerning the scope and application of the attorney-client privilege. Also, the Legal Profession Law itself provides limited guidance. However, the findings of an internal investigation would likely be protected.

---

9. Does attorney-client privilege also apply to in-house counsel in your country?

Attorney-client privilege does not apply to in-house counsel, as they are not registered as attorneys with the tax authorities and are not practicing law, as defined under the Legal Profession Law. In-house counsel employed as independent contractors rather than company employees may be covered by the privilege. However, this rarely occurs in Albania.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There is no statutory legal obligation to provide early notification to insurance companies. The relevant insurance contracts should, however, be checked.

b) Business partners (e.g. banks and creditors)?

There is no statutory legal obligation to provide early notification to business partners. The relevant contracts should, however, be checked for specific stipulations.

c) Shareholders?

There is no statutory legal obligation to provide early notification to shareholders.

d) Authorities?

There is no legal obligation to inform authorities before beginning an internal investigation.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

There are no immediate measures that have to be taken in Albania once an investigation is started. However, pursuant to the Albanian Criminal Procedure Code, any person, who has knowledge of or suspects the commission of a crime, must report the information to the relevant prosecutor's office. In addition, the company must make sure that ongoing criminal behaviour in the company is stopped.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutors do not generally have any particular concerns about internal investigations or ask for specific steps to be observed. However, prosecutors may try to use the findings of an internal investigation as evidence during criminal proceedings.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Pursuant to the Albanian Criminal Procedure Code, search warrants and dawn raids must be authorised by a court of competent authority. Information concerning, among other things, the nature of the search, the person(s) to be searched, and the authority conducting the search must be provided in the court order. Once a search is over, all involved parties should sign a record documenting the results of the search. In case a party refuses to sign the record, such refusal should be noted in the record. Where the procedural prerequisites are not fulfilled, there is a risk that the search will be declared invalid. Findings from an invalidated search may not be used in subsequent criminal proceedings.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Pursuant to the Albanian Criminal Procedure Code, before the initiation of court proceedings, and in the case of crimes subject to a maximum penalty of seven years' imprisonment or fines ranging from 500,000 to 5 million Albanian lek, the prosecutor and the defendant (including corporations) may enter into a deal. In practice, however, deals are not common in Albania.

Non-prosecution agreements and deferred prosecution agreements are not available to corporations. However, there are several mitigating factors, such as remedying the damages and eliminating the consequences, which may reduce the penalty on a corporation.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

A legal person (i.e. company) is liable under the Albanian law for crimes committed, through action or omission, in its name, or for its benefit, by its representatives, leaders, and managers (Law No. 9754 of 14 June 2007). A legal person is generally not liable for crimes committed by any employee, only by those who are under the authority of the person who represents, leads, and manages the entity. In practice, this includes managers of departments, who are directly under the authority of the administrator of the company. In addition, a legal person may be liable only for the omissions of the person who leads, represents, and manages the entity (i.e. its administrator), where this results in an absence of control and supervision.

A legal person is subject to so-called "principal" and "complementary" penalties. Principal penalties include fines and liquidation of the entity. Complementary penalties include, *inter alia*, the placement of the legal person under supervised administration, a ban from public procurement procedures and from obtaining or using licences, and the revocation of the right to perform one or more activities or operations.

Pursuant to the Criminal Code, the liability of the company does not discharge the individual who has committed the offence or crime. Individuals who have committed a criminal offence may be personally subject to principal penalties (mainly imprisonment and fines) and other complementary penalties in accordance with the Albanian Criminal Code. However, directors, administrators, and/or officers are not personally liable for crimes committed by other employees of the company.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Penalties for legal entities (i.e. companies) may be reduced if the legal entity has corrected the organisational deficiencies which have resulted in the criminal offence by implementing an efficient compliance system. The law seems to refer only to the case when the misconduct has already occurred. However, in our opinion, the mitigating

factor could a fortiori apply if the efficient compliance system has already been implemented before the alleged misconduct.

Regarding the criminal liability of directors, officers, or employees, such persons are liable only personally and not for offences committed by other employees of the company. Implementing an efficient compliance system prior to the alleged misconduct does not seem to be a factor that may reduce their penalties. However, it may have a certain role in establishing or excluding their criminal liability.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

In Albania, specific legislation or guidelines for ESG standards are not yet present. Nevertheless, Albania is in the process of harmonising its laws with those of the European Union, which may include new regulations and directives pertaining to ESG standards.

ESG requirements in Albania are outlined in various laws and regulations, some sector-specific and others more generally applicable. For instance, companies must adhere to Albania's environmental laws, which cover waste management, water protection, air pollution, and so on.

Social governance requirements may be addressed in labour laws, such as the Labour Code, Health and Safety at Work laws, and laws against discrimination. These regulations mandate that businesses ensure decent working conditions, protect workers' rights, and prevent discrimination.

Concerning corporate governance, companies are expected to maintain transparency, respect shareholder rights, and ensure sound management under regulations such as the Law No. 9901 of 14 April 2008.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

As the Whistleblowing Law is relatively new, no notable case law has yet developed concerning its interpretation and application. Companies operating in Albania are becoming increasingly aware of the law and taking steps to comply, for example, by establishing internal WUs.

CONTACTS

KALO ASSOCIATES

Kavaja Avenue, Building 27, 5th floor
Administrative Unit 10
1001 Tirana
Albania

Tel.: +355 4 2233 532
+355 4 2224 727
www.kalo-attorneys.com

Founded in 1994, KALO & ASSOCIATES has been at the forefront of legal services in Albania and Kosovo in representing prominent business organisations and IFIs, including many Fortune 500. The firm enjoys an international reputation and is "best friend" to many international law firms and IFI-s, development agencies, and embassies. The firm has made significant contributions in drafting modern commercial legislation such as banking, commercial arbitration, concessions, renewable energy, gambling, insolvency, secured transactions, financial leasing, insurance, corporate and municipal bonds, pension funds, and the collective investment funds law. It is a founding member of the South East Legal Group, the largest legal services provider in the Balkans, established in 2003 (www.seelegal.org). The firm has contributed in modernising the practice in Albania by adopting the structured practice areas, professional liability insurance, Corporate Social Responsibility, Pro Bono services, anti-corruption practices, art support, etc., which together give a law firm an undisputed reputation. The firm's earned reputation is related to the reputation of its founder, Perparim Kalo, who was representative of IBA for Albania since 1992 and invited as speaker to many international business and legal forums in four continents.

Shirli Gorenca
Partner
KALO & ASSOCIATES Tirana
T +355 4 2233 532
E sh.gorenca@kalo-attorneys.com

Shirli leads K&A's employment, labour, and immigration team in the Tirana Office. She joined the firm in 2007 and has been working with different departments and dealing with Employment, Tax, Real Estate, Banking & Finance issues that enhanced her professional growth in offering services to several international clients and fortune 500 companies.

Shirli is an active Member of the National Reconciliation Office of Tirana, representing some prominent employers' organisations on collective labour disputes matters, and has been admitted to Tirana Bar Association in 2012.

She has contributed articles in various publications of our firm and has attended several conferences and training on the employment and labour matters.

Eni Kalo
Partner
KALO & ASSOCIATES Tirana
T +355 4 2233 532
E e.kalo@kalo-attorneys.com

Eni is a Partner of the firm, head of the IP Department, and provides a strong knowledge of both IP practice and legal procedures that is of invaluable benefit both to the firm and clients. Her main focus is on IP, commercial contracts, telecoms, advertising, consumer protection, pharmaceuticals, anti-corruption, data protection, and whistleblowing. She is active in the registration of patents, trademarks, and domains, and she has forged good links with both the General Directorate of Patents and Trademarks and the Commissioner of Information and Protection of Personal Data through her long experience in this area being the key contact for various clients.

Frensis Nakuçi
Senior Associate
KALO & ASSOCIATES Tirana
T +355 4 2233 532
E f.nakuci@kalo-attorneys.com

Frensis is a Senior Associate in the Corporate and M&A Department, consolidating her expertise in the field of all aspects of corporate issues, including but not limited to company establishment, business restructuring, M&A, anti-trust, competition, etc. As part of the corporate department, Frensis provides legal advice to companies across all sectors on M&As and restructuring of companies, legal due diligence and drafting of relevant legal reports, drafting of letters of intent, share purchase agreements, shareholder agreements and advises clients on various corporate issues through the corporate life cycle.

Austria

KNOETZL HAUGENEDER NETAL Rechtsanwälte GmbH

Bettina Knoetzl

Thomas Voppichler

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	
No					X*

* The lack of "adequate procedures" has to be shown by the prosecution authority (see more details question 15) and may - if additional requirements are fulfilled - lead to the company's criminal liability.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

After a significant legislative delay, a new law for the protection of whistleblowers came into force in Austria (*HinweisgeberInnenschutzgesetz*, "**HSchG**") in February 2023 - finally implementing the respective EU Whistleblower Directive. Weathering significant public criticism, Austria mainly complied with the Directive but did not go beyond it. For example, the new law restricts the material scope of the HschG to the areas mentioned in the Directive and the therein listed corresponding European regulations.

Among other things, the HSchG sets out itemised requirements in establishing the whistleblower reporting system. *Inter alia*, the following Directive requirements are now extant for internal investigations:

- Companies with more than 50 employees are required to establish an internal body charged with processing whistleblower reports -with the necessary financial and human resources to perform its tasks. The internal body must be planned, set up and operated in a manner that secures confidentiality of the identity of the whistleblower and third parties mentioned in the report.
- The internal body is bound by a strict confidentiality regime. The identity of the whistleblower must be protected by the internal body and kept confidential within the company, including management. The identity may only be disclosed with consent of the whistleblower or, if ordered by an administrative authority, court or public prosecutor's office.
- When dealing with whistleblower reports, the internal body must proceed in an impartial and unbiased manner.
- No later than three months after receiving a whistleblower's report, the internal body must inform the whistleblower of follow-up measures taken or intended to be taken, or, if the investigation has been terminated, the reasons why.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

In accordance with the provisions of the HSchG, a company can assign the duties of the internal body to a joint body. Third parties, such as outside counsel, can also be entrusted with the tasks of the internal body. In such cases, the safeguards and requirements for the internal body apply equally to the joint body or engaged third party.

The provisions of HSchG do not contain any restrictions with regard to group-wide bodies for the operation of the reporting system. However, considerable practical challenges need to be mastered, in particular concerning the obligation to maintain confidentiality and the documentation requirements. If the technical solution allows assignment of rights by third party only, a group-wide system can be feasible. In addition, it is advisable to consider the latest interpretations by the European Commission.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) There is no provision under the Austrian Constitutional Labour Law specifically addressing internal investigations or establishing an obligation to inform the works council about suspected cases or internal investigations which have already started or to allow a works council representative to participate. However, the company's agreement with the works council (*Betriebsvereinbarung*) may give rise to specific information rights.
More information can be found at https://www.gpa.at/themen/datenschutz/whistleblowing.

b) If data will be processed or transmitted in an internal investigation, the provisions of the General Data Protection Regulation ("**GDPR**") and the Law on Data Protection apply. The law does not provide for specific rights in connection with internal investigations. However, data protection laws may impose a duty to inform the data protection authority. See question 5.

c) There are no other local authorities who have a right to be informed about the investigation or to participate in it. However, if a company wishes to take advantage of the "Crown Witness" regulation or a leniency programme, assuming all preconditions are met, it is advisable to involve the relevant authorities. The so-called "Crown Witness" regulation allows prosecutors to drop an investigation against a cooperating witness who freely confesses their involvement in a serious offence and provides new information that contributes substantially to the investigation. Failure to involve the relevant authorities may preclude the company from obtaining the benefit.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees are under a duty of loyalty vis-à-vis their employer (*Treuepflicht*). Pursuant to these duties, employees are required to participate in investigation interviews. At the same time, the interviews must be conducted within the confines set by law, notably the employer's duty of care vis-à-vis their employees (*Fürsorgepflicht*). Pursuant to this duty, which also extends to executives and managers, the employer is, *inter alia*, required to respect the private life of employees, protect their integrity, and treat them equally.

Although employees must participate in interviews, Austrian legal scholars are engaged in a contentious debate over whether employees are also obliged to answer the questions of private investigators, which may reveal personal misconduct. If there is such a risk, the employee should be expressly advised by the interviewer to engage a legal representative. This way, a conflict of interest by the interviewee can be avoided and the employer complies with the duty of care.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Under Austrian law, an employer may only dismiss an employee with immediate effect (*Entlassung*) if the employer exercises this right immediately after becoming aware of the justification for the dismissal. Employers forfeit this right if they fail to exercise it immediately (i.e. "without delay"). In case of doubt, the employer can suspend the employee (*Dienstfreistellung* or *Suspendierung*) until the investigation yields more evidence or terminate the employee in a consensual manner (with the option for re-employment in case the employee is exonerated).

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The local, renewed Law on Data Protection ("**DSG**") came into effect in Austria, together with the GDPR.

The GDPR provides for, *inter alia*, the right of the individual to be informed about the processing of personal data. Moreover, companies with more than 250 employees or which process sensitive data are required to maintain a record of processing activities. Pursuant to the DSG, data may only be used in accordance with the law, in good faith, and only collected for specific legitimate purposes. The principle of proportionality also has to be respected.

b) reviewing emails?

A search with the express consent of the user is generally permitted. Without the consent of the user, it is important that the email account belongs to the company and is deemed to be for professional use. The interests of the parties and proportionality need to be considered.

Emails with private content may not be searched. If private emails are identified (e.g. by the subject line), only spot checks are allowed to clarify that the email is indeed private. As soon as an email is identified as private, it must be excluded from the search. If it has been opened by coincidence or as part of the spot check, it needs to be closed immediately after identification or confirmation that it is private.

c) collecting (electronic) documents and/or other information?

According to Article 5 of the GDPR, personal data may be collected only for specific, explicit, and legitimate purposes and, *inter alia*, be processed lawfully, fairly and transparently. In this regard, the processing of personal data is lawful only if, among other requirements, (i) the data subject has given consent, (ii) it is necessary for compliance with a legal obligation to which the data's controller is subject, or (iii) it is necessary for the purpose of the legitimate interests of the data's controller (see Article 6 GDPR).

The GDPR also provides for a catalogue of rights applicable to data subjects, including the right to be informed about the processing and storage of personal data, the purpose of data processing, and the duration of storage. GDPR provisions must be closely followed when it comes to processing data. For this purpose, the term 'processing' is defined as any operation or set of operations performed on personal data or on sets of personal data, whether by automated means, such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting upon, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying (see Article 4 GDPR). During an internal investigation, a considerable amount of evidence, including personal data, will be processed by collecting, storing, using, disclosing, etc. To comply with GDPR provisions, the identification of

which data is classified as personal and which as non-personal should be well documented. Furthermore, investigating companies should document the purpose of processing personal data in detail and comply with GDPR provisions regarding storage limitations, integrity, and confidentiality. Besides that, companies should be especially careful when it comes to transnational data transfers, especially from or to non-EU Member States.

d) analysing accounting and/or other business databases?

If accounting/business data contains no personal data, the data privacy rules do not apply.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no legal obligation to provide the employee with written instructions prior to the interview.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

The applicability of the right against self-incrimination in internal investigations is unsettled. As long as this legal uncertainty persists, it is advisable to inform interviewees of their potential right against self-incrimination. There is, however, no such duty of care between a company and third parties who are not employees.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

If an interview is conducted by outside counsel, they will have to comply with the attorneys' Code of Conduct. This Code requires the avoidance of conflicts of interests. Therefore, the interviewee has to be informed that the outside counsel is only acting on behalf and for the benefit of the company.

d) be informed of their right to have their own lawyer attend the interview?

Prior to the interview, the employer (or third party acting for the employer) should inform the employee that they have a right to be accompanied by their own legal representative. If the employee tends to make self-incriminating statements, it is strongly recommended to advise about this right.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Employees have no specific right to have a works council representative attend their interviews or otherwise participate in the investigation. They, therefore, also do not have to be informed in that regard. However, if the investigation is carried out according to the HSchG following a whistleblower's report, the company's agreement with the works council must be considered.

f) be informed that data may be transferred to another country (in particular to the United States)?

The GDPR and the Austrian DSG protect against the transmission of personal data abroad. Uncontrolled data transfer to the United States is, therefore, problematic. A mere notice to the affected person will not suffice. The employee will have to provide their informed consent prior to the transfer, which can be revoked at any time.

g) sign a data privacy waiver?

Employees are under a duty to share any information they obtain in their capacity as employees with their employer. Such data is not considered to be "private", and no waiver is required. The situation is different for data that qualifies as private. The employer must respect the employee's private sphere. A waiver to collect and use private data is required and may be legitimately withheld by the employee.

h) be informed that the information gathered might be passed on to authorities?

The employer has a duty to inform the employee of the exact use of the information gathered in an internal investigation, including the persons outside the company with whom the information might be shared. It is of particular importance if information might be passed on to prosecution authorities.

i) be informed that written notes will be taken?

It is common that minutes are written of an interview. The interviewee should also be informed of this. Moreover, data protection law requires the respect of the principle of proportionality in using data gained from the interview. Therefore, the company should not collect more personal data than the minimum amount required to conduct the investigation properly.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

All persons are under a legal duty to refrain from destroying evidence, including material that may become relevant in a legal dispute. Under Austrian law, suppression of evidence is a criminal offence. In order to protect employees from violating the law, it is advisable to remind them of this duty. Such warnings contain clear instructions to refrain from deleting emails or documents from the system.

In Austria, best practices require the immediate preservation of relevant data (by, for example, "imaging" the laptop assigned to an employee) if allegations of illicit behaviour arise.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Investigation reports drafted by attorneys are protected by attorney-client privilege. However, it only extends to attorney work product created to defend the client and not to previously existing evidence. This evidence cannot "gain" privilege through its inclusion in an investigation report.

The attorney work product should be stored in a way that the data remains in the custody of the attorney to ensure privilege protection (e.g. sharing work product over a secure server provided by the attorney).Regarding data that is in the attorney's custody, more extensive legal remedies are available than in the case of a seizure at the client's site, such as the sealing and judicial review of the data upon objection by the attorney.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

In Austria, the attorney-client privilege applies only to outside counsel.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Austrian law does not require companies to issue notifications when starting investigations. Usually, insurance policies encourage policyholders to inform the insurer of internal investigations. If there is a substantial risk that the insurer will be asked to cover the event if a claim arises, then the insurance company must be informed.

b) Business partners (e.g. banks and creditors)?

In general, there is no duty to inform business partners of the start of an investigation. *Ad hoc* or regular notification duties might apply to stock exchange listed companies. Banks tend to include provisions in their contracts that require notification of events that affect a partner company's creditworthiness.

c) Shareholders?

Companies publicly listed on the Vienna Stock Exchange are under a legal obligation to issue *ad hoc* notifications regarding insider information, i.e. information that has not been made public and which, if it were made public, would be likely to have a significant impact on the price of the company's shares or other related financial instruments.

d) Authorities?

There is no legal duty for private companies to report misconduct to law enforcement authorities. There may be such a duty for state companies or agencies exercising sovereign power.

Self-reporting may be advisable in circumstances in which the company can take advantage of a leniency programme, such as the "Crown Witness" regulation or the so-called "diversion" or to gain the "victim status" in proceedings (as the injured party).

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Authorities would expect, among other measures, sanctions to be imposed, including the immediate termination of employment contracts or – if the situation needs to be clarified – at least a suspension; a revision of existing policies; a repetition or improvement of training programmes; and the compensation of damages suffered by victims of the criminal conduct.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Internal investigations conducted according to best practices may be regarded as helpful if the results are openly shared with the prosecutor's office. The sharing of the results of an internal investigation may be considered, and can be an important factor in leading the prosecutor to refrain from prosecution of the company itself, under the Company Criminal Liability Act. It may happen that the prosecutor expressly request that certain questions be asked or certain investigative measures be taken, or avoided. Companies tend to comply with such requests.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

With the court's approval, the public prosecutor may order the search of a specific location – for instance, an office building – to collect, temporarily secure, or seize evidence to be used in criminal and civil proceedings. In highly urgent matters, the public prosecutor may order the search warrant and subsequently seek court approval.

House searches shall only be ordered if there is a "founded suspicion" (this threshold is higher than the "initial suspicion" required to open investigations) and the coercive measure complies with the principle of proportionality, meaning that there are no less intrusive means available. If, for example, the information could be obtained through obtaining the cooperation of the defendant, the application of coercive means, such as house searches or dawn raids, could be deemed to lack the requisite proportionality.

Persons against whom a search warrant was issued or whose premises were subject to a house search can file an objection with the competent office of the public prosecutor within six weeks from the measure. The public prosecutor can either comply or, within four weeks, refer the objection on to the competent criminal court.

Improperly obtained evidence can be used against the company. Some exceptions apply, for example, in cases of attorney-client privilege.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Non-prosecution agreements do not exist in Austria. There are, however, two related concepts: the so-called "diversion" and termination of proceedings. Owing, in part, to cultural opposition to "agreements" offered by the prosecution authorities, neither option is used frequently.

"Diversion" allows the prosecutor to end the criminal prosecution of a corporation if punishment of the corporation does not seem to be necessary. A number of factors are considered, including the conduct of the corporation after the alleged offence (here, self-reporting is of particular importance), the weight of the alleged offence, the amount of the fine to be imposed, and the detriment suffered by the corporation due to the misconduct. In some instances, the prosecutor must pursue diversion, provided certain requirements are met.

While the termination of proceedings leads to a full acquittal, "diversion" is positioned between a conviction and an acquittal. In contrast to a conviction, a "diversion" is not entered in the criminal register for corporations. Also, the related fines are lower.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Corporations are liable for the unlawful and culpable actions of their "decision-makers" (i.e. higher ranked individuals with authority to represent the company) and, under more restrictive conditions, also for the actions of their "normal" employees, provided that the offence was either committed for the benefit of the corporation or the offence violated duties incumbent upon the corporation itself.

If the offence was committed by a regular employee, it must have either been rendered possible or facilitated by the decision-makers' failure to take essential precautionary measures (e.g. implement a proper compliance system). The prosecution bears the burden of establishing the lack of adequate procedures. In practice, the corporation will usually try to show the proper implementation of adequate procedures.

Corporations are subject to fines, which are measured in per diem units, and court directives (e.g. to compensate harm done, implement a proper compliance system, or make charitable donations). The current maximal fine for offences, such as severe fraud, embezzlement, or corruption, is €3.9 million and depends on the corporation's earnings.

Natural persons are subject to the whole range of penalties and other sanctions if they are found personally guilty of an offence.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

The amount of the fines imposed upon corporations is determined according to aggravating and mitigating factors. As grounds for reduction of fines, the law explicitly and equally mentions both precautionary measures taken by the company to prevent crimes prior to the alleged misconduct and precautionary measures taken to prevent further misconduct installed after an offence was committed. Other mitigating factors for fines against corporations are, e.g. significant assistance the company may provide in clarifying the facts of the case, compensation for the consequences of the misconduct, and significant legal disadvantages that the company has already suffered as a result of the misconduct. Apart from a reduction, fines may be partially or fully suspended under certain preconditions.

Penalties imposed on natural persons are calculated according to aggravating and mitigating factors based on the individual's personal culpability.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Austria implemented the EU Non-Financial Reporting Directive in 2017 with the introduction of the Sustainability and Diversity Improvement Act. Due to the law's limited scope only a few companies are affected (apparently no more than 75). However, the Austrian legislature is currently working on implementing the EU Corporate Sustainability Reporting Directive ("**CSRD**"). The CSRD is expected to bring change.

While the issues of greenwashing and ESG fraud have been widely discussed in public, no major investigations by the Austrian authorities have been reported.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

In December 2023 the Austrian Constitutional Court rendered a landmark decision for the rule of law and respect of human rights, annulling the previously relevant legal provision applicable to the seizure of smart phones and turning the – now unlawful – practice upside down.

To date, the seizure of objects does not require authorisation from a court but only the order by the public prosecutor's office, whereas a house search requires the court's prior approval. As one smartphone likely contains more sensitive data than a typical house search, the practice of the prosecution authority to seize smartphones without court approval was successfully challenged before the Constitutional Court as being unconstitutional. By the end of 2024 the relevant pre-existing provisions will be annulled.

In its ruling, the Austrian Constitutional Court decided that the new regulation must in any case include a judicial authorisation for the seizure of smartphones and similar data carriers and that the processing of data must be limited to specific data categories. According to statements made by the government, the new regulation is planned to come into effect within the set deadline, perhaps even sooner.

CONTACTS

KNOETZL

Herrengasse 1
1010 Vienna
Austria

Tel.: +43 1 3434 000
Fax: +43 1 3434 000 999
www.knoetzl.com

Bettina Knoetzl
Partner
KNOETZL HAUGENEDER NETAL
Rechtsanwälte GmbH
T +43 1 3434 000 200
E bettina.knoetzl@knoetzl.com

Bettina Knoetzl is one of the founding partners at KNOETZL HAUGENEDER NETAL Rechtsanwälte GmbH, a leading, Austrian based, international law firm specialised in Dispute Resolution, Business Crime, Compliance and Corporate Crisis Management.

Bettina is a trial lawyer with 25 years' experience in international and Austrian matters of high profile, scoring notable successes in criminal defence work on insider trading, price fixing, fraud and corruption cases. For more than a decade Bettina has been assigned the highest tier rankings by international directories, such as Chambers, in both civil litigation and white collar crime. In 2017 she has been awarded worldwide recognition as "Lawyer of the Year" in Asset Recovery by Who's Who Legal, London Business Research Society. She is a designated thought leader in the legal community and is known for her vast, practical and creative experience in structuring settlements in complex disputes. In addition to her civil litigation work, she handles business crime cases, internal investigations, including FCPA and #MeToo-matters in the banking, insurance, pharma and automotive industry, with a significant focus of her practice on investors' protection and asset recovery. Bettina advises clients in mission-critical and notorious disputes, including class actions, and has a proven track record of winning judgements and strong, favourable settlements for both companies, government instrumentalities and private clients.

Bettina is the President of Transparency International (Austrian Chapter), the exclusive Austrian representative of the ICC-FraudNet and lecturer at the Austrian Lawyers' Academy (AWAK), in dispute resolution. She is heavily engaged in the International Bar Association where she co-chaired the global Litigation Committee throughout 2016/2017.

Thomas Voppichler
Partner
KNOETZL HAUGENEDER NETAL
Rechtsanwälte GmbH
T +43 1 3434 000 201
E thomas.voppichler@knoetzl.com

Thomas Voppichler is a Partner at KNOETZL and heads the firms' White Collar Crime Department. His practice is focused on business crime matters, asset recovery and international litigation.

Expert in all areas of white collar crime, Thomas delivers effective experience to clients through high-profile criminal proceedings, especially in the aggressive pursuit of injured parties' recovery of damages suffered through embezzlement, fraud and bribery.

Thomas has longstanding experience conducting internal and external corporate investigations, essential both for revealing internal misconduct or enhancing compliance, and for gathering evidence and preparing for criminal and civil enforcement claims for injured companies.

Thomas also routinely acts as defence counsel in cases involving corporate and business crimes, and handles mission-critical cases for national and international clients. Thomas also maintains significant active and current expertise in asset tracing and recovery techniques, applied successfully in a wide array of jurisdictions.

Thomas publishes as an author in professional journals on subjects concerning corporate criminal liability, corruption and antitrust offences, investigation procedures, and leniency programmes.

Belgium

Hogan Lovells International LLP


Fabien Roy


Hélène Boland


Grégoire Paquet

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	
No					X*

* No formal "Adequate Procedures Defence", but such procedures are recommended to show lack of intent/negligence.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The Belgian law transposing the EU Whistleblowing Directive for the private sector, the Law of 28 November 2022, B.S. of 15 December 2022 ("**Belgian Whistleblowing Act**") was adopted per 28 November 2022 and entered into force on 15 February 2023.

Legal entities with 50 or more employees are required to set up channels and procedures for internal reporting of the violations targeted by the Belgian Whistleblowing Act and for following up on such reports (Article 11 paragraph 1). Companies that are active in the field of financial services, products and markets and those that are vulnerable to money laundering and financing of terrorist activities are compelled to set up internal reporting systems regardless of the number of employees (Article 11 paragraph 2 under 3).

According to the Belgian Whistleblowing Act, legal entities are free to choose how they organise the required internal reporting procedures, as long as they comply with specificities such as:

- The internal reporting system must be established in consultation with the existing ´social partners´, i.e. employee representative bodies, works council, trade union delegation, health and safety committee (Article 11 paragraph 1). Reporting channels may be operated internally by a designated person or department but also outsourced to a third party (Article 11 paragraph 4);
- Information relating to the procedure that should be followed to report a breach must be provided in a clear and easily accessible form (Article 12 paragraph 1 under 6);
- The internal reporting procedures must allow for reports to be submitted in writing or verbally, or both (Article 12 paragraph 1 under 1). If provided verbally, the information may be provided either by telephone or through any type of voice messaging system and may involve an in-person meeting, if the whistleblower requests so (Article 12 paragraph 1 under 1);

- The internal reporting procedures must allow for anonymous reporting (Article 8 paragraph 2 under 1). Please note that legal entities with fewer than 250 employees are not obliged to handle anonymous reports (Article 8 paragraph 2 under 2);
- The internal reporting procedures must grant the person reporting the right to not have his or her identity disclosed to third parties, without the person's express and free consent (Article 20 paragraph 1);
- There must be restricted access to the personal data contained in the internal informational system. Personal data shall be accessible only to authorised staff members (Article 12 paragraph 1, under 1; 15 paragraph 1 under 1; 20 paragraph 1);
- Employers and competent authorities are required to maintain a register of reports received. The register must respect applicable rules of confidentiality (Article 22 paragraph 1 and 20);
- An acknowledgement of receipt needs to be sent to the person reporting within seven calendar days following the receipt of the report (Article 12 paragraph 1 under 2);
- A reporting manager needs to be appointed to follow up on the report, maintain communication with the person reporting, and, where necessary, ask for further information and provide feedback. This can be the same person or department who was appointed internally to receive the reports (Article 12 paragraph 1 under 3; 4 paragraph 2);
- The internal reporting procedures must provide for feedback to be given to the person reporting, within three months from the date of notification of receipt, or, if no notification was sent, within three months from the expiration of the seven day period after the receipt of the report (Article 12 paragraph 1 under 5);
- The Federal Ombudsman's Integrity Centre has been designated as the coordinating competent authority for external reporting in the private sector (Article 14 paragraph 1 and Article 18 paragraph 1). They coordinate the processing of external reports: Receipt of the reports, feedback, forward to the relevant competent authority and appropriate follow-up thereon;
- Persons reporting are to be protected against any form of retaliation - if they had reasonable grounds to believe that the reported information was accurate at the time of reporting and that the information fell within the material scope of the Belgian Whistleblowing Act. Protection includes protection against several kinds of actions including suspension, dismissal, negative performance assessment, withholding of training, changing employment conditions, disciplinary sanctions, etc. Retaliation against protected persons is criminally sanctioned (Chapter 7).

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Pursuant to Article 11 paragraph 4 under 2 of the Belgian Whistleblowing Act, legal entities in the private sector with 50 to 249 employees are allowed to share resources in relation to the receipt of reports and the conduct of investigations. However, legal entities with more than 250 employees will need to have their own internal reporting procedure.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) According to the Collective Bargaining Agreement ("**CBA**") No 81 and other applicable CBAs, employee representative bodies must be involved when specific investigative tools are applied, such as the monitoring of online communication (CBA 81) or placing cameras in the workplace (CBA 68). Failure to comply with these CBAs may result in criminal sanctions. In addition, companies may have included specific provisions in their internal labour regulations which oblige them to inform employees' representatives when an internal investigation is launched.

b) Internal investigations involve the extensive processing of personal data. Thus, the investigations should comply with the EU General Data Protection Regulation ("**GDPR**") and the Law of 30 July 2018 implementing the GDPR. In light of Article 38 of the GDPR and Article 63 of the Law of 30 July 2018, internal investigations will generally have to involve the Data Protection Officer, where the company has one. Infringement of the GDPR and the Law of 30 July 2018 may lead to administrative fines.

c) Some laws require authorities to be informed when specific criminal offences were potentially committed. For instance, the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and the restriction of the use of cash financing provides that when relevant companies become aware of or suspect that a transaction is connected specifically with money laundering or terrorist, they must inform the Finance Intelligence Unit ("**CFI-CTIF**") (Article 33). Some laws impose reporting obligations to the Federal Agency for the Safety of the Food Chain ("**AFSCA/FAVV**") or the Federal Agency for Medicines and Health Products ("**AFMPS/FAGG**"). Such a report may trigger an investigation by one of these agencies, although they will not get involved in the internal investigation of private companies. Failure to comply with an obligation to report is subject to criminal sanctions.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees must comply with the instructions of their employer within the context of their employment contract. This includes requests to take part in interviews during an internal investigation. However, the employer may not use coercion, for instance, to prevent employees from leaving the interview room. Employers may impose disciplinary measures for failure to comply with legitimate instructions.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

To be able to immediately dismiss an employee (e.g. for serious misconduct), the employer must act within a strict deadline which elapses after three days. The period starts as the moment the employer obtains certainty about the facts. Taking the time to do an internal investigation may reveal important information. However, when the relevant acts or omissions of the employee are already known, the internal investigation does not extend the deadline. Even if internal company regulations provide that an employee must be heard before being dismissed, companies that wish to immediately dismiss an employee must ensure that they do so in a timely manner.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The GDPR governs the processing of personal data. When conducting an interview in the context of an internal investigation, the investigator will process personal data as soon as any personal information is written down or otherwise stored. The processing of personal data collected during or after the interviews must comply with the requirements of the GDPR.

b) reviewing emails?

The employer reviewing employees' emails must respect the general data protection principles and the requirements imposed by the GDPR. The Belgian CBA 81 provides rules concerning employer monitoring of employee emails. Furthermore, Articles 124 and 125 of the Belgian Electronic Communications Act and Article 314bis of the Belgian Criminal Code ("**BCC**") prohibit the processing of specific communications of employees, including emails, without the consent of all parties involved in the exchange of communications. In this context, we advise employers to draft a policy or Standard Operating Procedure ("**SOP**") that sets out the appropriate use of professional email addresses and how the employer may supervise or monitor the use of those email addresses.

c) collecting (electronic) documents and/or other information?

The collection of electronic documents and/or other information also needs to comply with the general provisions of privacy law outlined under section 3a. In order to set clear standards and ensure that employees have realistic privacy expectations, companies should put in place a clear corporate policy on the use of electronic devices provided by the employer or personal devices used for professional purposes. The GDPR will apply to any collection of written or stored information that includes personal data. We suggest that employers draft relevant policies and SOPs.

d) analysing accounting and/or other business databases?

If the databases include personal data, such analysis is likely to amount to data processing. Therefore, the company must comply with the requirements of the GDPR. If these databases do not contain such personal data, their analysis is not subject to privacy legislation.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

Belgian law does not provide specific rules concerning employee interviews during an internal investigation. However, it may be helpful to provide the employee with a document which contains the employee's rights during the interview and to request the employee to sign that document. The purpose of the signature is to document that the employee had the opportunity to acknowledge the content of the document.

The document aims to diminish the risk that Belgian judges find the statements inadmissible as evidence. In some cases, Belgian judges ruled that the employer or prosecutor may not rely on statements which were not made voluntarily, as evidence. Judges may consider all the circumstances surrounding the interview during which the statements were made to determine whether the statements were made voluntarily. For example, judges may consider the use of misleading promises, physical violence or psychological violence by the interviewer coercion to make the employee provide these statements.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

No. However, Belgian judges ruled that there may not be any indication that the employee was coerced to make the statements or that the statement was made in conditions that raise questions concerning the voluntary nature of the statements. If the employee makes a self-incriminating statement, the judge may strictly scrutinise its voluntary nature in court proceedings.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

Although the so-called 'Upjohn warning' is not a requirement, we would suggest informing the interviewee that the lawyer attending the interview does not represent the employee. If the interviewer does not inform the employee about the identity and the capacity of all persons present, the employee may be able to claim that the employer collected the statement through deceit, which detracts the statement of its credibility. Further, all Belgian lawyers are bound by a Professional Code of Conduct. The Code of Conduct provides that Belgian lawyers should be clear about who they do or do not represent during an interview. If the lawyer gives the employee the impression that they are representing the employee or both the company and the employee, that lawyer may violate the Code of Conduct.

d) be informed of their right to have their own lawyer attend the interview?

No. However, it may be helpful for the company to decide that the employee may be assisted by a lawyer and inform them thereof. In court, this may add to credibility that the employee has provided the statements voluntarily.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Belgian law does not require employers to inform the employee that they have the right to have a representative of the union or works council to be present at the interview.

It may, however, be helpful to inform the employee of this right. The presence of an employee representative may add credibility to the voluntary nature of the statements in potential court proceedings.

Some employers include the possibility of employees being accompanies by a union representative during interviews, in the employer's labour regulations.

f) be informed that data may be transferred to another country (in particular to the United States)?

Any transfers of personal data outside the European Union must be subject either to an adequacy decision or appropriate or suitable safeguards according to the GDPR. Whether the transfer may take place would need to be assessed on a case by case basis.

g) sign a data privacy waiver?

No, the Belgian Data Protection Authority has taken the position that, in general, employees cannot give their consent freely to an employer. However, in accordance with Article 13 of the GDPR, the employer must provide the employee with a privacy notice that specifying the intended purpose of the processing and the legal basis for the processing. This applies if any records of the interview are made which include personal data. It may be helpful to request the employee to sign the document containing this information to document that the employer provided the employee with this information.

h) be informed that the information gathered might be passed on to authorities?

If the employer may share personal data with the competent authorities, the employer shall inform the employee thereof as set out in the section g above. Furthermore, documenting that the employee was informed increases the credibility of the voluntary nature of the statements if challenged during court proceedings.

i) be informed that written notes will be taken?

No. However, if written notes are taken that include personal data, the GDPR applies to the processing of the personal data. The employer will have to comply with the general principles of the GDPR and then have to inform the employee of the personal data processing with a privacy notice in accordance with Article 13 GDPR.

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Yes. If the documents contain personal data, the GDPR applies to their processing and storage. Personal data may not be kept longer than required for the purpose for which the data has been collected. The hold notice would be an exception to the employer's data retention policy. Any document hold notice should include the scope and purpose of the retention and be sent to the employee in a timely manner.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege, or legal professional privilege ("**LPP**"), may be claimed over findings of the internal investigation. In Belgium, LPP applies to lawyers (Avocat/Advocaat) who are members of the French and German Bar ("**OBFG**") or the Flemish Bar ("**OVB**"), as well as in-house counsel registered with the Belgian Institute for In-house counsel, the *Institut des Juristes d'Entreprise*.

LPP protects any information received by an attorney (acting in their capacity as an attorney) or obtained in the context of the provision of legal advice, legal proceedings, or any dispute in general, or in matters determining the client's rights and obligations. This may include emails, correspondence, notes, advice, or preparatory documents.

In order to ensure the most protection of LPP, it is essential for external counsel to conduct the internal investigation, particularly if the investigation has cross-border elements (see response to question 10 below). In the context of seizure by the authorities of documents regarding the internal investigation and which are drafted by a lawyer (e.g. an investigation or audit report), a specific procedure is in place, whereby the President of the Bar assesses the confidential character of documents and prevents the authorities from taking note of the content of those documents. Violations of LPP are criminally sanctioned (Article 458 of the BCC).

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

The Law of 1 March 2000 establishing the Belgian Institute for In-house Counsel. Under Article 5 of this law, in-house counsel advice is confidential. This applies if the advice is given for the benefit of the in-house counsel's employer and within the framework of activity as legal counsel. The Brussels Court of Appeal confirmed this in a judgement of 5 March 2013 (18th Chamber, No 2011/MR/3). The Court of Appeal held that, according to Article 5 of the Law of 1 March 2000 and Article 8 of the ECHR (right to privacy), the Belgian Competition Authority could not seize documents containing legal advice provided by in-house counsel. The Brussels Court of Appeal held that LPP also covered internal requests for legal advice, correspondence relating to legal advice, draft opinions, and preparatory documents. The judgement of the Brussels Court of Appeal stands in stark contrast with the Akzo judgement (C-550/07 P) of the Court of Justice of the European Union ("**CJEU**") on 14 September 2010. In Akzo, the CJEU ruled that, under EU law, correspondence from or addressed to an attorney is not protected by LPP if the attorney is bound to their client by a relationship of employment. Thus, the CJEU excluded advice by in-house counsel from protection by LPP (as well as advice from non-EEA-qualified external counsel). However, the Brussels Court of Appeal considered that there was no inconsistency between its ruling and the Akzo judgement. The court reasoned that the European Commission's investigatory powers are different from those of national competition authorities. This difference can justify a distinction between the rules on LPP at EU and at national level.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Under Belgian law, there is no requirement of notification to insurance companies. However, insurance policy agreements will often contain clauses obliging the policyholder to notify the insurance company in case of potential claims, within a specific period of time.

b) Business partners (e.g. banks and creditors)?

There is no general obligation to inform business partners of internal investigations. Nevertheless, depending on the circumstances, it may be recommended to inform business partners, especially if they would be harmed by the outcome of the internal investigation. Such an act could be considered as demonstrating good faith on account of a company performing an internal investigation.

c) Shareholders?

Conducting an internal investigation usually means dealing with sensitive information. Therefore, any disclosure of such internal investigation to shareholders (as with other disclosures) should be considered on a case-by-case basis and in the context of applicable contractual/corporate obligations. Since the revision of the Belgian Company Code in 2019 (see Articles 96 and 119 BCC), certain companies may now be required to disclose internal investigations in their annual report. However, this does not apply if they invoke the "comply or explain" clause of Article 96 BCC and justify why they may deviate from this obligation. However, companies must also take other applicable legislation (e.g. insider trading statutes) into consideration. For example, the law requires certain companies to inform the public of sensitive internal information that directly concerns the company (e.g. Article 17 of the EU Market Abuse Regulation, which provides such obligation for certain public market participants).

d) Authorities?

Please see section 2c.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Once the company is aware of damages, it should take all reasonable measures to limit the aggravation of those damages. The company must therefore cease any ongoing criminal behaviour. In addition, it will be in the interest of the company to distance itself from the wrongful behaviour of its employee(s) and to undertake disciplinary actions against them to avoid suspicions of bad faith and complicity on the part of the entity.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Belgian prosecutors are under no legal obligation to take internal investigations into account. Internal and external investigations are independent of each other. Nevertheless, the company can decide to share the results of its internal investigation with the prosecutor's office, e.g. when the company files a criminal complaint against an employee. Voluntary disclosure of the results of an internal investigation may be taken into account as a mitigating factor when penalties are imposed. If a company intends to submit a file to the prosecutor, it is recommended to ensure the credibility of the investigation by documenting every investigative measure and entrusting it to external counsel. In addition, it should be kept in mind that under Belgian Law, as a general principle, evidence obtained in breach of legal provisions (e.g. on the protection of employees, on the protection of data privacy) may not be admissible. As a result, each internal investigation must comply with all relevant legal provisions.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

In principle, search warrants in criminal proceedings have to be executed by the investigating judge (Article 87 of the Code of Criminal Procedure, "**CCP**"). However, they can and are often delegated to judicial police officers.

According to case law of the Belgian Supreme Court ("**BSC**") of 2003, now included in Article 32 of the preliminary title of the CCP, evidence that was obtained without fulfilling those requirements can be used unless the irregularity (i) affects the reliability of the evidence, (ii) violates the right to a fair trial, or (iii) does not comply with formal

requirements that are sanctioned by nullity. The competent court will examine whether these conditions were met, on a case-by-case basis.

The situation is similar to dawn raids for competition law purposes. Dawn raids are also not lawful without a prior judicial warrant. The requirement of a prior judicial warrant was included in the Competition Act in 2013 (Book IV of the Economic Law Code).

On 26 April 2018, the BSC confirmed that evidence seized during unlawful dawn raids or resulting from unlawful raids, should be excluded. The Belgian Competition Authority had argued that it could nevertheless use unlawfully obtained evidence based on the so-called 'Antigone' case law. In criminal cases, it is recognised that an error in the gathering of evidence may only lead to the exclusion of the evidence under certain circumstances. However, the BSC reasoned that this case law does not apply to competition cases. The judgement of 26 April 2018 states that an appropriate remedy for an unlawful dawn raid can only be provided by excluding all evidence obtained and resulting from the dawn raid.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Settlements (Article 216bis CCP) and guilty pleas (Article 216 CCP) are available for companies in Belgium. Guilty pleas were introduced in 2016 and are not common in Belgium. The Constitutional Court ruled in June 2016 that Article 216bis paragraph 2 CCP is unconstitutional to the extent that the prosecutor can end cases already handled by a judge without sufficient judicial control of this power of the prosecutor. The Law of 18 March 2018 amended Article 216bis CCP to align it with the Constitution. It now foresees in regulation on judicial scrutiny of the proportionality of settlements and not just the formal legitimacy thereof. In addition, where a settlement concerns tax or social security matters, the prosecutor must inform the relevant public authorities that a settlement has been reached. These authorities must then approve the settlement.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Companies can be held liable for the misconduct of individuals where the offences have a sufficiently strong connection to the interests of the corporation. The BCC provides that the penalties for companies can be: fines, confiscation, dissolution and prohibition to exercise an activity, the closure of one or more establishments, and the publication or dissemination of the decision. Furthermore, the Act of 17 June 2016 concerning public procurements provides that individuals may be excluded from participating in public tender procedures.

Under specific conditions, directors, officers, and/or employees may be penalised for the misconduct of other individuals. The penalties that apply to individuals are fines, imprisonment, electronic surveillance, confiscation, deprivation of civil or political rights, and standalone probation sentences. Furthermore, Royal Decree No. 22 of 24 October 1934 provides a legal basis for prohibiting individuals from pursuing certain professional activities.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

In Belgium, judges have a broad discretion to decide on and motivate potential penalties. The judge may take into account all circumstances leading to the potential penalty, including the implementation of efficient compliance systems. Thus, it is helpful to have efficient compliance systems in place before the ruling, to limit the penalties.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

From an environmental perspective, Book II of the BCC has been reformed to criminalise the newly created crime of ecocide. Belgium now officially recognises ecocide as a crime under international law, alongside genocide, crimes against humanity, war crimes, crimes of aggression, all already protected in the Criminal Code in alignment with established international legal frameworks. This qualification applies when the act constitutes an offence under federal legislation or an international agreement binding on the federal authority, even if the act cannot be localised within Belgium. It covers unlawful actions that result in the large scale destruction of the environment and nature in the broadest sense. The penalties hit hard, ranking at level 6 out of 8 in the new BCC hierarchy. Individuals face imprisonment ranging from 15 to 20 years, while corporations can incur fines ranging from €1.2 to €1.6 million.

Aside from that, we are not aware of Belgium intending to adopt national rules on ESG, only that it is following the initiatives being discussed at the EU level in that respect. For instance, Belgian law does not provide for a national supply chain due diligence legal regime in the vein of the recently adopted EU wide Corporate Sustainability Due Diligence Directive, which will have to be transposed into national legislation.

As regards enforcement, it is worth mentioning that we see enhanced oversight and investigations by the Federal Public Service ("**FPS Economy**") on greenwashing claims as a misleading commercial practice. FPS Economy encourages reports from consumers on these type of claims.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Belgium witnessed a number of scandals in recent years, both in the public sector, including politics, and in the private sector. This meant greater legal and reputational risks of doing business, as well as increased scrutiny from the authorities and the public. In March 2022, the Belgian Minister of Justice and the Minister of Internal Affairs validated the so-called National Security Plan 2022-2025 which covers security topics that require special attention from the police in that period. These themes include crimes against property, tax fraud and other financial and economic phenomena, social fraud, food chain and environmental crime, hacking, computer sabotage, computer and internet fraud, as well as horizontal phenomena such as corruption. Recently, public prosecutors devote more time and attention to social fraud, social dumping and modern slavery. Existing liability schemes in the labour law chain encourage investigations. It is also worth mentioning that the European Public Prosecutors Office initiated new prosecutions in Belgium in 2023, with a focus on tax fraud (evasion of customs duties and VAT-fraud) and other types of fraud affecting European Union financial interests. Internal investigations and audits have been increasingly used in the wake of this. Investigation teams added new technology options to their investigation toolkit. Data protection is currently at the core of many concerns. Therefore, and as discussed in this contribution, it will be relevant for companies planning internal investigations to closely consider the implications of the Belgian Whistleblowing Act, the GDPR and the Law of 30 July 2018 implementing the GDPR.

CONTACTS

Hogan Lovells

Rue Belliard 9
1040 Brussels
Belgium

Tel.: + 32 2 505 0911
Fax: + 32 2 505 0996
https://www.hoganlovells.com/en/locations/brussels

Fabien Roy
Partner
Hogan Lovells Brussels
T +32 2 505 0970
E fabien.roy@hoganlovells.com

Fabien Roy has been a member of the Brussels Bar since 2011 and a Partner at Hogan Lovells since 2019.

His practice focuses on EU and national regulatory matters involving medical devices and pharmaceutical laws and guidelines. Fabien follows the new EU regulations on medical devices (MDR and IVDR) and the GDPR very closely and regularly advises clients on the requirements applicable to their digital health technologies. Fabien is also a qualified lead auditor for ISO 13485 quality management systems. Consequently, he has a deep understanding of the range of quality issues encountered by companies and regularly advises clients in relation to internal/external audits and investigations.

Hélène Boland
Senior Associate
Hogan Lovells Brussels
T +32 2 505 0976
E helene.boland@hoganlovells.com

Hélène Boland has been a member of the Brussels Bar since 2017.

Her practice focuses on EU and national regulation of pharmaceuticals, biotechnology, medical devices, special foods and feeds, personal protective equipment, cosmetics, and other consumer products.

She assists clients in understanding the requirements introduced by the EU GDPR and various aspects of digital health technologies. Hélène regularly advises international companies on complex queries in relation to Belgian or EU law.

Grégoire Paquet
Associate
Hogan Lovells Brussels
T +32 2 505 0911
E gregoire.paquet@hoganlovells.com

Grégoire Paquet has been a member of the Brussels Bar since 2019.

As a member of our Global Regulatory practice, he regularly assists clients with commercial and regulatory questions in both EU & Belgian law. His practice focuses on both Life Sciences and Products Law, with a particular focus on the consumer goods, technology, automotive, and food industries.

He supports companies in the entire lifecycle of products, from early development and design stages, to marketing, and post-marketing issues. He has experience in handling product crises and product recalls through authority notifications and global corrective actions.

Grégoire lectures on Comparative Law at the Université Libre de Bruxelles as a Teaching Assistant.

Bulgaria

Kambourov & Partners

Ivo Alexandrov

Zlatko Grigorov

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X*	X	X	X	
No					X**

* No criminal liability for companies, but administrative sanctions may be applied in case of employee misconduct.

** No explicit legislation.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The Bulgarian Protection of Persons Who Report or Publicly Disclose Information on Breaches Act (the "**Bulgarian Whistleblower Act**"), which transposes the EU Whistleblower Directive, came into force on 4 May 2023. Initially, from 4 May 2023 to 17 December 2023 the Bulgarian Whistleblower Act applied only to obliged entities with over 250 employees. However, starting from 17 December 2023 the Act extended its application to all obliged entities. The Bulgarian Whistleblower Act implemented a specific procedure for whistleblower reports which trigger an internal investigation.

If a whistleblower report is submitted under the Act, an acknowledgement of receipt must be sent to the reporting person within seven calendar days following receipt by the person responsible for the internal handling of reports. Next, the responsible person shall collect the necessary confirmations and additional data from the whistleblower or other relevant persons. Afterwards, the responsible person shall conduct a hearing with the person against whom the report was submitted and provide them with the collected evidence, document their explanations and collect the evidence specified by them. Once the facts of the report are identified, the responsible person shall: (i) organise the follow-up of the report and may require the assistance of other persons or units within the structure of the obliged entity; (ii) shall propose the obliged entity to take specific measures in order to stop or prevent the breach; (iii) shall refer the reporting person to the competent authorities in case their rights were affected; and (iv) forward the report to the Commission for Personal Data Protection ("**CPDP**") where action by the CPDP is required.

The responsible person is obliged to provide feedback to the reporting person within three months after the acknowledgement of receipt of the report, on the actions taken. The responsible persons shall be obliged to ensure that the identity of the reporting person and of any other person mentioned in the report, be duly protected and shall take the necessary measures to limit access to the report by unauthorised persons. A strict prohibition on any and all forms of retaliatory measures is also prescribed by the law. Obliged entities

shall also keep a non-public register of the received reports which must follow the template register adopted by the CPDP.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Under the Bulgarian Whistleblower Act, reporting channels may be operated internally by a person or department designated for such purpose or established by the economic group to which they belong or be outsourced to a third party in compliance with the Act. Additionally, non-public obliged entities may share resources for receiving reports and for taking follow-up actions on them, and subject to compliance with the requirements of the Act regarding maintaining confidentiality, giving appropriate feedback, and properly addressing the reported breach.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Works councils do not exist in Bulgaria. The collective interests of employees are represented by trade unions and employee representatives which are elected by the employer. In general, trade unions represent and protect employees' interests before government bodies and employers. The Bulgarian Whistleblower Act explicitly states that the Act shall not affect the rights of workers under the Labour Code, specifically the right to consult their representatives and trade union organisations as well as the rules on the autonomy of the representative bodies of workers and employers and their right to enter into collective bargaining agreements. The Labour Code does not require that trade unions be informed about internal investigations. Hence, the participation of trade unions in internal investigations is not prevalent.

b) Under the EU General Data Protection Regulation ("**GDPR**") the Data Protection Officer ("**DPO**") must consult with employees about their data privacy rights. An employer must therefore inform the DPO about all investigations that implicate data privacy. Furthermore, the Bulgarian Personal Data Protection Act ("**PDPA**") requires employers to inform the CPDP when personal data collected during investigations is intended to be transferred to a non-European state.

Per Ordinance No. 1 of 27 July 2023, adopted under the Bulgarian Whistleblower Act, reports shall also be forwarded to the CPDP in the event that the internal investigation gives grounds to believe that further actions are required from the CPDP, namely if (i) the report was received by a non-obliged entity; (ii) the report concerns violations by high ranking public officials; (iii) the report refers to an obliged entity other than the one where the report has been received; and (iv) where processing and forwarding by the CPDP is required. Item (iv) refers to situations where the report concerns violations requiring further action by exhaustively enumerated public bodies, i.e. the Financial Supervision Commission, State Agency for National Security, Consumer Protection Commission, etc. In such situations, only the CPDP may forward the report to the competent bodies. If an obliged entity forwards a report to the CPDP it shall inform the reporting person prior to the handover.

c) The Criminal Procedure Code ("**CPC**") obliges employees to inform competent public authorities of criminal offences, regardless of the status of an internal investigation.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

The Bulgarian Whistleblower Act does not require employees to participate in internal investigation interviews. However, employees have a general duty to obey any lawful orders of the employer, follow internal rules adopted by the employer, and other duties provided by law. Employers may adopt internal rules regarding the conduct of investigations and may request that employees answer work-related questions during an investigation. An employee's refusal may be regarded as misconduct, which could justify imposing disciplinary measures. Prior to imposing disciplinary measures, however, an employer must consider an employee's verbal explanation or examine their written notes. Failure to do so may lead to revocation of the imposed disciplinary sanction by the court. Additionally, the principles of non-retaliation against whistleblowers shall be strictly observed regarding reporting persons.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Under the Labour Code, disciplinary sanctions (e.g. dismissal) must be imposed within two months after discovery of the breach and no later than one year after the commission of the offence. Sanctions imposed outside of the statutory period are invalid. Investigations should therefore be concluded quickly.

Additionally, under the Bulgarian Whistleblower Act, reporting persons shall not be liable for the acquisition of the information contained in the report, or for access to it, provided that such acquisition or such access does not constitute a stand-alone criminal offence. Reporting persons shall not be liable for breach of the restrictions on disclosure of information under a contract, legal or regulatory act or administrative act, provided that they had reasonable grounds to believe that the reporting or public disclosure of the information was necessary for the detection of the breach.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

In the PDPA, personal data is defined as any information related to an individual which, directly or indirectly, identifies the individual or makes them identifiable. If an employer plans to collect personal data during an interview, it is necessary to obtain the consent of the person whose personal data shall be collected prior to the interview.

b) reviewing emails?

Before reviewing emails containing personal data or information, consent should be obtained from the data subject. The data subject has the right to be informed about the purpose of the processing, the concerned categories of data, and the identity of the recipient(s) of the data.

Although the constitutional right to confidential correspondence in Bulgaria is not thought to apply to business or private correspondence sent or received via, or stored on, a company's electronic device, the European Court of Human Rights ("**ECHR**") recently ruled in *Bărbulescu v. Romania* that a company may not monitor an employee's work email without explicitly informing them in advance. As a member of the COE and a party to the European Convention on Human Rights and Fundamental Freedoms, Bulgaria is obliged to implement the decision of the ECHR.

c) collecting (electronic) documents and/or other information?

While collecting electronic documents, one should take into account the obligations under the PDPA and the Electronic Document and Electronic Signature Act ("**EDESA**"). According to Article 43 (4) of the EDESA, only personal data relating to the data subject may be collected; data from a third person may only be gathered with their explicit consent.

d) analysing accounting and/or other business databases?

It is not necessary to obtain an employee's consent to review accounting or financial records that do not contain personal data.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

While there is no legal obligation to provide an interviewee with written instructions, such a requirement might be found in a company's internal rules.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

There is no legal obligation to inform an interviewee about the right against self-incrimination during an internal interview. During a criminal interrogation, however, prosecutors must inform the individual of their right to remain silent.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

Although there is no legal obligation to provide an Upjohn warning, it is regarded as good practice to do so and may even be required by the employer's internal rules.

d) be informed of their right to have their own lawyer attend the interview?

There is no such obligation. The internal rules of the employer should also be consulted in this regard, as they may not allow third parties to attend interviews, including counsel for the interviewee.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Employees do not have the right to have trade union representatives attend their interviews.

f) be informed that data may be transferred to another country (in particular to the United States)?

Above all, the GDPR restricts transfers of personal data outside the European Economic Area, unless the rights of the individuals in respect of their personal data are protected in another way, or one of a limited number of exceptions in the legislation applies. Therefore, without the consent of the interviewee, the employer shall generally not transfer personal data cross-border. In addition, the PDPA requires employers to inform the Bulgarian Commission on Personal Data Protection when personal data collected during investigations is intended to be transferred to a non-EU member state.

g) sign a data privacy waiver?

Employers must receive written, informed consent in order to process personal data.

h) be informed that the information gathered might be passed on to authorities?

The interviewee must be informed that the information might be passed on to authorities, especially when it contains personal data. Reporting persons shall also be informed beforehand if the report is to be forwarded to the CPDP. Nevertheless, information on the processing of personal data may be withheld by the controller from the data subject to avoid prejudicing the prevention, detection, investigation, or prosecution of criminal offences or the execution of criminal penalties.

i) be informed that written notes will be taken?

There is no legal obligation to inform the interviewee that notes will be taken during the interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no law pertaining to the use of document hold or retention notices in Bulgaria. Employers must be careful not to retain certain documents in violation of the law. For example, retaining working files of a former employee may, under certain circumstances, be unlawful and could result in civil liability for the employer. Pursuant to the GDPR and the PDPA, processing of personal data outside its legitimate purpose is forbidden, and the personal data should be deleted once the legitimate purpose for which it was collected is fulfilled. Therefore, employers should limit the processing of personal data and not keep personal data once the processing purpose is completed. On the other hand, employers are might retain certain administrative documents, such as payroll files, even after the end of an employment relationship.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege is provided for in the Bulgarian Bar Act ("**BA**"). According to Article 33 of the BA, correspondence and conversations between a lawyer and a client are confidential. Attorney papers, files, electronic documents, computer equipment, and other carriers of information may not be subject to inspection, copying, verification, or seizure. The scope of protection is broad in order to guarantee the protection of privileged information. An internal investigation report would fall under the attorney-client privilege, as it is considered information exchanged in the course of an attorney-client relationship. The best way to ensure the applicability of attorney-client privilege is to engage outside counsel.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Communication with an in-house lawyer is not considered privileged under Bulgarian law. However, in-house counsel, as a regular employee of the company, should handle correspondence according to the internal rules of the company.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Pursuant to the Bulgarian Insurance Code, the insured entity is obliged to declare to the insurer all new circumstances, which the insurer has raised to the company at the conclusion of the contract. New circumstances must be revealed to the insurance company immediately after they are known. Early notification to the insurance company may be a subject of the terms and conditions of the insurance policy.

b) Business partners (e.g. banks and creditors)?

Early notification requirements may stem from contractual clauses. In addition, it is generally advisable to provide such notification to avoid future complication. It is common practice for banks to oblige borrowers to notify them in case of an adverse event which may harm the interests of the bank.

c) Shareholders?

If an internal investigation may affect the stock market price of a publicly traded company, this information must be disclosed in accordance with Bulgarian law and the disclosure requirements of Regulation (EU) No. 596/2014 on market abuse. However, the volume of the disclosed information shall be evaluated on a case-by-case basis, considering the imperative rules for trading with inside information and market manipulation (market abuse).

d) Authorities?

Prosecution authorities should be notified about any criminal offence that is discovered during an investigation, and the CPDP shall be informed in the event further action is required by any of the entities described in the Whistleblower Act. However, no general early notification at the start of an internal investigation is necessary.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Under the Whistleblower Act the person of the obliged entity responsible for handling the reports, shall take actions within its competence to terminate the breach or to prevent it, in accordance with the report and in case multiple reports were received, prioritise those regarding more serious breaches, following predetermined criteria and rules.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Under the Whistleblower Act, the report and the materials related to an investigation shall be immediately transmitted to the prosecutor office whenever the internal investigation uncovered that there are grounds to believe that a criminal offence was committed.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Search warrants or seizure warrants are strictly regulated in Bulgarian law. A search or seizure may only be conducted where there is sufficient reason to believe that information significant to the prosecutors' investigation may be found.

A valid warrant must be in writing, signed by a judge, and contain the necessary material requirements. The individual subject to the search or seizure or, in the case of legal persons, a representative thereof, must be present during the search or seizure. Where no representative of a legal person can be present, the search and seizure may be carried out in the presence of a representative of the municipality.

In urgent cases, authorities may perform a search without prior judicial authorisation, should it be necessary to preserve evidence. However, in this case, a report documenting the investigative actions taken must be made and submitted for approval to a judge no later than 24 hours after the search or seizure.

Improperly gathered evidence may not be used against the company. Only evidence collected lawfully, as provided under the CPC, may be used in criminal proceedings.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Corporations are not subject to criminal liability under Bulgarian law. Thus, they cannot be subject to deals and non-prosecution agreements.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Companies are not subject to criminal liability, but may be subject to administrative sanctions, such as fines. Should the activities of a company be regulated by the state, the regulatory authority may suspend or revoke the company's licence.

Individuals may be subject to the general criminal and administrative penalties for misconduct.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

The Bulgarian Whistleblower Act and related legislation do not provide any reduction of penalties for companies that have implemented the required internal reporting system.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

As of date no concrete legislative actions have been taken in Bulgaria in relation to ESG requirements. No bills or draft bills have been published regarding the transposition of Directive (EU) 2022/2464 – the Corporate Sustainability Reporting Directive.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Due to the lack of a centralised government agency that tracks whistleblower cases, the number of investigations and their outcome is not known. Many reports are made anonymously and sent to individual authorities. According to a European University Institute report, Transparency International Bulgaria's Advocacy and Legal Advice Centre, a non-governmental organisation providing free and confidential legal advice to witnesses and victims of corruption, has, thus far, received very few complaints from employees or civil servants reporting illegal activities or wrongdoing by their employers. Several whistleblowers accused of criminal defamation have been acquitted by the court, for instance, individuals who disclosed mismanagement of municipal property and reported concerns in a police agency.

The public consultations regarding the contemplated transposing Act of the Whistleblower Directive, as discussed under question 1, point to some developments that might be expected in the upcoming legislation. A predominant portion of opinions by interested parties includes a suggestion for the acceptance of anonymous reports, something not available under current legislation. Additionally, the Supreme Bar Council has submitted a suggestion for the inclusion of violations of national law in addition to EU law to the material scope of the transposing Act. However, the opinions lack consensus as to which administrative body should be responsible for monitoring compliance with the new rules, as well as whether to limit the scope of the Act to enterprises with more than 50 employees, or to seek universal applicability. Considering that the Bulgarian Whistleblower Act entered into force only in May 2023 for large companies and per December 2023 for all obliged entities, there is no aggregated data available on its effectiveness and actual impact on internal reporting standards. It is likely that some data on its initial efficacy will be available in the CPDP's annual activity report that is usually published during the second quarter of the following year.

CONTACTS

KAMBOUROV & PARTNERS

ATTORNEYS AT LAW

37 A Fridtjof Nansen St.
1142 Sofia
Bulgaria

Tel.: +359 2 986 9999
Fax: +359 2 986 9995
www.kambourov.biz

Kambourov & Partners is a leading Bulgarian law firm with 30 years of experience. It is specialised in general business law and provides services under Bulgarian jurisdiction to domestic and international clients within various practice areas including Banking, Finance, Corporate, Employment, Competition, IP, TMT, Litigation & Arbitration, Restructuring & Insolvency, Real Estate, Tax, Energy, White Collar, Regulatory & Compliance, etc.

Ivo Alexandrov
Partner
Kambourov & Partners
T +359 2 986 9999
E i.alexandrov@kambourov.biz

Ivo Alexandrov heads Kambourov & Partners' Regulatory & Compliance department, the Restructuring & Enforcement of Securities department and is a key member of the Banking & Finance and Corporate practices. Ivo represents local and international companies with respect to corporate crime investigations as well as financial institutions, investment and hedge funds, project sponsors, etc., in a multitude of transactions, e.g. large syndicated financings, cross-border finance, transactions escrow of shares and financial instruments, enforcement of netting arrangements, custodian and escrow arrangements of financial instruments. He advises clients from a wide range of industries, including finance, banking, insurance, retail on complex domestic and EU regulatory requirements and is experienced in all areas of business and financial services regulation, as well in cross-border M&As, foreign investments, project finance, regulatory issues (public, commercial, economic, environmental, etc.).

Zlatko Grigorov
Associate
Kambourov & Partners
T +359 2 986 9999
E grigorov@kambourov.biz

Zlatko Grigorov is a key member of Kambourov & Partners' Regulatory & Compliance department and Banking & Finance practice. Zlatko advises on a wide range of regulatory laws, from both a Bulgarian and EU law perspective, including in relation to continued compliance with applicable legislation, licensing requirements, and obligations placed on product and service providers in a number of key industries, including financial and payment services, banking, insurance, and technology.

Croatia

Babić & Partners Law Firm LLC


Iva Basarić


Lovro Klepac

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	
No					X*

* No specific defence, but greater likelihood of liability for failure to implement anti-corruption programmes.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Under the Croatian Whistleblower Protection Act, an employer is required to establish channels and procedures for internal reporting of irregularities. The Whistleblower Protection Act sets out specific procedures that need to be observed in case a whistleblower report triggers an internal investigation, such as an obligation to (i) examine the whistleblower report and to provide feedback about the report; (ii) notify the whistleblower of the outcome of the internal investigation; (iii) notify the competent authorities of the received whistleblower report, if the irregularity has not been resolved with the employer; (iv) undertake actions necessary to protect the whistleblower and to protect confidentiality of information included in the report, as well as information on whistleblower's identity; (v) notify authorities competent for external reporting about the received report and outcome of the investigation; and (vi) provide clear and easily accessible information regarding the procedures for reporting externally to competent authorities and, where relevant, to institutions, bodies, offices or agencies of the European Union.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Provisions of the Whistleblower Protection Act implementing Article 8(3) of the EU Whistleblower Directive, provide that the entity (employer) that employs 50 or more employees is required to establish an internal reporting system. In this regard, and in light of the interpretation issued by the European Commission in the summer of 2021, the Whistleblower Protection Act does not allow the use of group wide reporting systems.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) The employer must obtain the consent of the works council prior to collecting, processing, or delivering the personal data of employees to third parties. Since internal investigations typically involve collecting and processing personal data and possibly delivering such data to third parties, employers practically cannot initiate such investigations without the prior consent of the works council. In addition, if appointed by the employer, union representatives generally also need to be informed of investigations concerning employees, who are members of the union.

b) Under Croatian data protection legislation, one of the duties of the data protection officer is to ensure that employees' rights with respect to personal data processing are observed. In this regard, it would be advisable to inform the data protection officer of the investigation and to provide the data protection officer with any information requested.

c) There is no legal requirement to inform the prosecution authorities of an internal investigation unless the company has sufficient information to qualify the investigated misconduct as a criminal deed.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees have a general duty to cooperate in an investigation by providing information that directly relates to their work. Violation of this duty may qualify as a breach of employment duties, especially if it leads to economic loss for the employer. Depending on the severity of the breach, non-compliance with an employer's request to support an investigation may result in the termination of the employee's contract. Company policies may provide more detailed rules governing employee duties and sanctions for violating such duties.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

An investigative measure may be to set a 15-day deadline for summary dismissal for cause, in cases where the investigation uncovers gross misconduct of the employee. The deadline is triggered when the employer (i.e. a representative with authority to dismiss) becomes aware of the facts or circumstances reasonably leading to the conclusion that misconduct has been committed. To avoid triggering this deadline too early, the employer should be informed of the results of the investigation at a later stage, after comprehensive information has been gathered.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Before conducting interviews, in accordance with the transparency obligations set out in Croatian data protection laws, the employee must be informed of the purpose for which their personal data is collected and processed. Interviews should be limited to questions about work-related issues.

b) reviewing emails?

Employees' electronic communications may be monitored only in extraordinary circumstances when the following prerequisites are met: (1) the processed data may only be collected to satisfy the specific purpose of

such surveillance and cannot be used for any other purpose; (2) the possibility of electronic communication surveillance must be transparently communicated to the employees (e.g. by way of company policies); (3) there must be a legitimate purpose for monitoring; and (4) a proportionality test must be met, i.e. the surveillance should generally be limited to data traffic and not include content which may only be monitored if absolutely necessary. The abovementioned principles also apply under Regulation (EU) 2016/679 ("**GDPR**"). In addition, such processing would be subject to a data protection impact assessment ("**DPIA**") obligation in accordance with Article 35 of the GDPR and the review of the list of kinds of processing operations that are subject to the DPIA adopted by the Croatian Data Protection Agency.

c) collecting (electronic) documents and/or other information?

Although communication with authorities can trigger the applicability of data protection laws, a request from an authority will often be sufficient justification for collecting and using data to comply with the legal obligation to which the controller is subject.

d) analysing accounting and/or other business databases?

A company is generally free to analyse any accounting and other mere business databases.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

Croatian law does not provide for an express obligation on the employer to deliver written instructions to the employee before starting an interview. However, employees should always be timely informed about the processing of their personal data as required by GDPR transparency obligations. As a best practice, it is advisable to provide the employee with general information about the investigation and to document this in writing.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

In contrast to investigations initiated by the prosecution authorities, there is no right to remain silent during an internal investigation conducted by a company. However, the employer should avoid putting any pressure on the employee to self-incriminate in order to mitigate potential future duress claims by the employee.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no duty under Croatian law to provide an "Upjohn warning" to the interviewee, though it is advisable to do so.

d) be informed of their right to have their own lawyer attend the interview?

Croatian law does not expressly provide that an interviewee has a right to have an attorney present at their interview. However, if the employee requests to have their attorney present, it is advisable to allow it.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Under the default rules of Croatian labour law, employees do not have a right to have a works council representative present at their interviews. Company policies and collective agreements, if any, should be consulted in order to assess whether such rights are provided therein. In any case, it is advisable to allow the attendance of a member of the works council or other representative body upon employee request.

f) be informed that data may be transferred to another country (in particular to the United States)?

Transferring data to non-EU states or organisations is only permissible if compliant with Chapter V of the GDPR, i.e. if it is based on an adequacy decision, appropriate safeguards, etc. With respect to the United States, pursuant to the Commission Implementing Decision of 10 July 2023 on the adequate level of protection of personal data under the EU-US Data Privacy Framework, transfers to organisations included in

the Data Privacy Framework List would comply with Article 45 of the GDPR. Furthermore, employees must be informed about the transfer in accordance with GDPR transparency obligations.

g) sign a data privacy waiver?

The interviewee does not need to sign a data privacy waiver before conducting the interview. This is because the employee's consent would not be required for processing of the employee's data obtained during the interview or otherwise in the course of internal investigation. However, the employee should be informed of the processing of their data in accordance with the GDPR transparency obligations.

h) be informed that the information gathered might be passed on to authorities?

The data subject should be informed about the recipients of their personal data, including authorities. If the information is not obtained directly from the data subject, the controller may be exempted from the obligation to inform the data subject if the obligation to pass on information to authorities is expressly regulated by law. If an interview yields evidence of a crime investigated by the prosecution authorities, the employer must pass on such information and evidence to the authorities and does not need to inform the employee (1) that there is a duty to deliver such information to authorities; nor (2) that the information will be passed on to prosecution bodies. Processing of such data is expressly mandated by the rules of criminal procedure.

i) be informed that written notes will be taken?

There is no obligation under Croatian law to inform the interviewee that notes of the conversation will be taken. It is, nevertheless, advisable to inform the employee and to ask the employee to co-sign the notes, as confirmation of their accuracy, in case any litigation is subsequently initiated. Furthermore, if the interview notes are stored by the employer, employee should be informed about such storage and applicable retention period.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Croatian law does not address document hold or retention notices. However, the rules of criminal procedure provide for a general duty of any legal entity reporting a crime to preserve existing traces or evidence of a committed offence. In addition, special procedural rules exist to secure evidence in civil litigation. An application may be filed by any of the parties before or during (civil) litigation proceedings if justified doubt exists that certain events would hinder the examination of evidence at a later stage of the proceedings. If such an application is filed before the proceedings are initiated, the evidence shall be examined by the competent court in the territory where the evidence is located.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege may generally only be claimed with respect to correspondence with outside counsel and documents in the possession of outside counsel. In order to be considered privileged, internal investigations, including interviews, should be conducted by/through outside counsel.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Under Croatian law, attorney-client privilege does not extend to in-house counsel.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Generally, early notification to insurance companies will be required where circumstances are uncovered that may form the basis for an insurance claim. However, notification obligations depend on the agreement and the type of insurance.

b) Business partners (e.g. banks and creditors)?

The company may be required to inform its business partners of internal investigations and related findings, if required by the agreements with the respective partners. The company may also be required by the good faith principle to inform its business partners of an investigation, if the investigation and its consequences may have significant impact on the business partners. This should be assessed on a case-by-case basis, balancing the opposing interests.

c) Shareholders?

Depending on the information and/or misconduct uncovered and any provisions to this effect in the company's internal policies, the management board may be obligated to notify shareholders. However, the management board has rather broad discretionary power in assessing whether to notify shareholders or maintain confidentiality.

According to Croatian securities trading legislation, if the information gathered by an internal investigation is of a precise nature and would probably significantly influence the price of financial instruments issued by the company, it is the duty of the management board to report such information to the public.

d) Authorities?

There is no general duty to notify the State Attorney's Office or any other authority of an ongoing internal investigation. However, every person is obliged to report criminal activities. In some instances, such as for company directors or officers, violation of this duty may result in criminal prosecution.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Depending on the nature and severity of the alleged wrongful conduct, the company should strive to mitigate any further damage. Subject to the company's code of conduct and other policies, employees may be sanctioned for uncovered misconduct. In addition to sanctioning employees, the company should re-evaluate and improve its compliance system.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices do not generally have concerns about internal investigations conducted by companies. Documents gathered during a corporate internal investigation may be used in subsequent proceedings initiated by the local prosecutor. Therefore, the company should ensure retention of documents and any information that may be requested by the prosecutors later.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

A dawn raid may be undertaken when it is probable that a person who committed a criminal deed and the object of a criminal offence or traces of evidence can be found in particular spaces. Dawn raids conducted by the Croatian competition regulator must be approved in advance by the High Administrative Court. Warrants required to conduct a dawn raid are governed by the Croatian Competition Act and subject to special rules.

The court must render a decision within two days of the regulator's request. The warrant, which is issued by the High Administrative Court, must identify the object(s) of the search, the legal basis for the raid, the person(s) authorised to conduct the raid and the deadline for execution of the warrant. The warrant must be presented to the owner or operator of the premises on which the dawn raid is conducted. Authorised officials conducting the dawn raid may: inspect the entire premises; inspect and copy business records and other documents; and seal the premises, business records, or other documentation as long as necessary for conducting the raid. Based on amendments to the Croatian Competition Act implementing ECN+ Directive (Directive 2019/1), the exertion of the rights mentioned above must be proportionate and should not compel a person or undertaking to admit infringement of Croatian competition laws.

Search warrants must be issued by a competent court unless an immediate search is necessary to preserve evidence directly related to a crime that is in danger of being lost or destroyed. A search warrant must identify the object of the search and its purpose and name the authority conducting the search. A search warrant must be issued in writing and signed by a judge. The search must be conducted within three days of issuance of the warrant. The warrant must be presented to the person whose premises are to be searched, and the search must be witnessed by at least two persons of legal age. An authorised representative of the company must be informed of their right to attend the search. Failure to inform is a violation of criminal procedure but would not lead to the inadmissibility of evidence uncovered during the search.

Not every procedural infringement during a search will lead to the evidence collected being deemed inadmissible. Croatian criminal law and Supreme Court practice both recognise that only serious procedural violations may lead to a finding of inadmissibility in criminal proceedings. Specifically, only evidence gathered during a search undertaken without a warrant or without the required witnesses may be excluded from criminal proceedings.

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Deals, non-prosecution agreements, and deferred prosecution agreements are available and encouraged in Croatian criminal law and the practice of the State Attorney's Office. For a non-prosecution agreement or deferred prosecution agreement to be implemented, several substantive and procedural requirements must be met. First, the penalty prescribed for that particular offence cannot be more than five years' imprisonment. Second, the suspect or the accused must undertake either to compensate the injured person for damages suffered by the crime, donate to humanitarian or social causes, or participate in community service. If the suspect or accused satisfies the requirements within one year, the State Attorney must dismiss the criminal charge.

Plea bargains are also available under Croatian criminal procedural law. The accused and the State Attorney may negotiate the conditions of the plea and the subsequent sanctions. During such negotiations, the accused must be represented by an attorney. The deal negotiated between the accused and the State Attorney must be executed in writing, signed by both parties, and confirmed by the competent criminal court. Criminal procedural rules concerning the content of such deals must also be observed.

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Under Croatian law, companies and other legal entities may be subject to criminal liability for the criminal conduct of officers and directors. Companies that are found liable are subject to monetary fines, dissolution, and associated protective measures, such as operating bans, disgorgement of profits, exclusion from public tenders, and exclusion from obtaining licences, permits, and concessions. Administrative or misdemeanour fines may be imposed for less serious violations.

A company's directors and officers may be held liable for failing to report misconduct of other directors, officers, or employees and may face up to three years' imprisonment.

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Croatian laws do not expressly determine efficient compliance systems as mitigating factors in determining penalties. However, in practice, efficient compliance systems (whether implemented prior or following the alleged misconduct) may be argued as a mitigating factor with the intention of the courts/authorities reducing the fines to be imposed (especially in competition law cases).

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Based on the Croatian Accounting Act, implementing Directive 2014/95/EU, large entities which are public-interest entities on average having more than 500 employees during a financial year, must include in their management report a non-financial statement containing information relating to environmental, social and employment matters, respect for human rights, anti-corruption and bribery matters. The Croatian Ministry of Finance is authorised to supervise and enforce the provisions on non-financial reporting above, and has previously published a list of entities that did not meet the above requirements in years 2017 and 2018. Additional ESG requirements apply for sectors such as banking and investment services, as well as to companies whose shares are listed on the Zagreb Stock Exchange. There is no publicly available data on the number or frequency of enforcement proceedings related to ESG cases.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

In 2023 the Croatian Act on Criminal Liability of Legal Entities was amended to extend the scope of corporate criminal liability and to increase the level of fines which may be imposed on legal entities for criminal offences. Following these amendments, the maximum level of fines for criminal offences of legal entities has been increased from €1.9 million to maximum €25 million, or in specific cases up to 10 percent of an entity's total annual turnover achieved in the year preceding the judgement in criminal proceedings.

CONTACTS

BABIĆ & PARTNERS
LAW FIRM

Nova cesta 60/ 1st floor
10000 Zagreb
Croatia

Tel.: +385 1 3821 124
Fax: +385 1 3820 451
www.babic-partners.hr

Iva Basarić
Partner
Babić & Partners
T +385 1 3821 124
E iva.basaric@babic-partners.hr

Iva Basarić is a Partner at Babić & Partners. Iva earned an LL.M. degree in International Transactions and Comparative Law at the University of San Francisco, U.S. She regularly advises clients from diverse industries on various corporate/commercial, regulatory and data privacy issues. Iva has vast experience in assisting international clients with all aspects of internal investigations conducted in their Croatian subsidiaries. In 2006/2007 Iva participated in the Willem C. Vis international Commercial Arbitration Moot, as a member of the University of Zagreb moot team, which was awarded second place in the oral rounds of the competition.

Lovro Klepac
Senior Associate
Babić & Partners
T +385 1 3821 124
E lovro.klepac@babic-partners.hr

Lovro Klepac is a Senior Associate and member of employment law group at Babić & Partners. After graduating from the University of Zagreb, Faculty of Law, he earned an LL.M. degree in International Business Law at the Central European University in Budapest. Lovro's practice comprises all aspects of the firm's employment law practice, including advising on data privacy issues and employee investigations. He was a member of the University of Zagreb moot team at the Willem C. Vis international Commercial Arbitration Moot that was awarded honourable mention for Memorandum for Respondent in 2015/2016.

Cyprus

Chrysses Demetriades & Co LLC

Demetris L. Araouzos

Sophia Nearchou

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X*	X
No					

* Depending on the type of offence.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

On 4 February 2022, the Protection of Persons Reporting Breaches of Union and National Law of 2022 ("**Whistleblower Law**") was published in the Official Gazette, implementing the EU Whistleblower Directive into Cyprus law.

The Whistleblower Law provides protection of persons who report acts or omissions relating to the potential commission of a criminal offence. These include, in particular, corruption offences, acts or omissions related to non-compliance with legal obligations imposed on a person, infringements that endanger or are likely to endanger the safety or health of a person, and infringements that cause damage to the environment.

The Whistleblower Law applies to civil servants, employees, self-employed persons, shareholders, and persons belonging to the administrative, management, or supervisory body of a company, for example, non-executive members, volunteers, and trainees.

The Whistleblower Law requires, among other things, that any processing of personal data shall be carried out according to the EU General Data Protection Regulation ("**GDPR**"). It also highlights that entities are prohibited to retaliate against whistleblowers in any way.

As a general principle, under Article 7 of the Whistleblower Law, breaches may be reported through the internal reporting channels. Further, it is encouraged that reporting through internal reporting channels is done before reporting through external reporting channels. A potential breach can then be addressed effectively and without risk of retaliation for the whistleblower.

Appropriate information relating to the use of internal reporting channels shall be provided in the context of the information provided by legal entities in the private and public sectors.

The procedures for internal reporting and follow-up shall include the following:

a) Channels for receiving the reports that are designed, established, and operated in a secure manner that ensures the confidentiality of the identity of the reporting person and any third party mentioned in the report and prevents access thereto by non-authorised staff members;
b) Acknowledgement of receipt of the report to the reporting person within seven days of that receipt;
c) The designation of an impartial person or department competent for following up on the reports; this may be the same person or department as the one that receives the reports and which will maintain communication with the reporting person and, where necessary, ask for further information from and provide feedback to that reporting person;
d) Diligent follow-up by the designated person or department referred to in point (c).

The channels provided for in point (a) shall enable reporting in writing or orally, or both. Oral reporting shall be possible by telephone or through other voice messaging systems and, upon request by the reporting person, through a physical meeting within a reasonable timeframe.

The Whistleblower Law generally protects against retaliation. This includes any direct or indirect act or omission that occurs in a work-related context, prompted by internal or external reporting or public disclosure, and which causes or may cause unjustified detriment to the reporting person. Witnesses involved in proceedings related to a report will be subject to protection afforded under the applicable witness protection legislation.

Employers are obliged to protect employees from acts of their superiors or any other employee which constitutes retaliation for reporting. A reporting person's dismissal from employment, any detrimental change to their working conditions, or any retaliation measure will be deemed invalid unless the employer proves that such dismissal was based on other grounds.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The Whistleblower Law generally requires private companies with 50 to 249 employees to introduce internal reporting channels by 17 December 2023. The same obligation applies to public companies. The Whistleblower Law encourages companies with less than 50 employees to nevertheless introduce internal channels voluntarily, provided that the internal channels are distinct and autonomous from the external reporting channels. It also encourages private companies that do not meet the threshold of mandatory reporting mechanisms to appoint a specific person within the company who is responsible for the receipt and follow-up of the report.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Although employee representative bodies do not have a legal right to be informed of the start of an investigation, it is considered a best practice to allow an employee to have a union representative attend their interview, if the employee requests such attendance.

b) The Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and the Free Movement of such Data of 2018 (Law 125(I)/2018) ("**PDPL**") applies as of 25 May 2018. The PDPL was adopted for the effective implementation of certain provisions of the Regulation (EE) 2016/679 of the European Parliament and of the Council of 27 April 2016 and repeals Directive 95/46/EC (GDPR). It

regulates the duties of a Data Protection Officer ("**DPO**") to monitor compliance. In particular, the DPO may collect information to identify processing activities, analyse and check the compliance of processing activities, and inform, advise, and issue recommendations to the controller or the processor. Hence, the DPO should be notified before starting an internal investigation, which will require the collection and processing of personal data. A company conducting an internal investigation must also inform the DPO of all processing activities being conducted for the investigation.

c) No other local authority needs to be informed of an internal investigation, other than the regulators (if necessary) and/or the prosecution authorities, who must be notified if criminal conduct is uncovered during the investigation. The Public Service Law and the Code of Ethics of the Public Services oblige civil servants to report suspected cases of corruption or bribery to their respective authority. Failure to do so constitutes an offence.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Cyprus law does not refer to the employee's duty to support an investigation.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

No reference to the initiation or waiver of labour law deadlines is made in the Employment Termination Law of 1967.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The PDPL applies to any processing of personal data, including the gathering or recording of such data in an interview. Before personal data may undergo any processing, the data subject must be informed who is collecting the data, for what purpose, and with whom the data is to be shared. The consent of the data subject must also be obtained. Consent must be freely given.

b) reviewing emails?

According to the PDPL, personal data, such as emails, may only be collected and processed when: (1) the data subject has given explicit consent; (2) the processing is necessary for the data controller to fulfil its obligations or to perform its duties; and (3) the Data Protection Commissioner, the data protection authority in Cyprus, has authorised the collection, where data will be transferred outside of the European Union.

c) collecting (electronic) documents and/or other information?

The PDPL must be observed not only with respect to emails but to all documents and information containing personal data.

d) analysing accounting and/or other business databases?

Analysing mere business databases does not fall under the definition of personal data processing. Therefore, the provisions of the law regarding the right to be informed do not apply.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no statutory obligation to give written instructions to an employee before an interview. However, the employee must be given advance notice that an interview may occur.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Only when an individual is interviewed by criminal authorities, they have the right to remain silent.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no obligation under Cyprus law to provide an "Upjohn warning".

d) be informed of their right to have their own lawyer attend the interview?

Parliament is currently debating a bill that would provide an individual with the right to request the presence of their lawyer during questioning by police and/or prosecutors. Currently, no such right exists. The bill does not apply to internal investigations.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

It is considered a best practice to allow an employee to have a union representative attend their interview if the employee requests such attendance. However, the employee does not have a legal right to have the representative attend.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

The PDPL requires that the data subject be informed of data transfers, as the data subject's consent is required. If the data is to be processed for any purpose other than for which it was originally obtained, the data subject must again be informed. According to the PDPL, the cross-border transmission of data must be authorised by the Data Protection Commissioner. The Data Protection Commissioner will typically only authorise a transfer to another country if the country to which the data will be sent provides an adequate level of protection.

g) sign a data privacy waiver?

Under the PDPL, a waiver may be required if the personal data of the employee may be used for a purpose other than the original purpose given for the collection or may be given to third parties. The employee must be informed of the purpose and give their consent.

h) be informed that the information gathered might be passed on to authorities?

There is currently no legal obligation under the PDPL to inform an employee that information gathered during the interview may be passed on to authorities. However, under the GDPR, the data subject must be informed of why their data is being collected and how it will be processed. The data subject must also be informed if their data will be transmitted to a third party, including authorities.

i) be informed that written notes will be taken?

There is no legal obligation under Cyprus Law to inform the employee that written notes will be taken, but it is common practice to do so.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific provision in the law on whether document holds or retention notices are allowed. As internal investigations are not yet common in Cyprus, such notices are also not customary.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The Legal Professional Privilege derives from the Advocates' Law (Cap. 2) and the Advocates' Code of Conduct 2002 (the "**Regulations**"). According to the Regulations and as a general rule, communications and dealings of advocates with their clients are protected by the Legal Professional Privilege. The advocate is under a duty to keep strictly confidential information derived from communication with the client once the advocate-client relationship has been established. However, the privilege only extends to legal communications, i.e. communications seeking/obtaining legal services or advice. As internal investigations are not yet common in Cyprus, it is unclear whether the Legal Professional Privilege would apply to them. The privilege does apply in criminal and regulatory investigations by authorities.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Legal Professional Privilege also applies to in-house counsel in Cyprus, provided that in-house counsel is admitted to the Cyprus Bar.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Early notification requirements may stem from individual insurance policies, but there is no statutory notification obligation.

b) Business partners (e.g. banks and creditors)?

Notification to business partners is only necessary if the agreement between the partners and the company is required.

c) Shareholders?

A shareholders' agreement may provide an early notification requirement. Otherwise, if a company's shares are publicly traded, it has to inform the public about information that could affect the stock price. However, a company is not required to provide notification at the start of an investigation.

d) Authorities?

Generally, there is no obligation to inform authorities about internal investigations within a company. The obligation may arise if a criminal offence is involved.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

There is no law in Cyprus concerning the need to take immediate measures. Best practices, however, would mean that any criminal conduct is stopped immediately. Mitigation measures may include the dismissal of wrongdoers and the protection of whistleblowers against unfair dismissal or other punishment.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Generally prosecutors play no role in internal investigations. However, prosecutors may become involved if the company notifies them that an internal investigation is ongoing and their involvement is deemed necessary.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Certain prerequisites must be fulfilled for searches and dawn raids of companies in Cyprus.

According to Section 27 of the Criminal Procedure Law, a judge can issue a search warrant on the basis of a sworn statement that there are reasonable grounds to believe that evidence, which may be used as proof of the commission of an offence, will be found. The search warrant authorises the person named in the sworn statement to enter the premises and seize such evidence.

Various regulatory authorities, including CySEC and the Competition Commission, as well as government agencies, such as tax authorities, have the right to enter and seize evidence for their administrative purposes without warrants (dawn raids).

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Cyprus law has no provisions regarding plea agreements, settlement agreements, prosecutorial discretion or similar means without trial.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Depending on the type of criminal offence, a company may be fined and its directors, officers, and employees imprisoned and/or fined.

For administrative violations, regulatory authorities may, among other things, impose administrative fines, suspend professional licences, order disgorgement of profits earned through wrongful conduct, and/or ban individuals from discharging managerial responsibilities.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Compliance systems are audited and evaluated through on-site inspections by relevant authorities in each sector. Investigation powers are generally vested in the following authorities:

- Central Bank of Cyprus;
- Cyprus Securities and Exchange Commission;
- Superintendent of Insurance;
- Cyprus Bar Association;
- Institute of Certified Public Accountants;
- Unit for Combating Money Laundering (MOKAS).

If deficiencies are found in an entity's compliance systems, recommendation for corrections are made before penalties are imposed. For more severe deficiencies, a penalty may be imposed without warning.

There is no statutory defence on compliance systems. However, a court may consider compliance systems as a mitigating factor in case of conviction.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Cyprus has not yet adopted national legislation to implement the EU Directive 2022/2464 on corporate sustainability reporting.

However, Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment (the "EU Taxonomy Regulation") applies directly in Cyprus.

In addition, Article 3 of the EU Taxonomy Regulation sets out four conditions which an economic activity must satisfy to qualify as environmentally sustainable:

"*(a) contributes substantially to one or more of the environmental objectives set out in Article 9 in accordance with Articles 10 to 16;*

(b) does not significantly harm any of the environmental objectives set out in Article 9 in accordance with Article 17;

(c) is carried out in compliance with the minimum safeguards laid down in Article 18; and

(d) complies with technical screening criteria that have been established by the Commission in accordance with Article 10(3), 11(3), 12(2), 13(2), 14(2) or 15(2)."

Further, Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability - related disclosures in the financial services sector - is also directly applicable in Cyprus.

Regarding enforcement, even though various competent authorities such as the Central Bank of Cyprus, the Cyprus Securities and Exchange Commission, as well as government bodies and agencies, have expressed their commitment to ESG, we are not aware of any examples of actions taken against companies for violating relevant EU Regulations.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The newly-passed Whistleblower Law provides the protection of persons who report acts or omissions related to possible criminal offences, non-compliance of a person with their legal obligations, violations that endanger the safety or health of any person, or that cause or are likely to cause damage to the environment.

Representatives from all parliamentary parties welcomed the new Whistleblower Law, stressing it would greatly help in the effort to stamp out corruption. The Whistleblower Law is also expected to enhance transparency and address possible cases of corruption. However, since this is a new development in Cyprus, no case law exists on the Whistleblower Law.

The government expects that the Parliament will soon proceed with adopting other important bills concerning the reform of the Judiciary and the establishment of the Independent Authority against Corruption. This underlines that "these are important reforms that will contribute decisively to the fight against corruption and the promotion of transparency and accountability, consolidating the rule of law in our country".

CONTACTS

CHRYSSES DEMETRIADES & CO LLC

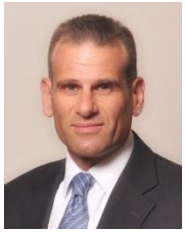
13 Karaiskakis Street
3032 Limassol
Cyprus

Tel.: +357 25 800 000
Fax: +357 25 588 055
www.demetriades.com

Established in 1948 – Chrysses Demetriades has always been instrumental to the development of Cyprus as an offshore and international financial centre. Widely acknowledged and consistently ranked as one of the leading law firms in Cyprus by the independent legal directories the Legal 500, Chambers and Law Firm Directory.

Chrysses Demetriades & Co. LLC is a Cyprus law firm providing a comprehensive range of legal services to local and international clients. We have long established relationships with many of the world's leading international financial institutions, professional advisers, and regulatory bodies, are consistently highly rated in independent research studies and regularly lead offshore league tables. Our success is founded on our ability to provide practical, creative, and cost-effective advice, combined with an uncompromising service commitment to our clients and a strong dedication to our lawyers, staff, and the communities in which we practice. We have been instrumental to the development of Cyprus as an offshore and international financial centre and are widely acknowledged as one of the leading law firms in Cyprus in the key areas of corporate activity:

- Banking & Finance
- Capital Markets
- Corporate and M&A
- Employment
- EU & Competition
- Intellectual Property
- Private Client
- Property
- Regulatory Compliance
- Shipping
- Tax
- Litigation & Dispute Resolution



Demetris L. Araouzos
Partner
Chrysses Demetriades & Co. LLC
T +357 25 800 000
E demetris.araouzos@demetriades.com

Demetris has extensive experience, *inter alia*, in commercial/corporate contentious matters that often involve large and well-known local or international groups or wealthy individuals, the proceedings of which invariably have to take place in multiple jurisdictions. Amidst the banking crisis in Cyprus in 2012-2013 and the collapse of one of the two major banks, Demetris was instructed to advise and bring proceedings on behalf of a failing bank against some of its ex-directors. He was also appointed by the Government of Cyprus as member of the legal team that defends Cyprus in ongoing ICSID proceedings that have been brought against it by certain Greek shareholders with substantial participation in the failing bank. He is occasionally retained to act for listed companies and their directors/officers on various regulatory issues and, as he invariably undertakes criminal work, he has been retained to defend ex-directors and senior officers of the largest Cyprus bank in market abuse criminal cases. Although Demetris spends most of his time before the Courts, he is often engaged in the negotiation and drafting of different types of agreements.

Sophia Nearchou

Associate
Chrysses Demetriades & Co. LLC
T +357 25 800 000
E sophia.nearchou@demetriades.com

Sophia is a Senior Associate and the Anti Money Laundering Compliance Officer of CHRYSSES DEMETRIADES & CO LLC.

She has extensive experience in dealing with Anti Money Laundering & regulatory compliance matters and one of her main responsibilities is keeping the firm's function in line with all relevant laws and regulatory requirements .

During the course of her employment she has also gained extensive experience, particularly in cases relating to various sanctions and other restrictive measure regimes, both domestic and international, as promulgated by the UN, the EU the U.S., and the UK. She has been involved in performing due diligence exercises on behalf of and has given legal advice to clients pursuant to the, EU and U.S. sanctions obligations and communication with the relevant authorities for securing authorisations and/or guidance for sanctions matters on behalf of clients.

Further, Sophia offers in-house and external training, as she is a certified trainer by the HDRA.

Sophia has established her expertise in the regulatory compliance and risk management field undertaking various courses and obtaining certifications such as the Financial Services and Regulatory Advanced Examination of the by Cyprus Securities and Exchange Commission (CySEC), which is recognised by the Charted Institute for Securities and Investment (CISI) - the examination of CISI on Global Financial Compliance and alongside the Certificate in Global Financial Compliance (Cyprus) which she successfully passed and was awarded the CISI Level 3 Award in Global Financial Compliance. Since then she has been an Associate of CISI.

Following a successful examination, she has obtained the Worldwide recognised and top level certificate in Money Laundering, the ACAMS certificate and is a member of CAMS Cyprus as well as the International Compliance Association's Compliance officer certificate with distinction. She is also a holder of the K2Integrity Sanctions Specialist certification.

Czech Republic

Kinstellar

Michal Kníž

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Companies with 50 or more employees must designate a person who is responsible for investigating whistleblower reports. The responsible person must acknowledge receipt of a whistleblower report within seven days, unless the whistleblower requests not to be notified or such notification could reveal their identity to another person.

The responsible person is obliged to assess the substance of the report and inform the whistleblower in writing of the results of the assessment within 30 days of receiving the report. In factually or legally complex cases, this period may be extended by up to 30 days, but not more than twice. The responsible person must notify the whistleblower in writing of the deadline extension and provide the reasons for it before the original deadline expires.

If the responsible person concludes that the report is justified, they must propose to the company appropriate measures to prevent or remedy the unlawful situation. If the company does not accept the proposed remedial measures, it must implement other appropriate remedial measures. The implementation of such measures must be promptly reported to the responsible person, who must then inform the whistleblower.

If the responsible person concludes that the report is not justified, they must without undue delay inform the whistleblower in writing. The notification should state that, based on the facts outlined in the report and the circumstances known to them, they do not suspect any infringement has occurred, or they have concluded that the report is based on false information. Additionally, the responsible person must inform the whistleblower of their right to report the matter to a public authority.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Czech law does not contain any specific provisions allowing the use of group wide reporting systems instead of requiring local systems.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Pursuant to Sections 279 and 280 of the Czech Labour Code, certain matters must be discussed with or at least brought to the attention of employee representative bodies. However, internal investigations do not fall within the scope of these matters.

b) Given that personal data is most likely going to be processed during an internal investigation, the data protection officer must be informed of such processing. Regarding the data privacy authority, since the implementation of the GDPR, there is no longer a general data processing notification (which existed under previous Czech data protection legislation). Only personal data breaches pursuant to the EU General Data Protection Regulation ("**GDPR**") should be notified pursuant to Articles 33 and 34 of the GDPR.

c) A public prosecutor has neither the right to participate nor to be informed about an internal investigation. Voluntary disclosure of the results of the investigation may still be beneficial in the event of subsequent criminal proceedings. However, a voluntary disclosure must be considered carefully. Due to insufficient regulations on structured criminal settlements and very few specific cases of leniency, the impact of voluntary disclosure on the outcome of a criminal proceeding is highly uncertain.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

The obligation to cooperate with the investigation is not explicitly stipulated by law. However, such obligation may be inferred from general employee duties. These include the duty to protect the employer's property, the duty not to act in violation of the employer's legitimate interests, and the duty to prevent damage to the employer. Refusal to cooperate with the investigation may be treated as a breach of the employee's duties. Therefore, the employee would be subject to disciplinary proceedings, which may even lead to a dismissal. The employer may also claim damages. However, in practice, the calculation of such damages is often complicated.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Investigative actions may trigger labour law deadlines under the Czech Labour Code. A supervisor, manager, or another person with authority must terminate or instantly dismiss an employee within two months after being informed of the employee's misconduct. Information about the investigation or its results should be shared with these decision-makers at a later stage in the investigation to avoid triggering these deadlines.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

It is essential to consider data protection laws when conducting interviews, especially the GDPR, including the Czech implementing Act No. 110/2019 on Personal Data Protection. The Czech data protection authority has not issued any specific guidelines in connection with internal investigations yet.

b) reviewing emails?

Data protection laws must also be considered before reviewing emails. General provisions of the Czech Civil Code and Labour Code regarding privacy protection should also be considered.

c) collecting (electronic) documents and/or other information?

Pursuant to the Czech Civil Code, electronic and paper documents are protected alike. Therefore, while collecting documents, the relevant provisions of the GDPR, Civil Code, and Labour Code should be taken into account.

d) analysing accounting and/or other business databases?

No specific laws have to be considered when analysing accounting and/or other mere business databases.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no obligation under Czech law to provide written instructions. However, it is advisable in certain cases to provide background information on the investigation to help expedite the investigation (i.e. no time has to be spent on clarification during the interviews).

b) be informed that they do not have to make statements that could potentially be self-incriminating?

In contrast with criminal proceedings, no warning regarding self-incrimination must be provided under Czech law during an internal interview.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

Czech law does not require providing an "Upjohn warning" to an interviewee. Nevertheless, it is advisable to do so.

d) be informed of their right to have their own lawyer attend the interview?

There is no obligation under Czech law to inform the employee of the right to counsel, as there is no right to counsel during an internal investigation. Participation in an interview is merely a fulfilment of an employee's duties. Therefore, there is no need for a lawyer to attend the interview.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

An employee has no right to have a representative from an employee representative body present during the interview.

f) be informed that data may be transferred to another country (in particular to the United States)?

Pursuant to the GDPR, an interviewee must be notified of potential cross-border data transfers. Privacy Shield provisions should also be considered.

g) sign a data privacy waiver?

Generally, the data subject's consent is necessary to process any personal data. However, the data controller (i.e. the employer) may process personal data without the data subject's consent if necessary for the rights or legitimate interests of the controller or another person. However, this exception should be considered on a

case-by-case basis since it requires a balancing test between the legitimate interests and the data subject's rights and freedoms.

h) be informed that the information gathered might be passed on to authorities?

There is no legal obligation to inform the interviewee that information gathered might be passed on to authorities.

i) be informed that written notes will be taken?

There is no legal obligation to inform the interviewee that written notes will be taken during the interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There are no specific laws governing hold or retention notices in the Czech Republic.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege is defined differently under Czech law than in other jurisdictions. In the Czech Republic, attorney-client privilege is an obligation of confidentiality for attorneys-at-law. It extends to all information that the attorney receives while providing legal services (with a few particular exceptions). The best way to ensure privilege protection over the findings of an internal investigation is to hire outside counsel. Only attorneys-at-law are exempt from the general duty to report certain crimes to law enforcement. The external counsel should also subcontract any third parties involved in the investigation (e.g. forensic accountants).

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Pursuant to Czech law, in-house lawyers do not fall under attorney-client privilege.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Insurance companies must not be informed under Czech law. However, each insurance policy should be reviewed for the inclusion of such a possible obligation.

b) Business partners (e.g. banks and creditors)?

There are no statutory requirements for notifying business partners. Such an obligation, however, may arise from agreements between the partners.

c) Shareholders?

Shareholders do not need to be notified at the start of an internal investigation. Publicly traded companies do not have any general notification requirements.

d) Authorities?

Generally, there is no duty to notify the prosecutor or any other authority of the start of an investigation. However, it is essential to take into account the reporting duty arising from the Criminal Code. This duty applies only to a limited list of crimes, including bribery. A breach of this duty is a criminal offence. Therefore, every investigation should be structured to minimise the risk of falling under this reporting duty. For example, it is advisable to hire external counsel to conduct the investigation since attorneys-at-law are not subject to the reporting duty.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Apart from the above-mentioned reporting duty, there are no special immediate measures to consider once an investigation has started. However, the company has to ensure that any ongoing criminal behaviour is stopped as soon as possible.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

It is uncommon in the Czech Republic for local prosecutor offices to be involved in internal investigations.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Search warrants, as well as dawn raids, must be pre-approved by the courts. Evidence obtained without prior court approval may not be used in subsequent criminal proceedings.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Corporations can enter into so-called "plea bargain" agreements with the prosecution. In such agreements, the defendant pleads guilty to certain offences and accepts a certain sanction. Plea bargains must be court approved. Corporations charged with misdemeanour offences (i.e. offences with a maximum penalty of five years imprisonment) can also receive a conditional suspension of criminal prosecution and a settlement.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

The most common sanctions for individuals are imprisonment or fines. However, the Czech Criminal Code recognises a wide range of sanctions, e.g. prohibition of an activity or forfeiture of assets.

The range of sanctions for companies under the Corporate Criminal Liability Act is even broader and includes, among other penalties: fines; forfeiture; prohibition of certain activities; publication of judgement; prohibition on receiving grants or subsidies; prohibition on taking part in procurement, concession proceedings, or competitive bidding; and dissolution.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

A company might be discharged from corporate criminal liability if it implemented an efficient compliance system before committing the crime. The Czech Supreme Prosecution Office has published guidelines on what factors should be taken into account when assessing whether a compliance system is effective. While these guidelines are not binding to courts (as they are addressed to state prosecutors), they are useful for companies to assess their compliance systems. In general, the guidelines are consistent with best practices from other countries. If an effective compliance system is implemented after the crime has been committed, the law does not set out an explicit discharge option. However, such implementation can be taken into account by the court as a mitigating factor.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

The ESG requirements in the Czech Republic primarily involve the implementation of the Corporate Sustainability Reporting Directive. As this directive has only recently come into effect and currently applies to a very limited number of Czech companies – with expectations of gradual expansion –, we are not aware of any public enforcement cases in this respect. There is currently no legislation regarding ESG supply chain due diligence in Czech law.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

A widely discussed topic in the Czech Republic is the adoption of a new Code of Criminal Procedure. The existing Code dates back to 1961. A draft of the new Code, prepared by a committee of judges, attorneys, and scholars has been published on the website of the Ministry of Justice for public comments. Although the current Czech government has included the adoption of the new Code of Criminal Procedure in its programme statement as one of the objectives of its term, recent indications suggest that the government is rather opposed to the current draft. As of now, no deadline has been set for its adoption.

CONTACT

Palác Myslbek
Na Příkopě 19
117 19 Prague 1
Czech Republic

Tel.: +420 221 622 111
www.kinstellar.com

Kinstellar is a leading independent law firm in Emerging Europe, Turkey, and Central Asia, with offices in Almaty (Kazakhstan), Belgrade (Serbia), Bratislava (Slovakia), Bucharest (Romania), Budapest (Hungary), Istanbul (Turkey), Prague (the Czech Republic), Sofia (Bulgaria), Tashkent (Uzbekistan), Kyiv (Ukraine) and Zagreb (Croatia).

Operating as a single fully integrated firm, Kinstellar delivers consistently high quality services across all jurisdictions in an integrated and seamless style. We are particularly well suited to servicing complex transactions and advisory requirements spanning several jurisdictions.

We have the leading Compliance, Risk and Sensitive Investigations, and White Collar Crime Practice in Emerging Europe and Central Asia. Our strengths include a multi-jurisdictional approach, deep knowledge of the region's anti-corruption laws and culture, familiarity with regional enforcement trends and proficiency in dealing with local authorities.

We have experience in crisis management and communications and expert knowledge in matters of legal privilege, data protection, employee privacy, document retention, security, and corporate and director liability.

Michal Kníž
Managing Associate
Kinstellar
T +420 221 622 111
E michal.kníž@kinstellar.com

Michal Kníž is a Managing Associate in Kinstellar's Prague office. He is a member of the Corporate group, and his specialisation includes compliance, risk and sensitive investigations, white collar crime defence, corporate matters and personal data protection. Michal graduated from the Faculty of Law and the Faculty of Economics of Masaryk University in Brno. During his studies, he spent one semester at the University of Bergen, Norway, and completed an internship at the Supreme Administrative Court of the Czech Republic. Michal has advised various clients in matters relating to internal investigations (including a global pharmaceutical company) and white collar crime matters (including a global IT company, an international professional services firm, and a major Czech insurance company).

Denmark

Kromann Reumert

Hans Jakob Folker

Elena Billestrup

Laura Gernyx Sejbak

Laura Fredslund

Niels Holm Jensen

Overview

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X		
No				X	X

Question List

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Yes. If the whistleblower report is within the scope of the Danish Whistleblower Protection Act (the "**Danish WPA**"), the internal investigation must be organised to ensure the rights of the whistleblower pursuant to this act. In particular, the internal investigation must maintain confidentiality and protect the identity of the whistleblower.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Yes. The Danish WPA allows for group wide reporting also in relation to workplaces with more than 249 employees. Given the possible inconsistency with the EU Whistleblower Directive, the Ministry of Justice has been empowered to amend the law, if required by the European Commission.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Not *per se*. However, it is always advisable to check whether there exist special agreements or local practices calling for labour law considerations.

b) Not *per se*.

c) There is no general obligation in Danish law to notify authorities of internal investigations. However, the individual matter must always be assessed since special obligations may exist to notify authorities of safety incidents or similar. These questions will depend on the industry involved. A number of industries are subject to reporting suspicious transactions and/or other financial crimes.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

This will depend on the nature of the investigation and under what circumstances it is carried out. From a criminal law perspective, participation in interviews generally is voluntary and a general principle of non-self-incrimination applies. From a labour law perspective, employees in work related matters will be obliged to support the investigation in a loyal and truthful manner. Non-cooperation may warrant disciplinary actions against the employee. The specific situation will have to be considered.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Generally, the commencement of an internal investigation will not trigger labour law deadlines. However, an employer must be careful of inaction if clear evidence of sanctionable behaviour is presented. Typically, the investigation process and subsequent labour law assessment must be kept separate so as not to short-circuit each other. The risk of passivity in relation to grounds for summary dismissal should be considered.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Principles of administration of justice should be considered before conducting interviews. However, an analysis will have to be carried out with respect to the industry in question, including the existence of secrecy requirements, etc. The risk of affecting potential witnesses should be considered, in particular, if the matter is also investigated by the authorities.

b) reviewing emails?

Emails are protected by GDPR, Danish Data Protection legislation, and the Danish Criminal Code (the "**DCC**"). Pursuant to applicable law, the employer is generally obligated to inform any data subject whose personal data are being processed on the identity and contact details of the data controller, the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, the recipients or categories of recipients of the personal data, etc. However, such an obligation does not exist if the data subject's interest in this information is found to be overridden by essential considerations of private interests, including the consideration for the employee themself. Thus, any review of emails belonging to employees is subject to a balance of interest test where the legitimacy of the review should be assessed.

c) collecting (electronic) documents and/or other information?

From a general point of view and depending on the nature of the investigation, the GDPR, Danish Data Protection legislation, the Danish WPA, and principles of administration of justice should be considered and complied with in connection with collecting documents and/or other information comprising personal data. The collection must be for a legitimate purpose and be of relevance to the case. In addition, personal data may only be stored if the data is needed. Therefore, the allowed period will always depend on an assessment of whether the processing is still necessary for the legitimate purpose for which the data is stored in the specific case. Technical aspects of collecting evidence should also be considered and complied with, in particular if the information potentially should serve as evidence in later criminal or civil proceedings.

d) analysing accounting and/or other business databases?

Only documents that contain personal data are subject to the general principles of the GDPR and the Danish Data Protection legislation.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

It depends on the terms of the employment and the nature of the interview. There is no statutory obligation to instruct an employee before conducting an interview. In some employment relationships, the employee will be entitled to assistance from a union representative, HR, or similar. Principles of administration of justice should be considered in serious matters.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

It will depend on the situation and the matter under investigation. In more serious matters with participation of external lawyers, it will be the professional responsibility of the lawyer to appropriately guide and caution the interviewee in connection with the interview, including with respect to self-incrimination.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

The role of external lawyer should always be explained to participants in an interview carried out as part of an internal investigation. Lawyers carrying out interviews in connection with internal investigation generally will be subject to ethical and professional standards.

d) be informed of their right to have their own lawyer attend the interview?

It will depend on the situation whether an external lawyer has a right to attend an interview in connection with an internal investigation. However, persons subject to internal investigations generally should be allowed to appropriate representation, e.g. a lawyer, union representative, or a union member representative.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

The employee is not entitled to have an employee representative present during the interview. However, it is recommended that the employer gives the employee such an opportunity unless detrimental to the investigation.

f) be informed that data may be transferred to another country (in particular to the United States)?

The employee should be informed about any potential cross-border data transfer. Under the GDPR, an additional legal basis is required when transferring personal data to non-EEA countries. Such transfer is only permitted if adequate safeguards are established or an exemption applies. An adequate safeguard may be entering into the EU standard contractual clauses with the recipient of the personal data. Further, requirements for the implementation of supplementary measures may be applicable. Only in exceptional cases, the consent from the employee will be the appropriate legal basis to allow the transfer of data to countries that do not ensure an adequate level of protection (see GDPR Article 49(1)(a)).

g) sign a data privacy waiver?

The protection granted under the GDPR and Danish Data Protection legislation cannot be deviated from to the data subject's disadvantage. Consequently, the rights of the data subject cannot be legally waived.

h) be informed that the information gathered might be passed on to authorities?

There is no general requirement in Danish law that an employer must inform the employee that a matter is passed on to the authorities.

i) be informed that written notes will be taken?

This will depend on the nature of the internal investigation and the matter investigated.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Yes. Retention notices and legal holds should be discussed early in the process. There are no specific requirements which must be observed.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Legal privilege is a procedural guarantee protected by the Danish Administration of Justice Act covering civil and criminal proceedings. Under Section 170 of the Danish Administration of Justice Act, defence counsels and lawyers may not be required to provide evidence about matters having come to their knowledge in the course of the exercise of their functions. The protection also extends to written advice and reports prepared by them in connection with such proceedings.

In civil proceedings, a similar protection is ensured with regard to advice received from the acting counsel provided the advice relates to legal proceedings. Generally, the privilege applies if the material covered by the privilege is clearly marked as privileged. However, the privilege does not protect evidence from being disclosed.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Legal privilege does not apply to work products and advice provided by in-house counsel to the management of a company. For legal privilege to apply, the advice must be provided by external counsel.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Any obligation to notify an insurance company of an investigation would stem from the individual insurance agreement. Where the investigation may reveal information that could form the basis of an insurance claim, the policy holder should notify the insurer.

b) Business partners (e.g. banks and creditors)?

There are no statutory duties in this regard. Notification requirements may arise from the contractual obligations between the company and its business partners, including banks.

c) Shareholders?

Internal investigations may deal with important matters that could be seen as inside information. On a case-by-case basis, the company needs to evaluate if there is a duty to notify its shareholders and the public, in accordance with the EU Market Abuse Regulation. Violation of disclosure requirements is a criminal offence (see Section 248 of the Danish Act on Capital Markets).

d) Authorities?

See above under 2. In general, there is no statutory obligation to inform the prosecutor or any other authority about an internal investigation or potential misconduct within the company.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

There is no general statutory obligation to take any immediate measures, unless for safety reasons or similar. However, the company has an ordinary obligation to minimise damages and take adequate steps to prevent new ones. In this regard, ongoing criminal behaviour must be stopped. The company may also have to re-evaluate its compliance system in order to eliminate potential deficits and improve its existing system.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Danish authorities, including police and prosecution, are required by law to investigate matters within their competence on their own and therefore do not depend on results from internal investigations. However, if an internal investigation is conducted, the involved authority typically will be interested in the results of the internal investigation. As noted above, coordination is advisable to avoid misunderstanding regarding the carrying out of an internal investigation in connection with parallel government investigations.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Under Chapter 73 of the Danish Administration of Justice Act, search warrants must fulfil formal and material requirements stipulated by law. Search warrants are issued by the court. A search warrant may be issued if there is a reasonable suspicion that an offence under public prosecution has been committed and the search is of material importance to the case. The police may carry out a search without a warrant if there is a risk that the evidence sought would be lost should the police wait for a warrant.

Generally, even when the formal prerequisites for search warrants are not observed, the seized evidence may still be used against the company.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Deals, non-prosecution agreements, and deferred prosecution agreements are not available in Danish law. Nevertheless, corporations can and commonly do accept fixed penalty notices when offered by the prosecution.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Both legal and natural persons are subject to criminal liability under Danish law.

Pursuant to Chapter 5 of the Danish Criminal Code, any legal person may be subject to fines where so provided by, or pursuant to, statute. For example, Section 306 of the Danish Criminal Code states that companies and other incorporated bodies (legal persons) may incur criminal liability, under the rules of Chapter 5, for violations of the Criminal Code. Section 306 covers all offences in the Danish Criminal Code. In addition, legal persons may be subject to disgorgement and debarment. Sanctions in relation to legal persons generally are tied to gross revenue. However, it depends on the regulatory regime governing the industry in question.

The ordinary penalties for individuals are imprisonment and/or fines, but individuals may also be subject to disgorgement and debarment.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

There are no specific rules or guidelines that set out principles for determining penalties if a company has implemented an efficient compliance system. Penalties will be determined on a case-by-case basis based on the specific circumstances, including aggravating and mitigating circumstances that must be considered when determining penalties.

However, from recent Danish case law it appears that it may have an impact on the court's decision on the penalty if companies have introduced stricter compliance procedures and guidelines for their future business after the violation has occurred.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

The main cross-sectional regulation of ESG matters is set out in the Danish Financial Statements Act, which incorporates the EU Non-Financial Reporting Directive. The EU Corporate Sustainability Reporting Directive ("**CSRD**") is expected to be implemented into Danish law by July 2024.

In recent years, Danish authorities have significantly intensified their focus on enforcing ESG-related legislation. Both the Danish Financial Supervisory Authority and the Danish Business Authority have announced plans to bolster their enforcement efforts by recruiting additional talent. Specifically, instances concerning violation of the prohibition against misleading consumers, such as greenwashing cases under the Danish Marketing Practices Act, are on the rise. Additionally, there is a noticeable increase in enforcement actions and legal proceedings being brought before Danish courts, where citizens are suing companies for alleged climate or environmental violations.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Danish lawmakers have increased their focus on combatting financial crime, fraud and tax offences. More resources have been allocated to enforcement agencies, leading to increased enforcement. Enforcement techniques traditionally applied to organised crime, such as custody and wiretapping, are also being applied in white collar crime cases resulting in more complex matters.

CONTACTS

KROMANN REUMERT

Sundkrogsgade 5
2100 Kopenhagen
Denmark

Tel.: +45 7012 1211
www.kromannreumert.com

Hans Jakob Folker
Partner
Kromann Reumert
T +45 61 61 30 09
E hjf@kromannreumert.com

Hans Jakob Folker heads Kromann Reumert's corporate criminal law and White Collar Crime & Investigation practice, focusing on financial regulation, fraud, bribery and corruption, forensics and internal investigations in Denmark and abroad.

He joined Kromann Reumert in 2013 after having served as deputy public prosecutor with the State Prosecutor for Serious Economic and International Crime (today the National Special Crime Unit).

As a seasoned litigator, Hans Jakob has acted as prosecutor and defence counsel in complex government investigations and proceedings. He deals with corporate criminal law matters and damage claims within all main business sectors, including anti-corruption, conflicts of interest, money laundering, and financial regulation. In recent years Hans Jakob has handled a number of large international matters regarding sanctions laws.

Elena Billestrup
Attorney
Kromann Reumert
T +45 61 61 30 33
E elb@kromannreumert.com

Elena joined Kromann Reumert in 2017 and has been part of the Crime & Investigation team since 2023.

Elena has experience with internal investigations assisting both national and international clients in relations to corporate criminal law, including financial crime, anti-corruption, bribery and sanctions.

Laura Gernyx Sejbak
Attorney
Kromann Reumert
T +45 61 55 11 57
E lgs@kromannreumert.com

Laura joined Kromann Reumert in 2019 and has been part of the team since 2020.

Laura has experience with internal investigations in relation to corporate criminal law, including financial crime, anti-corruption, sanctions, market abuse, internal fraud, and civil law claims in connection with criminal law cases.

Laura has previously worked for prosecution service.

Laura Fredslund
Assistant Attorney
Kromann Reumert
T +45 24 86 00 07
E lafr@kromannreumert.com

Laura joined Kromann Reumert and the corporate criminal law team in 2022.

Laura is assisting with preparation of internal investigations and filings to the police in fraud cases.

Laura has previously worked for prosecution service.

Niels Holm Jensen
Assistant Attorney
Kromann Reumert
T +45 24 23 46 21
E nije@kromannreumert.com

Niels joined the team in 2023.

Niels has experience with internal investigations in relation to corporate criminal law and assists both national and international clients in corporate criminal law disputes and internal investigations.

Estonia

Ellex Raidla

Marko Kairjak, PhD

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

No specific rules currently exist or apply in Estonia regarding the EU Whistleblower Directive, as it has not yet been implemented. The adoption of the Directive has been delayed due to significant political and public tensions.

Hence, there are currently no specific procedures in place at the national level. Nonetheless, organisations may have their own internal procedures for handling such situations. These could include measures to protect the whistleblower's identity, ensuring fair treatment, and preventing retaliation.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

As per the current draft bill, Estonia allows the use of group wide reporting systems.

While Estonia currently does not intend to implement non-mandatory provisions from the Directive, it is important to closely monitor the legislative process closely. Given the potential changes as the draft bill undergoes further readings and potential amendments in the Estonian Parliament, it is advisable to seek guidance from legal experts to fully comprehend the implications. Once the Directive is implemented, organisations may need to ensure that their internal systems comply with any new requirements or standards outlined in the legislation.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

No, there is no obligation to inform under Estonian law.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

No specific duty exists. There have been examples of employees refusing to cooperate, but no case law exists yet on whether this may trigger any labour law consequences or be grounds for disciplinary measures.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

In case an employee has been questioned by the police as part of ongoing criminal proceedings, they are prohibited from disclosing any information about the details of the interview during the internal investigation. However, the employee can disclose facts pertaining to the facts under investigation, even if disclosure had been made to the police during the interview. In case such facts are provided, this information may serve as grounds for termination of the employment contract. Although no specific grounds are outlined, termination may occur under the general provisions for breaches of duties. The deadline for termination depends on the length of the employee's tenure (e.g. 30 days for employees with up to five years of tenure).

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

State secrets cannot be disclosed during internal investigations by employees that have knowledge of them. As mentioned above, if the employee has been interviewed by the police, no facts about the contents of what was said to the police can be disclosed. Private information under the GDPR regime cannot be disclosed during interviews.

b) reviewing emails?

Reviewing employee emails is allowed when written consent has been provided by the relevant employee either when signing the employment agreement or separately.

c) collecting (electronic) documents and/or other information?

Reviewing electronic documents is allowed when written consent has been provided by the relevant employee either when signing the employment agreement or separately.

d) analysing accounting and/or other business databases?

No specific rules apply.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

No specific rules apply.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

No specific rules apply. Although no case law exists, it has been usual practice to notify the employee that refusal to provide information is allowed.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

No specific rules apply.

d) be informed of their right to have their own lawyer attend the interview?

No specific rules apply.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

No specific rules apply.

f) be informed that data may be transferred to another country (in particular to the United States)?

No specific rules apply.

g) sign a data privacy waiver?

No specific rules apply.

h) be informed that the information gathered might be passed on to authorities?

No specific rules apply.

i) be informed that written notes will be taken?

No specific rules apply. Nevertheless, case law has stated that in case of video or audio recordings, consent of the relevant employee must be taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

No specific rules apply.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Yes, findings are to be considered as communication between attorney and client and are subject to client privilege. If the information is held at the premises of a law firm, any search of such premises can only be permitted if a member of the firm (an attorney) is suspected of committing a crime. If such suspicion arises, the findings can only be seized by authorities if they are directly linked to the suspicion. In case the findings have been gathered but no grounds exist, they should be deleted by the authorities as part of correspondence. The European Court of Human Rights (ECHR) has indicated the necessity of this action; however, there are sadly no legal grounds to demand the deletion of such information from the police.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

The attorney-client privilege does not apply to in-house counsel in Estonia.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

No specific rules apply.

b) Business partners (e.g. banks and creditors)?

No specific rules apply.

c) Shareholders?

No specific rules apply.

d) Authorities?

No specific rules apply.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

No, although no legal obligation exists, local practice has required the management to pass a resolution to initiate an internal investigation.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

There is still a lack of knowledge about internal investigations, thus no known practice or position concerning this matter exists. However, the overall position on conducting investigations is positive and there have not been any attempts to interfere or restrict internal investigations.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

A decree to conduct a dawn raid must be passed either by the prosecutor or the court (based on such application of the prosecutor). The decree must provide a short description of the suspected activities, a short overview of the status of the criminal proceedings and also the reasoning why evidence cannot be gathered in any other, less intrusive way. Additionally, a very detailed overview of the documents or evidence to be gathered and seized must be provided. The decree must be introduced to the company representative and cannot be disputed.

Search warrants or dawn raids on companies typically require certain legal prerequisites to be fulfilled, primarily to ensure that such actions are conducted lawfully and respect individuals' rights. The legal prerequisites and procedures for obtaining search warrants or conducting dawn raids are governed by the Estonian Code of Criminal Procedure, as well as other relevant laws and regulations. Some key aspects include:

- Reasonable Suspicion: Authorities must have a reasonable suspicion of criminal activity or wrongdoing before seeking a search warrant or conducting a dawn raid on a company. This suspicion must be based on credible evidence or information indicating that a crime has been committed or is about to be committed;
- Judicial Authorisation: In most cases, the issuance of a search warrant requires judicial authorisation. Law enforcement authorities or public prosecutors must apply to a competent court, providing sufficient grounds and evidence to justify the need for the search. The court evaluates the application and grants the warrant if it finds the request justified under the law;
- Specificity of the Warrant: Search warrants must specify the premises to be searched, the items or evidence sought, and the legal basis for the search. This ensures that the search is conducted within the bounds of the law and does not infringe individuals' rights unnecessarily;
- Procedural Safeguards: During the execution of a search warrant or dawn raid, authorities must adhere to procedural safeguards to protect the rights of the company and its employees. This includes ensuring that searches are conducted in a manner that minimises disruption to business operations and respects individuals' privacy rights.

If the legal prerequisites for obtaining a search warrant or conducting a dawn raid are not fulfilled, any evidence gathered through such actions may be subject to challenge in court. In Estonia, the principles of legality and due process are fundamental to the admissibility of evidence in criminal proceedings. Evidence obtained unlawfully or in violation of procedural requirements may be excluded from court proceedings, potentially affecting the prosecution's case against the company.

The admissibility of evidence and the consequences of procedural irregularities may vary depending on the specific circumstances of each case and the applicable laws and regulations. Companies facing investigations or law enforcement actions should seek legal advice from qualified professionals to understand their rights and obligations under Estonian legal acts.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Yes, such agreements or agreements of termination of proceedings are very common and widely used. Two main types of agreements exist:

1) Settlement agreement – agreement between the defendant, defence counsel and prosecution. The settlement shall be approved by the court and the defendant shall be convicted;

2) Termination of proceedings on grounds of reasonability – the proceedings shall be terminated based on an agreement between the prosecutor and the defendant, whereby the defendant obliges to pay a certain sum to the state budget.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Under Estonian law, companies or their directors, officers, or employees can face various penalties for misconduct committed by individuals within the company either within criminal proceedings or misdemeanour proceedings. These penalties can include:

– Fines or monetary penalties: Companies may be subject to fines imposed by regulatory authorities in misdemeanour cases or courts in criminal cases for various types of misconduct, such as violations of laws, regulations, or contractual obligations;

– Imprisonment: In cases of serious misconduct or criminal offences committed by company directors, officers, or employees, individuals may face imprisonment as a penalty under Estonian criminal law. Monetary punishments are more common in case of economic crime breaches;

– Disgorgement: Requirement for individuals or companies to forfeit profits obtained through illegal or unethical activities. In Estonia, disgorgement may be ordered by courts or regulatory authorities as a penalty for financial misconduct or violations of securities laws;

– Debarment: Debarment involves the exclusion of individuals or companies from participating in certain activities, contracts, or public procurement processes. In Estonia, debarment may be imposed as a penalty for misconduct in public procurement or other regulated activities.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

No, there have been attempts to reason such reduction based on renewal of compliance systems, but case law has not (yet) accepted such grounds for reduction.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

There are no specific ESG related rules adopted yet.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Some general insights on potential areas of focus based on common global trends and issues that might also be relevant in Estonia:

1) Major AML cases: Investigations into financial crime, including money laundering, corruption, and fraud, are typically significant areas of focus for law enforcement authorities and regulatory agencies. Recent cases or legislative changes may aim to bolster anti-money laundering (AML) efforts, improve transparency in financial transactions, and combat corruption at various levels. The so-called big bank AML cases are being brought to court (Danske, for example).

2) Cyber Security and Data Protection: Given Estonia's reputation as a leader in digital innovation and its reliance on digital infrastructure, investigations related to cyber security breaches and data protection compliance are likely to remain a priority.

3) Environmental Protection and Sustainability: Investigations related to environmental violations, pollution, and sustainable practices may garner public attention, particularly as concerns about climate change and environmental degradation continue to grow globally. Legislative changes or regulatory initiatives may focus on enforcing environmental regulations and promoting sustainable business practices. It should be noted that there have not been significant cases within this field so far.

CONTACT

Ellex Raidla

Kaarli pst 1 / Roosikrantsi 2
Tallinn 10119
Estonia

Tel.: +372 640 7170
Email: estonia@ellex.legal

Ellex Raidla is the market's most valued strategic advisor and the most recommended law firm. Being a full-service law firm, Ellex Raidla provides consultations in all areas of business law. This specialised practice group approach ensures that highly qualified professionals will be working with our clients on the relevant issues within their competence. In case of necessity, efficient teams of various specialists are assembled to work together, which guarantees comprehensive problem-oriented advice in domestic and international transactions. Ellex Raidla is the first choice of local counsel for many international companies with projects in Estonia.

Ellex Raidla is also a member of Ellex – Baltic circle of legal excellence – the three leading law firms in the Baltics. With over 30 years of experience, Ellex represents the pinnacle of legal excellence in the Baltics and has set a new standard for legal innovation. At Ellex offices in Tallinn (Ellex Raidla), Riga (Ellex Klavins) and Vilnius (Ellex Valiunas), 250+ lawyers with top competences work in an integrated manner in specialised teams to support our clients across all business sectors.

Ellex has been awarded with the title of Northern European Law Firm of the Year (The Lawyer, 2022), Baltic Law firm of the Year (The Lawyer 2021, IFLR Europe Awards 2022-23, Who's Who Legal 2020-2022, Managing IP EMEA Awards 2022), as well as received TOP Tier in international rankings of the legal directories (Chambers & Partners, The Legal 500, IFLR1000).

Marko Kairjak, PhD, LL.M.
Partner
T +372 640 7170
E marko.kairjak@ellex.legal

Marko Kairjak, PhD., LL.M is a partner and financial regulatory and criminal compliance expert. He has extensive experience in criminal defence, internal investigations and compliance assessments having been involved in all the major and largest white collar cases in Estonia in recent history.

Marko Kairjak has also advised numerous financing transactions and regulatory matters within the alternative financing and fintech sector. He has been involved in setting up most of the regions' crowdfunding platforms and has also advised fintech companies in landmark financing transactions and provided regulatory and compliance support during licensing and post-licensing.

Marko Kairjak is the author of many academic books and articles and has been involved in university teaching since 2007. He has been a visiting scholar at various European universities and is considered the main academic expert on criminal compliance and AML.

Finland

Borenius Attorneys Ltd

Markus Kokko Matti Teräväinen

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X*	X	X	X	
No					X

* Criminal corporate fines possible in case an offence has been committed in the operations of the company.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

If a whistleblower report initiates an internal investigation, the company is required to protect the whistleblower from any form of retaliation. Finnish law strictly prohibits any retaliation against a whistleblower who has made a report in accordance with the law. This could be through the company's internal reporting channel, the centralised reporting channel maintained by the Office of the Chancellor of Justice, or to the public. It's also illegal to prevent or attempt to prevent such reporting.

Companies with 50 or more employees are required to establish their own internal reporting channels for receiving these reports. Once a report is received, the company must process it and take necessary follow-up actions. The whistleblower should be notified of the receipt of the report within seven days and informed about the actions to be taken within three months.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Companies in the same group can set up a shared system for whistleblowing, meaning they can use the same platform or process to handle reports from whistleblowers. However, companies not in the same group cannot share a whistleblowing system, with an exception provision for smaller companies. Those with fewer than 250 employees have the option to pool resources with other similar-sized companies to assist in tasks such as receiving whistleblower reports and conducting necessary investigations. Regardless, every company has a duty to investigate the reports they receive and address any issues that are found. If companies decide to pool resources, all participants must understand their duties and responsibilities.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) There are no specific regulations that grant employee representative bodies the right to be informed about or to participate in the investigation process. However, under the Finnish Act on Cooperation within Undertakings (1333/2021, "**Act on Cooperation**"), companies that regularly employ 20 or more employees must negotiate policies and processes for collecting employee personal data with the employees or their representatives. Some collective agreements may include more specific obligations and, therefore, should be consulted before beginning an investigation. Non-compliance with the Act on Cooperation may be sanctioned with a fine.

b) A Data Protection Ombudsman ("**DPO**") has the right to access any personal data being processed and any information necessary to supervise the processing and assess its legality. Under the Finnish Data Protection Act (1050/2018), which is based on the European data protection regulation (EU) 2016/679 ("**GDPR**"), the DPO is charged with advising employees on their data privacy rights and monitoring data protection. Consequently, the company is required to, on the DPO's request, report to the DPO any data privacy-related procedures and processes that are part of an investigation.

c) There is no obligation to inform the prosecution authorities before starting an internal investigation. However, voluntary involvement of the authorities can be beneficial depending on the circumstances of the specific case.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees have a general duty of loyalty toward their employer, the scope of which depends on the employee's position in the company. The employer has a general right to direct and supervise its employees and can, therefore, require them to participate in an internal investigation.

An employee's refusal to participate can, in some cases, be deemed misconduct and justify a warning or even dismissal if the employee has previously received a warning for the same or similar misconduct.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

According to the Employment Contracts Act (55/2001, as amended), if an employee's misconduct leads to a warning or dismissal, these measures should be initiated within a reasonable period after the relevant facts have become known. The reasonable period of time is evaluated on a case-by-case basis.

The employer may terminate an employment contract with immediate effect only with substantial cause. However, the right to terminate lapses if the employment contract is not terminated within 14 days of the date the employer was informed of the existence of the grounds for termination.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Data privacy regulations apply to the processing of all personal data. That includes personal information obtained from interviews. Therefore, it is essential to assess which data protection laws may or may not apply, and to document the measures taken before conducting interviews.

b) reviewing emails?

Pursuant to the Finnish Act on Protection of Privacy in Working Life (759/2004, as amended), the employer can only process personal data that is directly necessary for the employment. This is a mandatory legal provision that may not be waived by the employee. Under the Act, an employee's work-related emails can only be viewed if detailed provisions are observed. If these requirements are not met, reviewing employees' emails can constitute a criminal offence.

By contrast, employers are not permitted to review employees' personal emails. Personal correspondence may only be reviewed by authorities in connection with a criminal investigation.

c) collecting (electronic) documents and/or other information?

Finland has no blocking statute regime. Finnish data protection statutes are based on the GDPR, which has been implemented in Finnish legislation by the Finnish Data Protection Act.

Pursuant to these statutes, the processing of personal data must be appropriate and justified. This means that before an employer can process any personal data, the purpose of the processing, the data sources, and the data recipients must be determined. Processing or using personal data in a manner incompatible with the specified purpose is prohibited. At the employee's request, the employer must inform the employee of any personal data collected. As noted above, an employer can only process personal data that is directly necessary for the employment. Processing of other personal data can only occur in connection with investigations by the authorities.

d) analysing accounting and/or other business databases?

Data privacy laws do not apply to analysing accounting and other mere business databases.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

In Finland, there is no statutory obligation to give written instructions to the interviewee, although it is advisable to do so. Generally, the instructions would include a brief explanation of the background and focus of the investigation. It is advisable to provide these instructions in writing and ask the interviewee to sign them.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Regarding internal investigations, there is no right to remain silent to avoid self-incrimination, as is the case during criminal interrogations. Nevertheless, it is advisable not to pressure interviewees to incriminate themselves, especially if the interviewee is also subject to a criminal investigation.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

An Upjohn warning is only mandatory if there are links to U.S. law. However, in general, it is advisable to avoid behaviours that could mislead the employee into thinking that the company's lawyer represents them.

d) be informed of their right to have their own lawyer attend the interview?

In Finland, employers are free to handle internal matters independently without the involvement of outside lawyers. However, should the employer seek to dismiss the employee or terminate the employment contract, the employee has the right to be heard in the matter. Under such circumstances, the employee has the right to have a lawyer and should be informed of this right.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

In Finland, there is no statutory obligation to inform the employee of the right to have an employee representative present during an interview, even though such right usually exists. However, the specific rights of an employee and corresponding obligations of an employer might vary depending on the applicable collective agreement.

f) be informed that data may be transferred to another country (in particular to the United States)?

Pursuant to the GDPR and the Finnish Data Protection Act, the subject of the data must always be informed of the identity of the controller as well as of the purposes of the gathered personal data.

The employee should be informed of any potential cross-border transfers of personal data. Under Finnish data privacy legislation, the transfer of data to non-EU states is only permitted if an adequate level of data protection is guaranteed in the recipient country. All transfers of personal data to third countries or international organisations must be performed in accordance with Chapter V of the GDPR.

g) sign a data privacy waiver?

Under the Finnish Data Protection Act, an employee's consent is needed as far as personal data is concerned and as far as no legal exceptions apply. A data privacy waiver is particularly advantageous if the personal data of the interviewee may be used in future legal proceedings.

h) be informed that the information gathered might be passed on to authorities?

It is highly advisable to inform the employee that information gathered may be passed on to authorities. This is particularly true if information may be passed on to U.S. authorities.

i) be informed that written notes will be taken?

There is no legal obligation under Finnish law to inform the interviewee that written notes will be taken, but it is advisable to do so. It is also advisable to show the documentation of the interview to the employee for approval. There is, however, no statutory obligation to provide the employee with physical copies of notes from an internal interview.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

In Finland, there are no document hold notices or document-retention notices. However, as previously mentioned, the employer has the right to direct and supervise its employees and based on this right, can instruct them to preserve relevant documents and records. An objection to the employer's instruction can constitute misconduct.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Findings of internal investigations are generally not protected by attorney-client privilege, which is not absolute in Finland. However, it is advisable to consult outside counsel to ensure privilege. In principle, documents in the possession of outside counsel are protected. Documents and communications from outside counsel to in-house counsel in the possession of in-house counsel are not automatically protected. Whether such documents and communications are protected depends, in part, on when they were provided by the outside counsel. It is advisable

to clearly label correspondence and documents between in-house and outside counsel as being under the scope of attorney-client privilege. Ultimately, however, the courts will rule on what is admissible as evidence.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Generally, communication with in-house counsel and documents prepared by in-house counsel are not privileged under Finnish law.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There is no statutory duty. However, if there is a risk that the circumstances at hand could give rise to a claim, the policyholder should notify the insurer of these circumstances.

b) Business partners (e.g. banks and creditors)?

The decision to notify business partners must be determined on a case-by-case basis. For instance, a contractual obligation may provide that such information must be disclosed to the business partner. Even absent such a contractual provision, a company may still owe a general duty of loyalty to its business partners.

c) Shareholders?

Insider information that could influence stock prices must be disclosed to shareholders of publicly listed companies. A company may be liable for damages for breach of its reporting duties in accordance with Chapter 16 of the Finnish Securities Market Act (746/2012, as amended).

d) Authorities?

In general, there is no obligation to inform the authorities of an internal investigation or potential misconduct within a company. However, voluntary cooperation with the authorities can prevent harmful or unexpected measures by the local prosecutor or other authorities.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

According to general tort law principles, the company must minimise damages and try to prevent further damages. The company can, for example, impose sanctions, such as warnings, on the concerned employees to deter from future misconduct. Additionally, the company should assess its compliance systems to eliminate potential deficits and, if necessary, make improvements. In any case, ongoing criminal conduct in the company should be stopped immediately.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

As previously mentioned, depending on the nature of the investigation, early engagement with the local prosecutors can help ensure satisfactory cooperation and prevent unwanted measures. It is of paramount importance that the company does not destroy or otherwise remove any potential evidence or give the local prosecutors reason to suspect that such conduct could occur.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

According to the Finnish Criminal Investigation Act (805/2011, as amended), a search warrant must be issued by an official with the power to arrest, i.e. certain police officers. A search warrant may be issued if there is reason to believe that the search will reveal objects or information relevant to the investigation of an offence. The general principles of proportionality, minimum intervention, and sensitivity apply.

It is worth noting that even if these legal prerequisites are not met, the evidence can usually still be used in court proceedings unless the use of such evidence would jeopardise a fair trial.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

While plea bargaining is available for individuals under some circumstances, it is not an option for corporations under Finnish law, nor are deals. However, cooperation with authorities might, in some cases, be taken into account as a mitigating circumstance in sentencing.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Corporations can be fined up to €850,000 for certain criminal offences, such as bribery. Individuals can face sanctions, such as imprisonment, fines, or business prohibition. In some cases, a manager or a director may be liable for the misconduct of other employees, e.g. failure to adequately supervise.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

An efficient compliance system may reduce or even suspend penalties. The existence of an efficient compliance system may be considered an indication of no misconduct. In addition, the amount of a corporate fine shall be determined based on, amongst other things, the nature and extent of the misconduct. When evaluating the significance of the misconduct, for example, the nature and seriousness of the offence, and whether the misconduct manifests carelessness as to the law or authorities shall be taken into account. If the company had implemented an efficient compliance system, the misconduct could be considered less serious.

Generally, an efficient compliance system would only suspend or reduce penalties if it was implemented before the alleged misconduct.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

There is no specific national regulation regarding ESG (Environmental, Social, and Governance) beyond the regular legislation governing these issues. However, Finnish companies are subject to the European Union Corporate Sustainability Reporting Directive (2022/2464/EU, "**CSRD**"), which came into effect on January 5, 2023.

As part of the CSRD directive, the same auditor who approves the financial statements also checks, verifies and approves the ESG content, as it is part of the board's report in the financial statements. However, there are currently no authorities actively enforcing ESG-related cases in Finland.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Despite recent updates to whistleblower regulations, practices in Finland remain somewhat inconsistent. Furthermore, the implications and implementation of the CSRD reporting regime for Finland are still not entirely clear.

In recent years, Finland has seen a growing trend of investigations into misuse of public funds. This has been highlighted by a few high-profile cases that have gained significant public attention. These cases have involved allegations of misconduct and misuse of public funds, leading to increased scrutiny and calls for greater transparency and accountability in the public sector.

CONTACTS

BORENIUS

Eteläesplanadi 2
00130 Helsinki
Finland

Tel.: +358 20 713 33
Fax: +358 20 713 3499
www.borenius.com

Borenius Attorneys Ltd is one of the largest leading law firms in Finland. Borenius has been providing high-quality services in all areas of law since 1911. Borenius employs over 100 lawyers at offices based in Helsinki, Tampere, St. Petersburg, New York, and London and is ranked as a top tier firm by all leading legal directories

Markus Kokko
Partner
Borenius Attorneys Ltd
T +358 20 713 3482
E markus.kokko@borenius.com

Markus regularly advises major domestic and international clients on dispute resolution and corporate crime cases.

Markus has in-depth experience in domestic and international corporate and commercial disputes, and he has acted as lead counsel in numerous extensive cases. His field of experience encompasses cases related to a wide variety of business sectors, such as the chemicals industry, financial markets, international trade, retail and wholesale, mining, services and consultancy. Markus also has an exceptional track record in handling a broad range of litigation and arbitration cases, including *ad hoc* proceedings as well as proceedings governed by ICC Rules, SCC Rules, and the Arbitration Rules of the Finland Chamber of Commerce.

In addition, Markus frequently advises companies and executives in relation to complex corporate crime cases and criminal investigations regarding, *inter alia*, insider trading, environmental violations, corruption, imports and exports, and tax.

Markus' efficient and client-oriented approach has earned him an excellent reputation which has been recognised by rankings in Chambers Global, Chambers Europe, Legal 500, and Best Lawyers. Furthermore, Markus also serves as an arbitrator, and he has written many articles on litigation and arbitration.

Markus heads the Litigation & Arbitration and Corporate Crime teams at Borenius.

Matti Teräväinen
Associate
Borenius Attorneys Ltd
T +358 20 713 3425
E matti.teravainen@borenius.com

Matti Teräväinen frequently provides counsel on issues pertaining to dispute resolution and insolvency law across a broad range of industries.

France

Hogan Lovells (Paris) LLP


Arthur Dethomas


Christelle Coslin


Jean Pierre Picca


Jean-Lou Salha


Yaël Michel

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	
No					X

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The EU Whistleblower Directive was implemented in France by statute No. 2022-401 of 21 March 2022, which is enforceable since 1 September 2022. It largely follows the Directive but has implemented stricter standards in some respects. It has strengthened the procedure of internal investigations conducted after a whistleblower alert (that was initially set out in France by statute No. 2016-1691 of 9 December 2016 (the "**Sapin II Law**").

Under the Sapin II Law, companies with at least 50 employees must implement a whistleblowing policy. French law defines the whistleblower as a natural person who reveals, without direct financial consideration and in good faith, information relating to a crime, an offence, a violation of a law, a regulation or an international commitment ratified by France, or a serious threat or injury to public interests. Per 1 September 2022 whistleblowers are no longer required to have personal knowledge of the facts they denounce. In addition, individuals who helped whistleblowers file their report also benefit from the same protection against retaliation as the whistleblowers.

Under the Sapin II Law, whistleblowers can either file a report through the company's internal reporting system or directly to external authorities (i.e. the judicial authority or administrative authorities listed in the Decree n° 2022-1284). Since 1 September 2022 whistleblowers do not have to follow internal reporting procedure before filing an external report. They now have the possibility to choose directly between the internal or the external reporting procedure. If the external authority to which the whistleblower turned to, fails to address the alert within three months – which under certain circumstances can be extended to six months – the whistleblower may go public. In case of serious or imminent danger, when there is a risk of irreversible damage, or if the whistleblower risks retaliation as a result of approaching the external authority, the whistleblower may go public directly.

The identity of the whistleblower and any individuals targeted in the alert are to remain confidential and may not be disclosed to anyone except to judicial authorities. Any unauthorised disclosure is punishable by up to two years of imprisonment and a €30,000 fine for natural persons (€150,000 fine for legal entities).

A whistleblower whose alert is filed in accordance with the procedures set out above may not be retaliated against by their employer and may not be held criminally liable for the disclosure of secrets protected by law, provided the procedures were followed and the disclosure was necessary, and proportionate to protect the interests at stake. Any form of retaliation or threats thereof, against a whistleblower, may be punished by a three-year prison sentence as well as a €45,000 fine.

Pursuant to Decree No. 2022-1284, which completes the above mentioned statute, the whistleblowing policy must include specific provisions related to the processing of whistleblowers' alerts and define standards of confidentiality (e.g. anonymity of the whistleblower and of the persons targeted by the alert).

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Under French law, Article 3 I under 2 of statute No. 2022-401 allows, in principle, different companies belonging to the same group to implement a single reporting and investigation procedure for the entire group.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) In principle, **there is no legal provision in the French Labour Code ("FLC") compelling an employer (i) to inform its works council/staff representatives** when conducting an internal investigation within the company, irrespective of the matter of the conducted investigation, **nor (ii) to involve** them in the conduct of such investigations.

An exception is made in case of an internal alert was directly triggered by a member of the works council in the event of, *inter alia*:

– Infringement of the rights of individuals pursuant to Article L. 2312-59 of the FLC (i.e. threats to physical or mental health of employees or unjustified restrictions to their individual liberties – generally cases of moral/sexual harassment or discriminations); or

– Serious and imminent danger pursuant to Article L. 2312-60 of the FLC (i.e. imminent danger as well as threats to public health and the environment caused by manufacturing processes used or implemented in the company).

In case of such an internal alert, the employer **has no other choice than to launch an investigation immediately with the member of the works council responsible for the alert** and take the necessary steps to find remedies.

Lastly, despite the lack of mandatory legal provisions in this sense, a company can adopt **specific internal regulations, procedures and/or codes of conduct** regarding this subject which would grant the staff representatives some rights with respect to conducting internal investigations.

In this regard, the French Labour Code requires informing and consulting employee representative bodies, where they are in place and that they should have extended prerogatives (since they represent over 50 employees), before implementing employee monitoring tools and techniques. Thus, such bodies must be informed and consulted whenever the internal investigation process uses such monitoring tools and techniques.

Non-compliance may result in a criminal fine of up to €7,500 for the company and up to €1,500 for its legal representative, for hindrance of the rights of the employee representatives. Evidence collected in the context of an internal investigation, carried out without adequate consultation of employee representative bodies, might not be accepted in Court.

b) Under the GDPR and French law, there is no legal obligation to declare data processing or request an authorisation from the French Data Protection Authority the National Commission on Informatics and Liberty (*Commission nationale de l'informatique et des libertés*, "**CNIL**"). However, it is now required to draft a Data Protection Impact Assessment ("**DPIA**"). A DPIA consists of a risk assessment designed to assist a company identifying, analysing, and minimising the privacy risks that come with the processing activities that will be carried out in the context of an internal investigation. Additionally, it is necessary to record the corresponding data processing into the records of processing activities of the company. In both instances, the Data Protection Officer ("**DPO**") must be involved as part of the requirements of Article 39 of the GDPR.

c) Under French law, there is no legal obligation for an employer to report its decision to conduct an internal investigation or its findings to judicial authorities, including prosecution authorities, unless the investigation uncovers conduct that could qualify as a crime (i.e. offences punishable by at least ten years' imprisonment).

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees are not legally required to support an internal investigation. Due to stringent French labour law requirements, it may be difficult to sanction an employee for refusing to cooperate. Nevertheless, employees are, pursuant to their employment contract, bound to a duty of loyalty. This duty encompasses in principle their obligation to report on their work to their employer. Based on such principle, an employer may make participation in internal investigations mandatory, and consequently consider that active refusal to cooperate by not attending the interviews should be sanctioned disciplinarily. Nevertheless, these sanctions should be proportionate to the behaviour displayed by the employee.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Disciplinary sanctions must be imposed on an employee within two months of the employer becoming aware of the employee's wrongdoing unless it has given rise to criminal proceedings within the same period of time. After this two month period, no sanctions can be imposed for the concerned wrongdoing. If the employer conducts a fact-finding investigation, the two month period starts running on the day on which the employer obtains full knowledge of the extent of the wrongdoing. In practice, this usually means that the two month delay starts running from the date on which the findings of the internal investigation are issued and communicated in the investigation report.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) Data protection

Provisions of the GDPR, the updated French Data Protection Act, its implementing decree, and the CNIL's guidelines, especially on whistleblowing systems, have to be taken into account when implementing a whistleblowing system and when conducting investigations. Failure to comply is punishable by administrative sanctions of up to €20 million and four percent of the total worldwide annual turnover, criminal sanctions of up to €300,000 fine, and five years of imprisonment for natural persons (€1.5 million maximum fine for legal entities).

b) Secret State Law & banking secrecy

Credit institutions cannot share information covered by banking secrecy absent a court order (this covers information including, but not limited to, names, account numbers, and transactions). Violation of banking laws is punishable by up to one years' imprisonment and a €15,000 fine for natural persons (€75,000 for legal entities).

Since 2009 the communication of national defence secrets is punishable by five to seven years' imprisonment and a fine of up to €75,000 or €100,000 for natural persons, depending on how the discloser learned of the defence secrets (e.g. over the course of their work). The fine may reach €375,000 or €500,000 for legal entities. Negligent or reckless receipt of national defence secrets is punishable by three years imprisonment and a fine of up to €45,000 for natural persons.

c) Blocking Statute

The French Blocking Statute punishes anyone who tries to obtain or transfer documents or information for use in foreign judicial or administrative proceedings, unless this is accomplished under an existing treaty. Its broad scope covers any information or documents of an economic, commercial, industrial, financial, or technical nature. This broad scope may be interpreted as including information gathered in the course of interviews for use in foreign judicial or administrative proceedings. Breach of the Blocking Statute is punishable by six months' imprisonment and a fine of up to €18,000 (€90,000 for legal entities).

The Blocking Statute provides a legal defence to French or France based parties facing discovery requests outside France. However, it has rarely been enforced by French courts since its adoption in 1968. Foreign jurisdictions thus tend to disregard the Blocking Statute as a valid defence against discovery requests. The U.S. Supreme Court notably dismissed this defence in the *Aérospatiale* case.

Since 1 April 2022 companies that receive requests for information or documents from overseas that might be subject to the Blocking Statute, will need to submit reports to the Strategic Information and Economic Security Department ("**SISSE**"). This governmental agency then has one month to provide a response regarding whether the requested data is subject to the Blocking Statute.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no legal obligation to give written instructions to an interviewee beforehand, unless an internal procedure provides otherwise.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

There is no legal obligation to inform the interviewee of their right against self-incrimination. It is advisable to frame the interview as a discussion, rather than an examination. Accordingly, the interviewer should not subject the interviewee to any type of pressure during the interview.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

In September 2016 the Paris Bar Council published a vade mecum for lawyers conducting internal investigations, advising them to inform interviewees that they do not benefit from an attorney-client privilege, as the lawyer represents the company and not the interviewee (see Article 2.2). Also, in March 2023 the French Anti-Corruption Agency ("**AFA**") and the National Financial Prosecutor's Office ("**PNF**") issued a guide on internal investigations, which explains that the lawyer should inform the interviewee that the information arising from the interview may be used in disciplinary, civil, or even criminal proceedings.

If the lawyer fails to appropriately inform the employee about the scope of his mandate, an employee could claim in court that the information gathered during the interview was collected in an unfair manner. Courts (in particular employment courts) may then eventually decide to exclude the submitted evidence on this basis so that it is not opposed to the employee.

d) be informed of their right to have their own lawyer attend the interview?

No binding rules govern an interviewee's right to legal assistance in connection with internal investigations. However, the Paris Bar Council recommends informing interviewees that they can be assisted by an attorney when they are under serious suspicion of misconduct. This information is also echoed by the AFA and PNF guide. Information about the right of the employee to be assisted by counsel may be addressed in the notice of interview, but there is no legal provision governing the exact timing that should be complied with to inform the employee of this right prior to interviewing them. In particular, the Paris Bar Council Vade mecum specifies that such information can be delivered "at any point" in which it is revealed or it appears that the employee may have engaged in misconduct.

Again, if the lawyer fails to inform the employee of their right to be assisted, any information obtained during the interview could be rejected by civil or administrative courts, if the employee claims it was obtained in an unfair manner. Where applicable, this information shall generally be given before starting the interview.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Pursuant to the French Labour Code and to case law of the French Supreme Court, there is no right for an employee to be assisted by an employee representative during interviews conducted in connection with an internal investigation. The AFA and PNF guide specifies that interviews conducted in the context of internal investigations should not be considered part of the disciplinary procedure, which must be conducted separately. As mentioned above, internal procedures and/or customs may provide otherwise.

f) be informed that data may be transferred to another country (in particular to the United States)?

Under Article 13 of the GDPR, there is a legal obligation to inform interviewees of any transfers of personal data outside the European Union. In addition, Article 148 of the implementing decree of the updated French Data Protection Act states that the interviewee must be provided with the following information: country/ies of data recipients (in case this information is determined at the moment of collection of the data), categories of transferred data, purpose of the transfer, categories of data recipients, and the appropriate safeguards adopted to ensure the protection of the transferred personal data.

g) sign a data privacy waiver?

It is not possible for data subjects to sign a data privacy waiver.

h) be informed that the information gathered might be passed on to authorities?

There is no legal obligation requiring a company to disclose the findings of an internal investigation to judicial authorities and, accordingly, there is no obligation to inform the interviewee of this possibility.

i) be informed that written notes will be taken?

There is no legal obligation to inform interviewees that written notes will be taken. However, should *verbatim* notes be taken, it is best practice to inform the interviewees at the beginning of the interview, and to allow them to read and possibly sign a transcript of their statements after the interview, so their statements can be used. It is not advisable to give the interviewee minutes of the interview, in order to preserve confidentiality.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Document preservation notices are admissible, but this practice is not common yet. No specific legal provisions govern the issuance of legal holds. They shall, however, be written in French and comply with applicable data retention periods (e.g. data retention periods applicable within the company and those prescribed by the CNIL in its various guidelines).

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

French professional secrecy applies to communications between outside counsel and clients in all matters, whether advisory or litigation related. Lawyers cannot waive privilege, but clients can.

Judicial authorities have the possibility to issue a production order or perform a dawn raid to gather evidence, including the findings of an internal investigation. However, they cannot, in principle, seize documents covered by professional secrecy. Having outside counsel conduct the internal investigation can ensure that its findings are protected by privilege. By exception, authorities can seize documents exchanged between outside attorneys, acting as advisors, and clients under certain circumstances: (i) if the dawn raid is performed within an investigation for tax fraud, bribery, or terrorism financing, and (ii) if the document seized has been used in order to commit the alleged wrongdoing. The AFA and PNF Guide claims that the report does not benefit from privilege protection, which is not consistent with the Paris Bar Council Vade mecum.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

There is no attorney-client privilege for in-house counsel in France. They are considered as a distinct profession and do not benefit from the same status as members of the Bar. There are currently discussions at parliamentary level regarding a potential extension of attorney-client privilege to communications of in-house counsel.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There is no legal obligation to notify insurance companies of the launch of an internal investigation. Such notification could even jeopardise confidentiality. However, it is advisable to check whether applicable insurance policies contractually require disclosure.

b) Business partners (e.g. banks and creditors)?

There is no legal obligation to notify business partners of the launch of an internal investigation. However, it should be confirmed that disclosure is not contractually required.

c) Shareholders?

There is no legal obligation to inform shareholders of the launch of an internal investigation *per se*. However, in case an investigation's findings may be characterised as inside information, publicly listed companies must disclose this information (unless an exception allows a delay in disclosure). A duty to disclose the findings of an internal investigation may also be inferred from shareholders' general right to information. Company bylaws or shareholders' agreements may provide enhanced information rights about internal investigations and their findings.

d) Authorities?

There is no legal obligation to disclose the start of an internal investigation to authorities. However, if internal control or audit activities reveal facts of criminal nature, the AFA and PNF Guide recommends notifying the authorities thereof even before the opening of an internal investigation.

Moreover, auditors are legally required to reveal to the prosecutor any criminal offence they become aware of when performing their duties.

As an exception to attorney-client privilege, lawyers are bound by a similar obligation to disclose suspicious transactions regarding money laundering or terrorist financing when acting in an advisory capacity (e.g. advising on the sale or purchase of real estate), rather than as litigators. Generally speaking, a lawyer is considered to be acting as a litigator when they are representing the client in judicial proceedings. In all cases, if the lawyer is acting as a litigator, attorney-client privilege will not be waived.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

There is no legal obligation *per se* to take immediate measures once an investigation is started in France. However, this may be considered on a case by case basis.

Internal investigations and their findings may also be disclosed to authorities in a cooperation effort. Such cooperation effort may be taken into account should the company later face prosecution or sentencing, or in order to reach a settlement with the prosecutor, in particular, to enter into a Judicial Convention of Public Interest (*Convention Judiciaire d'Intérêt Public* or "**CJIP**"), which is a French type of deferred prosecution agreement.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Internal investigations are not completely part of the French legal culture yet, even if they are becoming more and more common. Traditionally, prosecutors did not have specific concerns and did not expect the company to take specific steps.

This has significantly changed with the creation of the CJIP. It is highly advisable that a company which is willing to enter into a CJIP with the prosecutor, participate in the determination of the truth and shows good faith. Conducting an internal investigation may be part of this cooperation effort.

Also, the AFA and PNF guide provides insight on the PNF's expectations regarding the conduct of an internal investigation. Moreover, the guide specifies that internal inquiries should not interfere with the authorities' own investigation.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Dawn raids may be performed (i) as part of a flagrancy enquiry; (ii) as part of a police preliminary enquiry under the authority of a prosecutor; or (iii) under a judicial investigation headed by an investigating judge. Prerequisites for dawn raids vary depending on the type of investigation. For example, absent special circumstances, express written consent of a company's legal representative is required to carry out a dawn raid that is part of a preliminary enquiry, which is not required for a dawn raid that is part of a flagrancy enquiry. Specific conditions may apply to dawn raids carried out in the context of tax, competition, data protection, anti-corruption, and consumer law proceedings.

Save under specific circumstances, dawn raids can only be launched between 6 a.m. and 9 p.m., though they may extend past these hours. Police officers or investigating authorities must establish an inventory of all documents and articles seized and sealed. If these prerequisites are not fulfilled, the seizure of documents may be deemed void and seized documents may not be used as evidence.

Certain formalities of the procedure are prescribed under the penalty of nullity. It is forbidden to use the annulled acts and documents or parts thereof against the parties.

Also, it has to be noted that French law on search warrants and raids is subject to upcoming changes. On 5 January 2023 the Minister of Justice unveiled a plan to rewrite the Code of Criminal Procedure, one of the aims being to simplify the framework for investigations by modifying the rules governing search warrants and raids.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Negotiating deals with prosecutors is not a common practice in France yet. However, the option of entering into deals has become increasingly relevant since the creation of the CJIP.

A guilty plea procedure (*Comparution sur Reconnaissance Préalable de Culpabilité* or "**CRPC**") is available to both individuals and legal entities for most criminal offences. CRPC is mainly used for non-complex cases, which do not require trial, and for which penalties and fines are capped by law. CRPC requires an admission of guilt by the defendant.

In December 2016 the Sapin II Law introduced the CJIP. The scope of CJIP is narrower than that of CRPC: CJIP only applies to legal entities and for criminal offences related to corruption, influence peddling, money laundering, and tax fraud. Unlike CRPC, CJIP does not require an admission of guilt from the defendant. Penalties incurred under a CJIP must be proportionate to the benefits derived from the misconduct and may not exceed 30 percent of the company's average annual turnover calculated by reference to the previous three annual turnovers. The company may also be obliged to implement a compliance programme monitored by the French Anti-Corruption Agency.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Managers and employees of a legal entity may be held criminally liable if they wilfully participated in the commission of an offence. Mere knowledge of the commission of an offence by an employee working under a supervisor is not sufficient to establish the supervisor's criminal liability, provided this supervising employee did not participate in the wrongful conduct. However, a CEO may be held criminally liable when the decision to commit an offence falls within the scope of their authority and such decision is, in practice, approved by the CEO.

Individuals can be fined, imprisoned, and/or subject to additional penalties, such as forfeiture, court-mandated treatments, affirmative injunctions, impoundment, closure of a business, and publication of the conviction.

Like individuals, legal entities may be held liable for criminal offences committed by their corporate bodies or representatives. Legal entities may be punished by a criminal fine and/or additional penalties, such as restrictions on running the business, judicial control of the company, and debarment.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

There is no specific requirement in French law providing for a reduction or suspension of the penalties in case companies implement an efficient compliance system. However, the behaviour of the company is carefully observed when it comes to determining potential sanctions and the possibility for the prosecutor to propose to the company to enter into a CJIP. In this regard, the AFA and PNF guide on internal investigation indicates that "the production of an internal investigation report is also an indication of the robustness of the company's anti-corruption compliance programme, which the public prosecutor's office will appraise with the assistance of the AFA". Moreover, according to the PNF guidelines published in January 2023 the fact that a company subject to the obligation to implement an anti-corruption programme is in default, may be considered an aggravating factor when considering procedural options or determining the public interest fine (up to 20 percent of the fine).

As regards legal persons excluded from the legal duty to implement a compliance programme, voluntary implementation of an effective compliance programme is a favourable indicator for being granted a CJIP.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

The last few years have seen the adoption of a legislative framework governing ESG issues. The Climate and Resilience Law (2021) encourages stakeholders to better assess companies' overall performance through ESG-related criteria. The French Commercial Code and the French Environmental Code now require some companies to publish a non-financial performance statement and an assessment of their greenhouse gas emissions. The Duty of Vigilance Law (2017) aims to identify and deal preventively with or remedy potential violations of human rights and the environment, requiring some companies to report on their national and international activities by drawing up a vigilance plan. The Sapin II Law (2016) involves the implementation of compliance programmes to fight against corruption. The Law on the EU Public Prosecutor's Office, environmental justice, and specialised criminal justice (2020) extended the scope of the CJIP, for the prosecution of offences committed in breach of the provisions of the Environmental Code. France is also the first country to have transposed the European directive on the publication of sustainability information by companies ("**CSRD**").

In France, the risk of litigation and investigation of ESG criteria issues is high and increasing, with several proceedings pending before the courts. NGOs play a key role in actions based on breach of duty of vigilance legislation, misleading commercial practices, or extracontractual liability.

Another major risk of litigation stems from greenwashing environmental claims as sanctioned by the French Consumer Code. These practices are punishable by heavy fines. Regulation is carried out by two main authorities: the *Autorité des marchés financiers* ("**AMF**"), which deals with the reliability of nonfinancial information provided to investors and the *Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes* ("**DGCCRF**"), which deals with misleading environmental claims.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Internal investigations, compliance programmes, and deal negotiations are a growing practice in France. Since the creation of the CJIP, around 50 agreements have been completed. Also, as mentioned, AFA and PNF have recently strengthened their cooperation with the publication of a joint guide highlighting the importance for companies to establish compliance programmes and to respect the protection of personal data as part of internal investigations. The importance of data protection in internal investigations was also put forth by the publication of a guide by the CNIL in July 2023.

CONTACTS

17, avenue Matignon
CS 30027
75378 Paris cedex 08
France

Tel.: +33 1 53 67 4747
Fax: +33 1 53 67 4748
www.hoganlovells.com

Arthur Dethomas
Partner
Hogan Lovells Paris
T +33 1 53 67 1877
E arthur.dethomas@hoganlovells.com

Renowned for his experience in corporate, stock exchange and financial litigation, and in white collar criminal law, Arthur Dethomas is licensed in Paris and in New York. Arthur has developed a recognised competency in complex cases and represents clients before courts as well as regulatory authorities. He has been involved in numerous internal investigations and has substantial experience representing clients in cross-border matters, including insider trading, financial fraud, and the Foreign Corrupt Practices Act.

According to the Chambers & Partners guide "Arthur Dethomas receives very positive commentary from clients who have only positive things to say about him: "he is extremely competent, very well known in the market and calm and measured in his work"; "He is highly experienced in shareholder disputes and financial liability claims" and "wins praise for his ability to design and execute strategies".

Christelle Coslin
Partner
Hogan Lovells Paris
T +33 1 53 67 4706
E christelle.coslin@hoganlovells.com

Christelle Coslin advises global companies on cross-border issues and mass tort litigation, including in a wide range of compliance matters, in particular the drafting, review, and implementation of compliance policies and programmes in light of French law. She also conducts risk assessments with respect to potential criminal liability and evaluates compliance programmes. She can train employees on these matters and prepare clients' organisation for dawn raids or authorities' visits.

She regularly advises clients on anti-corruption laws in both the private and public sectors. She also has significant experience in handling cross-border and/or internal investigations. Thanks to her understanding of the way global groups operate, Christelle is perfectly fit to supervise clients' internal investigations, whether the investigation was initiated by an authority or follows a whistleblower complaint.

Christelle is Co-Head of our global Business & Human Rights practice. Christelle has gained significant experience in advising clients when they are setting up compliance programmes to assess, prevent and address human rights risks of adverse impacts.

Jean-Pierre Picca
Partner
Hogan Lovells Paris
T +33 1 53 67 3853
E jean-pierre.picca@hoganlovells.com

Jean-Pierre Picca has 30 years of experience in the criminal area both as a prosecutor in France and in the United States and as a defence lawyer. He notably performed functions as a Senior Liaison Legal Advisor to the U.S. DoJ between 2002 and 2007. He was involved in landmark cases such as the crash of the Concorde, the Executive Life / Crédit Lyonnais matter and the criminal investigations in the aftermath of the 9/11 terrorist attacks.

A senior Legal Advisor to the President of the French Republic between 2010 and 2012 as well as Senior Prosecutor, Jean-Pierre held a variety of high-level duties within the French judiciary before joining the Firm.

Familiar with Anglo-Saxon legal concepts and American law in particular, he represents his clients, notably financial institutions, in the context of issues relating to complex criminal and regulatory internal investigations, compliance in all its aspects (prevention of money laundering and corruption) and international economic sanctions.

Jean-Pierre also advises several clients on issues issues related to the prevention of corruption, the implementation of ad-hoc compliance programmes and the controls carried out by the French Anti-Corruption Agency.

He teaches a class in Financial regulation at Sciences-Po Paris.

Jean-Lou Salha
Partner
Hogan Lovells Paris
T +33 1 53 67 2369
E jean-lou.salha@hoganlovells.com

Jean-Lou Salha acts as a litigator and advisor to financial institutions and corporates, as well as their senior management, on criminal investigations carried out by French and foreign authorities. He also represents clients at all stages of criminal proceedings connected to fraud, cybercrime, misappropriation of corporate assets.

Jean-Lou has deep litigation experience and advises clients spanning a range of financial institutions and corporates in criminal investigations led by French and foreign authorities, covering a wide range of offences, including corruption, tax fraud laundering, misleading commercial practices and cybercrime. He has significant experience in conducting internal investigations and has specific expertise in compliance with applicable regulations on anti-money laundering, anti-corruption, consumer protection and duty of vigilance.

He also represents clients as part of proceedings initiated by the French Banking Supervisory Authority for breach of consumer protection rules and in administrative and criminal proceedings for misleading commercial practices.

Prior to joining Hogan Lovells, Jean-Lou was a partner in another international law firm and previously worked in the corporate and M&A practice of a leading French law firm. In addition to his white collar and regulatory practice, he has advised listed and non-listed companies on mergers & acquisitions, capital issuances, tender offers and corporate law.

Yaël Michel
Associate
Hogan Lovells Paris
T +33 6 70 63 4503
E yael.michel@hoganlovells.com

Yaël Michel is an Associate in the Paris litigation team with a focus on commercial and civil litigations as well as criminal law and compliance issues.

He regularly advises clients on anti-corruption laws and has significant experience in handling internal investigations.

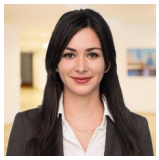
Germany

Hogan Lovells International LLP


Dr. Sebastian Lach


Désirée Maier


Carolin Binder


Angeliki Lampousi

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X*	X	X	X	X
No					

* No criminal liability of companies, but administrative fines possible in case of misconduct of employees.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The German Whistleblower Protection Act ("**HinSchG**"), effective from 2 July 2023, delineates specific requirements for implementing reporting channels and investigating reports. It provides protection to individuals who disclose information about violations connected to their professional activities.
The HinSchG is mostly in line with the EU Whistleblower Directive and has implemented its requirements accordingly. The law only provides for a few deviations from the directive. Notably, the act's material scope is broader than the EU Whistleblower Directive, encompassing criminal offences, fineable offences related to the protection of life, limb, health, or employee rights, and violations of Union law as defined in the Directive.

In addition, discussions in the context of legislation focused in particular on the submission of anonymous reports and the data retention rules. According to the HinSchG, companies should allow whistleblowers to submit reports anonymously. The legislator has deliberately decided against an explicit obligation.
With regard to the data retention regulations, the HinSchG expressly provides for the deletion of the data three years after completion of the procedure, as specified in Section 11 paragraph 5 sentence 1.

Moreover, the HinSchG deals with the handling of notifications that contain information on persons subject to notification and thus personal data within the meaning of Article 4 No. 1 EU General Data Protection Regulation ("**GDPR**"). Compliance with the processing of personal data according to the data protection regulations is essential for the reporting offices.

A significant consideration arises from the tension between the confidentiality obligations outlined in Section 8 paragraph 1 sentence 1 of the HinSchG and the information requirements of Article 14 GDPR, alongside the affected person's right to information under Article 15 GDPR. While the exact relationship between these standards is yet to be conclusively established, it is presumed, subject to further legal clarification, that data protection information and disclosure obligations regarding the whistleblower's identity are typically excluded when the information falls under the confidentiality requirement of

whistleblower law. This necessitates a case-by-case balancing act between the interests in information and confidentiality.

Additionally, the Protection of Trade Secrets Act ("**GeschGehG**"), adopted on 18 April 2019, already included the protection of whistleblowers in certain cases in which they are disclosing trade secrets. According to the law, there is no liability for disclosing trade secrets where disclosure is in the public interest and if the whistleblower reveals relevant information on misconduct, wrongdoing, or illegal activity.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The European Commission contends that group wide reporting systems would not satisfy the Whistleblower Directive's requirements. Companies with more than 50 employees must establish and maintain their own local reporting system for each subsidiary. Contrary to this interpretation, the German legislator permits a centralised group wide reporting system. An independent and confidential entity can be set up as a "third party" responsible for the whole group (e.g. parent company, sister company or subsidiary). This is based on Section 14 paragraph 1, sentence 1, and the explanatory memorandum (BT-Drs. 20/344, 79), explicitly stating the existence of a group privilege in Germany.

In addition, the HinSchG stipulates in line with the EU Whistleblowing Directive that legal entities with 50 to 249 employees may share resources with regard to the receipt of reports and the necessary follow-up measures (Section 14 paragraph 2). The duty to take action to remedy the violation and the duty to report back to the reporting persons remain with the individual employing entity.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) According to Section 80 paragraph 2 of the German Works Constitution Act ("**BetrVG**"), the employer is obliged to inform the works council about the investigation. The involvement of the works council is required if electronic data and emails are reviewed, transferred to external servers, or analysed with software (Section 87 paragraph 1 No. 1 BetrVG, see also "District Labour Court Cologne decision dated 9 May 2019 – 9 TaBV 125/18"). Further, the works council has the right to participate if uniform questionnaires are used that allow a conclusion to the employees' performance (Section 94 paragraph 1 BetrVG). Interviews performed as part of an internal investigation are generally not conducted based on such uniform questionnaires. In addition, an exemption from this participation requirement could be achieved by guaranteed anonymisation of these questionnaires' results. In case of non-compliance, there is the threat of a claim for injunctive relief by the employee pursuant to Section 23 paragraph 33 BetrVG.

b) According to Article 38 GDPR, controllers and processors shall ensure that the data protection officer ("**DPO**") is involved in all issues related to the protection of personal data. One of the DPO's duties is to generally consult the employees concerning their data privacy right. In addition, the DPO has the duty to monitor compliance with data protection regulations. Therefore, the company in general has to inform the DPO about all data privacy-related procedures and processes of an investigation.

c) The prosecution authorities do not have the right to be informed, but a voluntary involvement can be advantageous.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

In general, employees have the labour law duty to cooperate as far as the facts to be investigated relate to activities conducted or perceptions made as part of their work life. They must answer work-related questions truthfully and completely. If unrelated to work, a balancing of interests test is required to determine if a duty to cooperate exists. A relevant factor may, for example, be the employee's position in the company. A supervisory function may lead to greater cooperation duties. A balancing of interests also has to be performed in case the employee is subject to self-incrimination. However, even then, the duty to cooperate generally applies.

In case the employee is required to participate, the employee's refusal may be regarded as misconduct. Such misconduct may justify a dismissal if the employee had already received a formal warning for the same or similar misconduct before.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Investigative measures may trigger the two-week deadline for instant dismissal for cause. This deadline starts when the person of the company authorised to dismiss employees receives knowledge of the relevant facts. The employer should be informed of the results of the investigation at an advanced stage of the investigation after comprehensive information was gathered to avoid triggering this deadline too early. Further, the interviewer should especially avoid using terms such as "interrogation", "hearing", or "questioning". Using such terms increases the risk of triggering labour law deadlines, especially for possible sanctions. Therefore, the interviewer should refer to terms like "meeting" or "interview". Also, employees are generally more willing to participate in an "interview" than in an "interrogation".

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Data privacy laws apply to any processing of data. This includes securing, collecting, and reviewing data, as well as the creation of work products such as interview file notes and final reports. Therefore, it is very important to perform an early assessment of the applicable data privacy laws, document the steps taken, and generally inform the data subjects accordingly.

b) reviewing emails?

Private communication is highly protected under German law. Reviewing such emails may even constitute a criminal offence (breach of telecommunications secrecy) if data privacy requirements are not observed. Therefore, before conducting such an e-data-review, a thorough analysis of legal exposure should always be performed.

c) collecting (electronic) documents and/or other information?

Germany does not have a blocking statute regime. Its data protection statutes are based on the Data Protection Act and the EU General Data Protection Regulation.

Although communication with authorities can trigger the applicability of data protection laws, the request of an authority will often be a sufficient justification for gathering and using data. In critical cases, it may be advisable not to produce data on a voluntary basis but to await a written formal request with the announcement of enforcement from the authority. In addition, the rules of international data transfer apply to document requests by foreign (non-EU/EEA authorities).

d) analysing accounting and/or other business databases?

There is no specific regulation for the analysis of accounting and business databases. In case the databases contain personal data, an assessment of the German and European data protection regulation has to be performed.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no general and statutory obligation to instruct an employee about the legal circumstances and their rights. Nevertheless, many companies in Germany consider explanations to be ethically required and advisable. In general, this includes a brief description on the background of the investigation and the subject matter. For documentation and transparency purposes, it can be advisable to provide these instructions in written form to be countersigned by the interviewee. Such information should also contain a data privacy notification.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

In contrast to an individual's right to remain silent in case of self-accusation during interrogations of criminal authorities, there is no corresponding right with regard to employee interviews as part of internal investigations. However, there are non-binding provisions of the German Federal Bar Association that recommend avoiding any behaviour of the interviewer that might put pressure on the interviewee to incriminate themselves.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

An Upjohn warning must be conducted if relations to U.S. law exist. In addition, giving an Upjohn warning is an accepted best practice in Germany, too. However, there is no explicit legal obligation to do so under German law.

d) be informed of their right to have their own lawyer attend the interview?

Whether or not the employee has a general right to attendance of own counsel has not yet been fully confirmed or denied by case law. The companies often allow such attendance to have a fair set-up and/or if the employee is suspected of having committed criminal offences.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

The employee does not have a strict legal right to be attended by a representative of the works council. However, to reduce potential risks of escalation with the works council and to ensure "equality of arms", companies often allow such attendance.

f) be informed that data may be transferred to another country (in particular to the United States)?

The employee should be informed, and their consent should be requested. Transferring data to a recipient outside the EU/EEA is now only allowed if (in addition to a legal justification for the processing) the requirements for international data transfers with respect to ensuring an adequate level of protection at the recipient outside the EU/EEA are met (Articles 44 *et seqq*. GDPR). In addition, adequate safeguards need to ensure that sufficient data protection is provided.

g) sign a data privacy waiver?

There is no specific law requesting the signing of a data privacy waiver (i.e. consent of the data subject concerned) before conducting an internal investigation. At the same time, consent constitutes a legal basis for processing personal data in accordance with GDPR and BDSG. However, there are strict requirements for consent under the GDPR, in particular for consent requested by employees. Therefore it is generally advisable to (also) rely on the available statutory justifications for data processing (e.g. legitimate interest of

the employer or a works constitution agreement). In certain cases, however, it may be necessary to request a waiver on the secrecy of telecommunications to mitigate potential criminal liability risks.

h) be informed that the information gathered might be passed on to authorities?

Articles 13, 14 GDPR require that amongst other information, the data subject is informed of the recipients or categories of recipients of the personal data. This includes the (potential) disclosure to authorities. In practice, interviewees are also often informed of potential disclosure to authorities.

i) be informed that written notes will be taken?

For reasons of transparency, it should be explained how the information provided will be documented. As far as the documentation contains personal data, the interviewee also has a general right to be informed of the documentation and might also have a right to request access to the data. However, the interviewees' rights are limited to their personal data and do not extend to the entire documentation of the investigation.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law governing this question, but issuing such notices is a common procedure. Such notices should be clear, sent to all potentially relevant addressees, and issued as early as possible. In addition, the data hold has to comply with applicable data protection regulations, e.g. retention periods and deletion duties.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

German privilege rules are very limited. Privilege protection depends mainly on where the documents are located and for what reason they were created.

To ensure privilege, the safest way is to involve outside counsel. In general, documents in custody of external counsel are protected. Documents in custody of the company are, however, only protected in isolated cases. Ideally, newly generated work products should therefore only be available on outside counsel's servers instead of keeping them on the company's premises. This does not mean, however, that any existing document should be moved to outside counsel as this could mean a violation of German criminal laws.

Further, privilege protection will more likely be granted if the advice is provided in relation to a (potential) investigation by authorities. This can be shown by setting up a separate engagement letter for the internal investigation.

It may also be helpful to label privileged documents accordingly to prevent investigators' accidental access. However, the labelling itself does not automatically entail privilege.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Communication with and documents created by inside counsel are generally not privileged under German law. Only individual case law provided higher privilege protection to documents prepared by an inside counsel. According to this decision, documents prepared by inside counsel can be protected if drafted for the purpose of defence by outside counsel. This decision is, however, not yet established. Therefore, there is at least a significant risk that documents created by inside counsel are not privileged.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

As far as circumstances arise that could give reason to a claim against the insurance company, the policy holder should generally make a notification of circumstances to the insurer. In addition, the individual policy should be reviewed.

b) Business partners (e.g. banks and creditors)?

Information duties may arise from contractual obligations between the company and the business partner. Even if there is no explicit provision in the contract, there may be an obligation in case starting an internal investigation is highly important information for the other party and relevant to the purpose of the agreement. These interests of the business partner need to be evaluated against the legitimate interests of the company. Therefore, it depends on the individual case whether and when the business partner needs to be notified.

c) Shareholders?

Potential reporting duties towards shareholders compete with the company's intention to maintain (business) confidentiality. Internal investigations are highly important aspects and could be seen as insider information that may possibly influence the stock price. The company has to evaluate case by case if there is an *ad hoc* duty to report to the shareholders. If the internal investigation affects the market price significantly and fulfils different criteria (e.g. risk of the internal investigation, scope, involved suspects), an obligation to disclose generally exists. In case of a violation of the reporting duties, the company and individuals acting may be held liable to pay damages according to Section 97 paragraph 1 of the German Securities Trading Act ("**WpHG**").

d) Authorities?

In general, there is no duty to inform the prosecutor about an internal investigation or potential misconduct within the company. There may only be exceptions for very significant crimes. However, a cooperative approach with the local prosecutor may prevent adverse and unexpected measures by the authorities, such as dawn raids. It also has to be checked whether the company has a standing cooperation agreement with the authorities.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

The company has to minimise damages and try to prevent new ones to fulfil its supervisory duties. Additionally, the company may have to re-evaluate its compliance system in order to eliminate potential deficits and to improve its existing system. Further, the company may impose sanctions on the concerned employees to show that misconduct is not tolerated inside the company.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices generally appreciate internal investigations through external investigators e.g. law firms. Early involvement, communication, and coordination may be helpful for a good cooperation with local prosecutors. In this regard, it is crucial that the company does not destroy any potential evidence or convey the impression that evidence is or will be destroyed. Therefore, data-retention orders should be communicated at the earliest stage possible.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Both search warrants and dawn raids must fulfil formal and material requirements stipulated by law.

In general, the search warrant has to be issued by a district court or – in case of imminent danger – by the prosecutor. It has to be written and signed (unless in case of imminent danger). Further, it has to describe the alleged facts and the offence that the individual is being accused of. The search warrant also has to indicate what evidence is expected to be found and why it is expected to be found at the particular place of the search. Further, there must be a reasonable suspicion that an offence was committed based on the experience of a criminal investigator. In addition, the search warrant, but also the dawn raid itself, has to be based on reasonable balancing of interest decisions. According to German case law, a search warrant is only valid for six months.

In case these legal requirements are not fulfilled, generally, the seized evidence may still be used in court proceedings. In Germany, there is no absolute "fruit of the poisonous tree" doctrine. Only in severe cases of illegally obtained evidence, the evidence may not be used in court. This may be the case if there was no reasonable suspicion of a criminal offence or if the decision was made without balancing the interests of the searched individual/ company with the state's interest to prosecute. Formal legal requirements, such as a missing signature, will generally not lead to a prohibition of use of the seized evidence. According to German case law, exceptions can only be made in very severe cases, e.g. if the investigating authorities acted arbitrarily.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

While deals and non-prosecution agreements are available for individuals, they are not provided for corporations under German law yet. The draft law on the sanctioning of companies (*Verbandssanktionengesetz* – "**VerSanG**") aimed to introduce alternative sanctions that would correspond to deals and non-prosecution agreements. However, due to disagreements within the governing coalition, the draft was no longer discussed during the last legislative period and was not taken up again as an agenda item by the new government in 2022.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Although companies are not subject to criminal responsibility under German law, they can be subject to legal consequences, such as administrative fines, disgorgement, and debarment.

Individuals may face sanctions not only for their own misconduct but also for misconduct of other employees when they failed to implement a sufficient supervisory structure. Therefore they may face sanctions such as imprisonment, fines, or official debarment from their profession.

In the report is covered by the HinSchG, sanctions include a fine on the company of up to €50.000, especially if the system is not implemented properly or if the confidentiality of a report is breached. Sanctions can be also imposed on operators of the reporting office if they infringe confidentiality obligations intentionally or negligently.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

An efficient compliance system is a key factor for preventing or reducing corporate sanctions in Germany. If a company does not have an adequate compliance system to prevent misconduct and criminal offences of its employees, it might be sanctioned with an administrative fine of up to €10 million plus disgorgement of profits according to Articles 30 and 130 of the German Administrative Offences Act ("**OWiG**"). Such a fine requires an administrative or criminal offence constituting a breach of business-related duties by an employee in a managing position or a breach of supervisory duties.

An efficient compliance system should already be in effect when the alleged misconduct occurs to avoid such a breach. If this can be shown to the authorities, the compliance system will most probably have a reducing effect on a sanction or may even prevent a sanction in the first place. Even if an efficient compliance system has just been established as a consequence of misconduct, the implementation might have a reducing effect on a fine in case the new system ensures the prevention of similar future misconduct (see Federal Court of Justice, decision dated 9 May 2017 – 1 StR 265/16). In practice, prosecutors often tend to assess the compliance measures in place as insufficient. Therefore, documentation of the measures taken is very important.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

The German Supply Chain Due Diligence Act ("**LkSG**") mandates companies with at least 1,000 employees in Germany to actively monitor and mitigate human rights and environmental risks within their respective supply chains, covering the entire process from the extraction of raw materials to the distribution of the final product to the end consumer. The supply chain due diligence obligations are tiered and cover the company's own operations, its direct suppliers and, to a limited extent, even its indirect suppliers. The LkSG provides robust safeguards for both environmental and human rights concerns.

In cases where due diligence and reporting obligations are not met, fines ranging up to €8 million can be imposed, depending on the severity and nature of the violation. For companies with an annual turnover surpassing €400 million, fines can reach up to 2 percent of the average global yearly turnover of the economic entity (i.e. group).

It can be assumed that the competent authority, the Federal Office of Economics and Export Control (BAFA), will continue to proactively enforce the obligations of the LkSG also in 2024. Initial documents from BAFA suggest a very extensive interpretation of the obligations, meaning that particular attention must be paid to the precise implementation of the legal requirements.

Besides that, increasing media coverage shows that cases of fraud in connection with ESG reporting and public awareness of this are on the rise.

Particularly noteworthy is the spectacular search at the stock exchange-listed DWS Group at the end of May 2022 on suspicion of investment fraud through "greenwashing". DWS, a large investment manager controlled by Deutsche Bank, was accused by its previous head of sustainability of making incorrect statements about the size of ESG-compliant investments. Authorities are considering this case under the accusation of investment fraud, defined in Section 264a of the German Criminal Code (StGB), which may stem from deliberately incorrect or false presentations of ESG aspects. This underscores the importance for companies to establish a strong connection between sustainability, capital market compliance, and fraud prevention.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The VerSanG published in June 2020 was not further addressed in the last legislative period due to disagreements within the governing coalition. The original draft included the introduction of the obligation of the Public Prosecutor to initiate proceedings upon strong and grounded suspicion of a company's offence and a much wider range of sanctions for companies. The issue was also not addressed in the current coalition agreement.

Additionally, the number of dawn raids in Germany continues to be on the rise. Therefore, preparing for dawn raids is becoming even more important.

Furthermore, the BAG has confirmed (decision dated 29.4.2021 – 8 AZR 276/20) that employers may claim compensation from employees for the necessary expenses of an internal investigation by an external law firm. This claim may apply if there was a concrete suspicion of significant misconduct and the employee is convicted of a serious intentional breach of contractual obligations. However, the employer must show that the expenses were necessary and substantiate the specific investigation measures the commissioned law firm carried out due to the specific suspicion against the employee.

CONTACTS

Hogan Lovells

Karl-Scharnagl-Ring 5
80539 Munich
Germany

Tel.: +49 89 29012 0
Fax: +49 89 29012 222
www.hoganlovells.com

Dr. Sebastian Lach
Partner
Hogan Lovells Munich
T +49 69 96236 308
E sebastian.lach@hoganlovells.com

Sebastian Lach leads the German Compliance and Investigations practice and is co-CEO of ELTEMATE – the Hogan Lovells technology company.

Sebastian has successfully advised on a wide range of criminal investigations relating to more than 50 countries, including FCPA, SEC/DOJ implications. He is therefore familiar with appropriate use cases for all major eDiscovery platforms and tools as well as databases. Most of his investigations for Fortune 500 and DAX 40 clients included vast technology-driven data forensics, including data collection, data processing and data review. With his understanding of technology in the legal industry, he was instrumental in developing the firm's legal tech strategy. In his role as Co-CEO of ELTEMATE, he leads a market-leading team of AI experts, data scientists, software engineers and data analytics professionals focused on developing innovative AI solutions, particularly in the area of generative AI.

Sebastian Lach utilises his extensive experience of over 15 years working at the intersection of technology and legal practice to advise clients on the selection and implementation of cutting-edge legal tech solutions.

Désirée Maier
Partner
Hogan Lovells Munich
T +49 89 29012 340
E desiree.maier@hoganlovells.com

Désirée Maier advises clients on issues relating to white-collar criminal law and compliance. She has particular expertise in the life sciences and health care sector.

One focus of her work lies on setting up and conducting cross-border investigations and in the defence against allegations of a criminal nature. She has extensive experience in advising during dawn raids, coordinating compliance of investigations with requirements under German, local law, U.S. and UK law as well as communicating with law enforcement authorities.

Désirée also regularly advises on the establishment and implementation of global compliance systems, including the performance of compliance audits. In addition, she has expertise in connection with civil law claims arising from compliance matters.

Désirée worked in the legal department of a U.S. Fortune 500 company with global responsibility for internal investigations and is head of the compliance working group of the German Mergers & Acquisitions Association.

Carolin Binder
Associate
Hogan Lovells Munich
T +49 89 29012 841
E carolin.binder@hoganlovells.com

Carolin Binder advises national and international companies on white collar crimes, compliance and internal investigations. One focus of her work lies in the area of preventive compliance, including the revision and implementation of global compliance systems, in particular the implementation of global whistleblower systems.

In addition, she also advises clients on the set up and management of highly complex internal investigations, often in the context of public prosecutor investigations.

Carolin Binder studied law in Göttingen and Valencia. Prior to joining Hogan Lovells, she worked as legal trainee in international law firms. As part of her legal clerkship, she worked at the Federal Foreign Office in Berlin. She obtained a Master of Laws (LL.M.) from the University of Melbourne, Australia.

Angeliki Lampousi
Foreign Associate
Hogan Lovells Munich
T +49 89 29012 486
E angeliki.lampousi@hoganlovells.com

Angeliki Lampousi works on white collar crime related topics for national and international clients, including Fortune 500 and DAX 40 companies. She has particular experience in setting-up and conducting internal investigations.

Angeliki studied law at the National and Kapodistria University of Athens. She also holds a Master degree in European and International Economic Law (LL.M. Eur) from the Ludwig-Maximilians-Universität München.

Prior to joining Hogan Lovells, Angeliki Lampousi worked for various international and greek companies, including the European Central Bank of Greece.

Greece

Ovvadias S. Namias Law Firm

Dr. jur. Ovvadias Namias

Prof. Dr. Vasileios Petropoulos

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X*	X	X	X**	X
No					

* Criminal liability of legal entities only in bribery crimes after 23 February 2024. Otherwise, legal entities may only be liable for administrative violations, though company directors may be held criminally liable.

** Only in bribery cases.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The EU Whistleblower Directive was implemented in Greece in November 2022 through Law 4990/2022 ("**Whistleblowing Law**"). It is noteworthy that the material scope outlined in Article 2 (1) of the Directive is identical to that of the transposing law, as stated in Article 4 of the Whistleblowing Law. This means that the national transposing law protects only individuals reporting or disclosing breaches of EU law in the same areas covered by Article 2 (1) (a) of the Directive. Consequently, reports of infringements under national law or internal regulations (including criminal offences such as theft or embezzlement) are not protected under the Whistleblowing Law. Therefore, the reversal of the burden of proof against the employer does not apply to reports outside its material scope.

On the other hand, a whistleblower reporting bribery in the public sector may receive some protection if granted "witness of public interest" status under Article 47 of the Greek Criminal Procedure Code. This status is conferred by order of the special financial prosecutor and confirmed by the Supervisor of the Department of Financial Crime, responsible for supervising financial prosecutors. A "witness of public interest" is shielded from retaliation in criminal, administrative, and labour law proceedings. For example, if a criminal complaint is filed against a "witness of public interest" for defamation as a result of their report, the prosecutor has the discretion to refrain from pursuing charges. Similarly, a public servant with "witness of public interest" status cannot be terminated or otherwise subjected to retaliation due to their report.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Legal entities with more than 50 employees are obliged to set up an internal reporting channel, irrespective of the nature of their activities and the duration of each employee's employment within the year (Article 9 (1) of the Whistleblowing Law, in line with the EU Whistleblower Directive).
By way of exception, private sector entities operating in the financial services, products and markets, and transport sectors, as well as entities operating under a decision approving environmental conditions or whose activities may, by their nature, pose a risk to the environment and public health, are required to set up an internal reporting channel, irrespective of the number of employees they employ (Article 9 (4) of Whistleblowing Law).
Furthermore, companies with more than 50 and up to 249 may share and manage internal whistleblowing channels.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

There is no specific Greek law concerning the conduct of an internal investigation. There are, however, some rules which could apply:

a) Presidential Order 240/2006 (which implemented Directive 2002/14/EC of the European Parliament and Council of 11 March 2002) concerning the relations between employees and employers indicates that a works council has the right to be informed about an upcoming internal investigation and an obligation to keep it secret. There is, however, no provision concerning the active participation of the works council in an internal investigation.

b) Greek data protection legislation (Greek Data Protection Law 4624/2019 and the EU General Data Protection Regulation 2016/679) requires to inform the data protection authority before starting an internal investigation if the investigation results in the processing of employee personal data. This does not apply if the data subject consents to the processing.

c) Performing an internal corporate investigation falls within the employer's managerial authority. This means that there is no general obligation for the company to inform other public authorities thereof. On the other hand, if the internal investigation reveals an upcoming performance of a felony, not reporting this to the criminal authorities would result in the misdemeanour of harbouring a criminal.

The Whistleblowing Law mandates that the Labour Inspectorate must be notified about the establishment of internal reporting channels, including the designation of a person responsible for receiving and monitoring reports. This notification is facilitated through the use of a standardised information form.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

In general, there is no specific labour law obliging employees to support internal investigations and employees are generally not obliged to report misconduct. However, an obligation to participate in an internal interview could

derive from the general fiduciary duty towards the company (the "bona fides rule" under Articles 288 and 652 of the Greek Civil Code, as recognised in the Greek jurisprudence).

In addition, employees with a special duty to report misconduct, e.g. members of the compliance department, must support the company's internal investigation or face criminal liability. Imposing disciplinary measures on an employee for refusal to cooperate during an investigation is a matter of internal company regulation.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

There are no specific deadlines to dismiss for cause if a company uncovers employee misconduct. Although a company should, in practice, act as quickly as possible, the company must be careful when sanctioning employees so as not to give the wrong impression (e.g. if the only aim of the internal investigation is to release employees without compensation).

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Greek constitutional law protects the privacy of telephone and email communication as well as access to personal data. If an interview is recorded or summarised, the company should seek the employee's consent. Creating an archive of all employee interviews must additionally be announced to the Greek data protection authority.

b) reviewing emails?

Telephone and email communication is protected by communication privacy laws during the communication itself. The content of the communication is protected as personal data by the data protection legislation. If an internal investigation results in the processing of employee personal data, the Greek data protection authority must be notified in advance unless the employee consents to the processing.

Emails sent from or received by an employee via their corporate email address are protected as personal data (Article 9A of the Greek Constitution and Law 4624/2019). However, this protection is not absolute. The Greek Supreme Court decided in plenum that it can be limited according to the proportionality principle (Article 25 of the Greek Constitution) when the employee has acted against the company. This view is shared by the Greek data protection authority. It is not clear whether this limitation also applies to employees who have not acted against the company's interests but may have been implicated in an investigation. In such cases, it is recommended to seek the employees' consent. In any case, it is crucial that the company has previously enacted internal rules concerning the proper use of the corporate computers.

c) collecting (electronic) documents and/or other information?

The collection of electronic documents and/or other information might violate Greek data protection legislation. It is, therefore, recommended to either inform the Greek data protection authority about the classification of this information during the internal investigation or seek the employees' consent. Once more, it is crucial for the company to enact internal rules concerning the proper use of corporate computers, forbidding the employees from using them for personal reasons.

d) analysing accounting and/or other business databases?

The Greek data protection authority should be informed in advance if the databases contain personal data.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no specific labour law on this topic. It is, therefore, a matter of internal company regulations.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

In contrast to criminal procedure, the "*nemo tenetur*" principle does not apply in private law. Therefore, the company has no legal obligation to instruct the employee about self-incrimination. Internal company rules may, however, provide such an obligation.

If the company provides the interview material to the prosecution authorities, a criminal procedure may not start against the interviewee exclusively based on their interview. This would violate the "*nemo tenetur*" principle. However, in practice, the prosecuting authorities will most likely proceed with the initiation of a criminal procedure using supplementary material (e.g. interviews with colleagues).

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no such obligation according to Greek labour law. However, without prejudice to the internal rules of a company, a general briefing of the interviewee on this point is advisable.

d) be informed of their right to have their own lawyer attend the interview?

There is no such obligation according to Greek labour law. However, without prejudice to the internal rules of a company, informing the employee is recommended.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

There is no such obligation according to Greek labour law.

f) be informed that data may be transferred to another country (in particular to the United States)?

It is recommended to advise the employee about potential data transfers, as it would indicate that the data subject consents to the processing of their data. Informing the employee may count as silent consent if the employee is not opposed to the transfer.

g) sign a data privacy waiver?

It is recommended to ask the employee to sign a data privacy waiver. Informing the Greek data protection authority before starting with the processing of the data is generally mandatory unless the data subject consents to the processing.

h) be informed that the information gathered might be passed on to authorities?

As with cross-border data transfers, it is recommended to advise the employee about potential recipients of the data, as it would indicate that the data subject consents to the processing of their data. Informing the employee may count as silent consent if the employee does not object.

i) be informed that written notes will be taken?

It is recommended to inform the employee that notes will be taken as these notes might also be considered "personal data". Informing the employee may count as silent consent if the employee does not object.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Internal investigations are not common in Greek practice yet. A company can issue documents-hold notices or document-retention notices. The employees will have to comply with them based on the bona fides rule (Articles 288 and 652 of the Greek Civil Code, as recognised in the Greek jurisprudence).

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege is established in the Code of Lawyers. It is binding for all lawyers registered with the Bar, irrespective of their status as freelancers or in-house counsel. The privilege protection extends to documents, objects, data, or information obtained in the course of their representation of the client and applies to internal investigations.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

The attorney-client privilege is binding for all lawyers registered with the Bar, including in-house counsel. Nonetheless, it is possible that, according to internal company policy, only specific employees of the company, e.g. the President, Vice President, or the members of the Board of Directors, are considered the "clients" of in-house counsel. Hence, not all employee communications with in-house counsel may be protected by this privilege.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There is no general legal obligation to notify an insurance company of the start of an investigation. Nonetheless, such an obligation might be provided by the insurance contract.

b) Business partners (e.g. banks and creditors)?

A company is not generally obliged to inform its business partners as soon as it starts an investigation. However, the relationship between the parties might give rise to a notification obligation.

c) Shareholders?

If a company's shares or other financial instruments are traded in the stock exchange, the company is generally obliged to inform the public about important issues, including an ongoing investigation, if the internal investigation would be considered insider information under applicable capital market regulations. However, the company is not obliged to provide early notification of the start of an investigation.

d) Authorities?

Companies are not obliged to notify criminal authorities about the initiation of internal investigations unless there is specific knowledge that a felony is about to be committed. Nonetheless, informing data protection authorities about such investigations might be required, as described above.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Measures to eliminate or limit compliance violations should immediately be taken (e.g. giving the legal department control of production or finance, sanctioning liable personnel, and rethinking the compliance structure of the company). Depending on the alleged conduct and the sensitivity of each case, company management is typically advised to contact the competent administrative authorities (e.g. the Capital Market Commission or the Competition Commission). If applicable, company management may also contact the prosecuting authorities and declare the company's willingness to minimise damages and prevent further harms. The competent state authorities might call on the company to re-evaluate its compliance system or impose sanctions on employees. The company's cooperation is a clear mitigating factor should the authorities impose administrative fines.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Greek prosecutor offices have little experience with internal investigations. The results of an internal investigation may lead prosecutors to officially open a criminal proceeding by ordering a pre-trial inquiry. Within this inquiry, the company's officials are likely to be summoned either as witnesses or, more probably, as defendants. This has been the case in several recent criminal cases in the pharmaceuticals industry. In a recent market manipulation case, however, the Greek prosecution authorities started using the results of an internal investigation, which were delivered to them by the company itself, without conducting their own investigative measures. Following the latest changes of the Criminal Code (Law 5090/2024), the conduct of internal audits is now explicitly considered as a mitigating circumstance for legal entities in cases of corruption offences. The implementation and consideration of internal investigations by companies, as well as their recognition by the public prosecutor's office, will be observed in practice.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

According to the Greek Criminal Procedure Code and the Greek Constitution, every search performed by law enforcement officers in the suspect's residence or the company's seat requires the presence of a judge (including magistrate judges) or prosecutor (prosecutors in Greece are part of the judicial authority in the broad sense). Therefore, there is no procedure prescribed in Greek law concerning the issuing of a search warrant by the court. Dawn raids are similarly performed by prosecution (police) officers in the presence of a judge.

In practice, searches and dawn raids are usually performed at the stage of primary investigation of a felony. However, in cases of flagrant offences, or if there is imminent danger of losing important material evidence, law enforcement officers may directly proceed with a search or raid. They are then obliged to compose a written report (e.g. about the material they confiscated), which must be immediately submitted to the prosecutor.

Further serious investigative actions, such as surveying the company's seat, can only be performed after approval by a Judicial Council and only in serious cases as described in Article 254 and 255 of the Greek Penal Procedure Code. If the prerequisites for performing searches or dawn raids are not fulfilled, the evidence is, in most cases, considered illicit and cannot be used against the company.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Until July 2019, there were no legal provisions for non-prosecution agreements or deferred prosecution agreements in Greece. Since then, Greek prosecution authorities have been entitled to perform under the principle of opportunity. The new Articles 48 and 49 of the Greek Penal Procedure Code permit them to refrain from prosecuting several crimes, including several financial felonies, under specific conditions (e.g. full restitution of the victim, donation to charity programmes etc.). However, NPAs or DPAs are still not common. In practice, the behaviour of the defendant during the procedure is generally evaluated by the court at the hearing stage either as a mitigating factor or as an indicator of a lack of *mens rea*.

With respect to white collar crimes against the Greek State (e.g. tax and economic crimes), there is also a growing trend that criminal authorities do not press charges or press only minimal charges against defendants who fully compensated the State.

The latest criminal reform legislation (Law 5090/2024) introduced, for the first time in Greece, a criminal negotiation procedure applicable to legal entities as well. Under this provision, the liable legal person or entity is entitled, until the formal conclusion of the main investigation, to request a criminal negotiation procedure with the prosecutor's office, focusing solely on the sanction to be imposed. The practice will show how this kind of "deal" will be carried out.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

The latest criminal reform legislation (Law 5090/2024) introduced criminal liability for legal persons and legal entities in bribery offences (see point 18).

Apart from bribery crimes, there are no criminal sanctions for companies in Greece. There are, however, administrative sanctions, mainly fines, as well as the sanction of exclusion from business with the Greek State or revocation of permission. These are primarily described in the special anti-money laundering legislation.

Directors may, in contrast, be held criminally liable for the misconduct of employees, but only when, according to their duties, they were appointed with the specific obligation to prevent the misconduct at issue. Hence, it is important for a company to maintain a clear corporate governance diagram.

Felonies are severely penalised with up to 20 years of imprisonment, though actual prison time differs from case to case. Misdemeanour incarceration sentences were usually suspended. Under the Penal Code of 2019, they could no longer be converted to monetary penalties but only to community service. After the last legislative change of Law 5090/2024, however, the limit of the suspension of the execution of the sentence has been significantly reduced. Thus, sentences exceeding two years' imprisonment will now mandate partial execution. These provisions will enter into force from 01. May 2024 and the practice will show how they will be implemented. Consequently, individuals convicted of minor offences may now face incarceration, serving a portion of their sentence.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

There is no general provision obliging Greek criminal authorities to reduce or suspend a penalty imposed on the company officers due to implementing an efficient compliance system. However, there is a specific reference in the recent legislation regarding criminal liability of legal entities in bribery cases. According to this legislation, conducting an internal investigation that contributes to the detection of the infringement is considered a mitigating factor. Such actions should be based on an efficient compliance system. Furthermore, the absence of such a system might trigger criminal liability for directors in bribery cases in the public sector. An efficient compliance system is generally considered a mitigating factor when imposing administrative penalties on the company.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

German Companies operating in Greece, most notably Fraport, are adhering to a political commitment to extend the protection of human rights and the environment to their global supply chains. In this regard, they are aligning themselves with the German SCDDA. Currently, there is no relevant Greek legislation on this matter; instead it predominantly remains a subject of company policy. However, with view to the EU Taxonomy regulation, this is expected to change.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The latest reform of criminal code and criminal procedure code, enacted through Law 5090/2024 on 23 February 2024, introduced criminal sanctions for legal entities in bribery offences for the first time in the Greek criminal system. Additionally, for the first time it makes specific reference of internal investigations. According to Art 134 of this Law:

– If a bribery offence is committed for the benefit or on behalf of a legal person or entity by a natural person who acts either individually or as a member of a body of the legal person or entity, and holds a managerial position within them, or has the power of representation or authority to make decisions on their behalf, a fine ranging from €50,000 to €10 million shall be imposed on the legal person or entity. The fine may be up to twice the annual net profit before tax of the legal person if this amount exceeds 10 million euros. Where the lack of supervision or control by person holding a managerial position has made it possible for a subordinate manager or a person acting on behalf of the legal person or entity to commit any of the acts referred to in that paragraph for the benefit or on behalf of the legal person or entity, the legal person or entity shall be fined from €10,000 to €5 million;

– In the imposition and assessment of such penalties, all relevant circumstances shall be taken into account, particularly the actions of the legal person or entity following the commission of the infringement, including the conduct of an internal investigation which contributed to the detection of the infringement;

– Furthermore, the liable legal person or entity shall be entitled, until the formal conclusion of the main proceedings, to request, through a written statement by the person authorised to represent the legal person or entity, the opening of a criminal negotiation procedure, the subject of which may only be the sanction to be imposed.

In Greek case law, internal investigations are further discussed mainly in four different constellations:

First, when the outcome of an investigation conducted abroad becomes part – through mutual legal assistance – of the pending case file of the Greek investigating authorities. Second, when an investigation report drafted abroad becomes indirectly part of the domestic case file as part of evaluated material by a foreign authority sent through mutual assistance. The third constellation involves investigations by the Greek Capital Market Commission of listed companies regarding potential administrative sanctions. The investigation's outcome then sometimes becomes part of the case file of the respective criminal matter. The fourth constellation concerns investigations regarding potential criminal complaints about property offences against the company or breaches of trust against credit institutions. From 2019 to 2024, these offences were not considered *ex officio* crimes (see Article 405 of the Penal Code). Thus the Board of Directors could decide to file or refrain from filing the criminal complaint based on the investigation report. This legislation still applies to criminal acts that may take place until May 2024 as the most lenient law.

Although no specific legal provisions for internal investigations exist, the following should be kept in mind:

– Article 45 of the Anti-Money Laundering Law, under which the company's behaviour (i.e. conducting an internal investigation) limits possible administrative actions and sanctions;

– Article 102 of the Public Companies Act, under which the Board of Directors shall not be liable if its actions or omissions rely on the opinion or evaluation of an external expert;

– Article 263a of the Greek Penal Code, which restricts criminal liability for bribery offences if the suspect discloses information about the respective offence.

In addition, a potential legislative change could allow the Greek Capital Market Commission to require listed companies at their expense to conduct internal investigations to clarify potential criminal offences.

It has to be pointed out that the field of internal criminal investigations is gaining public attention. Many reasons led to the growing practice of internal criminal investigations in Greece already established in other countries: the improved financial situation; the improved and modernised socio-economic structures and institutions; the strengthening of Greece's competitive advantages; the stabilised political scene; and the call for a more effective and trustworthy administration of justice.

Furthermore, the practice has proven that companies are advised to have independent criminal law firms conduct the internal investigations for a series of reasons: establishment of client-attorney privilege, guarantees regarding the collection of evidence, evaluation and proper use of the findings, and expertise in the investigation's field.

Finally, and this is of particular importance, despite the criticisms of the theory and the ambiguity in how it will be applied in practice, the provision on the criminal liability of legal persons has been viewed as a precursor to the introduction of a criminal law for legal persons in general.

CONTACTS

OVVADIAS S.NAMIAS Law Firm

16, Voukourestiou Street
106 71 Athens
Greece

Tel.: +30 210 7239738
+30 210 3639793
Fax: +30 210 7239773
www.namiaslaw.gr

Dr. jur. Ovvadias Namias
Managing Partner
Ovvadias Namias Law Firm
T +30 210 7239738
+30 210 3639793
E ovvadias.namias@namiaslaw.gr

Ovvadias was born in Athens in 1964 and has been a member of the Athens Bar Association since 1993. He graduated from the Law Department of the University of Athens and received his PhD in Criminal Law from the University of Bonn in Germany. He lectured in the Law Department of the University of Athens and was an Attorney at Law of the National Bank of Greece for criminal matters from 1999 to 2006. He has been a member of the Board of Directors of the Hellenic Criminal Bar Association since 2004. He was awarded the Babakos Prize by the same Association in 2001. He is the acting President of the General Assembly of the Jewish Community of Athens. In 2006 Ovvadias established the Law Firm Ovvadias Namias. As a Managing Partner of the Firm, he managed major penal cases for crimes relating to the banking, stock-exchange, tax, customs office sector, crimes relating to the legalisation of profits from illegal activities (money laundering), the environment, personal data and sports, in all instances of the criminal courts. He also has experience in cross-border regulatory compliance and internal criminal investigations.

Ovvadias is fluent in English, German, and French.

Prof. Dr. Vasileios Petropoulos
Partner
Ovvadias Namias Law Firm
T +30 210 7239738
+30 210 3639793
E vasileios.petropoulos@namiaslaw.gr

Vasileios was born in Athens in 1980. He received his education at the Universities of Athens (2001, LL.B.), Munich, Ludwig Maximilian Universität, (LL.M, in German Law 2003; PhD in criminal Law 2005; "Habilitation" and Venia Legendi in Criminal Law, Criminal Procedure Law, European and International Criminal Law, Economic Criminal Law 2010) and Zurich (PhD in Capital Market Law 2008). He is an assistant Professor in the Faculty of Law at the National and Kapodistrian University of Athens.

Vasileios is a Partner of the Law Firm Ovvadias Namias. He joined the Law Firm in 2010 and has been a member of the Patras Bar Association since 2003.

Vasileios is fluent in German and English.

Hungary

Hogan Lovells Budapest, Partos & Noblet

Dr. András Multas

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The EU Whistleblower Directive (Directive (EU) 2019/1937) has been implemented in Hungary on 25 May 2023 by Act XXV of 2023 on complaints, disclosures in public interest, and related rules of whistleblowing notifications ("**Whistleblowing Act**").

The whistleblower may make the report in writing or orally. The internal whistleblowing system must be designed in such way that it prevents access to the personal data of the reporting person who reveals his identity. In addition, the provisions of the Whistleblowing Act establish further protection for whistleblowers by stating that all measures adversely affecting the reporting person for making the report lawfully will be deemed unlawful even if it would otherwise be lawful.

Furthermore, in the case of a lawful report, the whistleblower may not be considered to have breached a restriction on the disclosure of a secret protected by law or any other legal restriction on the disclosure of information, and may not be liable in respect of such a report, if the whistleblower had reasonable grounds to believe that the reporting of such information was necessary for revealing the circumstances affected by the report.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The Whistleblower Act sets out that employers with more than 50 but fewer than 250 employees employers may establish an internal whistleblowing system jointly, and/or together with another employer who is qualified to do so.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Employee representative bodies do not have the right to be informed about an internal investigation, however the investigator may inform them if deemed helpful under the given circumstances in the specific situation.

b) According to the General Data Protection Regulation ("**GDPR**") it is generally not mandatory to employ a data protection officer ("**DPO**"). The Whistleblowing Act does not contain any specific rules for notifying the DPO. However, the DPO can be a member of the investigation team, in which case they will be informed. There is no obligation under applicable law to notify the Hungarian data protection authority of the launch of an investigation.

c) Authorities have no right to be informed until the investigation is completed. After completion, the competent authorities may need to be informed, depending on the outcome of the investigation. If a criminal offence is confirmed, such an offence must be reported.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

The Labour Code provides that, as a general principle, employment relationships are governed by the principle of good faith and fair dealing. This may imply a duty to cooperate, as employees are not allowed to behave in a manner that violates the rights or legitimate interests of the employer.

An internal whistleblowing policy can establish a more concrete obligation for employees to cooperate. Breach of such an obligation can lead to disciplinary action if specified in the applicable collective bargaining agreement or in the employment contract. A disciplinary action can be a written warning, limited financial penalties, and/or the termination of the employment contract. Even if not specified in the collective bargaining agreement or employment contract, failure to comply with an internal policy can still result in the termination of the employment contract, depending on the seriousness of the breach.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

The employer's right to terminate an employee with immediate effect must be exercised within 15 days of discovery of the grounds for termination, but, in any case, must be exercised within one year after the misconduct occurred, or, in the case of a criminal offence, up to the expiration of the statute of limitations. Based on applicable case law, the 15-day deadline is triggered when the person or body entitled to issue the termination notice takes sufficient note of the facts to make the decision. In case of an ongoing investigation, the 15-day deadline does not start until the investigation is completed or at least at an advanced stage. The Whistleblowing Act provides that an investigation must be completed within the shortest time possible within the circumstances, not exceeding thirty days from the date of receipt of the report, which may be extended in exceptional cases, but, in any case, may not take longer than three months.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

When processing data concerning the interview, data privacy laws apply to the collection and processing of data, in particular, the GDPR and Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information. The Whistleblowing Act states also that the personal data of the whistleblower, the reported person and the person who has relevant information about the report, which are essential for the investigation of the report, may be processed solely for the purpose of investigating the report and remedying or stopping the conduct that is the subject of the report. Personal data may be transferred to the whistleblower protection lawyer or external organisation involved in the investigation of the report.

b) reviewing emails?

According to the Labour Code, an employer is obliged to inform employees in advance about possible access to, or monitoring of, their emails and devices. Moreover, pursuant to the GDPR, the employer is obliged to inform employees about all processing of personal data. This is usually accomplished with an internal policy. The distribution of the policy must be documented by the employer.

According to the GDPR, emails can only be accessed, stored, and monitored by the employer for a legally justified purpose, and access, storage, and monitoring must be limited to the review of necessary data. The Labour Code adds that monitoring must be limited to the employee's actions in relation to the employment relationship. The monitoring of private communications is prohibited. Hence, even where the employee uses office IT devices for private purposes, the employer cannot process private content and must delete it from backup copies. According to a decision of the Hungarian Data Protection Authority in an individual case, if the employee is allowed to store private information on the office computer's hard drive and use the office email address for private purposes, the employer must provide the employee time to remove this information before the monitoring starts. However, unless expressly permitted by the employer, it is prohibited to use corporate devices for personal purposes.

c) collecting (electronic) documents and/or other information?

If the collection of documents and other information involves the monitoring of the employee's computer and/or other devices, the rules set out in section 6b apply.

d) analysing accounting and/or other business databases?

There are no rules under Hungarian law that would impede the use or review of accounting and business databases during an investigation.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

According to the Whistleblowing Act, on submission of their complaint to the employer, the whistleblower must be informed of procedural deadlines, the possibility that a personal interview may be necessary, the consequences of a report submitted in bad faith, and the possibility to submit anonymous reports. The subject of the report must be informed, in detail, of the report concerning them, their rights, and the rules of procedure at the beginning of the investigation. While the affected persons must be informed about their procedural rights, there is no obligation for the investigators to hand out written instructions to the whistleblower.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

In contrast to an individual's right to remain silent during interrogations by criminal authorities, there is no corresponding right for employee interviews as part of internal investigations.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no explicit legal obligation to provide an "Upjohn warning" under Hungarian law.

d) be informed of their right to have their own lawyer attend the interview?

According to Section 27(2)of the Whistleblowing Act, investigators must ensure that the subject of the whistleblower report has the opportunity to seek legal representation before giving a statement regarding the report. This provision does not specify whether the legal representative may be present at the interview. However, Section 27(2) appears to imply a right to have a lawyer present.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

The attendance of an employee representative body is only possible if it is necessary for the investigation. The protection of the whistleblower and the investigation is the first priority.

f) be informed that data may be transferred to another country (in particular to the United States)?

Employees should be informed of all details concerning the processing of their data, including the transfer of personal data within Hungary, within the European Union, or to a third country, such as the United States. It is advisable to explain this possibility in the whistleblowing policy, including all relevant details, such as the legal basis of the transfer (e.g. standard contractual clauses). Furthermore, the Whistleblowing Act determines that the data processed within the framework of the internal whistleblowing system may be forwarded to a third country or international organisation only if the recipient of the transmission has made a legal commitment to comply with the provisions of the Whistleblowing Act in connection with reporting and if the recipient ensures observation of the regulations on the protection of personal data.

g) sign a data privacy waiver?

Data privacy waivers do not exist under Hungarian law.

h) be informed that the information gathered might be passed on to authorities?

According to the GDPR, the data subject must be informed of all relevant details concerning data processing. This includes details of data transmission to authorities. It is advisable to explain this possibility in the whistleblowing policy.

i) be informed that written notes will be taken?

According to Hungarian law, there is no explicit legal obligation to inform the employee that written notes will be taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law governing document holds or retention notices, but internal policies may regulate the relevant processes. IT policies may also entitle employers to scrutinise employee devices and retain information directly from such devices.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

If the documents containing the results of the investigation have been prepared by outside counsel or are in the custody of outside counsel, they fall under the confidentiality rules set out in Act LXXVIII of 2017 on attorneys and, therefore, are protected by attorney-client privilege.

According to Section 19(2) of the Whistleblowing Act, under a service agreement a whistleblower protection lawyer or other external organisation can also be engaged to operate the internal whistleblowing system. Therefore, it is advisable to engage outside counsel to operate the company's internal whistleblower system in order to have a

stronger claim to attorney-client privilege. It may also be helpful to label privileged documents accordingly to prevent accidental access by investigators. However, labelling itself does not automatically guarantee privilege.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

There are no specific rules for confidentiality applicable to in-house counsel under Hungarian law.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Certain notification obligations may be found in the relevant insurance policies. However, notification cannot violate the law.

The investigators must keep the content of the notification and the information on the persons concerned in the case confidential until the investigation is completed or criminal prosecution is initiated. Investigators are not allowed to share information with third parties. Actions might be taken once the investigation is completed.

b) Business partners (e.g. banks and creditors)?

The investigators must keep the content of the notification and the information on the persons concerned in the case confidential until the investigation is completed or criminal prosecution is initiated. They are not allowed to share any information with third parties. Actions might be taken once the investigation is completed.

Certain reporting obligations can apply under the relevant agreement, which, however, may not violate the law.

c) Shareholders?

There are no specific rules under Hungarian law in this regard. However, according to Sections 55 to 60 of Act CXX of 2001 on the Capital Market, issuers of securities that have been offered to the public must disclose to the public without delay any information that concerns, directly or indirectly, the value or yield of their securities issue, and which may have any bearing on the reputation of the issuer. Issuers must, at the same time, file that information with the Hungarian National Bank as well.

d) Authorities?

Authorities have no right to be informed until the investigation is completed.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

There are no explicit rules for immediate measures to be taken. However, an investigation should not disguise evidence or interfere with a public investigation. In the absence of any specific rules in this context, companies are obliged to act in accordance with the general principles of law and take measures in order to mitigate the damages caused by any potentially unlawful conduct and suspend any activity that could potentially qualify as a criminal offence. The nature of the actions to be performed by the affected company depends on the actual circumstances and should be assessed on a case-by-case basis.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Since the Whistleblowing Act covers internal investigations, such concerns should not arise as long as the investigation complies with applicable laws.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Search warrants are used in criminal proceedings and must comply with the formal and material requirements of the law. They must be issued by a court, the prosecutor, or the investigating authority, such as the police or the National Tax Authority. A search warrant may be issued if it can be reasonably presumed to lead to finding a criminal suspect, evidence of a crime, or property/items subject to confiscation. A search warrant must be issued in writing and must describe what evidence or items are expected to be found. Evidence obtained improperly by a court, the public prosecutor, or the investigating authority may not be considered and used as evidence.

In addition to criminal proceedings, on the basis of authorisation by the court, the Hungarian Competition Authority in antitrust matters, and, on the basis of authorisation by the prosecutor, the Hungarian Tax Authority in tax matters, may carry out dawn raids.

The Hungarian Competition Authority is empowered to conduct "site searches" of any premise, vehicle, or data medium to find evidence connected to the infringement investigated. Investigators may enter premises without the consent of the owner or tenant and without anyone present. They may also open any sealed-off area, building, or premises during the search. The Hungarian Competition Authority is entitled to prepare forensic copies and seize objects. It may request police assistance where deemed necessary for the successful and safe conduct of the site search. A site search may only be carried out in possession of a prior court order. Furthermore, as of 1 January 2021, the Hungarian Competition Authority is empowered to use covert recordings as evidence, provided that such recording is not the only proof of the infringement. That being said, evidence unlawfully obtained by an authority (including the Hungarian Competition Authority) shall not be admissible as evidence during competition supervisory proceedings.

The Hungarian Tax Authority has similar authority to carry out dawn raids in tax matters.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

According to Act XC of 2017 on criminal procedure ("**Criminal Procedure Code**"), the prosecutor is entitled to dismiss a criminal complaint or suspend an investigation if the person involved in the criminal offence cooperates in the investigation by providing evidence and if the interests of national security or law enforcement take priority over the interest of the state to prosecute. Under Hungarian law, corporations cannot benefit from these deals since the criminal offence itself is always committed by individuals.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Act CIV of 2001 provides criminal sanctions against legal entities for wilful criminal offences committed by their directors, representatives, supervisory board members, employees, or contractors. Sanctions such as dissolution, limitation of activity, or fines may be imposed on the legal entity if the legal entity benefited from the criminal conduct or used a vehicle to carry out the offence.

The Criminal Procedure Code lays down specific rules for the criminal liability of executive officers and directors in relation to the misappropriation of company funds and passive corruption, i.e. the request, acceptance or receipt of an unlawful advantage. In both cases, the maximum term of imprisonment is three years. However, in the case of

passive corruption, if the perpetrator breaches their official duty in exchange for unlawful advantage or commits the offence with accomplices or on a commercial scale, he could face up to eight years' imprisonment.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

In competition matters, the Hungarian Competition Authority may reduce the penalty as follows.

For compliance programmes implemented prior to the proceedings in antitrust matters, a reduction of up to seven percent is subject to (i) the implementation of suitable compliance efforts; (ii) stopping the infringement after being detected internally; and (iii) substantiating that the infringement was stopped as a result of the compliance programme. In addition, if the compliance programme contributed to suitable evidence for a leniency application, a further three percent reduction can be reached. The lack of involvement of high-level officials is required in both cases. In consumer protection proceedings, the reduction percentage is not specified by law.

For compliance programmes implemented after the initiation of the proceedings in antitrust matters, the Hungarian Competition Authority may reduce the penalty by up to five percent if the implementation is undertaken in conjunction with a leniency application, a settlement or active measures to rectify the consequences of the infringement. In the event of a consumer protection infringement, the Hungarian Competition Authority may reduce the penalty by up to 20 percent subject to active reparation or the admission of the infringement, and up to five percent without such reparation or admission.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Act CVIII of 2023 on rules of sustainable finance and corporate social responsibility (the "**Sustainable Finance Act**") entered into force on 1 January 2024 enacting the Environmental part of the ESG regulations. In order to ensure compliance with the sustainability reporting obligations, the companies designated by the Sustainable Finance Act must establish a risk management system, carry out regular risk assessments, prepare a social responsibility strategy for preventive purposes, take corrective actions in the event of infringements, prepare an annual ESG report and establish an internal or external complaint system. With regard to the date of the entry into force of the Sustainable Finance Act, authorities are not yet enforcing ESG related cases, but this will most likely change in the near future.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The obligation to establish a whistleblowing system has been introduced gradually in Hungary, with the majority of businesses only being subject to the obligation from 17 December 2023. However, questions and problems with the systems had already been arisen. The main issues for businesses were the determination of the number of employees. Businesses operating at the threshold of the number of employees had difficulties whether or not the obligations to set up the system apply to them. The Hungarian legislator also gave companies the possibility of not investigating anonymous reports, thereby weakening the effectiveness of the whistleblowing systems.

CONTACT

Hogan Lovells Partos & Noblet

Gerbeaud House
Vörösmarty tér 7/8
Budapest 1051
Hungary

Tel.: +36 1 505 4480
Fax: +36 1 505 4485
www.hoganlovells.com

Dr. András Multas
Senior Associate
Hogan Lovells Budapest
T +36 1 505 4480
E andras.multas@hoganlovells.co.hu

András is a member of the employment team in the Budapest office. András advises on various employment law areas including policy implementation and various compliance matters (including anti-bribery, whistleblowing etc.). András has also advised a number of clients on data protection and privacy matters.

Ireland

A&L Goodbody LLP


Kenan Furlong Clara Gleeson

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X		
No				X*	X**

* Only where specifically provided for (e.g. corruption legislation).

** Only in anti-corruption legislation.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Ireland recently implemented the EU Whistleblowing Directive via the Protected Disclosures (Amendment) Act 2022 which amended Ireland's pre-existing whistleblowing legislation, the Protected Disclosures Act 2014. This Act came into force on 1 January 2023 and does not materially deviate from the requirements of the Directive.

Procedures must take account of the Protected Disclosures Act 2014 as amended by the Protected Disclosures (Amendment) Act 2022, which provide protections for workers in Ireland who make "protected disclosures" of relevant information, which, in the worker's reasonable belief, tend to show one or more "relevant wrongdoings". A "relevant wrongdoing" is broadly defined and includes the commission of an offence, failure to comply with a legal obligation, miscarriage of justice, danger to the health and safety of any individual, damage to the environment, misuse of public funds or resources, gross mismanagement by a public official and destruction or concealment of information relating to any of the foregoing, as well as all the types of breaches prescribed in the EU Whistleblowing Directive.

Whistleblowers must be provided with protection from dismissal or penalisation and protection of their identity (subject to certain very narrow exceptions). Breach of these requirements is a criminal offence in Ireland. The Protected Disclosures (Amendment) Act 2022 has also introduced requirements to follow up on whistleblowing reports and to provide feedback to the whistleblower within three months of receipt of the report, as required by the Directive.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The Act does not allow for group wide reporting systems in entities with 50 or more employees. It requires all employers/entities that employ 50 or more employees to operate internal reporting channels and procedures for the making of reports at employer or entity level. However, like the Directive, the Act does allow entities with fewer than 250 employees to share resources for the receipt and investigation of resources. Nevertheless, there are a number of exclusions from this such as functions like following-up on a report or providing feedback to the reporting person, which means that it does not obviate the need for such entities to have their own entity-level procedures.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) There is no requirement for an employee representative body to be informed about an internal investigation before it commences.

b) There is no general requirement to notify the Data Protection Commissioner. However, this is likely to depend on the subject matter of the investigation.

c) If a criminal offence may potentially have been committed, then a mandatory reporting obligation to the Irish police could arise if the offence is included in a list of scheduled offences enshrined in legislation. This applies to a broad range of theft, fraud, company law, financial services law, and white collar type offences. A company (or members of its senior management) may also have mandatory reporting obligations to the company's regulator(s). It is a criminal offence not to comply with these mandatory reporting obligations.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

A common law duty of mutual trust and confidence is generally implied in employment relationships. This would require the employee to answer questions in connection with their employment, honestly and truthfully. A duty to cooperate in such investigations often features in company policies. It would be usual for a disciplinary process to apply to employees who refuse to cooperate.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

No labour law deadlines are triggered by investigative actions. Similarly no rights to sanction employees are waived by investigative actions. However, where an investigation is being carried out without affording the employees involved the benefit of fair procedures, an employee could bring civil proceedings seeking injunctive relief to restrain the continuation of the investigation. Observing fair procedures is a crucial component of the investigative process in Ireland, and will reduce the likelihood of an employee obtaining injunctive relief.

The Protected Disclosures (Amendment) Act 2022 has strengthened the ability of an employee to seek injunctive relief in that it provides that an employee can apply to the Circuit Court for interim relief to restrain an alleged act of penalisation within 21 days following the last instance of penalisation or such longer period as the Court may allow.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Data protection legislation (including the Data Protection Act 2018, General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and any amending legislation) applies to any processing of personal data.

The employer will be the data controller of personal data collected or used during interviews (whether it conducts the interview itself or delegates it to a third party). Thus it retains responsibility for the personal data and ensures that it is processed in accordance with data privacy laws (in particular the obligation in relation to fair and transparent processing). The employer will therefore be responsible for ensuring that employees are adequately informed that their personal data may be processed for the purpose of these interviews; about the categories of personal data processed; and the legal basis which the employer is using to process such data. Employees must also be informed who their personal data will be disclosed to; how long it will be retained and processed; whether it will be transferred to a non-EEA country (and if so the safeguards in place and means to obtain a copy of them), what their rights are in respect to their data (e.g. right of access, right of rectification, and right of erasure), their right to lodge a complaint with the competent supervisory authority, whether the provision of their personal data is a statutory or contractual requirement and the existence of any automated decision-making in relation to their data.

The employer will also need a lawful basis for carrying out such processing. If reliance is placed on legitimate business interests as the legal ground for processing, the employer must specifically outline what that legitimate business interest actually is. Consent is also a lawful basis for processing. However, due to the perceived imbalance of power in the employer/employee relationship, together with the much higher compliance threshold for relying on consent under GDPR, it is not advisable to rely on employee consent alone as a lawful basis for processing employee personal data.

If the interviews involve the processing of any sensitive personal data, the employer will need to ensure that one of the more limited legal bases for processing such sensitive personal data can be relied upon. Employers should seek to resist collecting or processing sensitive personal data wherever possible.

b) reviewing emails?

The same obligations in relation to fair and transparent processing, and having a lawful basis to carry out the processing outlined above, equally apply to reviewing emails. The employer should have an email monitoring policy in place with employees, which is brought to employees' attention so that employees are on notice that their communications are not private and are monitored. Employers should only monitor employee emails where it is reasonably necessary in the interests of the business and without prejudice to the fundamental rights, freedoms, or legitimate interests of employees.

c) collecting (electronic) documents and/or other information?

If the collection of documents includes personal data, the employer will need to ensure it meets its fair processing obligations (i.e. provides the individuals whose personal data is collected with information as to why their data is being collected, and for what purpose, as detailed in 5a above). This may be covered in a privacy policy or employment manual. There must also be a lawful basis for collecting such data, such as if it is required to comply with a legal obligation or for the legitimate business interests of the employer and where such interests do not outweigh the rights or freedoms of the employee.

d) analysing accounting and/or other business databases?

To the extent that business databases contain any personal data, the employer must ensure compliance with its fair processing obligations and have a lawful basis for collecting personal data as outlined above. Any investigation should take account of the Official Secrets Act 1963, which prevents disclosure, without authorisation, of "official information" of public office holders and confidential contractual information.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

Where possible, it is generally considered best practice, in advance of any interview, to communicate in writing the investigation terms of reference to the employee. This should be done where the investigation could lead to findings that may have an adverse impact on the employee in question. However, there is no legal requirement to state this in writing.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Irish law recognises a "privilege against self-incrimination". There is no statutory obligation to advise an employee of this, though there is a requirement to ensure that fair procedures and natural justice are applied in the course of the investigation. If there is an allegation of criminal wrongdoing involving the employee, fair procedures and natural justice are interpreted as requiring the employee to be notified of their entitlement to seek independent legal advice from their own lawyer.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

In accordance with fair procedures, it should be made clear to the interviewee that any lawyers present are acting for the company, and not the employee, who may in some cases have their own legal representation.

d) be informed of their right to have their own lawyer attend the interview?

This depends on the type of investigation. There is no right to (and therefore no right to be informed about) representation if the investigation is a fact-gathering exercise, prior to a separate disciplinary hearing that will decide if the allegations are proven or not. However, where the investigator appointed will reach formal findings, the principles of fair procedures and natural justice will apply, which can include in certain cases the right to legal representation and the right to cross-examine one's accuser.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

As mentioned above with respect to the right to legal counsel, the right to representation depends on the type of investigation, in particular, whether the investigator will reach formal findings against the employee.

f) be informed that data may be transferred to another country (in particular to the United States)?

Employees must be informed of all processing activity carried out on their personal data, including where the data is to be transferred to a country outside the EEA, such as to the United States.

g) sign a data privacy waiver?

Signing a data privacy waiver is not necessary, and, in fact, it would not be advisable to rely on consent of employees for processing their personal data. As outlined above, there are alternative lawful grounds available to employers to process personal data.

h) be informed that the information gathered might be passed on to authorities?

In order for the employer to meet its fair and transparent processing obligations, interviewees must be informed that their personal data may be passed on to authorities. The employer would need to have a lawful basis for sharing the data with the authorities, such as compliance with a legal obligation.

The disclosure of personal data to authorities would also be lawful to the extent that such disclosure is necessary for the purpose of preventing, detecting, investigating, or prosecuting criminal offences or preventing a threat to national security, or public security.

i) be informed that written notes will be taken?

It is best practice to inform employees that notes will be taken. It is advisable to share draft notes with the employee following the interview and afford the employee an opportunity to respond to the content, in particular where the investigator can make formal findings against the employee.

While this is not a strict requirement under Irish law, failure to adhere to principles of fair procedures and transparency may compromise an investigation.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Hold notices should generally be issued as a matter of good practice to "custodians" of material potentially relevant to the investigation in order to secure and ensure the safekeeping of the material.

It is also advisable to suspend routine/automatic document or data destruction processes for any records or materials potentially relevant to the matters under investigation to ensure that relevant material is not unwittingly destroyed.

There is no specific form such notices must follow. Typically they should be issued as soon as possible to persons (or "custodians") who are likely to hold potentially relevant records or materials to make the recipient fully aware of their obligations to preserve all relevant records and materials.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege may be claimed over the findings of the internal investigation if it can be established that either "legal advice privilege" or "litigation privilege" applies. Legal advice privilege protects communications between lawyers and their clients, the dominant purpose of which is seeking or providing legal advice. Litigation privilege protects confidential communications between a client and their lawyers and third parties, where the dominant purpose is to prepare for actual or reasonably apprehended litigation. The Irish courts have held that litigation privilege can apply in relation to materials generated in contemplation of a regulatory or criminal investigation.

Protection of privilege in an internal investigation requires advance planning and regular review. In order to maximise the prospects of successfully asserting a claim to privilege, it is generally advisable (among other things) to: (i) involve external lawyers at an early stage; (ii) where appropriate, label documents created in relation to an investigation with an appropriate "privilege" tag; (iii) limit the dissemination of legal advice, privileged work, and other sensitive documents to a small group and to what is strictly necessary in the circumstances; and (iv) ensure that material relating to the investigation is stored separately.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

In-house counsel is entitled to be treated in the same way as external legal counsel in respect of legal privilege in Ireland. The principal exception to this is in relation to European Commission competition investigations, where the European Court of Justice has held that communications with in-house lawyers are not legally privileged.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

It is generally advisable to check the insurance policy early on. Where required, a precautionary notification to insurance companies should be made as soon as possible to avoid any subsequent refusal of cover on the basis that the matter was not notified on a timely basis.

b) Business partners (e.g. banks and creditors)?

Early notification to business partners will depend on the nature and subject matter of the investigation. Assessment on a case-by-case basis will be required.

c) Shareholders?

Directors typically owe duties to the company rather than to shareholders. There may, however, be special circumstances where a duty could be owed to the shareholders, such that disclosure is required. Publicly listed companies may also have disclosure obligations to the market in certain circumstances.

d) Authorities?

This will depend on the nature of, and subject matter of, the investigation. The company (or its senior management, including, in particular, any persons in "Pre-Approved Controlled Functions") may have specific mandatory reporting obligations to relevant regulator(s), including for example, to the Central Bank of Ireland, the Corporate Enforcement Authority, the Data Protection Commissioner, and/or the Competition and Consumer Protection Commissioner.

Where the investigation relates to a matter potentially involving certain fraud, corruption and/or company law offences, a report to the Irish police under Section 19 of the Criminal Justice Act 2011 may be required.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Consideration should be given to whether any mandatory reporting requirements arise, and steps should be taken to ensure the preservation of all relevant materials. Consideration should also be given to taking appropriate mitigation steps while the investigation is ongoing, including any necessary notification to any impacted third parties, e.g. to customers who are potentially impacted by an employee fraud.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Where an internal and regulatory investigation are operating in tandem, it is generally advisable to maintain regular contact with the regulator to ensure that they are on board with the approach being taken in the internal investigation.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

In most cases, the Irish police will require a search warrant before searching premises, although there are statutory exceptions to this. Generally, search warrants are issued by District Court Judges.

The legal prerequisites which apply to regulators will depend on the statutory provisions under which they are appointed. Some regulators have statutory powers to conduct searches and "dawn raids" on business premises on foot of their warrant of appointment alone (without needing to apply to court for a specific permission to do so). However, a search warrant (granted by a court) may be required in certain circumstances, e.g. to search a private dwelling, seize original documents, and/or use reasonable force in connection with statutory search and seizure powers. The Irish Supreme Court has held that the regulator must exercise its search powers in an appropriate and

proportionate manner to ensure that, insofar as possible, only relevant material is seized for review and that where irrelevant material is seized, it should not be reviewed.

There is judicial discretion over whether to admit improperly gathered evidence. The Irish Supreme Court has held that evidence obtained unconstitutionally may still be admissible if the prosecution can establish that any breach of constitutional rights was due to inadvertence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

There is currently no general system for "non-prosecution agreements" or "deferred prosecution agreements" ("**DPAs**") in Ireland. A Cartel Immunity Programme operates under Irish competition law, which has some of the features of DPAs. There is also no formal plea or bargaining system in Ireland, although plea bargaining does operate informally in practice.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

The range of penalties will depend on the specific conduct, but can potentially include fines and/or imprisonment following a successful criminal prosecution. Companies convicted of an offence may also be excluded from participating in public tenders. Compensation orders and adverse publicity orders can be made in some situations. Some regulators may also have civil enforcement powers, which they can deploy as an alternative to prosecution. Such powers may include requesting undertakings or issuing compliance notices, as well as the power to impose fines.

In certain cases, where it is proved that an offence committed by a company has been committed with the "consent or connivance of", or was "attributable to any neglect" on the part of a director or officer of the company, the latter can also be found guilty and subjected to the relevant applicable penalties. Directors can also potentially face "restriction" and/or "disqualification" for a set period of time and can be made personally liable for the debts of a company in certain circumstances.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

The compliance system in place is likely to be a relevant factor in the mitigation of any penalty imposed on a company, its directors, officers, or employees. There are some instances where it could constitute a complete defence for a company. In particular, the Criminal Justice (Corruption Offences) Act 2018 holds companies accountable by providing that a company may be liable to prosecution for corrupt acts by its director, manager, employee, agent, or subsidiary. The only available defence is for a company to show it "took all reasonable steps" and "exercised all due diligence" to prevent corruption. The Criminal Justice (Theft and Fraud Offences) (Amendment) Act 2021 also provides for new corporate offences, including fraud and corruption, affecting the financial interests of the European Union on somewhat similar terms where there is a failure to exercise the requisite degree of supervision.

In the case of the offences above, the defence would only apply where the efficient compliance system was implemented prior to the misconduct. Otherwise, it is likely that the courts/regulator would view the implementation of an effective compliance system as a mitigating factor, although greater weight is likely to be attached to one implemented prior to the misconduct.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

The majority of the legislative requirements relating to sustainability or specific ESG matters in Ireland stem from EU legislation.

Disclosure remains a key area of focus from an ESG perspective. In the financial services sector, the Central Bank of Ireland (the "**Central Bank**") together with the European Supervisory Authorities remain in information-gathering and policy-setting mode in the context of sustainability disclosures. The Central Bank has conducted spot checks on fund disclosures on sustainability matters to ensure compliance with the Sustainable Finance Disclosures Regulation (EU 2019/2088 on sustainability – related disclosures in the financial services sector). As part of the Common Supervisory Action on sustainability related disclosures and risks launched by the European Securities and Markets Authority ("**ESMA**") last year, the Central Bank issued a questionnaire to a number of fund managers and will be reporting their findings to ESMA over the course of 2024.

More generally, with mandatory corporate sustainability reporting being introduced by Corporate Sustainability Reporting Directive ("**CSRD**") (EU 2022/2464), companies across all sectors are considering the sustainability information that will need to be disclosed in their annual reports as the reporting obligations kick in over the next few years. As the Irish implementing legislation has not yet been published, it is not clear which authority will be responsible for enforcement.

In the consumer law space, the Advertising Standards Authority for Ireland ("**ASAI**") Code of Standards for Advertising and Marketing Communications in Ireland contains specific rules in relation to environmental claims. The ASAI Code is not legally binding. However, the ASAI investigates and publishes decisions in response to complaints which are often reported on in the media. Complaints about green claims or 'greenwashing' are increasingly common and the ASAI strictly applies the rules set out in the Code. In the absence of specific binding legislation at present, the ASAI Code is also a useful best practice guide to align with the specific rules that will apply under the forthcoming EU Green Claims Directive (Proposal for a Directive of the European Parliament and of the Council on substantiation and communication of explicit environmental claims) and the specific provisions on environmental claims to be introduced into the Unfair Commercial Practices Directive (Directive amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through better protection against unfair practices and better information).

The majority of ESG litigation in Ireland to date has centred on climate and environmental law issues. Cases have been focused either on government implementation of climate obligations (Climate Case Ireland: Friends of the Irish Environment v. The Government of Ireland & Others [2020] IESC 49) or the integration of climate considerations into planning decisions (An Taisce – The National Trust for Ireland v. An Bord Pleanála & Ors [2022] IESC 8; Coyne & Anor v. An Bord Pleanála & Ors; Coyne & Anor v. An Bord Pleanála & Ors [2023] IEHC 412). As noted in the Strategic Climate Litigation on the Island of Ireland report (https://ejni.net/wp-content/uploads/2023/12/EJNI-Strategic-Litigation-on-the-island-of-Ireland-Final-Report-Dec-2023.pdf) such litigation is "*moving beyond reactionary litigation towards a coherent strategic approach*".

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

There is a general trend of increased regulatory activity and investigations in Ireland, which is, in turn, leading to an increase in internal investigations. In light of increased regulatory activities, it is expected that the Irish courts will continue to see applications for injunctions restraining investigative processes.

An apparent trend includes some agencies conducting initial interviews "under caution", i.e. the interviewee is cautioned that anything they say may be used in evidence against them, even where their status – whether a witness, subject, or a suspect – remains unclear.

Ireland adopted new anti-corruption legislation in mid-2018, which has made it much easier for the authorities to prosecute and secure convictions for corruption offences. The Companies (Corporate Enforcement Authority) Act 2021 also re-established the Office of the Director of Corporate Enforcement (which previously sat within the Government's Department of Enterprise, Trade, and Employment) as a stand-alone agency with a commission structure called the "Corporate Enforcement Authority" with increased independence.

In line with European legislation, the focus of regulators and law enforcement on money laundering and terrorist financing has grown in the past few years.

CONTACTS

A&L Goodbody

3 Dublin Landings, North Wall Quay
Dublin 1
Ireland

Tel.: +353 1 649 2000
www.algoodbody.com

A&L Goodbody LLP is a leading Irish corporate law firm with a dedicated and specialist Fraud and White Collar Crime team. We advise on managing relationships with regulators, corporate fraud & asset tracing, fraud investigations and criminal prosecutions. Our clients include Irish and international corporates, financial institutions and public bodies. We also represent boards, senior management and employees caught up in regulatory investigations. At all times, we strive to protect our clients from the reputational consequences that can flow from a criminal investigation.

We have extensive experience in dealing with regulators both in Ireland and abroad. In Ireland, we deal with all regulators including the Corporate Enforcement Authority (CEA, which was previously known as the Office of the Director of Corporate Enforcement), the Data Protection Commissioner (DPC), the Environmental Protection Agency (EPA), the Garda National Economic Crime Bureau (GNECB), the Central Bank, the Competition and Consumer Protection Commission (CCPC), the Revenue Commissioners and the Criminal Assets Bureau (CAB).

We regularly work with international law firms and other advisers in dealing with claims from regulators such as the Serious Fraud Office (SFO) in the United Kingdom, and in the United States, the Federal Bureau of Investigation (FBI), the Food & Drugs Administration (FDA) and the Department of Justice. We also have experience of dealing with various other regulatory authorities in a range of EU jurisdictions, Australia and Russia.

Kenan Furlong
Partner
A&L Goodbody LLP
T +353 1 649 2260
E kfurlong@algoodbody.com

Kenan Furlong is a Partner in A&L Goodbody's Disputes and Investigations Department and is co-Head of the Fraud & White Collar Crime Unit. He advises clients on internal investigations, whistleblowing issues, dawn raids, and money laundering issues. He also advises clients on managing their relationships with various Irish regulators and the Garda National Economic Crime Bureau (GNECB). In addition he assists with investigations by foreign regulators such as the SFO, the IRS and the SEC.

Clara Gleeson
Associate
A&L Goodbody LLP
T +353 1 649 2746
E cgleeson@algoodbody.com

Clara Gleeson is an Associate in A&L Goodbody's Disputes and Investigations Department and Fraud & White Collar Crime Unit. Her practice focuses on all areas of white collar and corporate crime, including bribery/corruption issues, fraud, money laundering and market abuse. She advises individual and corporate clients on internal and external investigations, whistleblowing issues and managing their relationships with various Irish enforcement agencies such as the Office of the Director of Corporate Enforcement (ODCE) and Garda National Economic Crime Bureau (GNECB).

Italy

Hogan Lovells Studio Legale

Francesca Rolla

Alessandro Borrello

Vincenzo Donadio

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X*	X	X	X	X
No					

* Administrative liability of companies.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

When a whistleblower submits a report through internal reporting channels, implemented under the Italian Whistleblowing Law (Legislative Decree No. 24 of 10 March 2023, the "**IWL**"), the person or department in charge of managing said channel must (i) acknowledge receipt of the report within seven days; (ii) properly follow up on the report; (iii) maintain communication with the reporting person (requesting additional information or clarifications on the report, if necessary); and (iv) provide feedback to the reporting person within three months. To ensure protection of the reporting persons, the IWL specifies that their identity must be kept confidential and that any form of retaliation is prohibited.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The IWL lacks explicit provisions addressing whistleblowing systems within group companies. Similar to the wording of the EU Whistleblower Directive, the IWL only allows companies with a workforce of up to 249 employees to share the reporting channel and its management.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) There is no obligation to inform and/or involve employee representative bodies before an internal investigation is initiated. In other words, the employer is free to launch an audit and investigation process at its discretion and within the limits set by law.

b) According to the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), which entered into force on 25 May 2018, the Data Protection Officer ("**DPO**") shall be involved, properly and in a timely manner, in all issues which relate to the protection of personal data, therefore also when commencing internal investigations.

In principle, internal investigations do not have to be reported to the Italian Data Protection Authority ("**DPA**").

c) There is no obligation to inform and/or involve government authorities at the start of an internal investigation.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

There is no specific obligation for employees to participate in interviews. However, due to the general duties of diligence, obedience, and loyalty that apply to the employment relationship, the employee is expected to cooperate as part of the obligations that come with their job. If the employee refuses to participate in the investigation, their refusal may be considered a breach of their obligations. It may justify initiation of disciplinary procedures by the employer, which may end with a disciplinary sanction if the relevant requirements are met.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Employers should initiate an investigation as soon as they become aware of any potential misconduct and/or wrongdoing. If an employee's misconduct emerges from the internal investigation, the employer must immediately start disciplinary procedures in compliance with the so-called promptness principle for disciplinary actions. The timing may vary depending on, among other factors, the severity of the conduct and the number of people involved. At the end of the disciplinary procedure, the employer may impose sanctions, including dismissal for just cause.

Italian law does not provide any specific guidance with regard to the upper time limit of the promptness principle. What is crucial is that the disciplinary action was taken as soon as the employer had been made aware of the employee's misconduct and that the employer had collected sufficient evidence to start a disciplinary procedure. In some cases, disciplinary proceedings, initiated six months after the start of an investigation, were held by courts to comply with the promptness principle, since the time was deemed necessary to investigate and ascertain the employee's misconduct.

Moreover, once a disciplinary procedure has been initiated and the employee has exercised their right to be heard, the relevant sanction (if any) must be imposed within the strict deadline set out by the applicable Collective Bargaining agreement.

If the employer does not act promptly and the employee challenges the sanction, there is a concrete risk that a judge might identify such delay as tacit acceptance of the employee's conduct and declare the sanction unlawful.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Legislative Decree No. 196 of 30 June 2003, as amended following the entry into force of the GDPR and implementing the GDPR itself (the "**Privacy Code**"), apply to any processing of personal data. If the interview requires the collection of and/or any other processing of personal data, such as the preparation of reports and/or notes, it is advisable to assess how these activities are carried out in this respect (including issuing privacy notices to the relevant employees, etc.).

In any case, when performing internal investigations, companies must comply with the general principles of data processing set out in Article 5 of the GDPR (i.e. lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality).

b) reviewing emails?

Private communication is protected by the Italian Constitution. The unauthorised and unlawful review of private communication constitutes a criminal offence punishable by up to four years imprisonment (up to five years for offences committed against a public authority system).

In the employment relationship, however, the review of emails is allowed under Article 4 of Legislative Decree No. 300 of 20 May 1970, "**Workers' Statute**", provided that the email use is related to the employment relationship. According to the DPA, it is therefore advisable to explicitly mention the lack of confidentiality of communications within internal company policies. If there are no specific policies in this context, the employee and/or third parties may reasonably expect certain types of communication to be treated as confidential.

Review of emails must, in any case, be carried out without being excessive. The process must be proportionate, in accordance with data protection principles. In addition, employees may exercise their rights under the Privacy Code and the GDPR, including, for example, the right of access, rectification, and, subject to specific conditions, the right to object and to erasure. In specific circumstances set forth by the Privacy Code and the GDPR, the abovementioned rights may be limited.

c) collecting (electronic) documents and/or other information?

The collection of documents and other information related to the employment relationship, whether for legal or organisational reasons, is not subject to any particular restriction. The collection, however, cannot exceed the purposes which are linked to the employment relationship and must comply with an obligation imposed by law or regulation. Such information shall be gathered and managed in compliance with the provisions of the Privacy Code and the GDPR. In this context, it is worth mentioning a recent decision issued by the DPA against a company which, instead of deactivating the email account of a former employee after they had left, used an email from said account as evidence in court proceedings, one year after the employee had left. The DPA found the procedures adopted by the company to be unlawful because they did not comply with data protection principles, which require the employer to protect the confidentiality of a former employee.

Finally, the Privacy Code and the GDPR apply to any document containing personal data of the employee. With respect to the processing of such documents, employees may exercise the rights granted by the Privacy Code and the GDPR, as mentioned above in 5b.

d) analysing accounting and/or other business databases?

If such accounting and/or business database includes personal data, the Privacy Code and the GDPR shall apply.

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

As long as the interview is conducted in compliance with applicable employment and privacy law provisions (e.g. the employee has received a privacy notice illustrating their rights under the Privacy Code and the GDPR), there is no legal obligation to inform the employee about the legal context of the investigation. However, providing information on the subject matter and a brief description of the investigation may be ethically necessary and advisable. For documentation purposes, it is advisable to provide these instructions in writing to be signed by the interviewee.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

This is not mandatory under Italian law. If the interview is designed to collect facts and not to challenge wrongdoings (meaning that the purpose of the interview is merely gathering facts and not accusing the interviewee), the employee is free to make any statements that they deem relevant for this purpose. If the employer learns of any misconduct during the interview, this must be dealt with by way of a dedicated disciplinary procedure.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

If the interview is conducted and/or attended by a third party (e.g. a lawyer), the employer should explain to the employee the role of that third party in compliance with the general principles of good faith and fairness. Therefore, if a lawyer takes part in the interview, the company should disclose their role.

d) be informed of their right to have their own lawyer attend the interview?

As mentioned above, the purpose of the interview is to collect facts. The employee's participation in the interview thus falls within their job duties. Accordingly, there is no strict obligation to allow the employee to be accompanied by a lawyer. However, if the company is assisted by a lawyer, and the employee asks for the same right to be granted, the company could evaluate whether such participation would allow for a fair set-up and decide to avoid an unbalanced situation altogether by allowing the employee to be assisted by a lawyer.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Similar to d) above, there is no provision for the employee to be accompanied by a representative of the works council or another representative body. Representatives of works councils or trade unions can only assist employees in disciplinary proceedings.

f) be informed that data may be transferred to another country (in particular to the United States)?

According to the Privacy Code and the GDPR, the interviewee needs to be informed about any transfer of personal data and the legal basis for such transfers, with a privacy notice (compliant with Article 13-14 GDPR). Consent to a cross-border transfer is not required if the transfer is legally covered. In particular, the Privacy Code and the GDPR allow the transfer of personal data outside the European Union if the transfer is necessary to defend a legal claim in which the Italian exporter is (or may be) involved. The transfer must take place under appropriate safeguards and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. The transfer is considered to take place under appropriate safeguards if: (i) the European Commission has certified that the laws of the country of origin of the imported data guarantee an adequate standard of data protection. In this regard, please note that since the invalidation of the Privacy Shield by the ECJ, which occurred on July 2023, the European Commission has issued another adequacy decision (known as the EU-U.S. Data Privacy Framework) allowing data flows to United States companies/organisations which have adopted the principles set out in EU-U.S. Data Privacy Framework through a mechanism of self-certification (a list of companies which adopted this certification mechanism can be found in the Data Privacy Framework List, managed by the United States Department of Commerce and available online); or (ii) the parties have entered into the privacy Standard Contractual

Clauses as approved by the European Commission or (iii) the transfer is governed by the Binding Corporate Rules of a Code of Conduct as approved by the competent DPA.

g) sign a data privacy waiver?

Data subjects must be informed about the methods and purposes of the data processing, including their rights. In certain cases, employees must give informed, voluntary, and specific consent.

h) be informed that the information gathered might be passed on to authorities?

According to the Privacy Code and the GDPR, data subjects (i.e. employees) should be provided with a privacy notice with information regarding potential (categories of) recipients of their personal data.

i) be informed that written notes will be taken?

For transparency reasons, it is advisable to inform the employee that written notes will be taken. Furthermore, if such written notes involve the processing of personal data (e.g. the notes mention the names of interviewed employees), the Privacy Code and the GDPR (as well as all related principles) apply to these notes (e.g. the data retention period, which the company determines in light of the purposes for which such data was originally collected).

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Document hold notices and retention policies are allowed in Italy, although there is no specific rule which must be observed.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

There is no general concept of legal privilege in Italy. However, according to civil and criminal law and the Code of Conduct of the Italian Bar, lawyers who are members of the Bar are obliged to maintain professional secrecy about any information they receive during the work for their clients. If criminal proceedings are pending, greater privilege protection can be achieved by appointing legal counsel in accordance with the rules of the Criminal Procedure Code.

In these cases, to ensure the highest privilege protection, investigation reports and legal memos should be prepared by the appointed outside legal counsel, kept at their office, and labelled with wordings such as "*corrispondenza riservata avvocato-cliente*", "*riservato e confidenziale*", thereby designating them as "legally privileged and confidential". Investigation reports and documents collected during an internal investigation, if kept at the company's premises, could be seized by enforcement authorities (e.g. the public prosecutor), as in-house counsel cannot assert legal privilege.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

In-house counsel communication is not protected by attorney-client privilege.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

There are no (statutory) legal provisions which require early notification to insurance companies. However, notification may be stipulated in the provisions of the insurance contract. Notification may be appropriate under certain circumstances, for instance if the D&O policy covers internal investigations.

b) Business partners (e.g. banks and creditors)?

There is no explicit requirement to inform business partners about internal investigations. However, there is a general obligation under Italian law to perform contracts in good faith. The initiation of an internal investigation could constitute relevant information for the other party with regard to the purpose of the contract. Therefore, the possibility of notifying business partners should be assessed on a case-by-case basis.

c) Shareholders?

Although there is no legal duty to inform shareholders that an internal investigation is starting, the decision to provide early notification should be assessed on a case-by-case basis and depends on the seriousness of the alleged misconduct.

d) Authorities?

There is no general obligation to inform public authorities.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

A company should minimise the damage and try to avoid committing other offences similar to those committed by its employees. Accordingly, when significant misconduct is discovered, the company should also consider reviewing and amending its compliance plan and taking all necessary and specific measures.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Prosecutors are generally not informed about internal investigations and therefore, do not ask for specific steps to be observed.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Both search warrants and dawn raids in criminal proceedings must comply with the formal and material requirements of the Italian Criminal Procedure Code. They can only be carried out if there is a concrete reason to believe that specific things relevant to the alleged criminal offence can be retrieved.

Search warrants can only be executed by order of the Public Prosecutor and in accordance with the conditions of the Italian Criminal Code. In exceptional cases, where it is necessary and urgent, the police can take provisional measures to seize items. The measures taken must be presented to the judge for confirmation within 48 hours. If this confirmation is not given within 48 hours, the provisional measures shall be revoked and considered null and void.

Evidence gathered in violation of relevant rules set forth by the Italian Criminal Code may not be used in the criminal trial, except when such evidence amounts to the *corpus delicti*.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Italian law does not provide for non-prosecution or deferred prosecution agreements for individuals or corporations. Under Italian law, however, the prosecutor and the defendant (including corporations) can enter into a plea bargain, even during preliminary investigations.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Legislative Decree No. 231 of 8 June 2001 ("**Decree 231**") introduced corporate administrative liability for offences listed in Decree 231 and committed by leadership in the interest or benefit of the company.

If a company is held liable under Decree 231, it may be fined according to the seriousness of the offence (up to around €1.5 million) and/or be subject to interdictory sanctions (such as debarment from exercising activity and disqualification from contracting with the public administration), confiscation, and publication of the court's decision.

The penalties for individuals vary depending on the type of offence committed. They can include imprisonment, monetary fines, and interdictory sanctions.

Furthermore, both companies and their employees can be held liable for damages under civil law by those who have been injured by the misconduct.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

According to Decree 231, a company may be exempt from liability if it has implemented a compliance programme under Decree 231 ("**231 Model**") prior to the alleged misconduct. The 231 Model shall include, among other things, the appointment of an *ad hoc* Surveillance Body —an autonomous, independent entity responsible for overseeing the implementation and updating of the 231 Model.

Moreover, the company can in certain cases mitigate its potential liability even after the perpetration of the relevant crime, by implementing an appropriate 231 Model to prevent the committed offence from recurring. Consequently, failure to take action following a compliance breach could prevent the company from relying on this defence.

Implementation of an efficient 231 Model does not *per se* entail suspension or reduction of penalties for the relevant company's directors, officers, or employees. In this context, it cannot be excluded that failure by the members of the board of directors, officers, or employees to take action in light of suspected compliance failures may lead to personal civil and/or criminal liability for those individuals (e.g. because the directors could be deemed to have failed their duties to the company).

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Although a comprehensive ESG regulation has not yet been implemented in Italy, there are several regulations that indirectly address ESG principles. In particular, the implementation of 231 Models can be used by companies to achieve sustainability goals, such as preventing the commission of environmental crimes (which are listed under the Decree 231), thus promoting sustainable behaviours within the company.

With the recent increase in penalties for ESG-related crimes (e.g. environmental offences), as well as the recent elevation of the protection of the environment as a principle embedded by the Italian Constitution, local authorities will most likely become more active in investigating and enforcing ESG related cases.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

In recent times, the Italian legislator widened the scope of criminal offences which may trigger corporate liability under Decree 231. *Inter alia*, the updated list of relevant crimes now includes a new set of crimes against public administration, increased penalties for environmental crimes, a new set of crimes against cultural heritage and the crime of digital piracy.

The main Italian enforcement trend currently involves the investigation of many Italian and multinational logistics companies for alleged tax offences, illicit intermediation and labour exploitation (all listed in Decree 231). These investigations focus on the purportedly fabricated externalisation of the workforce: In short, the allegation is that companies utilised fictitious service contracts to employ workers that are (only) formally employed by others, and this scheme would enable said companies to illegitimately obtain, *inter alia*, a substantial tax reduction.

Due to these recent legislative changes and investigative trends, companies are advised to thoroughly update their 231 Model, along with their policies and procedures, to effectively prevent and mitigate the risk of committing newly introduced, amended, or currently scrutinised criminal offences.

CONTACTS

Via Santa Maria alla Porta, 2
20123 Milan
Italy

Tel.: +39 02 7202521
Fax: +39 02 72025252
www.hoganlovells.com

Francesca Rolla
Partner
Hogan Lovells Milan
T +39 02 7202521
E francesca.rolla@hoganlovells.com

Francesca Rolla is a Partner at Hogan Lovells, founder of the Italian Litigation practice and head of the Investigations, White Collar, and Fraud team in Italy. With almost 30 years of experience as a litigator, Francesca represents international and Italian clients in product liability and tort disputes and advises on product safety and compliance issues, as well as on internal investigations. In respect of Investigations and White Collar Crime, she leads a team specifically dedicated to advising clients on how to avoid the legal, commercial and reputational risks posed by investigations and prosecutions. Francesca assists in handling internal investigations and investigations by criminal or other public authorities, coordinating the work of criminal counsels and external experts.

Alessandro Borrello
Counsel
Hogan Lovells Milan
T +39 02 7202521
E alessandro.borrello@hoganlovells.com

Alessandro Borrello is a Counsel in the Italian Litigation, Arbitration, and Investigations practice at Hogan Lovells, advising international and Italian companies across various industry sectors.

His work mainly focuses on representing clients in commercial and tort litigation and in assisting them with internal investigations related to a vast variety of potential misconducts.

Alessandro is the go-to lawyer in case of a whistleblower report, provides targeted advice on compliance measures and risk mitigation solutions and advises clients on the creation and implementation of compliance programmes and whistleblowing systems as required by Italian law.

Vincenzo Donadio
Associate
Hogan Lovells Milan
T +39 02 7202521
E vincenzo.donadio@hoganlovells.com

Vincenzo Donadio in an Associate in the Italian Litigation, Arbitration, and Investigations practice at Hogan Lovells. His work is mainly focused on commercial litigation, product liability and internal investigations, assisting international and domestic clients operating in various industry sectors such as technology and life sciences.

Being a member of the Investigations, White Collar and Fraud group in Italy, he regularly assists clients in the context of internal investigations providing advice to mitigate legal, commercial and reputational risks posed by investigations and prosecutions.

Latvia

Ellex Klavins

Irina Rozenšteina Edvijs Zandars

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes		X	X	X	X
No	X*				

* No criminal liability of legal persons, but "coercive measures" (e.g. liquidation) possible in case of criminal conduct by employees. Administrative liability of corporations is possible.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The Whistleblowing Act requires that whistleblowers are provided with protection of identity. The law also guarantees protection to relatives and related persons of the whistleblower. All reports are confidential and shall be treated as such. Information in the whistleblower's report and the related investigation thereof is limited access information. It is forbidden to disclose information revealing the identity of the natural or legal person that is reported by the whistleblower.

Disclosures may only be allowed to the person responsible for the investigation based on the whistleblower's report, or to those, who are involved in the investigation initiated and require the information to perform their duties. The persons involved in the investigation usually sign a document that ensures confidentiality and non-disclosure during the process of investigation and after it has been finalised.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

An internal whistleblowing system must be set up for each legal entity. A group of undertakings with parent and subsidiary undertakings (branches)

(1) shall establish an internal whistleblowing system in each subsidiary undertaking (branch), which shall be treated as a separate legal entity;

(2) may additionally establish a central channel in the parent undertaking.

Although the Latvian Whistleblowing Act allows private legal entities with 50 to 249 employees (e.g. medium-sized companies) to join forces and set up a common internal whistleblowing system for receiving and handling reports, no such cases have been observed in practice.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Employee representative bodies do not have a legal right to be informed about or participate in internal investigations. However, at their discretion, employers may choose to inform such bodies. In practice, if there is a works council in a company, it is often recommended to inform it about an investigation. However, there is no formal process for this.

b) Although a data protection officer should be well informed about personal data processing in the company, there is no statutory requirement to involve or inform them about an investigation. However, it may be recommended to avoid possible unjustified intrusion in the data subject's private life.

c) There is no legal requirement to inform local authorities about the start of an internal investigation. However, if, in accordance with the law, a serious (e.g. intentional serious bodily injury) or especially serious crime (e.g. death following such injury) had to be reported to the competent authorities, but a person has failed to do so, the Criminal Act provides for liability for failure to comply with this duty. Special provisions also provide a duty to report certain conduct to authorities (e.g. environmental pollution, money laundering).

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees do not have a duty to support an investigation and, therefore, cannot be disciplined for failure to cooperate. However, there is a duty of an employee to perform their employment duties. An employee is required, if asked, to provide the employer with information regarding the performance of job duties. Nevertheless, it is not possible to force the employee to provide information about other employees.

The employer may impose disciplinary measures on the employee if the employee has failed to perform their duties or has not provided complete information about the performance of the job duties.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

No Labour Act deadlines could be triggered or employee sanctioning rights waived by investigation actions.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

General data protection rules from the General Data Protection Regulation ("**GDPR**") should be taken into account before conducting interviews. This includes the obligation of the data controller (i.e. the person who organises the investigation, most commonly the employer) to ensure that personal data of all parties are processed strictly for the purpose of the investigation and proportionally and that only duly authorised persons have access to such personal data. The employees must also be informed concerning the purpose of the data processing.

b) reviewing emails?

General data protection rules should be taken into account before reviewing emails.

c) collecting (electronic) documents and/or other information?

General data protection rules apply to the collection of any documents that may contain personal data. In addition, please note that Latvia does not have a blocking statute regime.

d) analysing accounting and/or other business databases?

General data protection rules apply. If there is no personal data involved, the data processing rules do not apply.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no legal obligation to provide the employee with written instructions. However, a company's internal whistleblowing policy or any other internal policy could provide such an obligation.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Employees do not have an obligation to answer questions during an internal interview. It is advisable to remind the employee that they have no obligation to give any information that could be self-incriminating.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no legal obligation to provide the employee with such a warning. The Whistleblowing Act is silent on this matter. However, the employer should inform the employee who will participate in the interview and the basis for their participation.

d) be informed of their right to have their own lawyer attend the interview?

There is no legal obligation to inform the employee of the right to counsel. The Whistleblowing Act is silent on this matter. However, it is advisable to inform the employee of their right to legal assistance. The employee has the right to invite their attorney-at-law in any case (i.e. a qualified lawyer admitted to the Latvian Bar Association).

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

There is no legal obligation to inform the employee of the right to have an employee representative attend the interview. As the employee has the right to ask an employee representative to attend the interview, it is advisable to inform the employee accordingly.

The Whistleblowing Act only states that the representatives of employees have the right to provide support and consultations to the whistleblower or an employee who wants to submit a whistleblower's report. The Labour Act provides general rights for employee representatives to obtain information and consult with the employer before the employer takes decisions that may affect the interests of employees. The Act on Trade Unions also provides their right to represent and defend the rights and interests of their members without special authorisation. Consequently, the employee representative would generally be entitled to participate in such meetings.

f) Be informed that data may be transferred cross-border (in particular to the United States)?

General data protection rules should be taken into account in regard to the cross-border transfer of personal data. Article 13 and 14 of the GDPR stipulate what information must be provided to the data subject before the processing of personal data has commenced. Among other information, the data subject must be informed of data recipients and of the fact that the data controller intends to transfer personal data to a third country (outside the European Economic Area) together with an indication of appropriate safeguards used.

g) sign a data privacy waiver?

Based on general data protection rules, it is difficult to ensure that consent of the employee is given freely in employment relationships. Thus, consent should not be used as a legal basis for personal data processing. Instead, other legal bases should be used, e.g. a specific agreement, to comply with legal obligations or if the processing is necessary for legitimate interests pursued by the employer.

h) be informed that the information gathered might be passed on to authorities?

Except when authorities request disclosure according to law, individuals must be informed about recipients of the data, including that information may be passed on to authorities, if the information is acquired from the respective employee. In case the information gathered has not been obtained from the respective employee, Article 14 of the GDPR allows not to inform the data subject if the provision of such information could impair the achievement of the objectives of the data processing, e.g. the investigation.

i) be informed that written notes will be taken?

There is no legal obligation to specifically inform the employee that written notes will be taken during the interview (as long as the employee is informed of the data processing itself). However, notes or minutes of an interview may only serve as valid evidence if all participants sign the notes or minutes, confirming the accuracy of the information.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no law regulating document hold or retention notices in Latvia. Therefore, document hold notices in private relations are admissible and are regulated by the company's internal policies.

The Act on Accounting, the Archives Act, and other laws set mandatory retention periods for certain types of documents. At the same time, the GDPR requires that personal data be retained no longer than necessary for the specific purpose. Since there are no specific retention periods indicated for information collected during an investigation, such information must be retained no longer than necessary for the purpose for which it was collected.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege applies exclusively to information provided by the client to the attorney-at-law. The attorney-at-law may not disclose the secrets of their client, even after the case is closed or the attorney-at-law has been released from handling the case. A report prepared by an attorney-at-law for the client in connection with an internal investigation led by the attorney-at-law would be protected from disclosure by the attorney-client privilege. Nevertheless, the client may be obliged to inform the authorities of potential criminal conduct uncovered by the report without disclosing the report itself. It is generally advisable to involve outside counsel (attorney-at-law) in internal investigations to ensure investigation findings are protected by the attorney-client privilege.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

The attorney-client privilege does not apply to in-house counsel. An attorney is understood to be a person who is an attorney-at-law or attorney-at-law assistant and has been admitted to the Latvian Bar Association (and has not suspended their practice) or who has a right to practice in Latvia in accordance with EU laws.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Early notification to the insurance company on the start of an investigation is only necessary if required by the insurance policy.

b) Business partners (e.g. banks and creditors)?

There is no statutory obligation to inform business partners about the start of an investigation.

c) Shareholders?

There is no legal obligation to inform shareholders about the start of an investigation. Still, the company's internal policies may provide such an obligation. Article 194 of the Commercial Act provides shareholders the right to be informed regarding the activities of the company and to become acquainted with all of the company's documents.

d) Authorities?

There is no legal obligation to inform the authorities of the start of an investigation. In certain cases, everyone must report criminal offences or administrative violations.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

As there is no law governing the conduct of internal investigations, there are no specific measures that legally must be taken once an investigation has started, other than the observance of the Labour Act, the Whistleblowing Act and data protection laws. Moreover, if a breach of law is detected, the company must take measures to stop the misconduct and prevent or minimise potential liability.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Internal investigations are outside the scope of competence of prosecutors, who are only concerned with criminal matters in the context of criminal investigations. However, it is crucial that the company does not destroy any potential evidence during the course of its internal investigation. Furthermore, if a serious or especially serious crime is detected, the company should report it.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Typically, a valid criminal search warrant requires initiation of a criminal procedure and court approval. In emergency cases where, due to a delay, objects or documents may be destroyed, hidden, or damaged, a search may be performed with the decision of the person directing the proceedings or, in case the decision is taken by the investigator, with the consent of a public prosecutor. If the prerequisites are not fulfilled (in criminal liability matters), the gathered evidence may not be admissible.

Regarding administrative liability, "dawn raids" may be initiated by various authorities with slightly different prerequisites. For example, in order to carry out a dawn raid, the Competition Council must obtain a court order where the subject and purpose of the inspection; the assets, information, and documents to be searched for; and the timeframe for performing procedural actions are specified.

By contrast, the police and similar authorities must initiate an administrative violation procedure and either obtain the consent of the property owner or a court order (or the consent of the prosecutor in emergency cases) in order to perform an on-site inspection. The presence of the property owner (or its representative) or a representative of the municipality is required. If the prerequisites are not fulfilled (in administrative liability matters), the gathered evidence may not be admissible unless the deviation from the requirements was minor.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Although a corporation may face so-called "coercive measures" when its employees have engaged in criminal conduct, legal persons are not subject to criminal liability under the Criminal Procedure Law. Legal persons, however, may be liable for violations of administrative laws in accordance with Law on Administrative Liability. Settlements with regulators in administrative cases are common for corporations.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

The Criminal Act provides for the following "coercive measures", which can be taken against a legal entity when its employees have engaged in criminal conduct: liquidation, limitation of rights, confiscation of property, and levy. Penalties under the Criminal Act for natural persons depend on the crime committed. For instance, an employee acting as an intermediary for bribery could face up to five years' imprisonment, community service or a fine. Certain criminal offences, e.g. engagement in a prohibited business, may lead to a prohibition of business activity and a ban on holding certain offices.

The most common type of penalty for administrative violations is a fine. For example, members of the management board of a legal entity may be fined for tax debts to the company. Members of the management board of a legal entity may also be held criminally liable, for instance, for evasion of tax payments. Pursuant to the Criminal Act, in such cases fine or even imprisonment could be applied.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

A reduction of penalties is unlikely, as the authority may assume that, if there is a compliance system in place at the company and a director, officer, or an employee has perpetrated any misconduct, this system does not work properly. The fact that the company has a compliance system that was not observed and that misconduct still occurred might be considered an aggravating factor to some extent.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Laws and regulations concerning ESG matters are currently under active development and are expected to enter into force in early 2024. The Consumer Rights Protection Centre has developed guidelines to address greenwashing cases but there is limited public information on cases where sanctions have been applied.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The first Whistleblowing Act came into effect on 1 May 2019, which was a new development for the implementation of effective compliance systems for companies. The new Whistleblowing Act which came into legal force on 4 February 2022 has definitely further strengthened the requirements.

The market shows that the companies pay more and more attention to corporate compliance issues. The compliance issues are important also from the perspective of ESG principles. There is also a trend for companies to take an increasingly responsible approach to risk management and possible reputational risks, which includes the development of appropriate internal investigation policies as part of their mitigation processes. Therefore, even though no uniform regulation exists to conduct an internal investigation and there are still many unclarities for the companies during such investigations, it is already clear that the implementation of an effective investigation policy and the conduction of proper internal investigations shall be an integral part of internal compliance systems.

CONTACTS

Ellex Klavins

K.Valdemara 62
1013 Riga
Latvia

Tel.: +371 67814848
Fax: +371 67814849
www.ellex.legal

Irina Rozenšteina (Kostina)
Associate Partner
Head of Employment Law Practice
Ellex Klavins
T +371 67814862
E irina.rozensteina @ellex.legal

Irina Rozenšteina is the Head of Employment Law Practice. She has more than 18 years of legal experience specialising in various employment and dispute resolution matters. Irina is an expert on sensitive management and key employee termination and complex multi-jurisdictional transfer of undertakings issues. Irina represents corporate clients in court proceedings in disputes with their former or current employees and in front of the supervisory state institutions, as well as advices clients. Irina has extensive experience on consulting clients regarding the inspections performed by controlling institutions, initiated administrative cases and appeals on its decisions in court. Irina's experience includes also representation of numerous clients in civil and administrative cases in local courts and in arbitration on different contractual and corporate matters. She also advises and represents clients in relation to recognition and enforcement of foreign court rulings and arbitral awards, assists in collection of evidence and cooperates with state bailiffs in the execution stage.

Edvijs Zandars
Associate Partner
Ellex Klavins
T +371 67350550
E edvijs.zandars@ellex.legal

Edvijs Zandars specialises in Competition Law, Information Technology, Intellectual Property and Data Protection. He regularly advises clients in all product life cycle stages and has broad experience in introducing various software products, telecommunications equipment and consumer goods to the local market. Edvijs is also proficient in data protection matters and provides assistance to data controllers and processors in fulfilment of requirements by the Latvian and EU Law. He also has significant experience in advising international and local clients on protection and enforcement of intellectual property rights and other regulatory matters.

Liechtenstein

Gasser Partner Rechtsanwälte

M.A. HSG Thomas Nigg, LL.M.

Mag. iur. Johannes Sander

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X*	X
No					

* See paragraph 63 *et seq*. of the StGB.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Although there is still no specific whistleblower protection law in Liechtenstein, the Financial Market Authority ("**FMA**") created an external platform based on Articles 4 and 5 of the Financial Market Authority Act. The whistleblower platform serves as protection for whistleblowers, who report potential or actual violations, in order to effectively combat abuse and better protect clients of Liechtenstein's financial centre (cf. also Article 28a of the Due Diligence Act, the "**DDA**"). The platform was set up in order to bring Liechtenstein in compliance with European financial market regulations.

These reports can be made to the FMA either online or via post and may be anonymous. After reviewing the report, the FMA may contact the whistleblower to obtain additional information if necessary and provided that the identity is known. Reports that do not fall within the scope of the FMA's legal competencies are forwarded to the competent authority (e.g. allegations of criminal conduct are forwarded to the prosecutor's office).

With respect to internal whistleblowing, Article 28a (3) of the DDA states, for instance, that companies subject to the DDA with more than 100 employees must establish an internal, anonymous reporting procedure for whistleblower complaints. However, the law does not provide guidance on the content of the internal process. A duty to investigate such internal reports will usually be included in internal compliance guidelines and is incumbent upon the management of a company. However, a whistleblower does not have to be informed of the outcome of the investigation.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The EU Whistleblower Directive (Directive (EU) 2019/1937) is currently under scrutiny by the European Economic Area ("**EEA**"). This process and the subsequent adoption into the general acquis of the EEA is a

prerequisite for the incorporation of the Directive into Liechtenstein law. According to the Liechtenstein EEA Staff Unit, the timing and form of implementation for the Directive are currently uncertain.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

First of all, one must clarify that a specific (legal) concept of internal investigations, which may perhaps exist in other countries, does not exist in Liechtenstein. Potential internal wrongdoings are investigated based on internal guidelines.

a) Public and private labour law provide for employee representatives/employee representative bodies. These mainly deal with abusive wage payments, health protection issues, or mass redundancies (see Article 45 of the Labour Law). The law does not require that an employee representative body be advised of internal (whistleblower) investigations.

b) According to Article 13a of the Data Protection Ordinance ("**DSV**"), the data protection officer ("**DPO**") must have access to all information necessary to fulfil their duties, which includes monitoring the use of personal data and remedying data privacy violations. In addition, the DPO must maintain a data collection list and provide it to the data protection authority or persons concerned upon request. Therefore, in general, the company has to inform the DPO about all data privacy-related procedures, including process of an internal investigation.

c) With respect to internal investigations, local authorities do not have a specific right to be informed. However, in some cases, it might be useful to involve them on a voluntary basis.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

There are no explicit provisions concerning the participation of employees in internal investigations. However, according to labour laws, employees have to act in the employer's interest, which may – based on a case-by-case basis – include the duty to cooperate in and/or contribute to internal investigations to the extent it concerns their profession and/or area of work. If the employee refuses to participate in the investigation, their behaviour potentially qualifies as professional misconduct and may provide ground for the termination of the employment.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

If an employer obtains knowledge of relevant facts which could lead to an immediate dismissal, the employer must immediately dismiss the employee without notice. Otherwise, the employer forfeits the right to do so. There is no specific deadline, but in principle, the terminating party must declare the termination as soon as the reason for termination has come to their knowledge. An appropriate period for consideration is usually two to three working days and, in exceptional cases, one week. A "serious" suspicion of professional misconduct satisfies the knowledge prerequisite. Therefore, it is critical to know at which point during an investigation a suspicion becomes "serious". Except for cases of immediate dismissal, no other labour law deadlines are triggered or rights waived by investigative actions.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

By Resolution of 10 July 2018, the General Data Protection Regulation ("**GDPR**") was adopted to the general acquis of the European Economic Area. Since 20 July 2018, it is applicable in Liechtenstein. The GDPR governs any processing of personal data wholly or partly by automated means and any other processing of personal data that form or is intended to form part of a filing system (cf. Article 2 GDPR). Labour law allows for the processing of employment-related information if it is necessary to fulfil the employer's duties. This naturally includes protocols of employee interviews. However, processing and sharing data within the company and/or company group is only allowed within the boundaries of the GDPR.

b) reviewing emails?

The Department for Economics (*Amt für Volkswirtschaft*) released guidelines for the surveillance of employees. However, the latest version is dated February 2018 and therefore does not include the GDPR. According to Article 88 GDPR and Article 1173a paragraph 28a Liechtenstein Civil Code, the processing of an employee's data is admissible in order to conduct and fulfil the employment contract. Whether the general surveillance of employees is admissible, especially having regard to the principle of proportionality and reasonableness, has not been tested in court. Further, it depends on the facts of each case. For example, as German literature suggests, it may make a difference whether the employee is allowed to use their email for private purposes also.

c) collecting (electronic) documents and/or other information?

In principle, the same applies to collecting (electronic) documents and/or information. However, since (electronic) documents usually do not contain "private by-catch information", the issue is probably less of a practical concern. Provided that the employer and/or employee can demonstrate a justified interest in collecting documents, it may be admissible according to the GDPR. In our opinion, collecting data that assist in uncovering an infringement or violation of legal duties should be justified as the GDPR does not intend to cover up professional misconduct.

d) analysing accounting and/or other business databases?

Analysing accounting and business databases may be regarded as "processing" under GDPR. However, the GDPR only protects personal data of natural persons. Analysing accounting and business databases is, therefore, not covered by the GDPR regime.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no legal obligation to give written instructions to employees before internal interviews.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Under the Criminal Procedure Act of Liechtenstein, a suspect has the right to remain silent during interrogations by criminal authorities and in criminal proceedings in general. However, there is no corresponding "right" or "duty" with regard to employee interviews as part of an internal investigation.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

In Liechtenstein, there is no legal obligation to give an employee an Upjohn warning. However, the warning is, in practice, commonly given. According to the Liechtenstein Bar Association, lawyers are not allowed to represent more than one client in the same matter. Although they are not obliged to inform the employees of this fact, it is generally good practice to do so.

d) be informed of their right to have their own lawyer attend the interview?

There are no explicit provisions concerning the duty to inform an employee of their right to have a lawyer present during an internal interview.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

As already mentioned, there is no law in Liechtenstein regarding internal investigations. Such internal investigations are subject to and follow internal guidelines. Hence, internal guidelines must be checked to see if the employee has a right to have a works council representative attend the interview.

f) be informed that data may be transferred to another country (in particular to the United States)?

Since the GDPR is applicable, its provisions on sharing and transferring data cross-border need to be considered. Transferring data falls within the term "processing data", which is why the general preconditions for processing data must be fulfilled (Article 6 GDPR). Provided that processing data, including the transfer to third countries according to Chapter V GDPR is admissible, the employee does not have to be informed specifically.

g) sign a data privacy waiver?

As outlined in question 6b, we are of the opinion that collecting data for whistleblower purposes and/or for uncovering illegal activities within the boundaries of proportionality and reasonableness is admissible irrespective of the consent of the individual. The GDPR does not serve to cover illegal misconduct. As a consequence, we are of the opinion that a privacy waiver is neither necessary, nor is it necessary to inform the employee about a privacy waiver. However, this has not been subject to a decision by the Data Protection Authority or a court in Liechtenstein. Therefore, these remarks merely represent the view of the authors. Due to the lack of case law or decision of the Data Protection Authority, there is no claim to completeness.

h) be informed that the information gathered might be passed on to authorities?

There is no legal obligation to inform the interviewee that the information gathered might be passed on to authorities. However, it is advisable to inform about the possibility.

i) be informed that written notes will be taken?

There is no legal obligation to inform employees that written notes will be taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

With respect to this matter, there are no statutory provisions concerning document hold notices or document-retention notices in Liechtenstein nor is there any published case law in this regard.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

According to Article 15 of the Lawyers Act ("**RAG**"), attorneys-at-law are bound to secrecy concerning all issues related to their profession that are of interest to their clients. The right of an attorney-at-law to secrecy may not be circumvented by judicial or other official measures, and attorney-client privilege is not waived even if a privileged correspondence is found outside of the attorney's custody (Article 15 (2) and (3) RAG).

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Provisions regarding attorney-client privilege are only applicable to attorneys-at-law. Correspondence and documents of in-house counsel are not included in the scope of RAG. Nonetheless, in-house counsel bears a duty of confidentiality, resulting from the general duty of trust and loyalty to an employer. According to case law, the seizure of records of attorneys-at-law is forbidden, but this does not include documents written, gathered or

possessed by an in-house counsel. In order to ensure privilege protection, it is therefore recommended to involve outside counsel (attorneys-at-law).

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Possible reporting obligations may only arise from the insurance policy itself or general contractual duties of care and loyalty.

b) Business partners (e.g. banks and creditors)?

Information duties may only arise from contractual obligations between the company and the business partner.

c) Shareholders?

Internal investigations, depending on their subject matter and scope, may relate to insider information that could possibly influence stock prices. According to Article 5a of the Market Abuse Act, an issuer of financial instruments has to disclose to the public insider information that may affect the price of such instruments as soon as possible. Therefore, it is important to evaluate if there is an obligation to report to the shareholders on a case-by-case basis.

d) Authorities?

There is no general legal obligation to inform authorities about an internal investigation. However, taking into account one's own potential liability (e.g. omission or assistance), certain criminal offences should be reported to the public prosecutor. Also, other statues require that government/supervisory authorities be notified of certain circumstances.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Although there are no statutory obligations on companies with respect to internal investigations, a company should stop any criminal conduct of employees as soon as it becomes aware of the conduct and take steps to minimise damages. If employees are affected, this will be of the utmost importance to the company.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutors do not generally play a role in internal investigations. However, it is important that a company does not destroy any relevant information or evidence during an internal investigation. This could become relevant if certain criminal offences are later reported to the public prosecutor.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

There are formal and material prerequisites set forth in the Criminal Procedure Act ("**StPO**"), which must be met in order to have a valid search warrant or conduct a legitimate dawn raid.

A search warrant is usually initiated upon motion of the public prosecutor and ordered by a court. A search warrant must be based on exigent circumstances or a reasonable suspicion that a person suspected of a crime, or an item used for committing a crime, can be found (see Articles 91a and 98 *et seq*. of the StPO).

Competent supervisory authorities may carry out extraordinary on-site visits within the framework of the DDA (see Article 28(1)(c)).

According to the judgement of the Austrian Supreme Court, illegally gathered evidence may still be used in court proceedings unless expressly prohibited by law. According to the Liechtenstein State Court, the same applies in Liechtenstein.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Only under certain circumstances set forth in the StPO may deals and non-prosecution agreements between the court or the public prosecutor's office and a corporation be reached in association criminal proceedings (*Verbandsstrafverfahren*).

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

The liability of legal entities is regulated under Article 74a *et seq*. of StPO. Legal entities are responsible for the offences and crimes committed by managers and directors, which are culpably committed in the performance of business activities. However, a legal person should only be responsible for the offences of regular (i.e. non-managerial) employees, even if the offence was not culpably committed, where the commission of the offence was made possible or substantially facilitated by the failure of the managers to take necessary and reasonable measures to prevent such offences.

Typical criminal penalties that result from misconduct of individuals are fines, disgorgement of proceeds or, in the case of executives, imprisonment. Depending on the nature of the business or profession, individuals may be further punished during the disciplinary proceeding with disbarment from their profession or fines.

If a legal entity is held responsible for an offence, it shall be subject to a "corporate monetary penalty" (*Verbandsgeldstrafe*). The corporate monetary penalty is to be calculated in daily rates (*Tagessätze*) and can be conditionally suspended in whole or in part. The daily rate shall be assessed according to the income situation of the legal person, taking account of its economic ability apart from the income situation, the seriousness of the offence, and any remedial measures taken by the entity after the offence. The daily rate typically corresponds to 1/360 of annual corporate revenue but must be at least 100 Swiss francs and at most 15,000 Swiss francs.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Where the corporate monetary penalty imposed on a legal person is conditionally suspended in whole or in part, the court may issue instructions imposing technical, organisational, or personnel measures on the legal person to deter further offences for which the legal person is liable. The legal person shall, in any event, be instructed to rectify the damage arising from the act to the best of their ability, to the extent that this has not already occurred.

As a general principle, the implementation of a compliance system may also be taken into account when it comes to determining the level of guilt, which necessarily has consequences on the level of fines.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

The EEA-Sustainability Implementing Act ("**EWR-FNDG**"), effective from 1 May 2022, marks Liechtenstein's formal adoption of EU Regulations 2019/2088 and 2020/852 into its national legislation. This act is a strategic move towards achieving carbon neutrality by 2050, safeguarding investor interests, and combating "*greenwashing*". It mandates that financial market participants and advisors disclose detailed sustainability information, both at the organisational level and for the financial products they offer.

This transparency is aimed at encompassing environmental, social, and employee-related aspects, alongside a commitment to human rights, and the prevention of corruption and bribery.

Financial intermediaries in Liechtenstein are directly impacted by this legislation, compelling them to adhere to these disclosure obligations. They are required to present this information to the public in a transparent, understandable, and consistent manner. The enforcement of ESG-related regulations in Liechtenstein involves key regulatory bodies. The Office for Environment and the Financial Market Authority ("**FMA**") play pivotal roles in ensuring compliance with ESG standards, with the FMA specifically tasked with overseeing the integration of ESG factors into the risk management and reporting practices of financial institutions.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The recent creation of the FMA mechanism for handling whistleblower complaints is the most noteworthy trend. The topic is very relevant, and areas of conflict with various elements of criminal law, data protection, professional secrecy, and fiduciary duties must be considered.

CONTACTS

GASSER PARTNER

Wuhrstrasse 6
9490 Vaduz
Liechtenstein

Tel.: +423 236 30 80
www.gasserpartner.com

M.A. HSG Thomas Nigg, LL.M.
Senior Partner
GASSER PARTNER
T +423 236 30 80
E thomas.nigg@gasserpartner.com

Thomas Nigg is Senior Partner of GASSER PARTNER Attorneys at Law, one of the leading law firms in Liechtenstein and a Chambers Global and The Legal 500 top tier firm.

Thomas is admitted to the Liechtenstein bar and specialised in advising international and local clients with regard to all matters in relation to Liechtenstein corporations, foundations and trusts. His expertise extends to the setup and day-to-day management of these structures, as well as litigation in civil and criminal matters with a specific focus on commercial, corporate, foundation, and trust cases as well as banking and regulatory issues.

His career is highlighted by his involvement in complex litigation matters related to private wealth structures, including asset tracing and the enforcement of international judgements in Liechtenstein.

Mag. iur. Johannes Sander
Partner
GASSER PARTNER
T +423 236 30 80
E johannes.sander@gasserpartner.com

Johannes Sander is a Partner at GASSER PARTNER Attorneys at Law. He is admitted to the Liechtenstein bar and is also qualified as a lawyer in Austria. He is specialised in advising international and local clients with regard to all matters in relation to Liechtenstein corporations, foundations and trusts. Moreover, he advises his clients in classical civil law matters, white collar crime, corporate law, foundation and trust law, litigation and dispute resolution.

As part of the Private Client and Litigation team at GASSER PARTNER and due to his professional knowledge, Johannes Sander regularly advises international trust and fiduciary service providers, high net worth individuals, insurance companies as well as family offices.

Lithuania

COBALT

Dr. Dalia Foigt-Norvaišienė

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X			X
No			X	X	

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The Law of the Republic of Lithuania on Whistleblower Protection does not provide for any specific procedures. However, every company must maintain internal channels for whistleblower reports and keep the information on whistleblowers strictly confidential. In addition, the whistleblower must be notified within two business days about the receipt of the report and within ten business days about the progress of the examination (planned or performed investigative actions, their justification or refusal to examine the information).

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

In Lithuania, every private legal entity with 50 or more employees must install an internal reporting channel. The Lithuanian legislation remains silent about the use of group wide reporting systems.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) The Labour Code and/or other Lithuanian legislation do not provide an obligation to inform any employee representatives about an internal investigation.

b) According to the Lithuanian Law on Legal Protection of Personal Data ("**LPPD**"), there is no obligation to inform a data protection officer ("**DPO**") or a data privacy authority about an internal investigation. However, if a DPO is appointed, general GDPR principles apply. For example, any employee may inquire about their data privacy rights (including information provided in the whistleblower report). Also, the DPO shall be entitled to obtain the necessary information to respond to the request. In addition, the DPO has data processing monitoring duties. Thus, the company will generally have to inform the DPO about all data privacy related procedures and processes of an investigation.

c) Lithuanian legislation does not oblige the employer to inform the prosecution authorities about an internal investigation. However, the authorities need to be informed immediately if, during an internal investigation, the employer discovers signs of a current or future potential breach of criminal law.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

The Labour Code does not specify the duty of the employee to support the investigation. However, according to paragraph 1 of Article 24 of the Labour Code, employers and employees must act honestly and cooperatively. They must not abuse the law when performing their labour law rights and duties. This means that the employee has to participate in the investigation by answering questions related to their employment duties truthfully and completely.

If the employee is required to participate in the investigation, the employee's refusal may be regarded as misconduct. Such misconduct may justify a dismissal if the employee had already received a formal warning for the same or similar misconduct before.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

According to paragraph 3 of Article 49 of the Labour Code, the employer can remove the employee from their work for up to 30 calendar days during the investigation of circumstances on the possible breach of employment duties by the employee. During this time, the employer has to pay the employee their average salary.

Further, under Article 58 paragraph 6 of the Labour Code, an employer shall decide to terminate the employment contract for its violation within one month from the disclosure of the violation and no later than six months after the date of the violation. The latter period might be extended to two years if the violation committed by an employee results from an audit, inventory or inspection of an activity.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The LPPD provides certain specific local requirements. However, these requirements do not deal with employment-related investigations. Thus, the general GDPR principles of transparency, fairness, and lawfulness apply. Thus, employees have to be informed that (i) in case of any suspicion or a claim, an internal investigation shall be carried out by the impartial local investigation team, (ii) whether anonymous claims are accepted, (iii) how long the data obtained during the investigation is stored, (iv) who shall have access to it, etc.

b) reviewing emails?

General GDPR principles of transparency, fairness, and lawfulness apply. It is very important that employees are informed about the situations in which their emails or other electronic communication can be monitored. The Lithuanian supervisory authority has provided a public opinion about monitoring

employees' emails and other communication. According to this opinion, overall monitoring of emails is prohibited. There has to be a valid reason for such monitoring, for example, suspicion of fraud, long absence, and suspicion of unethical behaviour or breach of internal company rules. If emails are monitored, it is highly recommended that a representative of employees is present not to jeopardise any evidence.

Moreover, if an email is clearly marked as "personal" or "private", it should generally not be opened. In order to properly inform the employee, it is recommended to inform the employee in line with the internal policies of the company governing the monitoring of electronic communication at the workplace.

c) collecting (electronic) documents and/or other information?

All documents and data, both in written and electronic form, are the employer's property which means that there is no prohibition to collect and/or review this information. If a folder is marked "Personal" or "Private", it should generally not be collected unless there is reliable evidence that the file has been named "personal" in deceit.

d) analysing accounting and/or other business databases?

Analysing accounting and/or other mere business databases is not legally restricted.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no general and statutory obligation to instruct an employee about the legal circumstances and their rights before the interview.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

The right to remain silent to prevent self-accusation only applies if local authorities interrogate a person under the suspicion that the person may have committed a crime. This right is in no way connected to interviewing an employee during an internal investigation.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no explicit obligation to inform the employee that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee.

d) be informed of their right to have their own lawyer attend the interview?

If whistleblowers are recognised by the competent authority as such, they have a right to legal aid.

The employee's general right to have a lawyer present during the interview is not governed by Lithuanian law. However, companies often allow this kind of legal attendance in order to have a fair set-up or if the employee is suspected of having committed an offence.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

According to Lithuanian legislation, the employee does not have a strict legal right to be attended by a representative of the work council.

f) be informed that data may be transferred to another country (in particular to the United States)?

Yes, employees must be informed about their data transfer to countries outside the EU/EEA. Such countries must be disclosed, and applicable security measures must be indicated. The data transfer to third countries is performed according to the GDPR standards. There are currently no local regulations or guidelines on this topic.

g) sign a data privacy waiver?

The wording of applicable laws does not explicitly provide for the possibility of a privacy waiver. Moreover, there is a high risk in employment relations that such an employee privacy waiver would be considered forced due to subordination. Therefore, we have not witnessed such waivers in practice.

h) be informed that the information gathered might be passed on to authorities?

In accordance with the GDPR, an employee must be informed about all potential recipients to whom the employee's personal data may be transferred to.

i) be informed that written notes will be taken?

The content of the information to be provided to the data subjects is provided in Articles 13-14 of the GDPR. The mentioned provisions do not contain an explicit requirement to inform about interview notes being taken. However, in order to be transparent, the employer may provide as much information as they consider necessary.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law governing this question. However, issuing such notices is a common procedure.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The results of the internal investigation may not be revealed due to client secrecy. By the mentioned way, attorney-client confidentiality may be applied.

In accordance with the Law of the Bar Association of the Republic of Lithuania, an attorney-at-law cannot be summoned as a witness or provide explanations about the circumstances he gained knowledge about by providing legal service. This is because of their professional duties. It is also generally prohibited to inspect, check, or withdraw attorney at law's documents (in any form) related to their activity. Therefore, the search or examination of the attorney at law in their workplace, living place, vehicle, etc., can be performed only with the participation of the member of the Executive Board of the Bar Association.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

The Labour Code does not explicitly regulate attorney-client privilege for in-house counsel. Therefore, authorities can, in general, seize documents in the custody of in-house counsel.

However, under Lithuanian case law, in-house counsel have to inform authorities if they become aware of a potentially committed crime within their company.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

As far as circumstances arise which could cause claims against the insurance company, the policyholder should notify the insurer of the circumstances. However, there are no Lithuanian legal statutes that govern such explicit obligation.

b) Business partners (e.g. banks and creditors)?

Lithuanian legislation does not govern such an obligation. However, the duty to inform a business partner may arise from contractual obligations between the parties. It depends on the individual case whether and when the business partner needs to be notified.

c) Shareholders?

Lithuanian laws do not govern explicit obligations to inform shareholders about the internal investigation.

d) Authorities?

There is no duty to inform the prosecutor about the internal investigation or potential misconduct within the company. There may only be exceptions for very significant crimes, for instance, murder, serious health impairment, etc. However, a cooperative approach with the local prosecutor may prevent adverse and unexpected measures by the authorities, such as dawn raids.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

In accordance with paragraph 2 of Article 205 of the Labour Code, the employer has to inform and consult employees about all questions of particular importance. Starting an internal investigation may be considered such an event.

Further, if the company becomes aware of ongoing criminal conduct within the company, it may be advisable to conduct disciplinary measures to stop such misconduct. There are two ways to make sure that an individual's behaviour is stopped:

– In accordance with paragraph 3 of Article 49 of the Labour Code, an employer may, while examining the circumstances in which an employee may be subjected to the breach of their duties, suspend the employee for 30 calendar days, paying them their average salary;

– Under Article 58 paragraph 2, subparagraphs 5 and 6 of the Labour Code, there is a possibility to terminate the employment contract with the employee in case of the following circumstances:

  - Material damage done deliberately to the employer or an attempt to intentionally cause them material (property) damage;
  - An act having characteristics of a criminal offence was committed during work time or at the workplace.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices generally appreciate internal investigations through external investigators, such as law firms. Early involvement, communication and coordination may be helpful for good cooperation with local prosecutors. In this regard, it is crucial that the company does not destroy any potential evidence or convey the impression that evidence is or will be destroyed. Therefore, data retention orders should be communicated at the earliest stage possible.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Under Article 145 of the Code of Criminal Procedure of the Republic of Lithuania, in cases where there are grounds for assuming that there are, in some premises or any other place or the possession of some person, instruments of a crime, tangible objects and valuables that were obtained or acquired in a criminal offence, a pre-trial investigation officer or a prosecutor may conduct a search to discover and seize them.

The search is carried out on the basis of a reasoned judgement issued by the pre-trial investigation judge. This judgement must specify the objects to be searched for (possession of a person, instruments of a crime, tangible objects and valuables that were obtained or acquired in a criminal way, or certain items or documents potentially relevant to the investigation of the criminal offence). In cases of utmost urgency, the search may be carried out pursuant to the resolution of a pre-trial investigation officer or a prosecutor. However, in such cases, a pre-trial

investigation judge has to confirm the legitimacy of such a search within three days after the search. If the confirmation from a pre-trial judge is not received within the specified period, all objects, valuables, and documents seized during the search must be returned to the persons from whom these objects, valuables, or documents had been taken. Further, the results of such a search may not be used as evidence in further proceedings. The latter also applies if other requirements for the search are not met.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Deals and non-prosecution agreements are not provided for corporations under Lithuanian law.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

In accordance with the Penal Code of the Republic of Lithuania ("**Penal Code**"), there is no special provision for misconduct between companies or their directors, officers, or employees. However, if one of the mentioned subjects commits a crime against another subject, penalties can generally include fines, public work, arrests or even imprisonment. The type of penalty depends on the committed crime.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Lithuanian law does not provide for such a possibility. However, Lithuanian courts might consider on a case-by-case basis the possibility of reducing penalties in case the efficient compliance system has already been implemented prior to the alleged misconduct.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

In 2024, Lithuania will adopt a package of amended and supplemented Acts implementing Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, "as regards corporate sustainability reporting".

Lithuania approved OECD Guidelines for Multinational Enterprises and OECD Due Diligence Guidance for Responsible Business Conduct.

Lithuanian Government adopted Decree on Green public procurement.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

We are not aware of post-GDPR case law regarding internal work-related investigations. However, as mentioned in 6b above, the Lithuanian supervisory authority has provided a public opinion about monitoring employees' emails and other communication. In essence, this public opinion sets certain trends regarding data processing of employees, such as a prohibition of overall monitoring. In practice, it is also highly recommended that any extraction of evidence is performed in the presence of the employee representatives.

CONTACT

Lvovo 25
Vilnius 09320
Lithuania

Tel.: +370 5250 0800
www.cobalt.legal

Dr. Dalia Foigt-Norvaišienė
Specialist Counsel
COBALT
T +370 5250 0800
E dalia.foigt@cobalt.legal

Dr. Dalia Foigt-Norvaišienė is Specialist counsel at COBALT Lithuania. She has an extensive experience of over 28 years in advising clients on Employment and Corporate Law issues. Furthermore, she is a recognised expert on international and domestic arbitration. She provides both day-to-day counselling and assists clients in more extensive projects and cross-border transactions. She has assisted numerous local and international clients in choosing the best solution for establishing a business in Lithuania and in setting up and operating these businesses, including but not limited to employment matters. Dalia is frequently invited to share her experience and knowledge in international publications, conferences, seminars and training.

Before starting a private practice, Dalia gained her PhD in the area of Environment law and continued her career as a Senior Researcher and an Associated Professor at Vilnius University. Dalia has also taken part in legislative work in Lithuania in the areas of Environment and Litigation.

Dalia is an active member of the business community and maintains good contacts with municipal and central government institutions while representing the business community and seeking to improve the business environment. Dalia is an honourable member of the Business Women Association, member of the European Business Network, the France-Lithuanian Chamber of Commerce, Chairperson of the Ethical Court of Lithuanian Bar, the International Bar Association, and the Lithuanian Bar.

Luxembourg

LUTGEN + ASSOCIES


André Lutgen


Pierre Hurt


Florent Kirmann


Géraldine Mersch

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The recent law dated 16 May 2023 (hereinafter, the "Law of 16 May 2023") transposes the European Directive 2019/1937 on the protection of persons who report breaches of Union law in Luxembourg. Exceeding the minimum requirements of the directive, the Luxembourg Law covers violations of any legal provisions.

Employees, self-employed workers and members of governance systems have the right to report a violation of any legal provision. This right is accompanied by a detailed legal regime defining (i) the notion of whistleblower, (ii) the conditions for protection of the whistleblower, (iii) the protection measures due to the whistleblower, (iv) administrative and criminal penalties in the event of non-compliance with the law and (v) implementation of competent authorities intended to receive reports, in particular the new Reporting Office (*Office des signalements*) placed under the authority of the Minister of Justice.

The Law creates a general regime of protection in addition to the special regimes of protection already in place in certain domains such as corruption, influence peddling (*trafic d'influence*) and unlawful taking of interest (*prise illégale d'intérêts*) pursuant to Article L.271-1 of the Labour Code, anti-money laundering pursuant to Article 4 (4) of the law of 12 November 2004 on the fight against money laundering and terrorist financing and market abuse and insider trading pursuant Article 8 of the law of 23 December 2016 on market abuse.

The Law does not create a special regime for situations where an internal investigation follows a report by a whistleblower. The protection resulting out of the general regime or specific regime, where applicable, must be applied during an internal investigation. Hence, confidentiality of the whistleblower's identity must be guaranteed at all times, except with their prior consent or within specific derogative scenarios.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The Law does not specifically provide for group wide reporting systems.

However, the Law allows private companies with 50 to 249 employees to share resources for receiving and following up on reports. This provision may be interpreted as allowing entities within the same group counting each less than 250 employees to share their reporting system. The Law does not mention a territorial criterion, i.e. whether resources can only be shared when entities are based in Luxembourg or in the European Union.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Except for sexual and moral harassment investigations, the law does not provide for the implication of employee representative bodies in internal investigations. However, certain industry collective agreements may require this.

b) The employee's right to privacy in the workplace is protected under Luxembourg law. Under the General Data Protection Regulation ("**GDPR**") and the law of 1 August 2018 implementing the GDPR (hereinafter, the "**Law of 1 August 2018**"), most companies operating in Luxembourg, depending on their core activities, are required to appoint data protection officers ("**DPO**").

Neither the GDPR nor the Law of 1 August 2018 provide for specific hypothesis of an internal investigation. Given that the internal investigation however necessarily encompasses the processing of data, the investigation must be compliant with the GDPR and the Law of 1 August 2018. General provisions on the missions of the data protection officer and the information of the Commission Nationale de la Protection des Données (hereinafter, "**CNPD**") apply. The Law of 16 May 2023 on the protection of whistleblowers expressly provides for the rules of processing of data following an alert.

c) Depending on the revelations of the internal investigation, the information of the supervisory body of the financial sector, the Commission de Surveillance du Secteur Financier ("**CSSF**"), or the supervisory body of the insurance sector, the Commissariat Aux Assurances ("**CAA**"), should be carefully taken into consideration, if the stakeholder falls under such supervision.

If the internal investigation reveals ongoing or past criminal behaviour, the information of the judicial authorities must also be duly considered. On that note, it should be noted that established authorities, public officials, civil servants and all agents and employees charged with a public mission must inform the public prosecutor about crimes or offences that they receive knowledge of during the accomplishment of their mission.

The obligation to report suspicious operations pursuant to the law of 12 November 2004 on the fight against money laundering and terrorist financing must also be considered.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

An employee's duty to support an internal investigation is inferred from the employee's general duty of loyalty to their employer, i.e. the duty to act in the employer's best interests. Disciplinary measures, including dismissal, can be taken against an uncooperative employee where the lack of cooperation constitutes misconduct. Employers should be careful in assessing the gravity of an employee's uncooperative behaviour, as sanctions must be proportionate.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

When an employer gains knowledge of severe misconduct, which could justify immediate dismissal, the employer has one month to proceed with the dismissal. Such knowledge may be obtained through the investigation.

If the employer decides to sanction an employee for misconduct, the same misconduct cannot be used at a later stage as grounds for dismissal.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

The GDPR applies in Luxembourg since 25 May 2018 and is implemented by the Law of 1 August 2018.

In very limited cases, the protection of state secrecy must be taken into account pursuant to the law of 5 July 2016 providing for the reorganisation of the State's intelligence service.

a) conducting interviews?

Data protection rules apply to any processing of data. This includes securing, collecting, and reviewing data and creating work products, such as interview file notes and final reports. Therefore, it is very important to perform an early assessment of the applicable data protection rules with the DPO and to document the steps taken.

b) reviewing emails?

Private communication is highly protected under Luxembourg law. The employer has a general obligation to respect the privacy of non-professional electronic communications of employees. Therefore, a thorough analysis of legal exposure should always be performed before an email review is initiated.

c) collecting (electronic) documents and/or other information?

Data protection rules must be followed.

d) analysing accounting and/or other business databases?

No law in Luxembourg restricts the analysis of accounting and/or other mere business-related databases.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no legal obligation to provide written instructions to employees. It is nevertheless recommended to inform employees of the general context of the investigation and of their rights during the investigation, notably the right to be assisted by a representative of the employee representative body, where applicable. Such information should be provided in writing, with a copy to be signed by the employee.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Although an individual has the right to remain silent during interrogations by criminal authorities, there is no corresponding right with regard to employee interviews as part of internal investigations.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

A so-called Upjohn warning must be provided to the interviewee under the ethical rules of the Luxembourg Bar Association.

d) be informed of their right to have their own lawyer attend the interview?

It is unclear from the case law whether an employee has a right to have personal counsel attend the interview. However, companies often allow such attendance to have a fair set-up or if the employee is suspected of having committed criminal offences.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Where the right to be assisted by a representative of the employee representative body is applicable, the employee must be informed about that right.

Even when not legally required, a company may choose to allow a representative to assist the employee, especially if the company is itself assisted by a lawyer, so as to preserve equality of arms between parties.

f) be informed that data may be transferred to another country (in particular to the United States)?

The employee has the right of information about the processing of his data pursuant to the GDPR and the Law of 1 August 2018.

g) sign a data privacy waiver?

It is advisable to offer the employee a data privacy waiver to sign. The employer should, however, still independently assess the legitimacy and proportionality of the subsequent use of the data, as the courts may review the adequacy of the employer's data privacy assessment, even in instances when an employee signed a waiver.

h) be informed that the information gathered might be passed on to authorities?

Even though there is no legal obligation in Luxembourg to inform the employee that information may be passed on to authorities, it is common practice to add this caution to the interview instructions. An interviewee should be informed if the data may be transferred to non-EU authorities.

i) be informed that written notes will be taken?

There is no legal obligation under Luxembourg law to inform the interviewee that notes will be taken. However, in the interest of transparency, the potential future use of information provided by the employee (e.g. for reports and potentially for disclosure) should be explained.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law or practice governing this question in Luxembourg.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

For the findings of the internal investigation to be covered by attorney-client privilege, the employer has to mandate a lawyer to proceed with the investigation. The lawyer can then require the assistance of experts if necessary (e.g. the forensic department of a consulting or accounting firm), whose work would be covered by attorney-client privilege by being integrated in the lawyer's investigation.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Attorney-client privilege does not apply to in-house counsel in Luxembourg.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Notification to insurance companies when starting an investigation is highly advisable. In this regard, the relevant insurance contracts should be checked.

b) Business partners (e.g. banks and creditors)?

Information duties may arise from contractual obligations between the company and the business partner. Even if there is no explicit provision in the contract, there may nonetheless be an obligation in cases where the internal investigation concerns information that is highly important for the other party and relevant to the purpose of the agreement. These interests of the business partner need to be evaluated against the legitimate interests of the company. Therefore, it depends on the individual case whether and when the business partner needs to be notified. In any circumstance, the situation in regard to legal privilege must be carefully examined.

c) Shareholders?

Duties to inform shareholders only exist for publicly listed companies and may be at odds with the desire to maintain confidentiality or professional secrecy duties. The company must evaluate on a case-by-case basis if there is an *ad hoc* duty to report to shareholders.

d) Authorities?

Depending on the area of activity of the company or on the type of incident that is investigated, various authorities and supervising bodies may need to be notified (e.g. the CSSF, the CAA or the Cellule de Renseignement Financier).

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

A company is expected to show diligence in identifying the damage caused by the alleged misconduct, mitigating its effects, and preventing further damage (e.g. by strengthening processes or reinforcing its compliance system). It is also recommended that a company proportionately sanction misconduct to discourage further cases.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

The need to report the facts leading to an internal investigation or the results of such an investigation to the public prosecutor's office is to be evaluated by the company (except where there is a legal obligation to report). Should the prosecutor's office open its own criminal investigation, the authorities will typically take complete control of the investigation. Any parallel internal investigation will have to be coordinated with them.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

A search of company premises may only take place by order of an investigating judge and cannot begin before 6.30 a.m. or after midnight, except in cases of flagrante delicto. Furthermore, a search of company premises cannot devolve into a so-called "fishing expedition" to discover infringements. The search can only be used for the purpose of finding evidence to strengthen an existing investigation of identified infringements. All types of communication between a lawyer and the client are protected by legal professional privilege and cannot be seized, except if the lawyer is suspected of having committed a crime. Searches executed in breach of the legal prerequisites can be annulled, rendering seized evidence unusable. However, companies should be mindful of the short statute of limitations to file an annulment claim.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Corporations may make deals with the public prosecutor's office in cases of offences with a fixed sentence of up to five years of imprisonment and/or a fine of a minimum of €500. The maximum fine depends on the nature of the offence and could reach millions of euros. Such deals are mainly used in cases of minor offences and white collar crime. A deal may be entered into as long as the defendant's guilt has not been determined by a judgement on the merits. It is, therefore, recommended to begin negotiations with the prosecutor's office as early as possible if this step is considered an option.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

The prosecution of a company does not preclude the prosecution of the individual(s) involved in the commission of the offence.

Four types of penalties are applicable to companies: fines, asset seizure, exclusion of participation in public procurement procedures and winding up.

The main penalties for natural persons are fines, imprisonment and asset seizure. For some regulated professions, a criminal sentence may cause an individual to be barred from that profession.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Criminal courts can consider mitigating circumstances to reduce the sentence pronounced. There is no exhaustive list of circumstances that can be taken into account. It is up to the judge to determine which element is relevant to the sentence. In addition, according to the principle of the individualisation of the sentence, criminal courts must ensure that every sentence is adjusted to the person convicted.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Luxembourg has implemented the European sustainability-related disclosure regulations, particularly the SFDR and the EU Taxonomy.

Other specific texts may apply to the protection of social rights and the environment. The offence of misleading commercial practices could also potentially be applied to greenwashing scenarios, although there is no case law on this question yet.

As the supervisory authority for the financial sector, the CSSF is proactively supporting the financial sector's transition to sustainable finance. To this end, it has defined supervisory priorities designed to promote consistent implementation of the regulatory framework throughout the financial sector, and to ensure the integration of ESG factors.

Lastly, a bill in favour of a corporate due diligence has been tabled in parliament to ensure that companies, their subsidiaries and their supply chain do not have a negative impact on human rights and the environment. The bill proposes that companies which (i) employ at least 250 people, (ii) have annual revenue of more than 50 million euros and/or (iii) a balance sheet of more than 43 million euros must implement a due diligence plan.

The bill also provides for the creation of a due diligence authority. This will be an independent public body with legal personality and financial and administrative autonomy.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

On 27 September 2023, the Financial Action Task Force ("FATF") submitted its latest mutual evaluation report on Luxembourg. Luxembourg achieved a good overall result, ranking among the best evaluated countries. The FATF recognises the quality of Luxembourg's AML/CFT system, and that Luxembourg has achieved a high level of technical compliance. In its report, the FATF proposes several recommendations to further improve the effectiveness of the system.

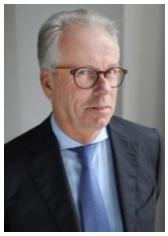
In addition, the Law of 16 May 2023 on the protection of whistleblowers has required stakeholders to put into place their internal whistleblowing channels. The implementation was and continues to be a complex operation for many of those stakeholders.

CONTACTS

LUTGEN + ASSOCIES

10, rue Sainte Zithe
2763 Luxembourg
Luxembourg

Tel.: +352 27 35 27
Fax: +352 27 35 27 35
www.lutgen-associes.com



André Lutgen
Partner
Lutgen + Associés
T +352 27 35 27
E al@lutgen-associes.com

During my long experience in defending company directors in criminal proceedings, I have found that behind each business manager, there is an individual with his own feelings and awareness. We need to accompany him, acting as a legal professional throughout proceedings, which are often much too long, while supporting him during the personal upheaval that marks this period, which is often perceived as a life-changing experience.

In business litigation, listening is the only means of understanding the real problem confronting us, which enables the identification of the appropriate remedy. The solution of the problem, as envisaged by the client, is frequently inappropriate, and my professional ethics forbid me from acting as a "procedures merchant".

Pierre Hurt
Partner
Lutgen + Associés
T +352 27 35 27
E ph@lutgen-associes.com

Following my doctorate thesis and after several years teaching at the Universities of Paris 1 Panthéon Sorbonne and Paris 5 René Descartes, I continued my academic activities at the University of Luxembourg whilst at the same time becoming a lawyer. I am convinced that a demanding professional practice does not in any way preclude a high level of theoretical competence – just the opposite. After having specialised in civil law and civil proceedings during my years at university, and my initial years at the bar, I have progressively built up a fund of knowledge in criminal law and criminal proceedings since joining Lutgen + Associés.

Florent Kirmann
Partner
Lutgen + Associés
T +352 27 35 27
E fk@lutgen-associes.com

Florent holds a doctorate in criminal business law and is a partner at Lutgen+Associés. He mainly advises clients on complex and often international criminal business law cases, as well as more general litigation matters. He assists his clients throughout the proceedings, from pre-litigation advice to representation before the Luxembourg courts. Alongside his activities as a litigation lawyer, Florent is also active in academic fields, teaching criminal law, giving lectures and regularly publishing articles or books, as well as through his participation in the Luxembourg Bar's criminal law commission.

Géraldine Mersch
Partner
Lutgen + Associés
T +352 27 35 27
E gm@lutgen-associes.com

Géraldine holds a bachelor's and master's degree in civil and criminal law from the Université libre de Bruxelles. Throughout her professional career, Géraldine has advised her clients in complex transnational business litigation. She assists her clients in commercial litigation as well as criminal and administrative litigation, whereby those fields are often deeply intertwined. Besides her professional implication, Géraldine is a former president of the Young Bar Association and a member of the Luxembourg Bar's commission on criminal law.

Malta

Camilleri Preziosi Advocates

Louis de Gabriele

Diane Bugeja

Peter Mizzi

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X		X
No				X	

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The Protection of the Whistleblower Act (Chapter 527 of the Laws of Malta) ("**POWA**") provides procedures that allow employees in both the private and public sectors to disclose information regarding improper conduct of their employers or colleagues. In addition, it ensures the protection of such employees from detrimental actions. Prior to the promulgation of the POWA, the Employment and Industrial Relations Act (Chapter 452 of the Laws of Malta) also protected whistleblowers, prohibiting retaliation against employees for having made a complaint to authorities or for having disclosed information to a public body regarding any alleged illegal or corrupt activities. Further, both the Public Administration Act (Chapter 595 of the Laws of Malta) and the Public Service Management Code obliges public employees and officers to report any unethical behaviour or wrongdoing by another employee or officer to a senior employee or officer.

Under the POWA, a disclosure is deemed to constitute a "protected disclosure" if the whistleblower:

– Had reasonable grounds to believe that the information on breaches disclosed was true at the time of the disclosure and that such information fell within the scope of the POWA; and

– Disclosed internally in accordance with Article 12 or externally in accordance with Article 16 or made a public disclosure in accordance with Article 18A.

With regard to internal whistleblowing procedures, Section 2 of the POWA provides that all employers to whom the Act applies (including the public administration, private sector organisations, and voluntary organisations meeting the thresholds laid down in the Second Schedule) must have internal whistleblowing procedures in place. These internal procedures should at least include:

a) Channels for receiving the reports in writing, orally, or both. The latter shall be provided through telephone or voice-messaging systems. Such channels shall be designed, established, and operated in a secure manner that ensures the confidentiality of the whistleblower's identity and the protection of any third party mentioned in the disclosure. This shall also prevent access by unauthorised staff members;

b) Providing the whistleblower with a physical meeting within a reasonable period of time, if requested by the whistleblower; and

c) The appointment of a Whistleblowing Reporting Officer ("**WRO**") competent for following up on the reports. The law is silent on where the officer must be based. In practice, however, the officer is not required to be based in Malta. Nor is the officer required to be present at the employer's place of business. It is therefore up to the employers to appoint officers where they can most effectively fulfil their functions and duties.

Additionally, employers are required to provide their employees with clear and easily accessible information about the existence and the use of internal procedures. This shall be republished at regular intervals. Information on external reporting procedures to the relevant competent authority and relevant EU institutions shall also be provided.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Article 12 (4) of the POWA provides that organisations in the private sector with 50 to 249 workers may share resources as regards the receipt of reports and any investigation that shall be carried out. This shall be without prejudice to the obligations imposed upon private sector organisations by the POWA to maintain confidentiality, give feedback, and address the reported breach. Thus, following the European Commission's interpretation of flexibility in Article 8(6) of the Whistleblower Directive, the POWA does provide for group wide reporting systems only to the extent that entities with less than 250 employees may share resources.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Article 2 (5) of the POWA provides that this Act shall not affect the right of workers to consult their representatives or trade unions, and to be protected against any unjustified detrimental action prompted by such consultations.

b) The Maltese legal framework does not impose an obligation to inform data protection officers or data privacy authorities of an investigation, nor does it provide for their participation in an internal investigation. However, it may be advisable to inform the data protection officer about all data privacy related procedures, including those related to an employee investigation, according to the Data Protection Act (Chapter 586 of the Laws of Malta), as well as the European General Data Protection Regulation, Regulation (EU) 2016/679, ("**GDPR**"), since the data protection officer must, *inter alia*, safeguard employees' data privacy rights and fulfil their data protection monitoring duties more generally. In particular, the data protection officer would be consulted by the employer to ensure that the lawful basis being relied upon for the processing of personal data in the context of the investigation is appropriate and whether the balance between an employee's right to privacy at work and other legitimate rights and interests of the employee would be violated as a result of this investigation.

c) The POWA requires the appointment of a WRO, which is defined as the person identified within an organisation to whom a protected disclosure may be made. Where the disclosure leads to the detection of a crime or contravention under any applicable law, the said WRO may refer the report to the police for investigation. An authority to whom a protected disclosure is made may disclose such information to another authority within 30 days where it feels that the matter can be better investigated by another authority.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Generally speaking, Maltese law does not make any reference to the necessary procedure to be adopted in such investigations and does not place any such obligation on employees. Investigations are to be carried out in accordance with the internal procedure adopted by the employer subject to other applicable laws (including those regulating employment and data protection, amongst others). Additional obligations may be expected in case the employee has management responsibility due to potential supervisory duties.

The POWA further provides that the existence of the internal procedures and adequate information on how to use the procedures must be published widely within the organisation. As part of the WRO's duties, they are to maintain communication with the whistleblower and, where necessary, ask for further information and provide feedback to the whistleblower. Thus, all employees should cooperate with any external or internal investigations carried out. With particular reference to external investigations, where the company in question is a regulated entity or is otherwise subject to Maltese Anti-Money Laundering/Combatting the Funding of Terrorism ("**AML/CFT**") laws, all employees are required by law to be fully cooperative and transparent in any investigations or inquiries conducted by the relevant competent authority.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

There are generally no labour law related deadlines linked to investigative actions. In particular, there is no formal deadline within which an employer must terminate the employment of an employee found to be in breach of the employment contract. The applicable law specifies that an employer may dismiss the employee without notice and liability when there is good and sufficient cause to do so. Moreover, accepted practice favours employers who set up internal disciplinary structures, *inter alia* to oversee fair disciplinary proceedings. Such fair proceedings include granting employees the chance to defend themselves with the aid of trade unions and/or legal representatives (if required) against the charges levied against the employee. This should be done prior to a decision being taken by the employer leading to dismissal. To not prejudice its rights, it would always be advisable for an employer to dismiss the employee as soon as an informed conclusion on the proper cause for dismissal is reached.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Personal data must be processed in accordance with the requirements of the GDPR and the Data Protection Act (which is largely based on the GDPR), which *inter alia* includes that the processing has to be fair and lawful as well as be conducted in accordance with good practice. Furthermore, the "processing" of personal data is attributed a very broad definition by the GDPR and as such, "processing" covers any operation or set of operations which is performed on personal data or sets of personal data. Accordingly, interviews conducted in pursuance of an ongoing investigation must comply with the requirements of the GDPR and the Data Protection Act.

b) reviewing emails?

Emails generally contain personal data and as a result, generally fall within the scope of the requirements of the GDPR and the Data Protection Act for processing of personal data. Thus, data subjects need to be informed of any reviews of emails or other electronic communications. Further, it should be noted that the Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 586.01) provide that no person other than the user, may listen, tap, store or undertake any other form of interception of any electronic communication, inclusive of emails, without the consent of the user concerned.

c) collecting (electronic) documents and/or other information?

The collection of documents, including electronic documents, or other information, which contain personal data, may only be undertaken if said collection is lawful under the GDPR and the Data Protection Act.

d) analysing accounting and/or other business databases?

Accounting and business databases fall within the remit of the GDPR and the Data Protection Act only if and to the extent that such databases contain personal data. Generally speaking, these databases would typically contain data that relates to the activities of the employer and its business rather than personal data.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

Maltese law does not specifically place any obligations on the employer to instruct the employee about their rights in relation to the investigation or any specifications on the conducting of the investigation itself.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Both Maltese and European Union law provide an individual's right to remain silent in case of self-incrimination. Maltese criminal courts have interpreted this right to mean that a suspect does not need to reply to incriminating questions during an interrogation. Although not expressly mentioned in the POWA, it would still be good practice to grant the employee the option to have their attorney present during the interview.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

The Upjohn warning does not currently feature in Maltese law. In fact, there is no law providing guidelines on the procedure to follow when the lawyer in attendance is the lawyer of the company or an independent lawyer appointed by the interviewee.

d) be informed of their right to have their own lawyer attend the interview?

Prior to recent legislative amendments, one had a right to speak to a lawyer only before an interrogation. However, the lawyer did not have the right to be present during the interrogation, notwithstanding numerous rulings from the European Court of Human Rights pointing toward the need to strengthen the right to legal assistance during such interrogation.

Recent legislative amendments now generally grant the right of access to a lawyer. These amendments were, *inter alia*, enacted to transpose the European Directive 2013/48/EU, which deals with "the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings", amongst other correlated rights.

Notwithstanding the above, these legislative amendments apply only to official proceedings of investigating authorities and do not extend to internal investigations of a company operating in the private sector. Moreover, the accepted practice in private organisations suggests that in disciplinary proceedings, the attendance of a lawyer as the employee's representative under investigation is allowed and at times encouraged to ensure as fair a process as possible.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

In practice, the interviewee should be allowed to seek advice from a trade union in relation to a potential or ongoing investigation and to consult with the trade union. Although there is no legal obligation to inform the employee, it is highly recommended that employers inform employees of such right before carrying out an interview.

f) be informed that data may be transferred to another country (in particular to the United States)?

Outwards data transfers are typically based on an adequacy decision (https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en), an official decision by the European Commission that the country in question provides a level of security that is essentially equivalent to that found within the EU. Additionally, data exporters may rely on the appropriate safeguards within Article 46 GDPR. Following the recent Schrems II judgement, transfers to the United States will only be deemed valid if the European Commission's updated Standard Contractual Clauses ("**SCCs**") are utilised. These are available on https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en. Additionally, there is now an indirect obligation for both data exporters and importers to conduct a Transfer Adequacy Risk Assessment ("**TARA**") over and above the SCCs.

g) sign a data privacy waiver?

There is no requirement for the interviewee to sign a data privacy waiver. However, should the company determine that the applicable lawful basis for processing the personal data for the purpose of the interview is the data subject's consent, the company would need to ensure that the data subject's consent is appropriately collected in accordance with the provisions of the GDPR, particularly Article 7 therein. That being said, in the event that the consent is deemed the appropriate lawful basis of processing, consent provided in this context would not be considered a waiver as such.

h) be informed that the information gathered might be passed on to authorities?

The employee must be informed, and their consent should be requested unless the respective employer is under a legal obligation to report the individual to the authorities.

i) be informed that written notes will be taken?

There is currently no obligation under Maltese law to inform the interviewee that written notes will be taken during the interview, which is largely unregulated by Maltese law.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Document retention would normally be tackled in a data processing policy. Such an internal policy regulates the procurement, processing, and retention of different data sets depending on the laws applicable to the individual data sets. However, there is no specific regulation relating to document hold/retention notices *per se*. The retention of documents generated as a result of a report made under the POWA would largely depend on the internal procedures established by the employer pursuant to the requirement of the POWA as well as the legally accepted standards for document retention in terms of data protection law.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

In Malta, the legal attorney-client privilege is sacrosanct and predominantly exists in the context of civil and criminal litigation as well as in criminal proceedings and any investigations by the competent authority. Lawyers and their clients are granted protection with regards to confidentiality by the Code of Ethics issued by the Maltese Chamber of Advocates.

In order to ensure privilege protection, in-house counsel and external legal counsel (if necessary) should generally be involved. Further, claims of privilege are more likely to be upheld where the company can demonstrate that the advice provided by members of the legal professional was given in relation to a potential investigation by the authorities or otherwise where litigation is reasonably in prospect.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

On 1 October 2021, the Malta Chamber of Advocates published a Legal Professional Privilege – Practice Note for Advocates (https://www.avukati.org/wp-content/uploads/2021/09/Legal-Privilege-Practice-Note-2021.pdf). Section 5.3 of the note clarifies that advice received from in-house counsel is indeed covered by the same legal advice privilege as that of outside counsel.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

The law does not explicitly list any obligation of the employer. However, certain obligations with regards to precarious potential and ongoing investigations may arise from the terms and conditions of the insurance policy.

b) Business partners (e.g. banks and creditors)?

Certain notification duties may arise from any contracts or agreements entered into by the employer and any third parties where a potential or ongoing investigation may prejudice the position of any creditors with regards to the collection of any outstanding debts. Therefore, any obligations in this respect are to be considered under the agreement itself and possibly any statutory law governing the relationship between the said partners.

c) Shareholders?

The directors of a company are responsible for the day-to-day running of the affairs of the company and thus act as fiduciaries of the company. The directors of a company have certain reporting obligations to the shareholders, especially where a potentially precarious situation risks diminishing the value of their shares.

d) Authorities?

Generally speaking, there is no obligation on the part of the company to inform the authorities about any internal investigation, whether it is ongoing or not. However, this depends on the gravity of the wrongdoing and whether it affects the public interest. Further, where the company is a regulated entity, the applicable laws may, in certain instances, require the company to inform the relevant competent authority with immediate effect of any significant events affecting their business, including any significant internal investigations.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

There are no general legal provisions in this respect. Although, with reference to regulated entities, these are required to take all reasonable measures in order to remediate any misconduct at the earliest while also establishing internal systems and controls to mitigate and manage the risk of such misconduct happening again in the future.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

The POWA requires every employer to have internal procedures in force, as described above. Wherever the disclosure involves an improper practice that constitutes a crime or contravention under any law, the WRO may pass on the report to the police for investigation. The POWA is a relatively new introduction to the local legislative framework, and, as such, there is little evidence, if any, on how local prosecutors are likely to react to internal investigations. There are no official or formal procedures that employers are expected to follow when conducting internal investigations (other than their own internal procedures required to be established pursuant to the POWA). Consequently, the approach to be taken by local prosecutors, including their treatment of the conclusions arising from internal investigations and the procedure that has been followed, is likely to depend on the facts of the case at hand.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Except in certain delineated cases expressly stated in the Criminal Code (Chapter 9 of the Laws of Malta), a police officer may not enter any private premises to affect a search within the said premises unless he is in possession of a warrant issued by a Magistrate. Apart from the police, raids may also be carried out by the Financial Intelligence Analysis Unit ("**FIAU**") where the criminal activity falls within the remit of the Prevention of Money Laundering Act (Chapter 373 of the Laws of Malta) ("**PMLA**") and the Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01). Raids are carried out on the basis of an 'investigation order' issued by the Criminal Court upon application by the Attorney General. The FIAU's powers include the authority to enter any property and confiscate material related to the investigation without warning. However, any search, whether carried out by the police or the FIAU, cannot extend to legal privilege, for example, for any communication between the suspect and their legal representative or to any excluded material. The search warrant or investigation order shall always be applied within the parameters for which it was issued. Once on the premises, the police or FIAU officer carrying out the search may seize anything if they have reasonable cause to believe that the object has been obtained in consequence of an offence or if it is evidence in relation to an offence. Under Maltese law, illegally obtained evidence may still be admissible in court.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

As of 2002, Maltese criminal law provides the option of sentence bargaining, which means that the Attorney General, appearing on behalf of the prosecution and the accused through their legal counsel, can discuss and predetermine what punishment and consequences arising from the finding of the guilt can be imposed by the court, in case of a guilty plea. The Maltese Criminal Code does not specifically mention whether corporations can avail themselves of this provision.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

The liability of the company falls on the directors of the company, as under Maltese law, companies are not subject to criminal responsibility. However, the company may be subject to certain administrative fines and penalties in certain specified cases. The nature and amount of the penalties vary depending on the industry or sector in question and the laws applicable thereto. This notwithstanding, a company may face administrative fines of up to €20 million or in the case of an undertaking, four percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. Such administrative fines may be imposed on a company by a supervisory authority where the company has processed personal data in reliance on a lawful basis deemed not to be the most

appropriate lawful basis under Article 6 of the GDPR. An example of this may arise where the company relies on consent as its lawful basis for processing personal data for a particular purpose, but it transpires that consent would not be applicable as the consent collected does not satisfy the requirements of Article 7 of the GDPR.

In June 2020, the Financial Intelligence Analysis Unit ("**FIAU**") extended its power to impose personal liability on directors, senior managing officers and Money Laundering Reporting Officers ("**MLRO**") for breaches by a subject person of its AML/CFT obligations, through cause, contribution or gross negligence. This provision does not apply where the individual in question demonstrates having done everything within his or her control to address the breaches in question. However, if it becomes clear that further action was possible to address a risky situation, personal liability may be triggered. This could result in the imposition of administrative fines ranging from a minimum of €1,000 to a maximum of €250,000.

In addition, the FIAU may also recommend to the relevant supervisory authority that the MLRO be suspended or precluded from exercising the role within the particular or any other subject person.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

As described in Question 2, Section 2 of the POWA provides that employers fulfilling certain criteria must have internal procedures in place for receiving and dealing with protected information and outlines the minimum requirements of how such mechanisms are to be designed and implemented.

The POWA does not lay down any penalties for non-compliance with this section nor does it provide for any aggravation and/or mitigation of other offences and penalties under the POWA or any other law in cases where organisations implement efficient compliance systems or *vice versa*. However, in practice, penalties could be mitigated in case the organisation or its representatives have done their utmost to implement proper internal mechanisms prior to or following the alleged misconduct.

In the case of regulated and/or obliged entities, the sanction policies of the respective competent authorities provide for a reduction or suspension of penalties. That's the case when, *inter alia*, effective compliance systems have been introduced, the company and its officials cooperate with the relevant authorities, and/or other mitigating measures had been introduced. From a criminal law perspective, particularly in the case of corporate criminal liability, the company may be able to argue in its defence that it had taken all reasonable measures to prevent the misconduct from taking place. If this argument is upheld by the courts, it may lead to a reduction or suspension of any applicable penalties.

From a data protection perspective, the fact that a company implemented an efficient compliance system may be taken into account when a supervisory authority has decided to implement an administrative fine in the event of a personal data breach or other infringements of the GDPR.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

There are currently no specific ESG requirements emanating from local Maltese law. The ESG regulatory requirements that exist locally are those that emanating from EU regulation such as the Taxonomy Regulation, the Sustainable Finance Disclosure Regulation and the Client Benchmark Regulation.

What has recently been introduced locally is soft law, in the form of ESG-related codes of practice that apply on a 'comply or explain' basis. In August 2022, the Malta Financial Services Authority ("**MFSA**") published a Corporate Governance Code. This Code provides a set of principles, complemented by supporting provisions, to be applied on a 'best effort basis'. These are organised into four main sections, as follows: [i] the Effective Board; [ii] Internal Controls; [iii] Stakeholder Engagement; and [iv] Corporate Culture, CSR and ESG. The Code applies to all persons authorised by the MFSA to provide financial services in or from Malta.

In November 2023, the Malta Gaming Authority ("**MGA**") published a voluntary ESG Code of Good Practice for the remote gaming sector, which aims to complement and build on existing industry efforts and serve as a reference point for remote gaming companies to regularly assess, report and improve their ESG practices.

The ESG code will prepare gaming companies for the upcoming reporting requirements of the **Corporate Sustainability Reporting Directive** (Directive (EU) 2022/2464, "**CSRD**"). At the same time, it will serve as a voluntary ESG framework for all those entities falling outside the scope of the EU reporting regime. Moreover, it will complement and build on existing industry efforts, and serve as a reference point for MGA licensed entities to regularly assess, report on, and improve their ESG practices.

From an enforcement perspective, there is no evidence that local authorities are actively enforcing ESG related cases.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The MFSA and the FIAU have been particularly active in the financial services sector in recent years. More specifically, they have upped their on-site and offsite inspections and levied numerous penalties for breaching the relevant rules and regulations. Any such penalties or other regulatory measures taken by regulators are made public on the respective websites.

MFSA

The MFSA is obliged to publish all sanctions and penalties it imposes on its licence holders. Article 16(8) of the Malta Financial Services Authority Act (Chapter 330 of the Laws of Malta) provides that:

Any administrative or disciplinary sanction or measure, of whatever type, including reprimands or warnings, imposed or decided by the Authority under any law for whose administration it is responsible, shall be published in such medium and in such manner and for such duration as may be deemed warranted by the circumstances and the nature and seriousness of the breach or wrongdoing.

FIAU

In terms of Article 13C of the PMLA and FIAU's policies and procedures on the 'Publication of AML/CFT Administrative Penalties and Measures' (https://fiaumalta.org/app/uploads/2021/06/Publication-of-AML-CFT-penalties-Policies-and-procedures-Final.pdf), administrative penalties exceeding €50,000 are subject to publication on the official website of the FIAU within five working days from the date of notification of the administrative penalty to the subject person.

The entities subject to such measures have the right to appeal against the imposition of certain penalties or other administrative measures. At present, the powers of the FIAU to levy fines against subject persons is being challenged through constitutional proceedings. Such proceedings are still ongoing.

Sanctions Monitoring Board

The Sanctions Monitoring Board (the "**SMB**", the relevant competent authority in Malta for the implementation of sanctions) as of 23 April 2020, is empowered to impose administrative penalties for any violation of Article 17(6) of the National Interest (Enabling Powers) Act (Chapter 365 of the Laws of Malta) ("**NIA**").

In light of recent developments in Russia and Ukraine, the SMB has been highly active in providing guidance to persons in Malta regarding their obligations under the applicable sanctions regimes under the NIA.

Any administrative sanction imposed by the SMB and exceeding €800 shall be subject to publication in accordance with policies and procedures established from time to time by the SMB. At present, there are only two entities on the list.

Other relevant competent authorities

The Office for Competition ("**OC**") has similarly made a concerted effort to concentrate its resources on decreasing the number of pending cases and has closed a relatively high number of cases. The sectors involved covered the carriage of passengers, food services, fuel sales, car parking rates, and yacht marinas.

The Information and Data Protection Commissioner's Office (the "**IDPC**", the relevant supervisory authority in Malta for data protection) has similarly made a concerted effort to actively enforce GDPR breaches and official decisions can be found on its official website.

The relevant competent authorities are expected to maintain their momentum insofar as on-site inspections and investigations are concerned, pending the outcome of the constitutional proceedings referred to above.

CONTACTS

CAMILLERI PREZIOSI
ADVOCATES

Level 3, Valletta Buildings
South Street
Valletta 1103
Malta

Tel.: +356 21238989
www.camilleripreziosi.com

Louis de Gabriele
Managing Partner
Camilleri Preziosi
T +356 21238989
E louis.degabriele@camilleripreziosi.com

Louis is the first Managing Partner of the firm and was appointed to the role in January 2022. In his role as Managing Partner, he works closely with other practice partners and the firm's general manager to develop and promote the firm's strategy and approach.

Louis acts for a number of corporate clients, banks and financial institutions in relation to the larger or more complex domestic and cross-border transactions; and also covers a broad spectrum of complex commercial litigation, particularly in the corporate and finance area.

He advises on an ongoing basis on corporate governance issues as well as regulatory matters in the financial services field. He is a recognised leader in capital markets, having been an active contributor to the development of Maltese capital markets since the 1990's, when he advised on the first public offer of securities in Malta in 1990 (Bank of Valletta plc), and subsequently handled most of the large privatisations of public enterprises in Malta

Diane Bugeja
Senior Associate
Camilleri Preziosi
T +356 21238989
E diane.bugeja@camilleripreziosi.com

Diane's principal role as a senior Associate is advising clients on their obligations and compliance with Anti-Financial Crime obligations; and compliance with other regulatory obligations in the wider financial services sphere. She has assisted a number of assignments in advising clients subject to regulatory investigations; as well appeals against regulatory decisions

Peter Mizzi
Compliance and AML Advisor
Camilleri Preziosi
T +356 21238989
E peter.mizzi@camilleripreziosi.com

Peter's main area of activity is in Anti-Financial crime and advises clients in connection with compliance obligations in this area. He also frequently participates in conducting due diligence exercises and in testing client systems for financial crime detection and compliance with other regulatory obligations.

The Netherlands

Hogan Lovells International LLP


Manon Cordewener


Joke Bodewits


Maria Benbrahim

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X		X
No				X	

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The EU Whistleblowing Directive was implemented in the Netherlands through the Whistleblower Protection Act ("**WPA**") and entered into force on 18 February 2023. The WPA replaces the former House for Whistleblowers Act.

As of 17 December 2023, every employer who employs at least 50 employees is obliged to set up a procedure for reporting (suspected) wrongdoing within its organisation. For employers employing more than 250 employees, these obligations already applied as of 18 February 2023. To assess the numerical criterion, an employee is defined as any person who, on the basis of a civil law employment contract or an appointment under public law (*publiekrechtelijke aanstelling*) or a person who otherwise performs work for payment in a subordinate relationship.

Employers with at least 50 employees are required to draft and implement an internal whistleblowing procedure. Companies operating in the field of financial services, products and markets, prevention of money laundering and terrorist financing, civil aviation, maritime labour, port state control, and offshore oil and gas activities are also required to establish an internal procedure even if they have less than 50 employees.

An internal whistleblowing procedure should:

- Describe how an internal report must be handled;
- Describe when a suspected abuse is deemed to exist, subject to the definition of a suspected abuse in the WPA;
- State that in any event an employee can report a suspected abuse in the following ways:
  - In writing;
  - Orally by telephone or other audio messaging system; or
  - Upon request within a reasonable period in a face-to-face conversation at a location.

– Identify the designated independent officer or officers to whom a suspected abuse can be reported and the independent officers who will follow up on the report with due care;

– State that an employee may consult an adviser confidentially about a suspected abuse;

– State that a reporting person must receive confirmation of receipt within seven days of the date on which the report is received; and

– Set a reasonable period of no more than three months after dispatch of the confirmation of receipt referred to in point 6 above within which information must be provided to the reporting person about the assessment of, and to the extent applicable, the follow-up to the report.

The employer provides its employees with information in written or electronic form regarding:

– The internal reporting procedure;

– The way in which a suspected abuse can be reported outside the organisation to the competent authorities and, where applicable, to Union institutions, bodies, offices and agencies; and

– The legal protection for an employee who reports a suspected abuse.

A whistleblower is no longer required to report suspected wrongdoing internally first but can report directly externally: An employee may report externally with the competent authorities responsible for receiving and following up on reports.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The WPA allows legal entities in the private sector with 50 to 249 employees to share resources for receiving reports and conducting investigations. This provision enables group entities to establish group-wide reporting systems for handling reports and conducting investigations.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) The employer is required to obtain consent from the works council in order to establish the internal reporting procedure. This approval is not required insofar as the procedure is explicitly set out in a collective labour agreement. If no works council or staff representation has been established, the employer requires the approval of more than half of its employees. Any changes to policies on complaints or whistleblowing are also subject to the prior right of consent of the works council.

If the employer establishes an internal reporting procedure without the works council's consent, the works council can challenge this decision by claiming nullity. The works council must do so within one month (a) of receiving notification of the employer's decision to go through with the internal reporting procedure; or (b) in the absence of such notification, of becoming aware that the employer is implementing the decision.

b) The General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") and the Dutch Implementation Act of the GDPR (the "**DIA GDPR**") do not explicitly require notifying a data protection officer ("**DPO**") about an internal investigation. However, a DPO should be involved in all matters which relate to the protection of personal data based on the GDPR. Further to this general requirement, and based on Guidelines for Data Protection Officers, issued by the Dutch Data Protection Authority ("**DDPA**") and the European Data Protection Board, it is advisable to inform the DPO on investigations.

Furthermore, where the processing activity is likely to result in a high risk to the rights and freedoms of natural persons a data protection impact assessment ("**DPIA**") has to be carried out, in which case the GDPR requires seeking the advice of the DPO. Such DPIA should contain (i) a description of the envisaged processing operations and the purposes for processing, (ii) an assessment of the necessity and proportionality of the processing operations in relation to the purposes, (iii) an assessment of the risks to the rights and freedoms of the data subjects, and (iv) the measures envisaged to address the risks. In case the DPIA indicates that there is a high risk in the absence of measures taken to mitigate the risk, the DDPA has to be consulted.

Apart from the aforementioned requirement to inform the DDPA in case of a high risk (after conducting a DPIA), the GDPR and the DIA GDPR do not require informing the DDPA about an internal investigation.

Consequences in case of non-compliance

The maximum administrative fine for not involving a DPO or not performing a DPIA when required is €10 million or two percent of the annual turnover. The DDPA recently issued updated guidelines for imposing administrative fines. According to the DDPA, its own DDPA Fining Policy rules 2023 apply to natural persons and government bodies acting in violation of the GDPR. To calculate fines for companies acting in violation of the GDPR, the DDPA makes use of the EDPB Fining Guidelines.

c) There is no statutory obligation to inform local authorities. However, a company's internal whistleblowing regulation could provide this obligation.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

The investigation department is authorised to request information and demand inspection of case data and documents. The employer suspected of the abuse, employees for whom it is responsible, witnesses and the reporter are all obliged to provide the specified information in full as well as truthfully, and are also obliged to appear before the investigation department. The persons summoned to appear before the investigation department or the employer obliged to submit documents to said department, may inform the investigation department that the information or documents may not be disclosed to other persons: Persons may refuse to furnish information or submit documents, if the provision thereof would be contrary to the interests of national security or entail a breach of a duty of professional secrecy or a statutory regulation. The disclosure obligation shall also not apply if the person concerned would consequently expose themself, a relation by blood or marriage in the direct or collateral line in the second or third degree, or his present or former spouse or his present or former registered partner to the risk of conviction for a serious offence. Non-compliance is not sanctioned in the WPA. The House of Whistleblowers is not legally obliged to continue the investigation if the employee requesting the investigation does not cooperate adequately.

If an investigation is not conducted by the House of Whistleblowers, there is no specific rule that requires an employee to cooperate. However, on the basis of the general principle that employees should act as "good employees", employees should, in principle, support and cooperate with an internal investigation. It is important to properly inform employees in advance about why, how, and by whom the internal investigation will take place. If an employee nevertheless refuses to cooperate, an assessment could be made to determine what appropriate disciplinary measures, if any, can be imposed. Circumstances to consider include, but are not limited to, the personal circumstances of the employee, the length of the employment, and the seriousness of the suspected misconduct.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Dutch law does not provide explicit rules for internal investigations initiated by an employer, in the sense that there is no particular statute or codified regulation.

However, employers should be aware of the following:

a) It is only possible to dismiss an employee with immediate effect if the dismissal is prompt (*onverwijld*). This means that after the suspicion was raised, an investigation should be carried out with minimum delay, and the employer should dismiss the employee immediately once the culpability is sufficiently established. Whether a dismissal was carried out quickly enough to be valid depends on the circumstances of the case.

b) The employer has a duty to act as a good employer. This means that an investigation should be conducted in a fair and reasonable way. If an employee was, for example, pressured or threatened during the investigation, this might hinder the employer's ability to take disciplinary measures. Moreover, if the employer engages in serious misconduct during an investigation, employees might be able to claim damages or high severance payments.

In addition, there are various regulatory frameworks that govern internal investigations, such as the principles of duty of care, based on the principles of proper governance (*beginselen van behoorlijk bestuur*) and the principles of good employer ship (*goed werkgeverschap*).

The main principles that must be taken into account by an employer who plans an investigation are:

- **Duty of care**: This entails the requirement of careful consideration of relevant interests and the related principles of transparency, proportionality, and subsidiarity;
- **Independence/neutrality**: The investigation team should not be involved in the (alleged) irregularity and/or have a significant relationship with the individuals (allegedly) involved in any way;
- **The principle of hearing both sides of the story**: The investigation team should allow the employer, the employee, and other parties involved to tell their side of the story and verify this based on substantiated information;
- **Fair play**: Classical fair play principles are the duty to give explanations, to manage legitimate expectations, and to respect the principles of proportionality, subsidiarity, and equality. It follows from Dutch case law that an employee should be allowed to be accompanied by any third person, including a lawyer, in the context of a (potential) dispute with the employer. In Dutch legal literature it is widely accepted that legal assistance should be allowed and even encouraged by the employer, as soon as once a particular step in an internal investigation may have consequences for the employee's legal position. In this respect, the nature of business activities, type of incident, the extent of the breach, and the person of the employee are relevant factors;
- **Détournement de pouvoir**: The information obtained may not be used for purposes other than investigating the irregularity encountered;
- **Substantiation**: Notes of interviews should be taken and presented for correction and/or confirmation to the relevant employee;
- **Honesty**: The employee should be able to rely on the statements of the employer throughout the process;
- **Equality**: Equal cases will be treated equally;
- **Presumed innocence**: It is important not to make any accusations pending the investigation but rather confront the employee with facts and ask explanatory questions (address assumptions).

These principles should be respected throughout each (further) phase of the investigation process, i.e. when preparing, conducting, and reporting on the investigation.

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Under Dutch data protection law, a legal basis for the processing of personal data is required, in line with the GDPR. A legal basis cannot be found in the consent given by the employee, as employee consent is not considered freely given in an employment relationship, especially when it concerns investigations. Generally, a legal basis for conducting an internal investigation, including an employee interview, exists when the controller (in this case, the employer) has a legitimate business interest to investigate suspicions of misconduct, provided that the data subject has no overriding interest in the protection of their private life, and (i) the interview is relevant to the investigation; (ii) the same purpose cannot be achieved using less intrusive means (e.g. only document review); and (iii) the controller has implemented measures to protect the rights of the data subject (e.g. restricting access to interview data).

In case of an investigation by the DDPA, the controller will be required to demonstrate to the DDPA that it has taken into account the conditions above. When personal data is processed relating to criminal convictions and offences or well-founded suspicions thereof, or related security measures, the DIA GDPR requires an exception to apply, such as for the protection of the controller's interests, insofar as it concerns criminal acts that are (expected to be) committed against the controller or its employees.

Furthermore, where the processing activity is likely to result in a high risk to the rights and freedoms of natural persons a DPIA has to be carried out (see section 3b).

Data subjects should be informed about the purposes and means of the processing prior to the commencement of processing. An employee should be informed before the interview is conducted. An exception to this rule applies where there is a substantial risk that such notification would jeopardise the ability of the controller to investigate a matter properly or gather the necessary evidence or where notification may lead to the destruction of data. In such cases the notification to the data subjects may be delayed as long as such a risk exists, which should be determined on a case-by-case basis.

b) reviewing emails?

As with conducting interviews, there must be a legal basis for the email review. The legal basis is typically derived from the legitimate business interest of the controller provided that (i) the email review is relevant to the investigation (e.g. non relevant, private emails are excluded); (ii) the same purpose cannot be achieved using less intrusive means; and (iii) the controller has implemented measures to protect the rights of the data subject, including the right to privacy in the workplace (e.g. by engaging a third party to conduct the review, using an algorithm to search for emails, and restricting access to emails to a dedicated team subject to confidentiality obligations). In instances where personal data is processed relating to criminal convictions, offences, well-founded suspicions thereof, or related security measures, the DIA GDPR requires that one of the proscribed exceptions to the general prohibition on this form of processing applies. Furthermore, as described above, a DPIA may have to be carried out, and data subjects may have to be informed in advance unless an exception applies.

c) collecting (electronic) documents and/or other information?

As with conducting interviews and reviewing emails, there must be a legal basis for collecting documents, which is assessed using the factors described above. Also, as described above, a DPIA may have to be carried out, and data subjects may have to be informed.

d) analysing accounting and/or other business databases?

Dutch data protection law does not protect the processing of non-personal data, e.g. statistics or accounting information.

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no statutory obligation to provide an interviewee with written instructions before conducting employee interviews. However, a company's internal whistleblower regulation could impose this obligation. Moreover, from the perspective of good employership, the employer may be required to communicate the underlying reasons to invite the employee for an interview, such as potential irregularities or unacceptable behaviour and/or the investigations, in writing (in brief) and thus allowing the employee to understand the context and seek legal assistance.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Employees should be informed that they must not make statements that would lead to self-incrimination. This is in line with the principle of protecting employees from potential legal consequences resulting from their statements during the interview.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no statutory obligation to provide an Upjohn warning. However, a company's internal whistleblower regulation could impose this obligation. At the same time, from the perspective of good employership, it is required to inform the employee thoroughly about the context and setting of the interview. The process should be fair, properly defined/clear, and not misleading.

If lawyers are involved in the internal investigation, Dutch rules of conduct for lawyers (*Gedragsregels advocatuur*) provide that the lawyer should make clear that they are acting in the capacity of a (biased) representative of the company.

d) be informed of their right to have their own lawyer attend the interview?

If the interview is conducted by the police, where the employee is a suspect in a criminal investigation, then the interviewee should be informed that they have the right that their lawyer attends. If the interview is not conducted by the police, there is no such right or corresponding information obligation. However, a company's internal whistleblower regulation could impose this obligation. In addition it could follow from the principle of good employership that if the interview is not conducted by the police, a similar obligation still applies. This would ensure that the employee is better informed and might attribute more credibility to the (outcome of) the investigation in the end.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

The employee does not have the right to have a works council representative attend the interview. However, a company's internal whistleblower regulation could include this right and the corresponding information obligation. Moreover, the employee is free to have anyone he wishes to be present during the interview. This could be a relative, colleague, trust person, lawyer, or friend.

f) be informed that data may be transferred to another country (in particular to the United States)?

As a rule of thumb, personal data may not be transferred to countries outside of the European Economic Area unless the data recipient offers an adequate level of protection. On 10 July 2023, the European Commission has adopted a new adequacy decision for U.S. data transfers: the EU-U.S. Data Privacy Framework. However, in light of the previous Schrems judgements of the Court of Justice of the European Union, this new adequacy decision remains under increased scrutiny. A Data Transfer Impact Assessment ("**DTIA**") should be conducted prior to the transfer with a view to offer an adequate level of protection for personal data. A DTIA should establish the safeguards in place to respond to any identified risks associated with the transfer. Data subjects must be made aware of a transfer of their data to a third country or international organisation and be provided information about the recipients, or categories of recipients, of their personal data. Moreover, the GDPR requires that the data subject be informed of the safeguards implemented to legitimise the international transfer, for instance, by reference to model clauses approved by

the European Commission or Binding Corporate Rules (BCR) approved by the DDPA, and be informed of the means to obtain a copy of the safeguards or where they have been made available.

g) sign a data privacy waiver?

Under Dutch data protection law, employee consent does not qualify as valid consent for investigations. As a result, a signed data privacy waiver has no legal effect.

h) be informed that the information gathered might be passed on to authorities?

Employees should be informed that the information gathered during the interview might be shared with authorities if necessary for the investigation of suspected abuses.

i) be informed that written notes will be taken?

There is no statutory obligation to inform the interviewee that written notes will be taken; however, the internal whistleblower regulation could provide this obligation. At the same time, from the perspective of good employership, it is required to inform the employee beforehand that their feedback will be recorded in writing. The process should be fair and not misleading.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Pursuant to the GDPR, personal data may not be kept longer than required for the purpose for which the data has been collected. Data subjects have to be informed about retention periods or the criteria used to determine the retention period. After the storage period has passed and the company no longer needs the data, the company must destroy it. An exception to the disposal of documents after the maximum retention period has lapsed can be established by issuing a document hold notice, which suspends the retention policy. Such a legal or tax hold notice prevents the disposal of relevant documents in case of any expected litigation or investigations.

In case personal data will be retained after an initial retention period, further to a hold notice, the data subject has to be informed about this new purpose and (criteria used to determine the) retention period unless there is a substantial risk that such notification would jeopardise the ability of the controller to investigate a matter properly or gather the necessary evidence or where notification may lead to the destruction of data.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

In principle, the attorney-client privilege applies to the oral and written information received, drafted, and sent by the attorney in relation to their client or case.

In 2021, the Supreme Court ruled that a limitation of the attorney-client privilege, in the sense that the attorney-client privilege would *not* cover documents that do not contain legal findings, qualifications, or conclusions, is not supported by Dutch law. In principle, it is up to the lawyer to determine whether information entrusted to them falls under the privilege. In other words, it is up to the lawyer to decide whether the knowledge of this information would lead to a breach of professional confidentiality for the lawyer. If the lawyer is of the opinion that the information is covered by privilege, the inspector and the court must respect this position.

In 2023, the Disciplinary Appeals Tribunal (*Hof van Discipline*) emphasised that it is up to the Dutch bar (*Nederlandse orde van advocaten*) to formulate a professional standard with regard to factual investigations by a lawyer or that it is up to the legislator to establish more detailed rules. The Disciplinary Appeals Tribunal also called into question whether a lawyer acting as an investigator can claim attorney-client privilege: The Tribunal considered that the duty of a lawyer who is acting as an investigator and whose duty it is to investigate objectively and report as comprehensively as possible, might be at odds with claiming attorney-client privilege.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Attorney-client privilege (*verschoningsrecht*) applies to lawyers registered with the Dutch bar (*Nederlandse orde van advocaten*). Hence, a lawyer who is registered with the Dutch bar and is working for a company, may benefit from privilege protection.

In 2022, the Supreme Court of the Netherlands confirmed that:

– In-house lawyers registered with the Dutch bar; and

– In-house lawyers who are entitled to practise in another member state of the European Union or European Economic Area or in Switzerland under the designation of lawyer (or a corresponding title in the language of the state of origin) and who (a) performs work in the Netherlands by way of the provision of services or (b) works in the Netherlands under the original professional title,can claim attorney-client privilege if they entered into a "professional statute" (i.e. an agreement with their employer guaranteeing their independence) and their employer.

In other cases, attorney-client privilege may be claimed in the Netherlands if:

– The foreign lawyer is entitled to privilege under the law of the country of origin in relation to the activities involved;

– The privilege could also be claimed if the activities had been performed in the Netherlands by a lawyer registered with the Dutch bar; and

– The foreign lawyer and its employer have entered into an agreement that provides guarantees for independent practice and uninterrupted compliance with the rules of professional conduct, and practice equivalent to the "professional statute".

In any event, an in-house lawyer may only claim attorney-client privilege in respect of what is entrusted to them in their capacity as a lawyer.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

The requirement to notify an insurance company of the start of an investigation depends on the terms and conditions of the individual insurance policy.

b) Business partners (e.g. banks and creditors)?

In general, there is no requirement to notify business partners of the start of an investigation. However, certain financing and similar agreements may stipulate an obligation to notify the bank.

c) Shareholders?

The obligation to notify shareholders of the start of an investigation may arise from the articles of association, internal whistleblower regulation, and/or shareholders' agreement. According to the Dutch Civil Code, the management board and supervisory board are generally required to provide all requested information at the general shareholders meeting, unless an overriding interest of the company precludes them from doing so (e.g. when sharing the requested information harms the company's competitive position). According to the Dutch Corporate Governance Code, listed companies must substantiate the reason for invoking such overriding interest.

d) Authorities?

In general, there is no duty to inform the prosecutor about an internal investigation or potential misconduct within the company.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

There is no statutory provision that prescribes immediate measures that have to be taken upon the start of an investigation. However, the company must stop potential ongoing breaches of the law as soon as possible. Failure to do so may be attributed to the company in the context of civil, administrative, or criminal proceedings.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Whether a local prosecutor has concerns about an internal investigation depends on the specifics of the case.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Generally speaking, a search warrant or dawn raid can only be executed upon approval by the relevant authorities, such as the Netherlands Authority for Consumers & Markets ("**ACM**") or the Dutch public prosecutor (*Openbaar Ministerie*).

In administrative proceedings, supervisory officers are allowed to search all locations, except homes, when needed to fulfil their supervisory duties. No warrant or court order is needed. Houses may only be entered after a court order from the investigative judge. During a dawn raid, the authorities gather evidence. The authorities are obliged to inform the company of the purpose and scope of the investigation at the start of a dawn raid. In general, a written description of the purpose is provided to the company. Fishing expeditions, where the authorities extensively search for evidence without a defined purpose and scope of the investigation, are not permitted.

In administrative proceedings – in principle – unlawfully obtained evidence does not have to be disregarded.

In criminal investigations, the public prosecutor is allowed to enter and search the premises of a company suspected of a crime. In that case, no court order is required. If the company is not a suspect, the search or seizure can only be conducted by the investigative judge. The search can be requested by the public prosecutor. This request must be detailed and show that all the legal requirements are met. The investigative judge and the (assistant) public prosecutor are also required to be present during the search or dawn raid.

In the event evidence was unlawfully obtained in criminal proceedings, the court has the discretion to exclude the evidence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

The Dutch public prosecutor may decide to offer an accused company to make a payment in lieu of prosecution (*transactie*). The amount to be paid is non-negotiable. If a company agrees to such offer and pays, the case will stay out of court. If a company rejects the offer or fails to pay, the prosecution will proceed nevertheless.

The Dutch public prosecutor will announce that it has reached such a "deal" via a press release, stating the amount to be paid by the company. The press release will include an extensive factual account that outlines investigation findings, why the public prosecutor opted for a deal and what offences the prosecutor believed the company committed.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

A company can be held criminally liable for the misconduct of its employees. The public prosecutor or specific supervisory authorities are able to impose fines on the company for breaches of statutory provisions. A fine of up to 10 percent of the annual revenue of the company in the prior financial year may be imposed.

Employees may also be held individually criminally liable. This could lead to a fine or even imprisonment. An individual convicted of public bribery, for example, may face up to six years in prison or a fine of up to €103,000.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

As explained in question 2 above, the WPA requires employers with at least 50 employees to implement an internal whistleblowing procedure. According to the Money Laundering and Terrorist Financing (Prevention) Act, some financial institutions are obligated to appoint a compliance officer. No such obligation exists for other companies.

In the Netherlands, no specific sentencing guidelines exist that provide for a reduction or suspension of penalties in cases where a company had implemented an efficient compliance system. However, when determining the punishment, the judge will consider all circumstances of the case. It is possible that the judge will take into account whether the company has implemented an efficient compliance system. Also, in negotiations about a possible deal with the prosecutor, such circumstances can be of importance.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Legislative Proposal for the Responsible and Sustainable International Business Act (*Wet verantwoord en duurzaam internationaal ondernemen*)

The legislative proposal for the Responsible and Sustainable International Business Act (*Wet verantwoord en duurzaam internationaal ondernemen*) is currently under parliamentary review. The legislative proposal establishes a legal duty of care for all Dutch companies engaged in international trade and addresses various forms of human rights violations, environmental damage and climate-related harm throughout the entire value chain. The ACM is to be responsible for enforcing compliance with the Act on Responsible and Sustainable International Business.

Companies must take reasonable steps to prevent, mitigate and rectify adverse effects and provide solutions within their value chains. Large Dutch companies engaged in foreign trade are also obliged to implement due diligence in their value chains, and align with the OECD guidelines. A large company means an entity that meets two of the following criteria:

– A net turnover of more than €40 million;

– Balance sheet total assets greater than €20 million; and/or

– More than 250 employees.

Corporate Sustainability Due Diligence Directive

Parallel to the legislative proposal for the Responsible and Sustainable International Business Act, a legislative proposal is pending on European Union level: The Corporate Sustainability Due Diligence Directive ("**CSDDD**").

According to the explanatory memorandum, the CSDDD "*will set out a horizontal framework to foster the contribution of businesses operating in the single market to the respect of the human rights and environment in their own operations and through their value chains, by identifying, preventing, mitigating and accounting for their adverse human rights, and environmental impacts, and having adequate governance, management systems and measures in place to this end*". On 14 December 2023, the Council of the European Union announced that it reached a provisional deal with the European Parliament on the CSDDD. This agreement defines the scope of the CSDDD, clarifies liability for infringements, improves the definition of the various penalties and completes the list of rights and prohibitions that companies must observe. The provisional deal now needs to be endorsed and formally adopted by both the Council of the European Union and the European Parliament.

Child Labour Due Diligence Act (*Wet zorgplicht kinderarbeid*)

The purpose of the Child Labour Due Diligence Act (*Wet zorgplicht kinderarbeid*) is to ensure that consumers may are able to rely on the fact that goods and services offered on the Dutch market are offered by companies, which have taken the reasonably necessary steps to prevent those goods and services from being produced using child labour. The Act has not entered into force yet. To the extent that it will, it will apply to:

– Any company located in the Netherlands which sells or supplies goods or services to Dutch end-users; and

– Any company located outside the European part of the Netherlands that sells or supplies goods or services to Dutch end-users at least twice a year.

The Child Labour Due Diligence Act requires such companies to:

– Investigate whether there are reasonable grounds for suspecting that the goods or services to be supplied have been produced using child labour, and establish and implement an action plan if such suspicion exists; and

– Submit a declaration to the regulator that it takes due care to ensure that the goods or services are not produced using child labour.

Companies that only sell goods or services from suppliers who have themselves submitted such a declaration are exempted from the obligation to submit the declaration, but will still be required to exercise due care.

Although the Child Labour Due Diligence Act is already passed by the Dutch Senate, it is still unclear if and when the Act will enter into force. In 2020, the Dutch legislator namely indicated that it prefers to await comprehensive international corporate social responsibility legislation at European Union level. In addition, the explanatory memorandum to the aforementioned legislative proposal for the Act on Responsible and Sustainable International Business emphasises that such Act also covers the purpose of the Child Labour Due Diligence Act. Once the legislative proposal for the Act on Responsible and Sustainable International Business is passed by the Dutch Senate, the Child Labour Due Diligence Act will be repealed.

Implementation of the Corporate Sustainability Reporting Directive

On 5 January 2023, the Corporation Sustainability Reporting Directive ("**CSRD**") entered into force. This new directive modernises and strengthens the rules concerning the social and environmental information that companies have to report on. A broader set of large companies will now be required to report on sustainability. A legislative proposal implementing parts of the CSRD is currently in the consultation phase. This legislative proposal specifically addresses the verification of compliance with sustainability reporting requirements by an external auditor. Please note that there is some overlap between the implementation of the CSRD and the above-mentioned legislative proposal. The implementation of the CSRD will take place in phases. The CSRD will apply to companies currently subject to the Non-Financial Reporting Directive ("**NFRD**") from 1 January 2024. Large companies not currently subject to the NFRD, will be required to comply from 2025. Listed small and medium-sized enterprises (SMEs) are expected to adhere with the CSRD starting from 1 January 2026.

Dutch Decree CO2 Reduction Work (Besluit CO2 Reductie Werkgebonden Personenmobiliteit)

Organisations with 100 or more employees must report on their employees' work-related travel under the Dutch Decree CO2 Reduction Work (*Besluit CO2 Reductie Werkgebonden Personenmobiliteit*) with regard to how their personnel commutes. The report should include details on the total kilometres travelled, vehicle type and fuel type. In case of non-compliance, enforcement actions may be taken by the Environmental Service (*Omgevingsdienst*).

The date of entry into force of this Decree has been postponed from 1 January 2024 to 1 July 2024.

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

In 2022, the opinion of the advocate general of the Supreme Court of the Netherlands on the appeal to the ruling of the Court of Rotterdam in 2021 (discussed under 10 above) was published.

CONTACTS

Hogan Lovells

Atrium, North Tower
Strawinskylaan 4129
1077 ZX Amsterdam
The Netherlands

Tel.: +31 20 55 33 600
Fax: +31 20 55 33 777
www.hoganlovells.com

Manon Cordewener
Partner
Hogan Lovells Amsterdam
T +31 20 55 33 691
E manon.cordewener@hoganlovells.com

As head of the Litigation practice in Amsterdam, Manon brings a wealth of knowledge and extensive experience in contract disputes, shareholders disputes, antitrust litigation, product litigation and professional liability disputes. Industry sectors in which she is active are as diverse as automotive, energy and natural resources, financial institutions and consumer.

Joke Bodewits
Partner
Hogan Lovells Amsterdam
T +31 20 55 33 645
E joke.bodewits@hoganlovells.com

As a core team member of the global Cybersecurity practice of Hogan Lovells in Amsterdam, Joke Bodewits counsels clients in global cybersecurity matters at all levels of an organisation. Joke brings to her practice years of experience advising companies and boards on cyber and data risk management and data governance, breach preparations and response, ransomware negotiations, regulatory inquiries and global data strategies. Joke has counselled many clients during enforcement actions following cyber incidents.

Maria Benbrahim
Partner
Hogan Lovells Amsterdam
T +31 20 55 33 622
E maria.benbrahim@hoganlovells.com

As Partner of the Employment Team, Maria focuses, *inter alia*, on "strategic" corporate/employment law matters, such as the employment law aspects and consequences of restructurings, outsourcings and M&A transactions, employee consultation related matters, negotiations with works councils and trade unions. Clients turn to Maria Benbrahim for a sharp and focused lawyer, with not only a deep understanding of employment/corporate law, but also a down to earth and practical mind-set. Maria is a pragmatic, effective and bold negotiator and litigator.

Norway

Wikborg Rein Advokatfirma AS

Elisabeth Roscher

Geir Sviggum

Tine Elisabeth Vigmostad

Kristin Nordland Brattli

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Section 2 A-1 of the Working Environment Act (the "**WEA**") gives any employee or hired-in worker the right to report issues of concern. When an employee reports issues of concern, Section 2 A-3 (1) of the WEA requires the employer to ensure that the matter is adequately investigated within a reasonable time. The WEA does not mandate particular measures to be implemented for the investigation to be adequate. Therefore, the assessment of what constitutes adequate follow-up must be made concretely in each individual case, depending, amongst other things, on the nature and seriousness of the reported issues. The investigation does not need to go in further depth than what the facts underpinning the complaint warrant, and it can sometimes be readily concluded that a report is unfounded.

Section 2 A-3 (2) of the WEA provides that the employer shall particularly ensure that the whistleblower has a fully satisfactory working environment, and, if necessary, ensure that measures are taken to prevent retaliation.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The current Norwegian legislation does not contain requirements regarding the establishment, compositions or features of whistleblower reporting systems as such. Section 2 A-6 of the WEA requires undertakings that regularly employ at least five employees to have routines for internal whistleblowing. Undertakings with fewer employees shall have such routines if the conditions at the undertaking so indicate.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) There are no requirements *per se*. However, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") is incorporated in Norwegian legislation as a part of the Personal Data Protection Act. In general, the provisions of applicable data protection legislation must be followed when conducting internal investigations, including the Regulation on employers' right to access employees' emails.

b) Please refer to our answer to question 2a.

c) There are no general requirements in Norwegian law that a company must liaise with national or local government authorities before starting an internal investigation, but there may be possible benefits to such early involvement. There may also be specific obligations to notify authorities of health and safety incidents and similar. Furthermore, a number of industries are required to report suspicious transactions etc. to the national Financial Intelligence Unit (FIU) .

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

It is generally assumed that employees' duty of loyalty towards their employer involves an obligation to cooperate with their employer's internal investigation, including providing information that may serve as evidence and participating in interviews. Employees may also be instructed to support in the acquisition of relevant documents. However, the duty to cooperate is assumed to be limited to investigations whose facts relate to the employee's position and work. Therefore, the extent of the duty to participate in interviews must be considered on a case-by-case basis.

In any event, interviewees shall be informed, in line with the right to protection against self-incrimination, that they do not have a duty to provide information that may expose themselves to criminal liability. Moreover, Section 4.4 of the Norwegian Bar Association's Guidelines for private investigations state that employees should be informed that they may be exposed to labour law consequences such as dismissal if they provide false testimonies.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

There are no labour law deadlines or rights to sanction employees which are waived in Norwegian law by taking investigative actions. However, once an employee has reported an issue of concern in accordance with the WEA, retaliation against an employee who reports such issues is prohibited.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The Personal Data Act (the "**PDA**"), which implements the GDPR, applies to all processing of personal data, whether or not by automated means. Consequently, any collection and further processing of personal data in the context of interviews must adhere to the GDPR.

b) reviewing emails?

In addition to the PDA and the GDPR, Regulation 2018-07-02-1108 contains requirements relating to employers' access to their employees' personal email accounts, the employees' personal areas in the company's data network and other electronic equipment provided by the employer for work-related use. The regulations stipulate strict conditions and procedural requirements for such access to be legal.

c) collecting (electronic) documents and/or other information?

The collection of electronic documents and/or other documents are, if they contain personal data, subject to the requirements of the PDA and the GDPR. If documents and/or information are collected from employees' email accounts, personal areas in the company's data network or electronic equipment provided by the employer for work-related use, the requirements in Regulation 2018-07-02-1108 must be complied with.

d) analysing accounting and/or other business databases?

Unless accounting and/or mere business databases contain personal data, i.e. any information related to an identified or identifiable natural person, the PDA and the GDPR do not apply.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There are no specific laws or regulations that apply to employee interviews, but according to the Norwegian Bar Association Guidelines for internal investigations, the process should be as open and transparent as possible and the interviewee should receive written information about the background and the topic of the interview. Furthermore, the interviewee must be informed of their right to be assisted by a lawyer, and that they do not have a duty to disclose information that may expose themselves to criminal liability (the protection against self-incrimination), cf. Section 4.4 of the Guidelines. It is advisable that these instructions are given by written notice and signed by the interviewee.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Section 4.4 of the Bar Association Guidelines recommend that interviewees should be informed of their right to be assisted by a lawyer, and that they do not have a duty to disclose information that may expose themselves to criminal liability (the protection against self-incrimination).

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no formal requirement to provide an Upjohn warning under Norwegian law, but the interview process should, according to the Bar Association Guidelines, be transparent and procedurally fair. Therefore, it is considered best practice to provide an Upjohn warning.

d) be informed of their right to have their own lawyer attend the interview?

Pursuant to Section 4.4 of the Bar Association Guidelines, interviewees should be given the right to be assisted by a lawyer or other adviser, and be informed of this right.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Although there are no binding rules entitling an employee being interviewed to be represented by an employee representative, Section 5.2 of the Bar Association Guidelines states that affected persons have the right to be assisted by a workers' representative.

f) be informed that data may be transferred to another country (in particular to the United States)?

The transfer of personal data from Norway to countries which have implemented the GDPR, and to countries which the European Commission have deemed to have an adequate level of data protection, is permitted if there is a legal basis for the processing (including transfer) of the data. The U.S. has been subject to such an adequacy decision by the European Commission from 10 July 2023.

For the transfer of personal data to countries which have not been subject to an adequacy decision to be legal, specific requirements must be adhered to. Typically, EU Standard Contractual Clauses must be used, and additional measures must in some cases be implemented. Additionally, certain derogations enshrined in Article 49 of the GDPR may be relied on for cross-borders transfers of personal data.

g) sign a data privacy waiver?

Article 6 of the GDPR requires a lawful basis for the processing of any person data, of which consent constitutes the main basis. If the individual has not consented to the processing of their personal data, it must be demonstrated that the processing is necessary to fulfil contractual obligations towards the individual, compliance with legal obligations, the protection of vital interests, public tasks, or other legitimate interests which are not overridden by the interests or fundamental rights and freedoms of the data subject.

h) be informed that the information gathered might be passed on to authorities?

Article 13 (1) letter e of the GDPR requires the data controller to provide the data subject with information about the recipients or categories of recipients of the personal data. Thus, individuals have the right to be informed that the information gathered might be passed on to authorities.

i) be informed that written notes will be taken?

There is no legal requirement to inform interviewees that written notes will be taken, but it is good practice to give such information, in order to fulfil the aim of a transparent and fair process.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific legislation regulating this question under Norwegian law, but such notices are frequently used. The notices should be clear, sent to all potentially relevant addressees, and issued as early as possible. Also, applicable data protection legislation must be observed.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The Supreme Court of Norway has ruled that internal investigations are considered part of the legal practice covered by attorney-client privilege under Section 22-5 of the Civil Procedure Act and Section 199 of the Criminal Procedure Act, provided that investigations are undertaken by lawyers, and the findings have some sort of legal implications. If the investigation is solely for fact-finding purposes, the privilege does not apply. However, since the collection and systemisation of facts is often closely interlinked with legal considerations, the privilege will often be applicable based on a concrete assessment.

The attorney-client privilege applies to qualified lawyers, and in general also to persons who assist lawyers in their work, including external experts. For such assistants to be covered, their engagement must be derived from the engagement of the lawyer. The privilege does not apply to independently or separately engaged assistants.

The attorney-client privilege covers all information, documents, parts of documents and emails disclosed, sent directly to or copied to, the lawyer. For the privilege to apply, the relevant findings must have been communicated to the lawyer in connection with the provision of legal advice, i.e. in his or her capacity as a lawyer. If the lawyer receives or gives information when acting in another capacity, for instance, as a member of the Board of Directors, the privilege does not apply.

The attorney-client privilege is subject to some exceptions, for instance in criminal investigations if it can lead to a serious crime being committed or an innocent person being convicted.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

The attorney-client privilege applies equally to in-house counsel under Norwegian law. Thus, there are no differences between investigations directed by externally engaged or in-house lawyers in respect of legal professional privilege.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

This would depend on the terms and conditions in the insurance policy.

b) Business partners (e.g. banks and creditors)?

The contract with the business partner may contain disclosure requirements covering the initiation of an investigation. In exceptional circumstances, there may also be an implicit obligation to inform the business partner, e.g. in light of the contractual duty of loyalty.

c) Shareholders?

The mere initiation of an investigation does not trigger a requirement to notify shareholders. However, an investigation may concern matters that constitutes insider information, which may cause Regulation (EU) 596/2104 on market abuse to apply. Additionally, if the investigation could have an impact on the financial position of the company, the Norwegian Company Act Section 5-15 provides a shareholder with a right to request further information.

d) Authorities?

There is no general requirement to inform authorities when initiating an investigation, but there may be notification requirements relating to particular types of incidents, such as related to personal data security and Health Safety and Environment incidents. With respect to investigation of potential economic or other crimes, there are in general no formal procedures that require companies to self-report under Norwegian law, and consequently no required steps for making a disclosure. However, the enforcement authorities (including ØKOKRIM) encourage companies to disclose any suspicions of corporate crimes and to cooperate with the authorities on any subsequent investigation.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

With the exception of health and safety matters, there are no statutory obligations for immediate measures in Norwegian law. However, companies are expected to minimise damages and take adequate steps to prevent similar incidents from happening again, including assessment of possible improvements to the company's compliance system. Ongoing criminal conduct or other offences must also be stopped and, if relevant, reactions against employees should be considered.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

The authorities often encourage companies to share the results of a private investigation with them. In the case of a parallel criminal investigation, the authorities frequently also request that investigative steps be coordinated to prevent the risk of the private investigation interfering with the authorities' investigation, e.g. in that evidence is weakened and/or witnesses are influenced and thereby prejudice the public investigation.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Both search warrants and dawn raids by public authorities must fulfil formal and material requirements as set out in the Norwegian Criminal Procedures Act. In general, a written search warrant from a court is required, but the police can carry out a search without a court warrant if there is a risk that the evidence sought will be lost should the police wait for a warrant. A search warrant may be issued if there is a reason to believe that a criminal offences punishable by imprisonment has been committed.

In the event that the legal requirements are not met, generally, seized evidence can generally still be used in legal proceedings. against the company. Only in serious cases of illegally obtained evidence, the evidence cannot be used in court. For example if evidence is gathered in a manner contrary to ECHR Article 6.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

In Norway, the prosecution may not enter into deferred prosecution agreements similar to what is common in certain other jurisdictions.

However, the authorities encourage companies to cooperate and share results of any investigation with them. Such cooperation will be viewed positively and will also be taken into consideration when, for example, ØKOKRIM exercises its prosecutorial discretion in considering whether a company should be charged and the nature of such charges, and also when it comes to assessment of liability or the amount of any penalty imposed.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Companies in Norway may face corporate criminal liability, such as fines. In addition, there may be orders or injunctions, such as loss of the right to operate.

Individuals, including employees, officers or directors conducting the relevant misconduct, and provided that the misconduct is subject to criminal liability may be sentenced to prison if such individual has acted with the necessary degree of guilt.

In addition to criminal liability, revenue resulting from a criminal act will normally be confiscated.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

For natural persons, if all conditions for imposing a penalty on the individual are met, a penalty will as a the main rule be applied.

Corporate criminal liability in Norway is subject to prosecutorial discretion. This means that there is no general presumption of corporate liability under Norwegian law, and that the imposition of corporate penalty depends on the circumstances of the case. A relevant element in the assessment of whether to impose a penalty is whether the company, prior to the criminal act taking place, had implemented a suitable and efficient compliance system.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

The Norwegian Transparency Act entered into force on 1 July 2022, and requires companies to *inter alia* carry out human rights due diligence in accordance with the OECD Guidelines for Multinational Enterprises. The Norwegian

Consumer Authority actively monitors companies' compliance with the act, and the Authority may issue prohibitions, orders and penalties in case of non-compliance.

The Norwegian Accounting Act (Section 3-3c) imposes an obligation on large enterprises to prepare a statement on corporate social responsibility, including relating to human rights, labour rights, the environment and prevention of corruption. These requirements are about to be considerably extended as a result of the Corporate Sustainability Reporting Directive (CSRD).

According to the Norwegian Pollution Act (Section 7), there is a general prohibition against pollution. If pollution occurs, the pollution control authorities may order those who are responsible for the pollution to implement measures. Such measures could for instance be further investigations, to remove the pollution, or to limit its effects.

The Norwegian Consumer Authority prevents and stops illegal marketing, unfair contract terms and other forms of illegal commercial practices targeted to consumers. The most important law in this area is the Marketing Control Act, augmented by guidelines addressing greenwashing practices. Also, the Green Claims directive from the EU will most likely be incorporated into Norwegian law and impose stricter regulations.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The Norwegian Bar Association Guidelines relating to external investigations were revised in 2023. The reviewed guidelines clarify a number of issues, including that an investigation shall be carried out in a manner that does not involve a violation of anyone's human rights or a significant risk of such violation.

A recent judgement from the Norwegian Supreme Court, issued 21 December 2023, clarifies that the threshold for what constitutes a whistleblowing report under the Norwegian Working Environment Act, which triggers the employer's duty to adequately investigate the report within a reasonable period of time, is rather low. The court held that there are no specific requirements as to the format of the report, and the only requirement is that the report is submitted to one of the persons listed in the Norwegian Working Environment Act, typically a representative of the employer.

CONTACTS

WIKBORG | REIN

Dronning Mauds gate 11
0250 Oslo
Norway

Tel.: +47 22 82 75 00
Email: oslo@wr.no
www.wr.no

Elisabeth Roscher
Partner
Wikborg Rein
T +47 22 82 76 65
E elr@wr.no

Elisabeth is the head of the firm's ESG, Compliance and Investigations practice. Elisabeth's main areas of practice are corporate compliance systems, including anti-corruption, anti-money laundering, international sanctions/trade control, responsible business conduct and human rights, private investigations, crisis management and criminal law.

Elisabeth was ranked the best compliance lawyer in Norway in the Norwegian Financial Daily's annual lawyers survey in 2023. She is also ranked by Chambers Europe within the Compliance category, and as a Leading Individual by The Legal 500 within the Regulatory, Compliance and Investigation category.

Geir Sviggum
Partner
Wikborg Rein
T +47 22 82 76 76
E gsv@wr.no

Geir Sviggum is Wikborg Rein's Managing Partner. He headed the firm's Shanghai office from 2008 to 2013, was Managing Partner International with overall responsibility for Wikborg Rein's international practice from 2012 to 2016, and Chairman of the Board of Directors from 2018 to 2023.

Geir's compliance specialty focuses primarily on anti-bribery and crisis management, including criminal law consequences and civil disputes triggered by potential misconduct. His experience spans from a role as public defender in Norwegian courts to crisis management on behalf of listed Norwegian companies following suspected misconduct, and preventive advisory work for Norwegian companies and public authorities in their anti-bribery work.

Tine Elisabeth Vigmostad
Partner
Wikborg Rein
T +47 22 82 76 92
E tvi@wr.no

Tine is part of the firm's ESG, Compliance and Investigations practice, as well as the Trade Compliance and Sanctions Team. Tine provides advice regarding a wide range of issues relating to corporate compliance and crisis management, both on the preventive and responsive side. Her main areas of practice are: (i) sanctions and export controls, where she provides advice from a multijurisdictional perspective; (ii) sustainability and responsible business conduct; and (iii) investigations and crisis management.

Kristin Nordland Brattli
Partner
Wikborg Rein
T +47 22 82 75 77
E knh@wr.no

Kristin is part of the firm's ESG, Compliance and Investigations practice, as well as the Trade Compliance and Sanctions Team. Kristin focuses on anti-corruption, anti-money laundering and international sanctions, as well as responsible business conduct/human rights. Kristin has extensive experience from several cross-border private investigations and crisis management cases, including one of the largest corruption and money laundering cases to hit a Nordic company in the past five years. Kristin also assists in setting up compliance programmes and advising on preventive corporate compliance measures.

Poland

Hogan Lovells (Warszawa) LLP

Dr. Wojciech Marchwicki

Aleksandra Połatyńska

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

As of April 2024, the EU Whistleblower Directive has still not been implemented in Poland. The new Polish government that took office in December 2023 has proposed yet another draft bill of the Polish Act on the Protection of Whistleblowers ("**Draft Act on Whistleblowers**"). The draft has been passed by the government on 17 April 2024 and is pending to be enacted soon.

The Draft Act on Whistleblowers introduces a clause prohibiting retaliation against whistleblowers. This means that terminating an employment contract or neglecting to renew one, when the whistleblower anticipated renewal, along with actions such as intimidation, exclusion, mobbing, discrimination, or unfair treatment, reducing salary, failing to grant an expected promotion, or providing a negative performance appraisal, are all prohibited.

Moreover, the Draft Act delineates precise obligations regarding the safeguarding of personal data collected throughout the reporting process. These include refraining from disclosure, adhering to retention periods, and ensuring confidentiality, with exceptions outlined for informing data subjects about data sources. In general, the principles arising from the Polish Labour Law and other regulations concerning, *inter alia*, the protection of personal data shall apply.

Specific procedures only apply to financial institutions, such as banks, investments firms, and certain entities set out in the Polish Act on the Prevention of Money Laundering and Terrorist Financing. These entities are legally required to adopt procedures for anonymous reporting of infringements of law to the selected members of the management board or to the supervisory board. As part of the procedures, they must particularly ensure that employees who report violations are protected against acts of a repressive nature, discrimination, or other unfair treatment.

Moreover, these entities have specific duties of notifying prosecution or public authorities in the event of justified suspicion that their activities are being used to conceal criminal activities or other offences.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

As of April 2024 there are no specific regulations in place.

The Draft Act on Whistleblowers mandates that entities with a workforce of at least 50 individuals, encompassing both employees and those under other employment arrangements like B2B contracts, must establish an internal reporting channel for legal violations. Additionally, it provides that employees in the private sector with at least 50 but no more than 249 employees can agree to use group wide reporting systems, provided that the activities preformed within this reporting system comply with the Act.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Under Polish law, there is no legal obligation to notify any specific persons or bodies about an internal investigation a company is about to or is currently conducting. There is also no statutory obligation to ensure the participation of employee representative bodies in the investigation.

Nevertheless, if an individual employee requests that a union or work council representative participate in the interview, the employer might want to consider allowing their presence. Moreover, employee representative bodies have to be consulted in connection with certain post-investigation actions involving employees that are members of trade unions.

b) There is no statutory obligation to notify the data protection officer about an investigation. However, under the EU General Data Protection Regulation ("**GDPR**"), the Data Protection Officer's ("**DPO**") general obligation is to monitor compliance of personal data processing with personal data protection regulations. Thus, the DPO should be informed about any investigation that includes personal data processing since investigations, as a rule, carry an increased risk to the rights and freedoms of data subjects.

The Data Protection Authority ("**DPA**") does not have the right to be informed of or participate in any particular investigation. The DPA may, however, carry out inspections to assess the compliance of the processing of personal data under personal data protection regulations.

c) There is no obligation to inform other local authorities or officials about a pending investigation. However, parallel cooperation with the prosecution authorities can be advantageous under certain conditions.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Under Polish employment law, an employee is obliged to care for their employer's interests. There is no other explicit duty for employees to support an investigation. However, as long as an employee's support for an investigation aims at safeguarding the company's interest, the employer can legitimately expect its employees to cooperate within the limits of their employment relationship. Therefore, under certain circumstances, a refusal to cooperate can be treated as a material breach of the employee's fundamental duties. This would justify disciplinary measures.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

As a rule, the termination of an employment contract without notice due to the fault of the employee (disciplinary dismissal) cannot come into effect later than one month after the employer learned about the circumstances justifying the termination.

The disciplinary dismissal must be based on credible grounds. According to the Supreme Court, the beginning of the above-described time limit can be calculated from the moment the employer learned of the comprehensive grounds for dismissal after the completion of the internal investigation.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?
b) reviewing emails?
c) collecting (electronic) documents and/or other information?
d) analysing accounting and/or other business databases?

There are no specific legal boundaries under Polish law that would limit how an interview is conducted. However, it is advisable that the interview is carried out with an awareness of the employee's fundamental rights, including human dignity, the right to defence, the right to privacy, and the right to a fair trial.

In addition, it would be legitimately expected that an employee will not bear any negative consequences in connection with their participation in the interview. This includes, but is not limited to:

– Confidentiality of their involvement to protect the employee from any social disadvantage in their workplace;

– No extension of working hours by the hours spent in the interview; or

– No requirement to answer questions in a foreign language that the employee does not usually speak during their normal conduct of work.

The scope of the internal investigation is also limited by the protection of professional secrecy (e.g. the professional secrecy of doctors, attorneys, journalists, tax advisors).

The interview is also subject to limitations based on the GDPR or the Act on Classified Information Protection ("**CIP**") if it has been established that the entity where the investigation is taking place, or the relevant persons involved, are authorised to access classified information.

The Draft Act on Whistleblowers exempts the GDPR's obligations to inform and obtain the consent of a reported person for processing data. Upon receipt of a report, for verification of the report and follow-up, the obliged entity can collect and process personal data of the reported person, even without consent (which can include a review of emails and collecting documents).

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no general or legal obligation to provide the interviewees with written or oral instructions or inform them about their legal position. It is, however, advisable to briefly inform the employee about the nature and purpose of the interview. It is also advisable to instruct the employee that the interview is confidential. If the employee is expected to cooperate during an investigation, it should be made clear that participation in the interview will not exceed the scope of their employment duties or knowledge acquired during the employment.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

There is no general or statutory duty to inform the interviewee about their rights, similar to a warning by authorities during a criminal investigation in Poland. It is, however, advisable to explain the employee's role during the interview and that they have the right to avoid answering questions that could incriminate them.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

The company is not required to provide an Upjohn warning. However, maintaining clarity during the interview is highly recommended.

d) be informed of their right to have their own lawyer attend the interview?

There is no obligation to inform an employee of their right to have a lawyer attend the meeting.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

As an employee cannot effectively expect the attendance of such bodies, there is also no obligation to inform the employee of this right. It is nevertheless advisable.

f) be informed that data may be transferred to another country (in particular to the United States)?

The interviewee must be provided with information required under Articles 13 or 14 GDPR. In particular, he should be informed that data could be transferred cross-border.

g) sign a data privacy waiver?

Under Polish privacy laws, the interviewee is not required to sign a data privacy waiver.

h) be informed that the information gathered might be passed on to authorities?

There is no legal obligation to inform the interviewee that the data might be passed on to authorities. However, it is advisable to warn the employee of this possibility.

i) be informed that written notes will be taken?

If one of the people attending the interview is taking notes, it is advisable to explain the role of this person, along with the purpose of the notes.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no formal requirement for issuing document hold notices or other specifics to be observed under Polish law. However, these documents are allowed and recommended.

The above rule does not apply to public and local government institutions that, in connection with their activity, become aware of an offence to be prosecuted *ex officio*.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege can be claimed over the findings of an internal investigation if these have been elaborated by the attorneys and/or communicated to the client within the scope of the legal assistance they provide to the company.

In order to ensure privilege protection, communication with attorneys and attorney-client work products should be labelled as privileged and confidential (Polish: *Objęte tajemnicą adwokacką/radcowską*). During dawn raids, the company's employees or outside counsel should inform the enforcement authorities which documents and data are privileged, ensuring they are left unread and that the investigators place them in sealed packages. Information about the seizure of privileged documents should be documented in the dawn raid protocol.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Attorney-client privilege generally also applies to in-house counsel, as long as the in-house counsel acts in its capacity as an attorney and provides legal assistance to the company.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

An investigation does not necessarily mean that any irregularity in fact existed. However, the company may be obliged to notify the insurance company, depending on the terms of the insurance agreement.

b) Business partners (e.g. banks and creditors)?

This is usually not required unless the agreements between the parties expressly state so.

c) Shareholders?

There is generally no formal requirement to notify the shareholders of an investigation unless the investigation or the underlying facts can have a significant impact on the company's financial situation.

d) Authorities?

Under Polish law, there are no specific notifications required when starting an investigation. In certain cases, only the findings of an investigation or the irregularities that triggered the investigation need to be disclosed to the relevant authorities.

As a rule, anyone who becomes aware of an offence prosecuted *ex officio* has a social duty, rather than a legal obligation, to notify the public prosecutor.

This does not apply to public and local government institutions, which are obliged to immediately report offences to the authorities if they become aware of an offence prosecuted *ex officio* in connection with their activity.

A legal obligation to notify the authorities rests upon anyone who has reliable information about certain most serious criminal offences (e.g. terrorist offences, offences against humanity, or homicide). Moreover, under the Polish Act on the Prevention of Money Laundering and Terrorist Financing, the obliged institutions are required to notify the authorities of suspicions of money laundering or terrorist financing.

Depending on the type of irregularity revealed in connection with an investigation, certain other notification requirements might apply.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

There are no specific measures a company is expected to take. However, it is advisable to consider the potentially required actions at every milestone of the investigation and seek advice from external counsel.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Criminal authorities rarely become involved in an internal investigation of a company.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

A dawn raid can be conducted by the public prosecutor, the police, or another authorised agency (e.g. the Central Anti-Corruption Bureau or the Internal Security Agency) acting upon an order from the court or the public prosecutor. Prior to the actual searching process, the person or entity must be summoned to voluntarily hand over the requested documents or devices. A person whose premises are to be searched should be provided with a search warrant issued by the court or the public prosecutor. The documents to be seized should be covered by the scope of the search warrant. However, in urgent cases, the search can take place upon an order from the head of the unit conducting the search or even just upon presentation the official identity card of the official. The court or the public prosecutor's decision approving the search must be requested in the search protocol and delivered within seven days from the day of searching.

Specific rules apply to documents containing classified information, information constituting a professional secret, other legally protected secrets, or private information. If any of these documents are seized, the company should alert the investigators about the potential breach of secrecy. The investigators should then refrain from reading them and refer the documents to the prosecutor or court in a sealed package. Subsequently, to use the documents containing classified information or information constituting a professional secret as evidence, the court or prosecutor has to issue a decision in this respect. Documents that cover circumstances related to the performance of a defence counsel's function can never be used as evidence in criminal proceedings.

Using evidence gathered by public officials (e.g. police officers or prosecutors) in breach of these rules is inadmissible.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Deals, non-prosecution agreements, or deferred prosecution agreements are not available for corporations under Polish law.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Under the Polish Criminal Corporate Liability Act, a company can be found criminally liable and sanctioned for the misconduct of individuals if their action was or could have been beneficial for the company. The company can be fined from PLN1,000 to 5 million but not exceeding three percent of the revenue earned in the business year in which the offence was committed. Potential sanctions are forfeiture, various prohibitions, loss of benefits, and publication of the judgement, which can be severely detrimental to the company's reputation.

Polish criminal law generally does not stipulate criminal liability for individuals for the acts or omissions of third parties. Under limited circumstances, directors, officers, or employers can be subject to fines for obstructing an investigation.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

The Criminal Corporate Liability Act does not provide any explicit reduction or suspension of penalties if the company has implemented an efficient compliance system. Nevertheless, the court could take the functioning of the compliance system into account when assessing the company's liability and/or determining the amount of penalty.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

In Poland, there is no uniform act regulating ESG issues, instead, specific ESG provisions are found in a number of legal acts, including those on competition and consumer protection, financial market, environmental protection, labour law or commercial law. There are therefore a number of different specialised bodies that have ESG compliance monitoring as part of their remit, for example: the labour inspectorates, the environmental inspectorates or the Financial Supervision Authority.

These bodies are usually quite active and the investigation of ESG violations within their competences. We also expect this activity to increase once the Draft Act on Whistleblowers is implemented.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The Draft Act on Whistleblowers is expected to be adopted in the Q2 2024.

Despite the lack of general whistleblower protection under Polish law to date, internal whistleblower protection procedures in the private sector and at the central government offices already exist in preparation for the forthcoming adoption of the Act on Whistleblowers.

The provisions for the protection of whistleblowers, currently in force in Poland, require establishing procedures for anonymous reporting of the infringements of law in the selected sectors (banking, financial instruments, protection against money laundering and competition law).

The case law on whistleblowers shows that the courts are mostly unanimously in favour of the necessity to protect the whistleblower from being dismissed from a job or other negative consequences. In 2019, the Regional Court in Kalisz issued a precedent-setting judgement, finding that an employee had been discriminated against in the workplace for being a whistleblower despite the absence of relevant legal provisions. The employee was entitled to protection against discrimination under the general principles of labour law (judgement of the Regional Court in Kalisz of 1 July 2019, V P 20/17, see also judgement of the District Court in Toruń of 12 July 2023, IV P 171/22).

However, the protection is not absolute. In the opinion of the courts, protection is limited if the allegations raised by the whistleblower are unfounded or irrelevant. Exercising whistleblower rights cannot collide with the principle of loyalty to the employer. The Supreme Court stated that this principle is breached in cases of insulting, unspecific, and undocumented criticism of the employer (judgement of the Supreme Court of 3 September 2020, II PK 215/18).

CONTACTS

Pl. Trzech Krzyży 10/14
00-499 Warsaw
Poland

Tel.: +48 22 529 29 00
Fax: +48 22 529 29 01
www.hoganlovells.com

Dr. Wojciech Marchwicki
Partner
Hogan Lovells (Warszawa) LLP
T +48 22 529 86 40
E wojciech.marchwicki@hoganlovells.com

Wojciech heads the Dispute Resolution practice in Warsaw.

He has many years of experience in conducting complex, multi-layered court and arbitration proceedings. He supports clients in developing dispute resolution strategies and managing risk related to potential claims. He has participated in numerous proceedings before Polish courts, as well as arbitration disputes in Poland and abroad, primarily disputes related to infrastructure and construction projects as well as financial sector.

Wojciech represents clients in criminal proceedings in business-related cases, particularly involving white collar crimes. He has advised companies on numerous matters involving civil law liability and compliance procedures.

Wojciech is qualified in Poland (advocate) and in the state of New York (attorney-at-law). He is a graduate from University in Poznan, Poland and Harvard Law School, USA. He holds a doctorate in constitutional law from the Polish Academy of Sciences. He also completed a clerkship at the Supreme Court of Israel in Jerusalem.

Wojciech is the author and co-author of publications on constitutional and procedural law published in Poland and abroad. He teaches Warsaw bar trainees and he examines on commercial law (contracts and torts) and civil procedure. He is a judge at the High Disciplinary Court for Advocates. He collaborates with the Helsinki Foundation for Human Rights in a precedent-setting programme.

Aleksandra Połatyńska
Associate
Hogan Lovells (Warszawa) LLP
T +48 22 529 86 51
E aleksandra.polatynska@hoganlovells.com

Aleksandra is an advocate and a member of the Dispute Resolution team in the Hogan Lovells Warsaw office. She assists Polish and international clients in a range of disputes before state and arbitration courts, as well as before the enforcement authorities.

Her practice focuses on cases of a commercial nature, including disputes based on civil law, medical law, the protection of intellectual property rights and white collar crime. Aleksandra also has experience in anti-money laundering, and terrorist financing regulations.

Aleksandra graduated from the Faculty of Law and Administration at the University of Warsaw in 2016, and completed a one-year American law class at the Centre for American Law Studies at the University of Warsaw.

Portugal

Uría Menéndez – Proença de Carvalho

Nuno Salazar Casanova

Lua Mota Santos

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Portugal implemented the Whistleblower Directive through Law No. 93/2021 of 20 December, which entered into force on 20 June 2022.

Pursuant to Law 93/2021, whistleblowers who reveal infractions of professional duties are protected from retaliation. They are protected in such a way that any disciplinary penalties imposed on them within two years of them reporting the unlawful conduct are presumed to be unfair. Whistleblowers are entitled to judicial protection and may benefit from the witness protection programme during criminal proceedings.

According to Article 18(1) of Law 93/2021, the reporting person's identity, as well as information that directly or indirectly identifies them, are confidential and must only be accessed by those competent to receive or follow up on reports. Law No. 93/202, unlike Article 16(1) of the Whistleblower Directive, does not refer to the reporting person's consent and hence it seems that the reporting person's identity may not be disclosed even if they give their consent. Furthermore, the duty of confidentially in Law No. 93/202 is broader than that in the Whistleblower Directive because it refers not only to the reporting person's identity but also to information that may directly or indirectly identify them.

How whistleblowers and their reports are to be treated is regulated by specific Portuguese laws, such as (i) the Corruption and Financial Crime Law ("**Law 19/2008**"), (ii) the Money Laundering and Terrorism Financing Law ("**Law 83/2017**"), (iii) the Legal Framework of Credit Institutions and Financial Companies ("**RGICSF**") and (iv) the Portuguese Securities Code ("**CVM**").

All these pieces of legislation include safeguards to protect the whistleblower's identity and, under specific circumstances, enable them to benefit from witness protection programmes during criminal proceedings. This keeps whistleblowers anonymous when specific conditions are met, thereby limiting any potential retaliation against them. We highlight that, in some cases, information about a potential crime or infringement needs to be communicated to the competent authorities.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Pursuant to Article 8(1) of Law 93/2021, public or private companies who have 50 or more employees (or who fall within the scope of the European Union acts identified in parts i.B and II of the Annex to Directive 2019/1937) must have internal reporting channels in place. However, according to Article 8(2) of Law 93/2021, private entities who have between 50 and 249 employees may share resources for receiving reports and the respective follow-up actions. This also applies to Portuguese branches of companies headquartered abroad.

As we see it, under Article 8 (1), (2) and (3) of Law 93/2021, only companies who have between 50 and 249 employees (including those at their headquarters) may share their resources for the abovementioned purposes. This does not mean that there can be no group-wide reporting systems, as long as reporting channels are available at the subsidiary level. In other words, there needs to be a local reporting system, although there may also be a central reporting system at the same time. We still have no official guidance on this aspect of Law 93/2021 from any public authority.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Employee-representative bodies must not be informed about or be part of an internal investigation before it starts. The works council can only take part in disciplinary proceedings after the employee in question has been formally accused of any wrongdoing.

b) The data protection officer ("**DPO**") must be involved in all issues relating to personal data protection. As such, it is generally advisable to inform the DPO of the internal investigation before it starts and to involve the DPO throughout the process. The Portuguese Data Protection Authority ("**CNPD**") must not be informed before the internal investigation. It only has to be involved if a complaint is actually filed against the employer.

c) The prosecution authorities need not be informed either; however, taking the initiative and cooperating may be beneficial in the event of a potential conviction.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees are obliged to cooperate if management decides to conduct an internal investigation into potential wrongful acts within the company. However, employees have the right to not incriminate themselves in accordance with the Portuguese Criminal Code ("**PCC**"), which in turn means that they are not obliged to self-report.

An employee's refusal to cooperate in an internal investigation is a breach of their duty of obedience towards their employer, and as such, the latter can discipline them for not collaborating.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Employers must start disciplinary proceedings within 60 days of becoming aware of the facts (i.e. who is responsible and the specific circumstances surrounding the infringement). The 60-day period is only interrupted if the employee is sent notice of misconduct (*nota de culpa*). If the employer does not know the circumstances surrounding the infringement, it must start preliminary enquiry proceedings within 30 days of suspecting the improper conduct.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The General Data Protection Regulation ("**GDPR**"), Law 58/2019 of 8 August ("Law 58/2019") which transposes the GDPR into Portuguese law and Law 59/2018 of 8 August, which approves the rules for processing personal data for the purposes of preventing, detecting, investigating or supressing criminal offences or imposing criminal sanctions.

b) reviewing emails?

Private communications are highly protected under Portuguese law. The Portuguese Constitution establishes the right to privacy and the inadmissibility of evidence collected by intruding in the personal life, residence, communications or telecommunications of citizens. The Portuguese Labour Code ("**PLC**") establishes that personal messages and non-professional information are, as a rule, confidential. Law 58/2019 and Resolution 1638/2013 of the CNPD prohibit employers from accessing employees' personal communications or any non-professional information. This means that employers need the employees' express consent to process private or non-professional information in the workplace. To ensure that private communications remain confidential, they must be accessed in the presence of the data subject (employee) – if they choose to be present – and by using specific keywords.

c) collecting (electronic) documents and/or other information?

Please refer to our answer to question 5b.

d) analysing accounting and/or other business databases?

There are no specific laws on this matter.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

No, there is no general and statutory obligation to provide written instructions to interviewees.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Interviewers are under no obligation to inform interviewees that they must not make statements that could incriminate them. But individuals are not obliged to self-report any wrongdoing to the company or to any authorities concerning crimes or administrative offences.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

Although the interviewers are not obligated to inform the interviewees that they are the company's legal representative, it is advisable to do so.

d) be informed of their right to have their own lawyer attend the interview?

Pursuant to the Portuguese Bar Association statutes, a lawyer can be present at all times – which applies in all jurisdictions and cannot be precluded by any authority, or public or private body – specifically to provide legal protection or within verification procedures. But employees must not be informed that they have a right to be assisted by a lawyer.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Interviewees have no legally established right to be assisted by a works council representative.

f) be informed that data may be transferred to another country (in particular to the United States)?

Employees must be informed, and appropriate safeguards be put in place in the absence of an adequacy decision of the European Commission. Pursuant to the GDPR, data can only be transferred to non-EU/EEA countries if the controller and processor fulfil the conditions established in Chapter V of the GDPR.

g) sign a data privacy waiver?

The employee must generally sign a data-privacy waiver concerning personal data and non-professional information before the interview takes place. This waiver could prove useful in subsequent potential judicial proceedings.

h) be informed that the information gathered might be passed on to authorities?

The employee should be informed of the possibility that the collected information will be passed on to the authorities. Moreover, under Law 58/2019 and the PLC, images and other personal data recorded through video or other remote surveillance mechanisms may only be used within the scope of criminal proceedings (and within the scope of disciplinary proceedings insofar as it is used within criminal proceedings). Note that video surveillance may only be used to keep goods and persons safe and the employer must both warn the employees that it has implemented these mechanisms and explain its reasons for doing so in accordance with Article 13 of the GDPR.

i) be informed that written notes will be taken?

The employee must in general be informed that written notes will be taken during the interview. Within a disciplinary procedure (i.e. once the employee has been sent the accusation note), interviews with witnesses or the accused party must be recorded in writing, according to settled case law on the matter.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Although there is no specific law on this matter, issuing document hold notices is standard practice in Portugal. Such notices should be clear, detailed, clearly delimited and issued as early as possible. These notices can only include professional information, given that companies are generally prohibited from accessing non-professional information. Please refer to our answer to question 5b.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Should the internal investigation be conducted by lawyers, companies may claim attorney-client privilege over any findings arising from the investigation. In fact, any attorney-client relationship is subject to strict duties of professional secrecy regarding facts and circumstances acknowledged exclusively by the respective client's disclosure. Lawyers can only waive their duty of professional secrecy under exceptional circumstances and with the approval of the president of the respective Regional Council of the Portuguese Bar Association.

Additionally, companies are also protected from self-incrimination as established in the PCC. Please refer to our answer to question 3.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Yes. Attorney-client privilege applies to both documents created by and communications with in-house counsel.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

These notifications are generally not required unless the respective insurance policy specifically states that they are.

b) Business partners (e.g. banks and creditors)?

These notifications are generally not required unless a specific contract states that they are.

c) Shareholders?

These notifications are generally not required. But if the internal investigation concerns an issuer of financial instruments, the company must inform the public, as soon as possible, about any inside information directly concerning that issuer (per Article 7 of Regulation 596/2014 of the European Parliament and the Council of 16 April 2014).

d) Authorities?

These notifications are not required. But voluntarily involving the authorities and being cooperative can be beneficial in case the investigation leads to a conviction. Moreover, note that the line between not notifying the authorities about an investigation and the crime of providing personal advantages (*crime de favorecimento pessoal*) – i.e. when an individual conceals the crime committed by another individual – is rather thin.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

No measures with regard to the authorities need to be taken when an internal investigation starts. But the company must make sure that any alleged ongoing breach of law by the company or its employees ceases immediately.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices do not ask for specific steps to be observed, nor do they have concerns about internal investigations. Portuguese law does not establish a general duty to report criminal or administrative offences to the local prosecutor's offices. However, the prosecutor's office may use the conclusions drawn in internal investigations against the company as evidence of misconduct. Therefore, voluntarily involving the authorities should be carefully considered when initiating internal investigations.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Pursuant to the Portuguese Criminal Procedure Code ("**PCPC**"), searches and seizures are admissible if the formal and material legal requirements are met.

Searches must be authorised, ordered or validated by a judicial authority if there is reasonable evidence that any objects related to a crime or which may be used as evidence are in a private or restricted space. Court orders are valid for 30 days.

Seizures also need to be authorised or ordered by a judicial authority. Police authorities may seize objects during a search in urgent or danger in delay cases. But when they do, the competent judicial authority still needs to validate the seizure within the next 72 hours. Seizing communications must be authorised or ordered by a judge while seizing personal documents or documents protected by legal privilege is strictly forbidden. Please refer to our answer to question 6b.

Regarding financial institutions, a judge needs to personally seize documents, securities, valuables, monetary amounts and other objects (in the presence of the police authorities, if necessary) once the sound reasons linked to the crime in question have been verified.

Evidence collected in breach of these formalities is inadmissible and as such cannot be used against the company.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Beyond specific leniency provisions, any deals and non-prosecution agreements with legal or natural persons are strictly prohibited. So any evidence collected within criminal proceedings as a result of giving (unlawful) promises of leniency is inadmissible. However, if some circumstances at met, the prosecutor's office may agree not to indict the defendant and suspend the criminal proceedings (*suspensão provisória do processo*) until the defendant performs the specific injunctions it voluntarily undertook to perform and then close the proceedings. This is not technically a deal since the prosecutor's office is hypothetically bound to suspend the proceedings if the legal requirements are met. Despite not being a deal, some of the requirements are highly subjective (e.g. absence of a high degree of guilt). Therefore, in practice, the prosecutor's office has wide discretion to decide on this point. The prosecutor's office is thus undoubtedly tempted to demand cooperation from the suspect in return for suspending the proceedings.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

The main penalties companies face are fines or dissolution when they have been incorporated exclusively or mainly for unlawful purposes. Potential ancillary sanctions include injunctions and prohibitions against pursuing specific activities or applying for subsidies or grants.

Corporate liability does not exclude individual liability. Individuals may be subject to sanctions such as imprisonment, fines, dismissal for just cause and potential debarment from respective professional associations.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Pursuant to the PCC, corporate liability can potentially be excluded if the company had adequate compliance systems in place before the alleged misconduct happened. This may apply if an individual acted contrary to the company's specific orders or instructions. Moreover, the court may consider reducing the sanctions applicable to legal persons if they had adequate compliance programmes in place before the criminal actions occurred.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Although most of the measures the European Union has implemented apply directly at a national level, we highlight the following ESG-related Portuguese legislation:

(i) Decree-Law 89/2017 of 28 July, which imposes an obligation on large companies and groups to file a non-financial statement relating to ESG factors;

(ii) Decree-Law 109-F/2021 of 9 December, which imposes an obligation on collective investment undertakings and their managers to consider sustainability factors;

(iii) Decree-Law 109-H/2021 of 10 December, which regulates the sustainability factors imposed in relation to financial product governance; and

(iv) The Framework Climate Law (Law No. 98/2021 of 31 December).

Furthermore, environmental activists have filed a lawsuit against the Portuguese State for an alleged violation of the abovementioned Basic Climate Law, in particular for failing to combat greenhouse gas emissions and neglecting the "right to life". In addition, in 2020 six young Portuguese citizens filed a lawsuit with the European Court of Human Rights (ECHR) against 33 European countries (including Portugal), accusing them of failing to fulfil their obligations to minimise the impact of climate change. The court has not yet decided on this case.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The Portuguese government approved the 2020–24 national anti-corruption strategy, which includes several legislative amendments (notably, the general framework to prevent corruption). It has also been discussing whether to include in the PCPC the possibility of entering into deals concerning the applicable sanctions during the trial stage of criminal proceedings, if the defendant willingly and voluntarily confesses to the offence.

Very recently, the Portugal's prime minister resigned after his official residence was raided, and the attorney general issued the following statement: "*Moreover, in the course of our investigations, the public prosecutor's office became aware of suspects using the prime minister's name and authority and his involvement to unblock procedures in the aforementioned context. These references will be independently analysed within the scope of an inquiry that Supreme Court of Justice initiated, as that is the competent forum*".

The prime minister was not formally identified as a suspect (*arguido*) or charged with any crime, which raises doubts as to whether the public prosecutor's office should have made such a statement that casts doubt on the prime minister's integrity.

CONTACTS

URÍA MENÉNDEZ
PROENÇA DE CARVALHO

Edifício Rodrigo Uría
Praça Marquês de Pombal, 12
1250-162 Lisboa
Portugal

Tel.: +351 21 030 8600
Fax: +351 21 030 8601
www.uria.com

Nuno Salazar Casanova
Partner
Uría Menéndez – Proença de Carvalho
T +351 21 030 8609
E nuno.casanova@uria.com

Nuno has been a lawyer in the litigation practice area of Uría Menéndez Proença de Carvalho's Lisbon office since 2004. He was made partner in January 2015.

Nuno leads high-profile – often cross-border – disputes, including regulatory investigations and enforcement, class actions and other major reputation-threatening litigation, especially those requiring a global strategy to deal with intertwined civil, criminal, regulatory and administrative issues.

He has ample experience representing clients before the public prosecution office in investigations involving corporate and economic crimes and before supervisory authorities in relation to infringements of banking, finance, securities, and environmental law.

Lua Mota Santos
Associate
Uría Menéndez – Proença de Carvalho
T +351 21 030 8631
E lua.motasantos@uria.com

Lua joined Uría Menéndez – Proença de Carvalho in 2021 and has been an associate since 2023.

She advises on a wide range of litigation matters involving civil, commercial and criminal law, with a particular focus on the latter.

Romania

Mareş & Mareş

Dr. Mihai Mareş

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Directive (EU) 2019/1.937 was transposed through Law No. 361/2022 on the Protection of Whistleblowers in the Public Interest ("**LPOW**"), which came into effect on 22 December 2022. Article 22 of the LPOW expressly prohibits any form of reprisals against whistleblowers in the public interest, threats of reprisals, or attempts at reprisals, especially those related to suspension, modification, or termination of employment relationships; application of disciplinary sanctions; coercion; discrimination; or causing any type of prejudice. This article includes a detailed list of the above. In case the whistleblower reports on corruption offences, offences assimilated to corruption offences, forgery offences, offences committed in office or work-related offences, and offences against the financial interests of the European Union, the protection measures set out under Article 12 paragraph 2 of Law No. 682/2002 on the protection of witnesses shall be applied *ex officio*.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Based on Article 5 of the LPOW, the whistleblower who reports a violation of the law may choose between internal and external reporting channels. Also, in choosing the reporting channel, the whistleblower may consider aspects such as:

- Whether there is a risk of retaliation or whether the reported breach could not or would not be effectively remedied through internal reporting channels; or
- Whether there is a lack of internal reporting channels at private legal entities with less than 50 employees.

The LPOW does not explicitly allow or prohibit the use of a group-wide reporting system. Article 9 paragraph 4 of the LPOW states that private entities with 50 to 249 employees can group together to use or share resources in receiving reports and with regard to subsequent actions. However, this possibility is not explicitly provided for companies with over 249 employees. The law remains unclear in this respect.

Regional administrative units with fewer than 10,000 inhabitants or fewer than 50 employees can group together and use or share resources regarding the reception of reports concerning legal violations and subsequent actions.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) In case of an internal disciplinary investigation, the law requires that the employee be summoned in writing for an interview, by the person empowered by the employer to carry out the investigation. If the employer does not comply with this requirement, a decision sanctioning the employee will be void.

The only measure that may be ordered without carrying out a disciplinary investigation is the warning.

There is no other obligation for informing other people or employee representative bodies.

An employee who is being disciplinarily investigated has the right to request that a member of the trade union, which they are a member of, participates in the interview.

The law does not provide any regulations for conducting an internal investigation for any other type of misconduct. Nevertheless, provisions regarding internal investigation for other types of misconduct may be provided by internal regulations of any legal person.

b) The Romanian Law does not impose an obligation for a data protection officer or data privacy authority to be informed about the investigation. Nevertheless, in case the operator detects a data security breach, the Romanian Data Protection Authority must be notified.

c) In accordance with Article 267 of the Romanian Criminal Code, if a public servant becomes aware of a criminal offence that is related to the work place where they carry out their job duties, the public servant must immediately refer it to the criminal prosecution body. Otherwise, the public servant may be subject to criminal liability punishable with imprisonment of three months to three years or with a fine when committed wilfully, or imprisonment of three months to one year or by a fine when committed negligently. There is no such reporting obligation for an employee of a private sector company.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

There is no explicit obligation of this nature under Romanian law in case of an internal disciplinary investigation. The employee who is summoned to an interview does not have a duty to support the investigation; and they may participate in the interview or not. Also, they may provide information regarding the accusation brought against them, or not. However, if the employee unjustifiably refuses to adhere to their employee's instruction to appear, the company may impose disciplinary measures without having to perform the prior disciplinary investigation.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

According to the Romanian Labour Code, the employer can apply a sanction within 30 calendar days as of becoming aware of the disciplinary misconduct following a disciplinary investigation, but no later than six months from the date of the act.

Regarding the first time-period of 30 calendar days, the Romanian Supreme Court established that the term starts to run from the date the employer took note of what is written in the report following the disciplinary investigation.

Should any of the two time-periods elapse, the employer loses the right to sanction the respective employee.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Data privacy laws or laws protecting classified information apply to any type of data processing, depending on the case.

The relevant legal framework applicable in Romania essentially comprises of the following pieces of legislation:

- Romanian Criminal Code: Articles 226 (violation of privacy), 302 (violating privacy of correspondence), 303 (disclosure of information classified as state secret), 304 (disclosure of information classified as professional secret or not public), 305 (negligence in storing information);
- Regulation (EU) 2016/679 – the General Data Protection Regulation ("**GDPR**");
- Directive (EU) 2016/680 – the Data Protection Directive (transposed in Romania mainly through Law No. 363/2018 regulating data protection and other pieces of domestic legislation);
- Law No. 129/2018 amending and supplementing Law No. 102/2005 regarding the establishment, organisation and function of the National Supervisory Authority for the Processing of Personal Data, as well as for the repeal of Law No. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data;
- Law No. 182/2002 regarding classified information.

b) reviewing emails?

Private communication is protected under Romanian Law, and access to private communications is permitted only under the conditions set out by law, namely if it is approved in advance by a judge and enforced by the judicial bodies.

Otherwise, accessing an email without permission may constitute the criminal offences of violating the privacy of correspondence (as per Article 302 of the Romanian Criminal Code) and of illegally accessing a computer system (Article 360 Criminal Code).

Criminal liability may be excluded and such private communication may be used without impunity if it was originally viewed accidentally and only if it proves the perpetration of an offence or if it serves a general interest (e.g. acts of public interest, meaningful for the community), of higher import than the potential damage caused.

In this context, when assessing the lawfulness of accessing professional emails used within an organisation, the ownership of the information contained therein must be established as a first step; either it is deemed to belong to the employer or it is attributed solely to the employee.

c) collecting (electronic) documents and/or other information?

Any and all processing of documents and/or data must take into account the applicable provisions of data privacy laws. In case of an internal investigation the company holds ownership over the equipment used and data/information processed by the employee under employment provisions. As such, the employer may secure, collect and review such work data and work products, subject to an assessment of the applicable data privacy laws.

On the contrary, accessing/collecting documents or information exceeding the scope of work relations may only be permitted to state authorities, pursuant to special legal procedures (e.g. searches and seizures).

d) analysing accounting and/or other business databases?

Analysing private databases is only permitted pursuant to the procedures provided for by law (e.g. expert reports). Any professional accounting and/or business databases pertaining to labour relations between the employer and their employees generally constitute the property of the employer, thus being fully accessible to such employer.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no legal obligation to provide written instructions to an employee regarding legal circumstances or their rights. Nevertheless, the company internal regulation, which shall be made available to all employees, must contain specific provisions and information as to the disciplinary procedures enforced by such company.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

The Romanian Criminal Procedure Code provides that a suspect or a defendant will be informed about the right to remain silent during interrogations conducted by the judicial bodies. There is no corresponding obligation for other types of interviews, including interviews as part of an internal investigation.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no obligation to give an Upjohn warning under Romanian law.

d) be informed of their right to have their own lawyer attend the interview?

According to Article 251 paragraph 4 of the Romanian Labour Code, during an internal disciplinary investigation, the employee who allegedly committed the wrongdoing has the right to defend themselves and to provide the person empowered to carry out the investigation all the evidence and motivations they consider necessary. The same paragraph offers the employee access to a lawyer, upon request. However, there is no explicit legal obligation of the employer to inform their employees about that right. The company's internal regulation, which shall be made available to all employees, must however contain specific provisions in that regard.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Article 251 paragraph 4 of the Romanian Labour Code provides the employee the right to be assisted, at their request, by a representative of the trade union of which they are a member in case of a disciplinary investigation. The company's internal regulation, which shall be made available to all employees, must contain specific provisions in that regard. However, there is no explicit legal obligation of the employer to inform their employees.

f) be informed that data may be transferred to another country (in particular to the United States)?

According to the provisions of Law No. 363/2018 as well as the relevant EU legal provisions (GDPR), the data subject has to be informed of the purpose of data processing. This includes any processing of personal data conducted during an internal investigation. The information process also has to include any references to where the personal data is transferred to and the rights of the data subject in relation to such processing.

g) sign a data privacy waiver?

Under Romanian law, the employer is not obliged to ask the employee to sign a data privacy waiver. However, in practice, the employer will request such document to be signed for evidentiary purposes.

The right to the protection of personal data, which applies to all employees, implies the right to information regarding all relevant data privacy matters (such as the identity of the operator, the purpose of data processing, the rights of the persons concerned and the conditions for exercising them), the right of access to

data, the right to rectification and erasure of data, the right to restriction of processing, the right to data portability as well as the right to opposition.

h) be informed that the information gathered might be passed on to authorities?

Under Romanian law, there is no obligation for the employer to inform the employee of passing information to authorities.

i) be informed that written notes will be taken?

There is no obligation for the employer to inform the employee that written notes will be taken under Romanian law.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no legal provision in Romanian law regarding this kind of activity. Thus, such notices are allowed and are generally at the discretion of the employer.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege may be claimed over findings of the internal investigation.

According to the Lawyer Profession Statute, the lawyer is required to keep professional secrecy on any aspect of the case entrusted to them.

The professional secrecy applies to any information and data of any kind, in any form and on any support, as well as any documents drawn up by a lawyer containing information or data provided by the client or based on them for the purpose of providing legal assistance; and whose confidentiality has been requested by the client.

In order to ensure privilege protection any documents, information or data regarding an investigation should be kept only at the professional headquarters of the lawyer – which can also be situated at the lawyer's domicile – or in areas approved by the Bar. Documents of professional nature are inviolable.

Also, for ensuring professional secrecy, correspondence with a client or notes regarding the defence of a client are exempted from seizure and confiscation. Moreover, the attorney-client relationship cannot be subject to technical surveillance measures unless strictly prescribed by law.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

In case the lawyer is an active member of the Bar and is not bound by an employee-employer relation but exercises the legal profession based on an agreement of legal services, the attorney-client privilege will apply under any circumstances in regard to the documents, data, and information mentioned at question 8.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

As a general principle, we note that there is no legal obligation under the Romanian law for such notifications, unless they are necessary under respective financing or insurance contracts of the respective legal entity. As such, a case by case evaluation must be performed.

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

To the extent that the internal investigation may generate any liability or claim under the employer's/employee's insurance policies, the specific notification obligations under the insurance policy must be thoroughly observed.

b) Business partners (e.g. banks and creditors)?

Specific contractual provisions pertaining to the respective business partnership must be reviewed and analysed in order to determine potential reporting obligations arising from an internal investigation.

c) Shareholders?

To the extent that the subject matter of the internal investigation may be interpreted as a potential trigger on the company's stock price, a thorough analysis should be performed as to whether the matter of the internal investigation should be notified to the regulatory/supervisory authorities and/or to the company shareholders.

d) Authorities?

There is no specific duty to inform criminal law authorities when conducting an internal investigation.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

If a company becomes aware of a breach of laws by the company or its employees, the company must take all suitable steps to end such behaviour.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

The prosecutor's offices will not be concerned about internal investigations.

In any case, if a criminal offence has been committed and the prosecutor office learns about it, either *ex officio*, or through complaint or denunciation, there is an obligation for criminal proceedings to be initiated.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

The domiciliary search warrant in Romania must be issued by a judge of a court of law and its content must comply with certain formal requirements.

The search can be conducted only by the prosecutor or by criminal investigation bodies, accompanied, as applicable, by operative workers and, as a rule, cannot be initiated before 6.00 a.m. or after 8.00 p.m.

In case the legal prerequisites are not fulfilled, the evidence may be subject to exclusion, carried out through the nullity sanction.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

The Romanian Criminal Procedure Code allows for the conclusion of a plea bargain between the defendant and the prosecutor. This possibility is also available to legal entities, although less common in practice. The effects of such agreement are the reduction of the penalty limits provided by law for a particular offence by one-third in case of prison sentences or one-fourth in case of criminal fines.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

A company can face either criminal or administrative penalties in Romania.

As far as criminal penalties are concerned, the primary penalty for companies is fines. Depending on the offence, companies may also face complementary penalties, i.e. closure of individual company sites or even liquidation.

The directors, officers or employees, as individuals, can face fines, imprisonment, or disciplinary measures, depending on the nature of the misconduct. Also, some of their rights may be restricted as part of the criminal sentencing system.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

From a criminal law perspective, the implementation of a compliance system is not a legal criterion for excluding penalties. These facts may be deemed as mitigating judicial circumstances at most, regardless of whether the effective compliance system was already implemented before the alleged misconduct or not.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

By Orders No. 1938/2016 and No. 3456/2018, which modified and supplemented certain accounting regulations issued by the Ministry of Finance, an obligation was established for companies with over 500 employees on average, to present certain information falling within the scope of ESG factors (i.e. environmental, social and personnel-related aspects) in their annual non-financial statement. We would like to mention at this point that the internal legal framework is subject to constant change.

No notable cases have been reported so far nor investigated by authorities in this regard.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The LPOW stipulated that the enforcement of the obligation to identify or establish internal reporting channels for private legal entities with 50 to 249 employees was postponed until 17 December 2023. Since its publication in the Official Gazette, this provision has generated conflicting discussions regarding the obligation of these entities to comply with the obligations arising from the mentioned law.

However, considering that the deadline has now passed, it will be of interest to continue to monitor how the supervisory authority will assess the extent to which the entities in question comply with that obligation, what its conclusions will be and to which sanctions it will be inclined.

CONTACT

MAREŞ & MAREŞ
AVOCAŢI

55-55 bis Carol I Blvd., 2nd District
020915 Bucharest
Romania

Tel.: +4 031 43 78 324
Fax: +4 031 43 78 327
www.mares.ro

Dr. Mihai Mareş
Managing Partner
Mareş & Mareş
T +4 031 43 78 324
E mihai.mares@mares.ro

Mihai is one of the founders and the Managing Partner of Mareş & Mareş, as well the partner in charge of the white collar crime department.

His practice focuses exclusively on criminal defence of senior executives, entrepreneurs, major industrial groups, financial institutions and large international and domestic companies, in a wide range of matters involving accounting, financial, securities and tax fraud; bribery, antitrust, and money laundering cases.

In addition, he advises clients in internal investigations and audits involving money laundering, fraud and other corporate misconduct. In international criminal law, Mihai acts in cases of international corruption, freezing of assets, multijurisdictional investigations and extradition.

Mihai Mareş is a member of European Criminal Bar Association and International Bar Association (Business Crime Committee) and regularly speaks at local and international seminars related to white collar crime matters.

Slovakia

HAVEL & PARTNERS s.r.o. attorneys-at-law

Ondřej Majer

Milan Černaj

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The EU Whistleblower Directive has been implemented in Slovakia, albeit almost a year and a half after the deadline for transposition by an amendment to the Slovak Whistleblowing Act No. 54/2019 Coll.

Apart from the employers with at least 50 employees, the Whistleblowing Act now imposes the obligation to implement the whistleblowing system on employers irrespective of the number of employees in case they provide financial services, services in the area of transport security or environmental protection.

This means an obligation (i) to implement internal reporting channels and (ii) to determine the responsible person, (iii) to adopt internal guidelines on whistleblowing specifying the details on receiving reports. This includes information on the investigation of reports, the duty of maintaining confidentiality, processing of personal data, record keeping of the reports, the prohibition of retaliation, measures to eliminate deficiencies found during the processing of reports and communication with the whistleblower about these measures, and implementation of measures against conduct that prevents persons from submitting reports.

The Whistleblowing Act now requires the responsible person (i) to acknowledge the receipt of the report within seven days of the receipt, (ii) to investigate each whistleblowing report within 90 days as of this receipt, (iii) to maintain the confidentiality of the whistleblower's identity and of the identity of a person concerned by the report. The duration of the investigation phase cannot be prolonged anymore.

The employers are obligated to request a prior approval from the Whistleblower Protection Office when taking legal actions or making decision in an employment relationship towards the whistleblower to which he did not consent. This applies if the whistleblower has previously requested and has been granted the protection by the public prosecutor's office or a relevant administrative authority.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Not without limitation, as the Whistleblowing Act imposes an obligation to also appoint an in-house responsible person, i.e. an employee of the employer operating in Slovakia, for the internal reporting and investigation process, who shall have a direct access to the reporting channels.
The employers with more than 250 employees may outsource or utilise the group wide systems only for receiving the reports and for their confirmation.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) There are no specific legal requirements stipulated by law. The possibility of including these rights of employee representatives is not excluded in collective agreements.

b) Neither the data protection officer (the "**DPO**") nor the data privacy authority (the "**DPA**") have to be informed. However, it is advisable to inform and/or involve the DPO in the investigation.

c) No specific legal requirements are applicable in relation to internal investigations.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

There are no specific legal requirements directly stipulated by the Slovak Labour Code No. 311/2001 Coll., as amended (the "**LC**").

The employees' obligations to support the investigation or participate in interviews stem from the provisions of the LC stipulating, *inter alia*, the obligation to: (i) comply with the instructions of senior employees, (ii) protect the employer's property against damage, loss, destruction, and abuse; (iii) not act against the justified interests of the employer; (iv) observe the internal rules of the employer, such as work rules (where the internal guidelines on whistleblowing can also stipulate a given obligation); and (v) maintain confidentiality over employment matters and matters in the interests of the employer. The employee's obligation to maintain confidentiality does not apply to the report of crimes or other antisocial activities defined by law.

The employee's refusal to support the investigation or participate in interviews may be considered a breach of their obligations. Depending on its seriousness, this may be a sufficient reason for a formal warning, giving notice, or even immediate termination of the employment.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

The internal investigation has no impact on any labour law deadlines, including the right to sanction employees.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

In general, the GDPR applies. Personal data processed in interviews are subject to data privacy laws. It is recommended to assess the information that shall be processed from the viewpoint of the applicable data privacy laws early, as well as the categorisation and sensitivity of the information to be processed. Also, the Whistleblowing Act requires internal whistleblowing guidelines to address details on data processing.

b) reviewing emails?

The employer is not allowed to intrude upon the privacy of employees by monitoring them, keeping records of telephone calls made with the employer's equipment, or reviewing emails sent from a work email address and delivered to such an address without prior notice. However, this does not apply for serious reasons relating to the specific character of the employer's activities. If the employer intends to implement a surveillance mechanism, the employer must consult with the employee's representatives and inform the employees in advance.

As to the employee's private communication, stricter legal protections apply.

c) collecting (electronic) documents and/or other information?

In case the electronic documents and/or information include personal data, data privacy laws apply. It is recommended to assess the information that shall be processed from the viewpoint of the applicable data privacy laws early, as well as the categorisation and sensitivity of the information to be processed.

d) analysing accounting and/or other business databases?

In general, the analysis of a company's accounting and other business databases is allowed. However, depending on the manner and purposes of the analysis and the categories of data, please see the information added to points 6a-c below.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

In general, there is no specific obligation to instruct an employee on their rights.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

The right to remain silent, which applies during interrogations of criminal authorities, does not apply. In general, there is no corresponding right in internal investigations.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no obligation to provide an Upjohn warning or similar information under Slovak law.

d) be informed of their right to have their own lawyer attend the interview?

There is no obligation of the company to inform the employee about their given right. However, the employee has a constitutional right to legal counsel. This right was also confirmed by the Constitutional Court of the Slovak Republic.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

There is no specific legal requirement stipulated by law regarding the attendance of an employee representative at the interview or the employee's right to have employee representatives attend.

f) be informed that data may be transferred to another country (in particular to the United States)?

The employee must be informed of the occasion of gathering the data, *inter alia*, that the controller intends to transfer the personal data to a third country (e.g. the United States).

g) sign a data privacy waiver?

The concept of an "in advance waiver" is not recognised in Slovakia. Thus, signing a waiver by the interviewee would not have the intended legal effect.

h) be informed that the information gathered might be passed on to authorities?

There is no specific legal obligation that requires the employee to be informed.

i) be informed that written notes will be taken?

Slovakia has no specific legal obligation to inform the employee that written notes will be taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There are no specific legal requirements for issuing document hold notices. Thus, there are no legal barriers to issuing such notices in practice.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The attorney-client privilege may apply to findings of the internal investigation. However, the privilege only applies to information gathered or created by an attorney registered with the Slovak Bar Association. The rules do not apply to in-house lawyers.

To ensure privilege, the safest way is to involve a registered attorney as external counsel. In addition, it may also be helpful to label the privileged documents accordingly.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

The attorney-client privilege does not apply to in-house counsel in Slovakia or any communication with in-house counsel and documents created by in-house counsel.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

No specific legal requirements are applicable. The notification in question will depend on the terms and conditions of the insurance contract, related circumstances, and the definition of an insured event that connects the company's claim against the insurer. For example, local terms and conditions for liability insurance typically require that the insurer be notified of any event that may give rise to a claim under the policy. If the investigation relates to such an event, the event needs to be reported to the insurer; however, it will typically not be necessary to report the investigation itself.

b) Business partners (e.g. banks and creditors)?

There are no specific legal requirements to notify business partners when starting an investigation. Any possible notification obligations may arise from the contractual obligations agreed between the company and its business partners. Even if there is no explicit provision in the contract, the company must consider notification with regard to the purpose of the agreement.

c) Shareholders?

No specific legal requirements apply to investigations. In general, the company must assess in all individual cases whether providing certain information could be a breach of law, cause damage to the company or its controlled companies, or threaten the interests of the company or its shareholders. The provision of information can be refused as long as the information does not relate to the company's economic activities

and property conditions. However, such refusal must consider the company's legal form and the provisions of corporate documents in which certain differences may apply.

d) Authorities?

In general, there is no legal obligation to inform the authorities of an internal investigation or potential misconduct within the company. However, depending on the information and outcomes of the investigation, the company is obliged under Act No. 301/2005 Coll., the Criminal Procedure Code, as amended (the "**CPC**"), to file a criminal complaint if there are circumstances suggesting that specific serious crimes were committed. Also, submitting a whistleblowing report does not relieve the whistleblower from the potential statutory obligation to report a crime.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Slovakia has no specific legal requirements. In any case, the company should audit its procedures, identify the breach, and eliminate or minimise ongoing illicit activities to mitigate any possible damage.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

In general, local prosecutors are not involved in internal investigations. Pursuant to the CPC, early communication and cooperation with the local prosecutor's office are recommended.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

The legal requirements for search warrants are stipulated by the CPC and for dawn raids by the Slovak Competition Act No. 187/2021 Coll. ("**Competition Act**").

Pursuant to the CPC, a search may be conducted if there is reasonable suspicion that the apartment or other premises serving as a residence or premises attached to them contains an item relevant to the criminal proceedings. The same applies if there is suspicion that a person suspected of committing a criminal offence is hiding within the respective premises or if the seizure of movable assets is necessary to satisfy the entitlement to damages of the victim. For the same reasons, a search of non-residential premises ("**other premises**") not publicly accessible may be performed. In all cases, the search warrant must be issued in writing and signed by the person determined by the CPC.

In the absence of a warrant or authorisation, a police officer may conduct the search of other premises or property only if the warrant or authorisation could not be secured in advance and in cases of emergency. The same applies if the search involves a person caught in committing a crime, a person for whom an arrest warrant was issued, or a persecuted person who hides on the premises in question. This procedure, however, has to be reported immediately to the body authorised to issue the warrant or grant authorisation.

In competition matters, the authorisation for a dawn raid fulfils the tasks stated by the Competition Act. It must be issued in writing by the Antimonopoly Office of the Slovak Republic ("**Office**"). The authorisation must contain information stipulated by the Competition Act, namely: (i) the designation of the person issuing the document (name, surname, and position – typically Vice-Chair or Chair of the Office); (ii) the designation of the premises and means of transport in which the dawn raid will be conducted; (iii) the time period of the dawn raid; (iv) instructions on the rights and obligations of the inspected entity; (v) the signature of the person issuing the document; and (vi) the authorisation number and Office's stamp. The authorisation is limited to the entry of all company premises and means of transport that are related to the company's activity or conduct.

Suppose there is a reasonable suspicion that materials or documents that can prove restriction of competition and relate to the company's conduct are located in non-business premises or means of transport or in private premises or means of transport. In that case, the Office may search those premises only based on the consent of the court with an inspection issued at the request of the Office.

The conditions for the Inspection conducted by the European Commission are similar to the Office's conditions stated above.

In general, if legal requirements are not fulfilled, the seized evidence should not be used, which has been confirmed by the Supreme Court of the Slovak Republic.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

The CPC provides possibilities corresponding to deals, non-prosecution agreements, or deferred prosecution agreements. All of them are available for individuals as well as for corporations.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

The company may face the following penalties:

a) Prohibition of activities (from one to 10 years);

b) Forfeiture of items;

c) Pecuniary penalty (from €1,500 to €1.6 million);

d) Forfeiture of property;

e) Dissolution of the corporate entity (if the activities were used fully or partially for committing a crime);

f) Prohibition of participation in public procurement (from one to 10 years);

g) Prohibition of receiving subsidies or subventions;

h) Prohibition of receiving help and support provided from EU funds (from one to 10 years);

i) Publication of condemnatory sentence (at the expense of the corporate entity).

Individuals may also face criminal prosecution in specific situations for the misconduct of other employees when they failed to implement sufficient supervision or control. In this case, they may face the following penalties:

a) Imprisonment;

b) Home confinement;

c) Community service work;

d) Pecuniary penalty (from €160 to €331,930);

e) Forfeiture of property;

f) Forfeiture of items;

g) Prohibition of activity;

h) Prohibition of residence;

i) Prohibition of participation in public events;

j) Loss of honorary degrees and distinctions;

k) Loss of military and other rank; and

l) Expulsion.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Under the Slovak Act No. 91/2016 Coll. on the Criminal Liability of Legal Entities, the existence of an efficient compliance system is not directly a reason for discharging or suspending the company's liability for the misconduct.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

No specific legal requirements apply. The European Commission Delegated Directive has not been implemented in Slovakia yet as the legislative procedure is in its initial stages.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The Whistleblowers Protection Office slowly swifts from being more educational oriented to gently enforcing the statutory obligations. The Office has imposed its first penalty on the employer who has breached the obligation of investigating the report within the statutory deadline.

Recently, the government's activities aim to introduce legislative changes to the protection of whistleblowers. The planned amendment shall introduce the possibility for the employers to request a review of the decision granting the protection to the whistleblower. The outcome of the review by the General Prosecutor's Office, or by a relevant administrative authority, may lead to the revocation of the protection.

CONTACTS

HAVEL & PARTNERS
CONNECTED THROUGH SUCCESS

Zuckermandel Centre, Žižkova 7803/9
811 02 Bratislava
Slovak Republic

Tel.: +421 232 113 900
Email: office@havelpartners.sk

HAVEL & PARTNERS, with offices in Prague, Brno, Bratislava, Pilsen, Olomouc, and Ostrava, has a team of 350 lawyers and tax advisors, approx. 200 associates and 500 employees in total, is the largest independent law firm in Central Europe.

Ondřej Majer
Partner
HAVEL & PARTNERS
T +421 232 113 900
+420 737 150 145
E ondrej.majer@havelpartners.sk

Ondřej specialises, *inter alia*, in commercial and contractual law, corporate law including compliance programmes, mergers and acquisitions, real estate law, litigation and bankruptcy law.

Ondřej has extensive experience in the automotive, energy, real estate and construction sectors, both in the Czech Republic and in Slovakia.

In mergers and acquisitions, he has represented a number of clients, on the side of both sellers and buyers, in the Czech Republic and in Slovakia.

In litigation and insolvency, Ondřej has represented clients in a number of comprehensive litigation matters, including cross-border disputes, cross-border insolvencies, disputes with an international element, and corporate law disputes.

Milan Černaj
Associate
HAVEL & PARTNERS
T +421 232 113 912
+421 910 822 533
E milan.cernaj @havelpartners.sk

Milan specialises in labour law, whistleblowing procedures, including litigation and bankruptcy law.

In the whistleblowing practice area, he prepares legal analyses and due diligence reports, revises, and creates whistleblowing guidelines for companies operating in various fields of law.

Milan also has extensive experience and many years of practice in litigation, representing clients before courts and competent authorities, including the Whistleblower Protection Office, including securing and protecting clients' claims in enforcement or insolvency proceedings.

Slovenia

Law Firm Senica & Partners, Ltd.


Uroš Čop


Katarina Mervič


Žiga Sternad

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X*	X	X	X	
No					X

* Corporations (legal persons) can be criminally liable under the conditions defined in the Liability of Legal Persons for Criminal Offences Act ("**ZOPOKD**").

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The Reporting Persons Protection Act ("**ZZPri**") sets out the methods and procedures for reporting and dealing with breaches of regulations that come to the attention of individuals in the work environment, as well as the protection of individuals who report or publicly disclose information about a breach.

The Trustee shall conclude the investigation of the reported infringements within three months of its receipt with a report stating whether and on what grounds the application is unfounded. If the report of infringements is substantiated, the report shall indicate in particular the measures proposed and implemented to bring the infringement to an end, to remedy the consequences of the infringement or to prevent future infringements, its findings on the effectiveness of the implementation of the proposed measures and any measures proposed and implemented to protect the whistleblower. At the end of the internal investigation, and no later than three months after receipt of the reported infringements, the facilitator shall inform the whistleblower of the merits of the reported infringements, the measures proposed and implemented, the outcome of the procedure, or if the infringement procedures have not been completed after three months, of the status of the internal notification procedure.

In the case of an internal investigation, it is important that the facilitator (this is the person who investigates the reported infringements – one person has to be responsible for internal investigation) conclude the examination of the reported infringements within three months of its receipt. The reporter is to be notified whether or not the grounds of the report of infringements are founded. If the report of infringements is substantiated, the investigation report shall indicate in particular the measures proposed and implemented to bring the infringement to an end, to remedy the consequences of the infringement or to prevent future infringements, its findings on the effectiveness of the implementation of the proposed measures and any measures proposed and implemented to protect the whistleblower.

The facilitator shall, subject to the protection of the identity of the whistleblower, communicate the findings of the investigation report to the management. At the end of the examination and at the latest within three months of receipt of the report of infringements, the facilitator shall inform the whistleblower of the validity

of the report, the measures proposed and implemented, the outcome of the proceedings, or the status of the internal reporting procedure, if the infringement procedures have not yet been completed after three months.

Any retaliatory measures against the applicant, such as dismissal, suspension, downgrading, preventing or withholding promotion, etc., are, of course, prohibited.

The law sets out the safeguards to be provided to whistleblowers with regard to the type of retaliation, in particular:

- The prohibition to disclose the identity of the whistleblower and confidentiality;
- Exclusion of the liability of the whistleblower;
- Judicial protection and interim injunctions in the event of retaliation;
- Free legal aid;
- Unemployment benefit;
- Psychological support.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

An internal reporting process must be in place. Public and private sector entities with 50 or more employees are obliged to set up an internal reporting channel.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) No, the ZZPri does not impose an obligation to inform the workers' representatives in the context of the handling of an internal complaint.

However, pursuant to the Slovenian Worker Participation in Management Act ("**ZSDU**"), workers can participate in companies' management via representative bodies or functions.

Although neither the ZZPri nor ZSDU specifically require employee representative bodies to be informed and/or to participate in an internal investigation, an agreement between the employer and the works council may stipulate such obligations.

b) The main regulation regarding the processing of personal data is the EU General Data Protection Regulation ("**GDPR**"). However, EU Member States can regulate certain substantive and procedural issues separately. These areas are regulated in the Republic of Slovenia by the Personal Data Protection Act ("**ZVOP-2**"), which regulates the exercise of human rights to protect personal data, obligations, principles, entitlements, procedures, etc., all to exercise the GDPR. According to the GDPR, one of the Data Protection Officer's ("**DPO**") duties would be to consult the employees regarding their data privacy rights. Subject to the company's internal regulations, the DPO generally has to be informed about all data privacy-related procedures and processes of an internal investigation. The DPO must be given the independence to carry out all the necessary activities to ensure that the business complies with the GDPR. The DPO works as a contact person for the Information Commissioner (the national DPO).

c) There is neither a need to inform authorities about the investigation nor do they have to be invited to participate. However, informing authorities may be advantageous.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

No, the ZZPri does not impose an obligation on employees to actively participate in the handling of internal investigation.

The reporting person (who also can be an employee) is also not obliged to cooperate in interview by employer, as their identity (if they does not want it) cannot be disclosed.

However, employees have a general obligation under ZDR-1 according to Article 34, to follow the employer's instructions in relation to the execution of its their contractual and employment's relationship obligations. Therefore, they generally have to participate in an internal investigation.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Investigative actions cannot trigger termination deadlines.

The facilitator must complete the processing of the report of infringements within three months of its receipt.

ZDR-1 sets objective deadlines for ordinary termination due to misconduct or extraordinary termination no later than six months after the occurrence of the violation.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

In accordance with the ZZPri, no one may disclose the identity of a whistleblower to anyone other than the trustee and the external application authority without the whistleblower's express consent or disclose any other information from which the identity of the whistleblower may be inferred directly or indirectly. In addition, provisions of the ZVOP-2 must also be complied with. Additional specificities will be defined below.

a) conducting interviews?

According to Article 48 ZDR-1, personal data may only be collected, processed, used, or transferred to third parties if required by statutory law or in case collecting, processing, using, and transferring of data is necessary for the execution of rights or obligations arising from the employment relationship.

b) reviewing emails?

Privacy of communication is normatively protected by international legal documents binding the Republic of Slovenia, such as the European Convention on Human Rights ("**ECHR**") and the International Covenant on Civil and Political Rights ("**ICCPR**"), and by domestic legal documents, such as the Article 37 of the Constitutions of the Republic of Slovenia, ZVOP-2 and Electronic Communications Act ("**ZEKom-2**").
In all digital communication, the content of the communication is protected, as are traffic and location data, the facts of unsuccessful attempts to establish connections, etc. Thus, we can conclude that this is a so-called hybrid electronic communication. The hybrid nature of electronic communication is reflected in the fact that it takes place in real time, while at the same time, data is also stored. This applies to a live, active email inbox or data in a mobile phone. It is precisely in these two communication environments that communication privacy is also the most vulnerable. Firstly, the individual can be the victim of real time surveillance and interception of communications, as well as the victim of the seizure of the content of communications already stored. In a live, active electronic mailbox, two-way communication occurs in real time, with incoming communications not always under the holder's control.

At the same time, the communication is stored, forming a communication database that is stored at his employer. It contains mail with all kinds of correspondence, even the most intimate. It follows that, in the case of communication by email and applications installed on mobile phones, even if the employer owns these two means of communication, it is not only individual electronic messages that are subject to protection. In particular, where a live, active electronic mailbox is involved, it is, therefore, for the reasons set out above, subject to protection under the ECHR and the constitutional provisions in itself as a whole. Differently, but reasonably similar, in the case of an extinguished, inactive electronic mailbox used by an employee, now just a mailbox, the situations of live communication and storage are separated. What is left is a controlled database of past communications, which is subject to the same restrictions.

A specific chapter of communications privacy law relates to communications privacy in the workplace. It is defined explicitly by two characteristics. The first is the clash between the employer's legitimate interests (control of its own resources, concern for the security and legality of electronic communications, etc.) and the employee's right to a certain degree of privacy, autonomy, and confidentiality. The second characteristic is the tame nature of life in the modern digital society, where most communication is electronic and takes place in the digital environment and where work can also be carried out remotely from home. The spheres of work and private are, therefore, inextricably intertwined. Both characteristics are also reflected in the company's email inbox (both for emails and mobile applications). By its very nature, the company's email inbox is protected as an independent entity under the right to privacy of communications. No matter how strict the internal rules are, firstly, the employee cannot control what emails will be sent to their email inbox. Secondly, the individual's private life at work cannot be reduced to zero (Bărbulescu v. Romania (61496/08) from 5 September 2017, paragraph 80.). Since this is the case, it follows that the work email inbox (or other comparable means of communication) is also constitutionally protected under communications privacy. This is also the practice developed by the European Court of Human Rights ("**ECtHR**") through its leading cases, such as Halford v. the United Kingdom, Copland v. UK and Bărbulescu v. Romania (ECtHR has provided a structured six criteria for balancing such situations).

We thus conclude that, if not all of the criteria set out in Bărbulescu v. Romania are met, the employer's supervision of emails and mobile phone communications, without the consent of each individual employee or former employee, would be in breach of Article 8 of the ECHR and the Article 37 of the Constitutions of the Republic of Slovenia and employees would, therefore, be afforded criminal law protection as well as civil law protection.

c) collecting (electronic) documents and/or other information?

The police may request employers to provide documents and/or other information based on the basis of the Slovenian Police Tasks and Powers Act ("**ZNPPol**"). In case of a doubtful legal basis, we suggest waiting until an authority makes a formal written request with the announcement for enforcement.

d) analysing accounting and/or other business databases?

There is no specific legal basis applicable for analysing accounting and/or mere business databases during an internal investigation. In the broadest sense, there are two (general) legal bases:

– Pursuant to Article 53 of the Slovenian Accounting Act ("**ZR**"), companies are obliged to regulate the controlling of data and internal auditing in accordance with applicable law and companies' internal acts. Further, Article 281a (5) of the Slovenian Companies Act ("**ZGD-1**") (applicable for joint-stock companies and private limited companies) stipulates that the supervisory board has to give its consent to the company's internal policies stipulating the purpose, meaning, and assignments of internal audit.

– According to Article 19 of the Slovenian Inspection Act ("**ZIN**") – regulating inspection procedures conducted by authorities – the inspector has a right to inspect business documentation and all other documents needed for the inspection. This documentation may also be retained under conditions specified in the ZIN.

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

The Slovenian law does not contain any statutory obligation to instruct an employee about the legal circumstances and their rights regarding internal investigation procedures.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

In contrast to an individual's right to remain silent in case of self-accusation during interrogations of criminal authorities, there is no corresponding right with regard to employee interviews as part of internal investigations.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

Giving an Upjohn warning is an accepted best practice in Slovenia. However, there is no explicit legal obligation to do so under Slovenian law.

d) be informed of their right to have their own lawyer attend the interview?

There is no such legal obligation. However, companies are obliged to allow such attendance of the employee's lawyer during termination procedure interviews.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

There is generally no such explicit legal obligation in internal investigations.

If the internal investigation is part of disciplinary or termination procedures, the employee representative body has the right to attend if the employee under investigation requests so.

f) be informed that data may be transferred to another country (in particular to the United States)?

When transferring personal data cross-border to third countries (also to United States), the employer is obliged to inform the employee.

g) sign a data privacy waiver?

This is not necessary if no other personal data shall be gathered than the data already gathered by the employer according to the applicable legislation, such as employee name, address, ID number, or tax number.

h) be informed that the information gathered might be passed on to authorities?

There is no such legal obligation with regard to internal investigations.

i) be informed that written notes will be taken?

There is no legal obligation to do so. However, it is a common practice in companies to inform the interviewee that written notes shall be taken.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Document hold notices and retention policies are allowed and are a common practice in the Republic of Slovenia. Article 37 of the ZDR-1 contains a general provision which can be applied *mutatis mutandis* when answering this question. The article stipulates that that workers are obliged to refrain from all actions which, given the nature of the work they perform for the employer, may cause material or moral damage or might harm the business interests of the employer. However, there is no specific law regulating expressly the document hold notices or document retention notices.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

The Slovenian Constitution protects the confidential relationship between a defence counsel and a defendant. This relationship is protected irrespective of whether the documents or information are intended for defence in criminal proceedings. This is because, for example, in the case of a search of a law firm, there is the danger that the police will obtain documents and objects that are not related to the criminal offence, which is the subject of the investigation. The investigating authorities have to adhere to the rights referred to in the Slovenian Constitution. Thus, they may not seize such documents when in the custody of the defence counsel. The legal protection of this confidential relationship encourages the client to communicate with an attorney or defence counsel without restrictions, i.e. without the fear that any subsequent disclosure of confidential information would jeopardise their legal position. Documents in the custody of the client may, however, be seized and used in proceedings against the client.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

No. The confidential relationship is binding only for attorneys who must keep secret everything that the client has entrusted to them (Article 6 of the Slovenian Attorneys Act). This obligation also applies to other persons working in a law firm, but it does not apply to in-house lawyers.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

If any kind of circumstance arises which could trigger a claim against insurance companies, the latter should be informed. A general duty to notify the insurance company is stipulated in Article 941 of the Slovenian Obligations Code ("**OZ**"). According to this law, the policyholder must inform the agency regarding any insurance case within three days after gaining knowledge about it.

b) Business partners (e.g. banks and creditors)?

Whether there is a duty to notify business partners should be evaluated in each individual case. Even if a business contract does not contain specific notification duties of the contracting parties, such duties may be construed on the basis of general principles of the Slovenian obligations law. This applies in particular if the information concerning the start of the investigation constitutes information important for the other party and is relevant with respect to the purpose of the agreement.

c) Shareholders?

Slovenian Law does not provide any specific duty to inform shareholders about starting an investigation. However, according to Article 305(1) ZGD-1, shareholders have a right to be informed about "*reliable information on the company's affairs if this information is important for the assessment of the agenda [for the general meeting*]". According to Article 305(2) ZGD-1 the management is not required to provide information in the following cases:

- If the provision of information could, by reasonable economic judgement, cause damage to the company or its affiliate;
- If the information refers to the methods of accounting and assessment, provided that the statement of methods of this kind in the annex is sufficient for an assessment of the actual situation of the company in terms of property, financial standing; and profitability;
- If the provision of information would constitute a criminal act, a minor offence, or a breach of good business practice; or
- If the information is published on the company's website in the form of questions and answers at least seven days before the general meeting.

Please be advised that information regarding internal investigations may have a significant effect on stock/shareholding price and may be considered insider information, which may be subject to abuse.

d) Authorities?

There is no general duty to inform authorities about internal investigations. However, in certain cases, failure to report that particular severe crimes may have been committed could be criminally prosecuted.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Companies under investigation are generally not obliged to cooperate in the investigation or in investigative actions. The public prosecutor is the institution in charge that investigates and collects evidence in order to confirm the suspicion of a criminal offence.

However, there may be a duty to reveal evidence. The Criminal Procedure Act ("**ZKP**") stipulates that anyone possessing objects which must be seized under the KZ-1 or which may be evidence in criminal proceedings is obliged to hand them over to the court upon request. A custodian who declines to deliver the requested objects may be fined. If they are fined and still refuse to surrender those objects, they may be arrested. The detention lasts until the objects have been delivered or until the end of the criminal proceedings, but no longer than one month.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Authorities may regard actions conducted by companies' management or supervisory bodies as positive counteractions aimed at remedying the consequences of criminal acts or misdemeanours committed by the company's employees and/or responsible persons. Article 11(1) Liability of Legal Persons for Criminal Offences Act ("**ZOPOKD**") stipulates that a company's criminal sanction, which derives from management or supervisory bodies' lack of control over employees, is to be mitigated in cases where companies' management or supervisory bodies voluntarily indicated to authorities the person who committed the criminal act (on behalf of the company) before authorities gain knowledge about that person.

Pursuant to Article 11(2) of ZOPOKD, a company's criminal sanction, which derives from management or supervisory bodies' lack of control over employees, is to be remitted if the perpetrator is indicated to authorities before they gain knowledge about them and

- an order for the immediate return of unlawful gains is given; or
- the damage is otherwise remedied; or
- the merits of other criminal liability of the company are indicated to authorities.

Similarly, pursuant to Article 21 of the Minor Offences Act a reprimand instead of an administrative fine may be issued to the company in an administrative procedure if the misdemeanour was committed in circumstances that make the misdemeanour evidently insignificant (paragraph 1) or if the damage consequential to the misdemeanour was remedied prior administrative body fined the perpetrator (paragraph 2).

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Slovenian searches conducted by authorities are led by an investigative judge. Authorities' searches cannot be initiated without the prosecutor's motion. The latter has to be made by a competent prosecutor and contain the following information:

- The subject of investigation;
- The description of facts pertaining to alleged criminal offence;
- Reasonable doubts; and
- A list of already gained evidence.

There is no general bright line rule regarding the admissibility of evidence in Slovenia.

Article 18 ZKP stipulates that only evidence permissible by law may be part of the procedure. Inadmissible means of evidence on this occasion is evidence obtained in violation of the Slovenian Constitution, the ZKP, if expressly stipulated, poisonous tree evidence or fishing expedition evidence.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

The prosecution is bound by law to prosecute all alleged criminal offences *ex officio* regardless of the will of other subjects (e.g. injured compromised party). Therefore, non-prosecution agreements are not possible. However, prosecution could be put on hold in the course of alternative extra-judicial resolving of criminal matters. The latter can be done with the compromised party's consent in case of criminal offences punishable with fines or imprisonment of up to three years.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

In Slovenia, legal entities can generally not be held criminally liable. However, in specific cases, legal entities could be subject to criminal liability to the extent that the conditions specified in the ZOPOKD are met. The following punishments may be imposed upon legal entities:

- Financial punishment, such as fines;
- Assets forfeiture;
- Termination of legal entity; and/or
- Prohibition of disposing securities held by the legal entity.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Under Slovenian law, the implementation of an efficient compliance system is not regulated as a specific and explicit reason for the suspension or reduction of penalties. It can be, however, evoked in substance when (generally) claiming mitigating circumstances in relation to the setting of the penalties.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

For companies (for which the management report is an integral part of the annual report), ZGD-1 already provides a loose legal basis for reporting and information on environmental impact or environmental matters.

In accordance with Article 54 of the ZGD-1, companies and entrepreneurs are required to keep books of accounts and to close them annually in accordance with accounting standards. On the basis of the closed accounts, an annual report must be drawn up for each financial year. The reporting in the annual report shall be based on a balanced and comprehensive analysis of the development and results of the Company's operations and of its financial position. It shall include key accounting, financial and other indicators, ratios and other performance measures, including information relating to environmental and labour protection, the company's expected development, financial risk management objectives and measures, and the exposure to price, credit, liquidity and cash flow risks.

Companies subject to audits are also required to include a corporate governance statement in their management report.

Additional annual report requirements apply to public interest entities where the average number of employees in the financial year as at the balance sheet cut-off date is greater than 500 - these are required to comply with Article 70c of the ZGD-1 (which is consistent with Directive 2014/95/EU of 22 December 2014). They must also include in their management report a statement of non-financial performance. This contains at least information on environmental, social and human resources matters, respect for human rights, and anti-corruption and anti-bribery matters. These are principal risks that are associated with the company's activities, including its business relationships, products or services, where relevant and proportionate, that could have a material adverse effect in those areas, and the ways in which the Company manages those risks, and the key non-financial performance indicators relevant to each activity.

Further, in the Republic of Slovenia, a Regulation on implementing Regulation (EU) 2019/2088 of 27 November 2019 on sustainability-related disclosures in the financial services sector, is in force since 25 February 2023.

Lastly, the Slovenian Enterprise Fund has developed an advanced online tool for self-assessment of sustainability performance, for start-ups, fast-growing companies and other innovative micro, small and medium-sized enterprises (SMEs), called the "ESG Tool".

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The topic of business compliance is gaining more and more attention every day in Slovenia. Slovenian corporations are establishing their own compliance departments (e.g. banks, insurance companies or pharmaceutical companies) and are implementing their own internal compliance policies.

Moreover, certain non-governmental organisations and business associations are addressing this topic daily and intensively.

Further legislative changes implementing Directive (EU) 2019/1937 are envisaged. The national act that would implement the Directive is currently in interdepartmental coordination and in the service of the government for legislation.

CONTACTS

SENICA

A member firm of ANDERSENGLOBAL

Law Firm Senica & Partners, Ltd.
Barjanska cesta 3
1000 Ljubljana
Slovenia

Tel.: +386 1 252 8000
Fax: +386 1 252 8080
www.senica.si/en

After more than 37 years of its existence, SENICA is a brand that needs no introduction. It guarantees excellence, quality, and individual treatment and is recognised in Slovenia and worldwide.

SENICA has 12 partners and more than 40 experts specialising in various legal and tax fields. It regularly works together with a range of well-known and reputed experts, professors of the faculties of Law and Economics in Ljubljana and Maribor, as well as scientific institutions and faculties such as the Economic Institute at the Faculty of Law in Ljubljana and the Commercial Law Institute at the Faculty of Law in Maribor.

SENICA is a member firm of Andersen Global, an international association of legally separate, independent firms, involving only carefully selected first-class tax and legal experts worldwide. SENICA is Andersen Global's, regional coordinator for the entire region of the Western Balkans region, and SENICA's Managing Partner, Katarina Kresal, is Co-chair for Andersen Global CEE Region and a member of the Andersen Global Management Committee. Additionally, with its subsidiaries, Andersen in Slovenia and Andersen in Serbia, SENICA provides clients with a comprehensive full range of tax, accounting, valuation, and other business advisory services in Slovenia and Serbia.

Uroš Čop
Managing Partner
Law Firm Senica & Partners, Ltd.
T +386 1 252 8000
E uros.cop@senica.si

Uroš is an expert in Constitutional Law and Public & Regulatory Law.

He focuses mainly on Public and Regulatory Law, Public and Regulatory Law Dispute Resolution, Constitutional Law, White Collar Crime, Data Protection and Cybersecurity Law, Fintech and IT, Intellectual and Industrial Property Law. During his career he advised and represented clients in many of the most complex Public and Regulatory disputes, defended clients in prominent White Collar criminal procedures and participated in all major M&A's concerning the Intellectual and Industrial Property. He is a co-author of Extensive scientific commentary of Criminal code of the Republic of Slovenia, which was recognised as an excellent achievement in science in 2019 by the Slovenian Research Agency.

Uroš is the Manager of the Adriatic Legal Network which was co-founded by the Law Firm Senica & Partners, Ltd.

Katarina Mervič
Partner
Law Firm Senica & Partners, Ltd.
T +386 1 252 8000
E katarina.mervic@senica.si

Katarina is an expert in Criminal Law.

She focuses mainly on representing clients in criminal proceedings. Over the years she led the defence of several high-profile cases on white collar crime. Her field of expertise is also minor offence law. She is a co-author of Extensive scientific commentary of Criminal code of the Republic of Slovenia which was recognised as an excellent achievement in science in 2019 by the Slovenian Research Agency.

Katarina is Secretary General of the Parus Foundation which was established by Miro Senica in 2006 and grants scholarship to most talented graduates at the Faculty of Law, University of Ljubljana.

Žiga Sternad
Senior Associate
Law Firm Senica & Partners, Ltd.
T +386 1 252 8000
E ziga.sternad@senica.si

Žiga is an expert in Labour and Employment Law with more than 18 years of experience.

He focuses mainly on employment relationships, employment law compliance, workforce restructuring, employment dispute resolutions, immigration and has participated in all major Labour Law litigations led by Law Firm Senica & Partners, Ltd.

Žiga is known as an expert in the operational resolution of complex labour and other disputes, including environmental disputes which require a wide range of knowledge from other disciplines, such as medicine, chemistry and environmental issues.

Spain

Hogan Lovells International LLP

Ignacio Sánchez

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

In Spain there is no comprehensive regulation on internal investigations, neither a detailed caselaw on the subject. The more advanced field is that related to the protection of whistleblowers, as Spain has implemented Directive (EU) 2019/1937 (the "**Whistleblowing Directive**") by means of the Spanish Act on the Protection of Whistleblowers ("**SAPW**").

The SAPW does not regulate investigations in detail but does include some provisions which will have to be taken into consideration by the following companies:

- Entities established in Spain and employing more than 50 individuals;
- Entities carrying out activities referred to in Sections I.B and II of the Whistleblowing Directive, regardless of their number of employees. For instance, this includes entities obliged to implement internal reporting channels by the Spanish Act on the Prevention of Money Laundering and the Financing of Terrorism;
- Any entity that voluntarily implements a whistleblowing channel.

These entities must have mechanisms in place to properly receive and investigate complaints through an internal whistleblowing channel, meeting the following characteristics:

- Acknowledgment of receipt to the whistleblower within seven calendar days from its receipt, unless this could jeopardise the confidentiality of the communication;
- Response to the whistleblower in the shortest possible time and within a maximum of three months. This period may be extended to three additional months in cases of special complexity;
- The investigated parties must be recognised with a set of rights that include, among others, being informed of the actions or omissions attributed to them; being heard (the time and manner could vary to ensure the proper conduct of the investigation), as well as the right to presumption of innocence, right to honor and right to confidentiality;

– Protection of personal data involved in the investigation in light of the European and national legislation in force; and

– Providing the Public Prosecution Office with the relevant information when the investigated facts could trigger criminal liability. Scholars have opposed this obligation in the case of private entities given that it may curtail the right against self-incrimination that legal entities are entitled to.

The SAPW also provides for obligations that must govern investigations triggered as a result of communications reported through external channels (those set up by the competent authorities). While not compulsory obligations for private companies, these may serve as best-standards for their own internal mechanisms.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

In Spain, there has been no intense debate on this issue, nor have many interpretative problems arisen following the publication of the Law. This is because SAPW is clear insofar as it dedicates Article 11 specifically to groups of companies, stating literally: "The person in charge of the System may be one for the entire group, or one for each company within the group, subgroup, or group of companies, on the terms established by such policy. The Internal Information System may be one for the whole group in Spain".

The authorities will probably set criteria at a later stage, but if the system can be the same for the whole group and only designate a single person responsible for it, it seems that the only possible interpretation is that there is a special regime for groups of companies which does not lay down additional conditions. In cases where such a possibility (one system for the group and one responsible) has been realised, the main concern will be to ensure that the system is also accessible at a local level and adapted to the requirements of Spanish law.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Unless otherwise stated in collective bargaining agreements, employees' legal representatives are only required to be informed of and allowed to be present in investigative actions involving the search of personal belongings and lockers of the employees.

b) Neither data privacy authorities nor the DPO have to be informed of the performance of an investigation.

c) It is not compulsory to inform any other local authorities before starting an internal investigation.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees' refusal to support or participate in internal investigations could entail a loss of trust and eventually be deemed a violation of the contractual good faith. This could result in sanctions or even dismissal pursuant to the Spanish Workers' Statute ("**WS**").

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

As a general rule, different deadlines apply depending on the severity of the misconduct. The deadlines may vary between 10 to 60 days since the company became aware of the infringement or, in any case, six months since the infringement was committed. The company may attempt to prove that it did not become aware of the infringements until the internal investigation was completed, hence postponing the triggering date of these deadlines.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The interviewee shall be informed about the processing of their personal data before the interview.

Further, access to the information processed as part of the investigation must be granted strictly on a need-to-know basis to those roles/teams assigned to perform internal control and compliance functions. Moreover, only personal data that is relevant for the purposes of the investigation should be processed in compliance with the data minimisation principle.

b) reviewing emails?

Generally, private communications are highly protected under Spanish law. Hence, emails sent from/to employees' corporate email accounts might be considered as "private" communications.

Labour and data protection caselaw require the company to adopt the following steps prior to monitoring corporate communications, which are aligned with the Barbulescu criteria:

– Adoption of a policy regulating this monitoring: (i) this policy shall include written criteria/rules for the use of digital devices respecting minimum standards of the employee's privacy protection; (ii) in the event that the employer allows the use of digital devices for private purposes, the authorised uses must be precisely specified in advance and adequate safeguards must be put in place to preserve employees' privacy; (iii) employees' representatives need to be involved in the development of these criteria/rules; and (iv) having proof of the employees being informed of this policy.

– Conducting of the e-review respectfully with the proportionality test (e.g. use of keywords, limiting the search in time and concerns employees).

Non-compliance with the above criteria may lead to the respective evidence being declared null and void, or even result in criminal liability for discovering and disclosing of secrets.

c) collecting (electronic) documents and/or other information?

Please see the answer to 5b above. Furthermore, please note that in the event that personal data is collected from sources other than the data subject, the information requirements set forth in Article 14 General Data Protection Regulation ("**GDPR**") must be fulfilled.

d) analysing accounting and/or other business databases?

Please see the answer to 5b above. Furthermore, please note that in the event that personal data is collected from sources other than the data subject, the information requirements set forth in Article 14 GDPR must be fulfilled.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There are no specific regulations on how to conduct employee interviews. However, as a matter of best practices, interviewees are normally provided with written instructions, including a brief description of the background of the investigation, a confidentiality clause and the purposes behind the interview.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

Right against self-incrimination should be guaranteed when conducting an internal investigation. It is advisable to inform interviewees who are subject to investigation of this right and that their collaboration is voluntary (and that no disciplinary actions would apply for their refusal to collaborate in their case).

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no legal obligation to do so, though it is advisable and customary to make this clarification.

d) be informed of their right to have their own lawyer attend the interview?

There is no specific provision under Spanish law, although this may be provided for in collective bargaining agreements. It is advisable and customary to make this offer to investigated employees.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

There is no specific provision under Spanish law, although this may be provided for in collective bargaining agreements. In case the employee requests such attendance, the person conducting the interview should not refuse it. Only in exceptional cases, the interviewer could refuse the attendance of an employee representative (e.g. when the works council is also subject to the investigation).

f) be informed that data may be transferred to another country (in particular to the United States)?

Yes. Under the GDPR, the data controller must inform the data subject about certain mandatory aspects of the processing of their personal data (e.g. the data transfers outside the European Union, the identity of the data controller, the purposes of the processing and the legal basis).

g) sign a data privacy waiver?

Entering into a data privacy waiver would not be required. However, the data subject must receive prior information about the processing of their data.

h) be informed that the information gathered might be passed on to authorities?

Yes. In compliance with the information obligation referred to above, the data controller must inform data subjects about the recipients of the personal data, if any. In the context of whistleblowing systems, the Spanish Data Protection Act ("**SDPA**") expressly refers to the transfer of data to the competent authority when necessary for the adoption of disciplinary actions or the handling of legal proceedings.

i) be informed that written notes will be taken?

There is no legal obligation to do so, though it is advisable and customary to make this clarification.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific legal provision in this regard. However, document-retention notices are generally admitted and used to preserve the aim of internal investigations and for the company to prove that this notice was served and received by the individuals involved.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege is not expressly provided for in Spanish law. A similar institution would be the professional secrecy. This is a wider concept and is based on the duty of confidentiality that lawyers owe in respect of any information received from their clients while acting on their behalf. Therefore, as both concepts entail similar consequences, attorney-client privilege or professional secrecy rights may be claimed over the findings of an internal investigation.

Recommended steps to ensure this protection would be as follows:

- Labelling privileged documents accordingly;
- Appointing one or few individuals as the contact persons with the attorney to be considered as the "client";
- Limiting access of other individuals in the company to privileged communications or documents and, of course, avoid disclosure to anyone outside the company;
- Limiting the amount of work products where findings and conclusions over the investigations are described; and
- Avoiding keeping work product at the company's premises, but at the outside counsel's instead.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

In Spain, it has traditionally been under discussion whether attorney-client privilege also applies to in-house counsel. While the European Court of Justice ruling on Akzo Nobel Chemicals Ltd. v. European Commission excluded in-house lawyers from this right, the Spanish regulations did not foresee an equal exclusion (nor did they expressly include them).

In March 2021, a new General Statute of the Spanish Legal Profession was adopted, expressly extending the applicability of legal privilege to in-house lawyers (Article 39). It is yet soon to anticipate how the courts will uniformly apply this new regulation, which could be interpreted as contradictory to the European criteria. However, the new regime has already been successfully invoked in criminal proceedings before the National Court by in-house counsel (*Diligencias Previas 96/2017* before the Central Investigating Court No. 6).

The new regulation extends legal privilege to any facts, communications, data, information, documents and proposals that, as professional Legal Counsel, the lawyer may have been aware of, issued or received while exercising its professional activity.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

This communications is advisable whenever the facts may give rise to a claim against the insurance company.

b) Business partners (e.g. banks and creditors)?

This has to be decided on a case-by-case basis. The following aspects should be taken into account:

- Contractual obligations to provide such information; and
- Assessing if the notice be deemed utterly important for the counterparty with regard to the purpose of the agreement, according to contractual good faith and taking into account the legitimate interests of the company.

c) Shareholders?

The Securities Market Act imposes the obligation to communicate relevant information to investors of listed companies. "Relevant information" refers to information that could influence investors in their decision to trade securities or affect the securities' price.

d) Authorities?

Listed companies also have to notify the Securities Market National Commission of any relevant information as described under 10c above.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Companies would be expected to make sure that any ongoing breach of law is immediately stopped, review their control mechanisms and adjust their compliance programme and structure to avoid future misconduct, and adopt other mitigation action (when applicable). Also, it is crucial to ensure the preservation of all relevant material which could serve as evidence in a judicial case to prove the company's due diligence when reacting to the alleged misconduct.

Depending on the results of the investigation, the company shall decide on its approach towards the authorities and the potential parallel or future government proceedings (e.g. self-reporting, collaborative approach or defence approach based on for instance denying any wrongdoing if the outcome of the investigation supports it).

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

In Spain, internal investigations are not broadly developed. However, the General Public Prosecutor's Office recently stated that providing the prosecution with the results of an internal investigation is an indication of ethical commitment and could entail exoneration from corporate criminal liability. In addition, the Spanish High Court included the development of an internal investigation upon the acknowledgment of wrongdoings as one further element that shows an effective compliance culture within a company.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Search warrants and dawn raids are foreseen in the competition, tax and criminal local regulations:

- The Spanish Competition Authority has the right to access business and domestic premises if there are indications of anticompetitive behaviour if approved by the Director of Investigation or a judge;
- Tax inspectors can only perform a dawn raid upon a judicial warrant or when the owner or entitled individual of the company expressly authorises them to access the premises;
- In the context of criminal proceedings, search warrants and dawn raids have to be ordered by an examining magistrate, *ex officio*, or at the police's request (only in the exceptional event of flagrante delicto could this judicial order be excused). These measures have to be strongly justified, specifying reasons with solid indications of a criminal offence, the dawn raid's goal, the objects to be searched, how and when the search should be performed, who must be present, etc. Account books and documents may not be seized by the police unless the order mentions them specifically.

For the event that legal requirements are not fulfilled, it will generally lead to a declaration of the seized pieces of evidence (and related pieces of evidence) as null and void.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Spanish law does not provide for NPAs/DPAs. It is not possible pursuant to Spanish law to reach an agreement with the Public Prosecutor Office without admitting to the criminal offence and accepting a penalty.

In the case of companies, the Spanish Public Prosecutor Office has instructed not to press charges against a company self-reporting an offence, although this is not provided for in the Criminal Code and creates a contradiction with the regime applicable to individuals.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Under Spanish law there is no automatic transfer of liability to individuals or companies resulting from misconduct by a third party. In both cases, it is necessary to prove their own contribution to the criminal offence. In the case of corporate criminal liability, this contribution relies on the lack of controls to prevent the commission of the offence within the company.

Penalties for individuals can include fines, imprisonment, or even special barring from public employment and office, profession, trade, industry, commerce, etc.

Companies usually face a fine. Other penalties may be imposed additionally, such as suspension of activities, closure of premises, prohibition to develop the activities through which the offence was committed or concealed, prohibition from receiving public subsidies and public procurement debarment.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

According to Section 31 B of the Spanish Criminal Code, the company shall be exempt from liability if the following conditions are met:

- The management body adopted and effectively implemented, prior to the commission of the offence, a compliance programme to prevent the commission of similar offences, or significantly reduce the risk of the commission thereof;
- Supervision of the compliance management system was entrusted to a person or a body of the legal entity which has independent powers of initiative and control;
- The perpetrators committed the offence by fraudulently evading the compliance programme; and
- There was no negligent lack of supervision or control by the person or body in charge of the compliance programme.

If only partially fulfilled, these circumstances shall mitigate the penalty.

There is no specific legal provision in Spanish law with respect to directors, officers, and employees. However, the existence of compliance measures and compliance may help their defence by showing that they did act with due diligence towards their dependants.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

On 3 May 2022, the Government of Spain submitted for public consultation a draft law on the Protection of Human Rights, Sustainability and Due Diligence in Business Activities. The consultation concluded with more than 80 proposals from individuals and legal entities. Nevertheless, to date, no further legislative steps has been followed to complete the drafting of this law.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

There were various developments in Spain, including the following:

- Further case law has been issued dismissing criminal judicial proceedings against companies that have proven the effective implementation of a criminal compliance programme (see section 16);

- A milestone case law has established that a criminal compliance programme as well as the reports filed within its reporting structure cannot be subject to a judicial compulsory request; these materials may be produced by the company on a voluntary basis (or obtained through a dawn raid);
- The appointment of the Spanish Independent Authority (*Autoridad Independiente de Protección del Informante* or A.A.I.) has not yet been established, although some regions have designated their own independent authorities (e.g. Cataluña);
- The SAPW foresees leniency programmes, although it seems to leave it to the authorities' discretion to apply this exemption or not, and this section only refers to administrative infringements.

CONTACT

Hogan Lovells

Paseo de la Castellana, 36-38
Planta 9
28046 Madrid
Spain

Tel.: +34 91 349 82 00
Fax: +34 91 349 82 01
www.hoganlovells.com

Ignacio Sánchez
Partner
Hogan Lovells Madrid
T +34 91 349 82 93
E ignacio.sanchez@hoganlovells.com

Ignacio Sánchez is a vocational criminal lawyer who will go the extra mile by using creative alternatives, meticulous preparation and attention to detail. He advises on the full life- cycle of serious misconduct in companies, both from the preventive and from the reactive side. As regards the latter, he represents high profile clients -companies and individuals- in complex and sensitive criminal proceedings acting either as a prosecuting party or defence. According to his clients, he "knows how to handle the situation, and when things get complicated, I like having a lawyer like him".

His experience in the different criminal proceedings allows him to identify the key aspects to which the authorities will pay most attention in the field of compliance. He is therefore in the best position to advise companies on the compliance risks arising from the activity and on the adequacy and effectiveness of the measures in place. In addition, he conducts independent investigations on behalf of corporate boards and supervisory authorities to assess liability, determine implications and deal with authorities and agencies.

Sweden

Nordia Law


Hans Strandberg


Olle Kullinger


Carl-Johan Allansson

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes		X	X	X**	X***
No	X*				

* No criminal liability for companies, but companies can, under certain circumstances, be imposed a corporate fine for crimes committed by employees or executives acting within the scope of their duties.

** Only for certain crimes, but wide interpretation of when a crime has been committed in Sweden.

*** Only in some cases, and not if a crime has been committed by a leading individual of a company.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

When a whistleblower report sets off an internal investigation the Protection of Persons Reporting Irregularities Act (2021:890) ("**Whistleblower Act**"), implementing the EU Whistleblower Directive (EU) 2019/1937, applies and specific procedures need to be considered. Such considerations concern e.g. the implementation of a competent body for conducting the investigation, rights and protections of the whistleblower, and personal data and confidentiality. Special procedures also apply to documentation, preservation, and deletion of reports.

The whistleblower is, in general, protected in the form of exemption from liability for breach of duty of confidentiality/provision concerning gathering of information, and against obstructive measures and retaliation. The whistleblower shall, as a main rule, receive some follow up to the report within certain timeframes and shall also be informed if information that might identify the whistleblower is to be disclosed.

In addition to data privacy laws, the Whistleblower Act regulates that processing of personal data in follow up cases is, as a main rule, only valid if the processing is necessary for the follow up. However, several exemptions apply. Further, access to personal data is restricted to the competent body. Confidentiality applies, in general, to information that could reveal the identity of the whistleblower but can also apply to the investigation itself and for other individuals. The scope of the confidentiality depends on whether the operator is within the private or public sector.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The Whistleblower Act does not allow corporate groups with 50 employees or more to rely solely on centralised whistleblowing reporting channels at group level. Nevertheless, operators in the private sector with 50 to 249 employees may share internal reporting channel resources regarding the receipt of reports and any investigation conducted due to reported misconduct, which does not, however, include contact with the whistleblower. Nevertheless, the sharing of resources requires that the other operator is also a medium-sized operator allowed to share resources.

Municipalities may also share internal reporting channels and reporting and follow up procedures with other municipalities, and with municipal companies, foundations and organisations that are also subject to the obligation to have channels and procedures in place.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Unless disciplinary actions are initiated against an employee, there is no requirement to notify the works council of an internal investigation.

b) In accordance with the European General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the data protection officer ("**DPO**") must consult with employees regarding data privacy rights and must monitor data protection. A company, therefore, will need to inform the DPO about all data privacy related procedures and processes of an investigation.

c) Companies do not have a general duty under Swedish law to inform the prosecution authority of an internal investigation. However, special legislation exists that requires reporting to authorities, e.g. the Money Laundering and Terrorist Financing (Prevention) Act, the Public Employment Act, and the Companies Act (in regard to auditors of limited liability companies).

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Under Swedish labour law, employees have a duty of loyalty to their employer, which is extensive. In general, due to the duty of loyalty, employees are required to support an investigation and participate in interviews. The employer cannot force an employee to participate, but a refusal to participate may be regarded as misconduct and can lead to sanctions, such as dismissal.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Notice of termination/dismissal must be given by the employer within two months of knowing the reason for the termination/dismissal. If the company initiates an internal investigation, the two-month deadline would most likely begin if/when the employer has sufficient information concerning the conduct of the individual.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Data privacy laws, mainly the GDPR and the Swedish Supplementary Data Protection Act, which is a supplement to the GDPR, apply to the processing of data, including securing, collecting, and reviewing personal data. This includes the compiling of (electronic) documentation, which relates to the scope of an investigation (e.g. creation of a database). It is important to perform an early assessment of the applicable data privacy laws and to document the steps taken.

b) reviewing emails?

The employer needs to adhere to the GDPR and the Swedish Supplementary Data Protection Act, which means that the employer, in general, must inform the employees about the inspections that might be performed and the purpose for which their personal data will be processed. As a main rule, the employer has no right to read or otherwise take note of an employee's private emails or files. Exceptions exist where there is a serious suspicion of unfair or criminal conduct or where the employee is using IT equipment contrary to internal guidelines. It should be stressed that such personal data may only be processed if the employer has a legitimate interest in processing the data and that such an interest is not overruled by the rights or freedoms of the employee.

c) collecting (electronic) documents and/or other information?

Data privacy laws apply to the collection of personal data.

d) analysing accounting and/or other business databases?

An employer may analyse any documents that belong to the company. However, data privacy laws may be implicated if such databases include personal data.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There are no regulations in Sweden governing the conduct of internal interviews of employees by companies. Therefore, a company has no legal obligation to instruct employees about the legal circumstances and their rights. However, ethical considerations speak in favour of giving the employee a brief description of the background and subject matter of the investigation. There is no specific form prescribed for such a description.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

There is no legal obligation in Sweden to inform an interviewee in an internal investigation about self-incrimination.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no legal obligation in Sweden to give an interviewee an Upjohn warning, but it is required, according to the Code of Ethics for members of the Swedish Bar Association, to do so in certain situations. Members of the Swedish Bar Association are legally obliged to follow the Code of Ethics in their business. If a company's lawyer is attending the interview, the interviewee can be informed that they have the right to hire their own lawyer. There is, however, no duty to inform.

d) be informed of their right to have their own lawyer attend the interview?

There is neither a legal right in Sweden for the interviewee to have a lawyer attend nor a legal obligation for the company to inform the interviewee. However, the company should recommend that an interviewee suspected of criminal misconduct retain legal counsel. If the interviewee has already retained counsel, the interviewee should not be contacted directly by the company's lawyer without prior approval from the interviewee's lawyer.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Unless disciplinary actions are taken against the employee, there is neither a right for the employee to have a representative attend the interview nor a requirement for the company to inform the employee.

f) be informed that data may be transferred to another country (in particular to the United States)?

The relevant employees must be informed in the event their personal data will be transferred to a recipient in a country outside of the European Union/European Economic Area. Moreover, personal data may only be transferred outside of the European Union/European Economic Area if the conditions for such transfers, laid down in the GDPR, are complied with. For example, personal data may be transferred outside of the European Union/European Economic Area without prior consent of the person concerned if the data protection level in the foreign country is considered to be adequate pursuant to an adequacy decision adopted by the Commission. In accordance with the Commission's adequacy decision on EU-U.S. Data Privacy Framework on 10 July 2023, the United States are again approved as "adequate" if the data receiver is connected to the EU-U.S. Data Privacy Framework. Hence, the adequacy decision on the EU-U.S. Data Privacy Framework constitutes a valid basis for transfers of personal data to data receivers in the United States under the GDPR. However, if the data receiver is not connected to the EU-U.S. Data Privacy Framework transfers of personal data to the recipient in the United States must either be subject to appropriate safeguards (according to Article 46 of the GDPR) or fulfil at least one of the conditions for derogations specified in Article 49 of the GDPR (derogations for specific situations).

g) sign a data privacy waiver?

There is no requirement in the GDPR and/or the Swedish Supplementary Data Protection Act that a data privacy waiver shall be signed prior to an employee interview. The employee shall, however, receive information about the processing of their personal data at the time when the personal data is obtained, pursuant to the GDPR. Such information can be provided in writing or be supplied orally at the interview.

As already mentioned, personal data may be processed if the employer has a legitimate interest in processing the data, and such an interest is not overruled by the rights or freedoms of the employee. In the context of an investigation, an employer generally has a legitimate interest to process personal data. Thus, the employer must always balance their interest against the employee's rights and freedoms.

The GDPR sets out certain requirements that must be met for a consent to be valid. Among others, the consent must be freely given, i.e. consent is not valid if it was given under pressure from the employer. It is therefore questionable whether and/or to what extent the processing of personal data for the purpose of an internal investigation may be based on the employee's consent.

The GDPR does not contain any provision that governs how consent should be obtained. It is, nevertheless, good practice to sign a data privacy waiver when the employee's consent constitutes the applicable legal basis for the processing. This is, however, not a pre-requisite for an interview.

h) be informed that the information gathered might be passed on to authorities?

There is no legal obligation in Sweden to inform the interviewee that the information gathered might be passed on to authorities. It is, however, considered good practice.

i) be informed that written notes will be taken?

There is no legal obligation in Sweden to inform the interviewee that the interview will be documented. It is, however, considered good practice.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is neither a regulation applicable to document hold notices in Sweden nor an accepted practice in this regard.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Swedish regulations concerning attorney-client privilege are limited. Their applicability is highly dependent on where the documents are located and the type of information in the documents. Documents collected in the course of an internal investigation (e.g. emails) are not *per se* protected by privilege. However, analysis and conclusion drafted by an attorney, as well as correspondence relating to such analysis and conclusions, may be protected.

In order to ensure privilege, it is recommended to involve an attorney admitted to the Swedish Bar Association (*Swe. advokat*). In accordance with the Code of Ethics for members of the Swedish Bar Association, an advokat has a duty of confidentiality. Therefore, correspondence with an advokat is, in general, treated as confidential. Further, attorney-client privilege also applies to correspondence with attorneys admitted to the bar in the EU when they conduct business in Sweden. This provision is not applicable when a non-Swedish attorney provides services from their home country to a client in Sweden through a letter, phone, or telefax. Therefore, documents or correspondence from an attorney operating outside of Sweden are not covered by attorney-client privilege. Documents in the custody of external attorneys are also, in general, protected. Therefore, for sensitive matters, it is recommended that any documents generated in the course of the investigation to be stored only on external attorney's servers instead of on the company's premises.

It is recommended to label documents as privileged and confidential, even though labelling is neither required for privilege protection nor ensures privilege.

Privilege protection will more likely be granted if the advice is provided in relation to a (potential) investigation by authorities. This can be shown by setting up a separate engagement letter for the internal investigation.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Under Swedish law, communication with in-house counsel is not protected from disclosure by attorney client-privilege, as an in-house counsel may not be a member of the Swedish Bar Association.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

It is always advisable to notify the insurance company as soon as possible, as the insurance agreement can impose different notification requirements. Further, the Swedish Insurance Agreements Act Chapter 7 Section 4 contains provisions on the statute of limitations.

b) Business partners (e.g. banks and creditors)?

There is no general requirement to notify business partners of an internal investigation, except for business partners that may have a claim for damages due to the underlying conduct.

c) Shareholders?

A listed company is obliged to disclose price-sensitive information to the market. Knowledge of an internal investigation constitutes price-sensitive information when a director is served a notice of suspicion by authorities, but it may also be price-sensitive well before that occurs.

d) Authorities?

There is no requirement to notify the prosecution authority of an internal investigation. It is advisable to be cooperative with the prosecutor as this may prevent unexpected measures by the authorities, such as dawn raids. However, there is no legal ground for relief from penalties (e.g. corporate fines) for cooperating with authorities.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

As mentioned under 10c above, a listed company is obliged to disclose price-sensitive information. A company should also try to stop ongoing criminal behaviour conducted within the company's operations. When permitted under labour law, it is further considered good practice to investigate and freeze email accounts and other similar measures.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Local prosecutor offices do not, in general, have any concerns about internal investigations. An internal investigation is the company's matter, and the prosecutor has no right to intervene. However, the prosecutor may take independent actions against the company, such as confiscating documents. If covered by attorney-client privilege, documents concerning the investigation itself will not be confiscated.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

The police, the prosecutor, or the court can decide to issue a search warrant if there is reason to believe that a criminal offence punishable by imprisonment has been committed. A search warrant can be obtained for a company if: (i) the offence is believed to have been committed on the company's premises; (ii) the suspect was detained on the company's premises; or (iii) extraordinary reasons indicate the search will lead to an item or information regarding the offence. In relation to extraordinary reasons, there must be one or more factual circumstances that substantially show one can reasonably expect to recover evidence for the investigation.

The principle of free adducing of evidence and the principle of free evaluation of evidence under Swedish law allow the prosecution authority to use and the court to evaluate evidence obtained even through an unlawful search and seizure.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

No deals, non-prosecution agreements, or deferred prosecution agreements can be made under Swedish law.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Corporations are not subject to criminal liability under Swedish law but can be fined for crimes committed by employees or executives acting within the scope of their duties where (i) the company has not done what was reasonably required to prevent the crime, or (ii) the crime is committed by an individual in a leading position or with a particular supervisory or control responsibility in the company. In such situations, any illegally obtained profits may be forfeited.

There is no possibility for a court to impose a general debarment on a company in a criminal trial, but according to the Swedish rules on public procurement, a prior verdict imposing a corporate fine on a company may, in certain cases, lead to the company's debarment from a procurement.

Directors and/or employees to whom certain responsibilities have been delegated may be criminally liable for their acts of omission, for example, bookkeeping crimes, work environment crimes, and reckless financing of bribery. Penalties for such crimes are fines or imprisonment, but several combinations and types of conditional sentences may be imposed.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Sweden's Penal Code only criminalises acts by natural persons (individuals), which is in line with the principles of the Swedish Criminal Law that only natural persons can be held criminally responsible. As a result, companies cannot be prosecuted.

If a person has committed a crime, and the act was committed as part of a company's business activity, the company could face a criminal trial and be imposed corporate fines between 5,000 and 500 million Swedish kronor. Corporate fines under Swedish law are not a criminal sanction, even though closely related, but a special effect of a crime (committed by an individual) and sanction companies for not effectively preventing crimes. Hence, a company could be subject to corporate fines if it fails to act in a way that reasonably would have prevented a crime.

There is no specific provision stating that penalties for individuals may be reduced if the company in question has implemented a compliance system. But a corporate fine may be suspended or reduced if the company has tried to prevent a crime or taken action to mitigate the effects of a crime on a best effort basis. Corporate fines could also be reduced if a compliance system has been implemented after a crime has been committed and the company reports the crime as a consequence of the implementation.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Legal provisions concerning sustainability in general are in Sweden included in different areas of the law such as company law, the Annual Accounts Act, anti-bribery and corruption legislation, labour law, marketing law, data privacy law and environmental law.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The recent most significant event is still the revised provisions concerning corporate fines that came into effect on 1 January 2020. The new rules contain several amendments, the most noteworthy being that the maximum fine is increased from 10 million to 500 million Swedish kronor. Also, Swedish courts are given extended jurisdiction to try international bribery crimes.

The new provision will make it possible to impose corporate fines not only on corporations or other entities that conduct business but also on public sector entities whose operations are comparable to business activities. The new provisions have so far been scarcely used. Thus, there is still no case law specifying how the provisions should be applied.

CONTACTS

NORDIA
SWEDEN • NORWAY • DENMARK • FINLAND • LAW

Waterfront Building
Klarabergsviadukten 63
101 37 Stockholm
Sweden

Tel.: +46 8 563 08 100
Fax: +46 8 563 08 101
www.nordialaw.com

Hans Strandberg
Partner
Nordia Law
T +46 8 563 08 100
E hans.strandberg@nordialaw.com

Hans Strandberg is a former judge in District Court and the Court of Appeal where he served for 10 years. He has been a lawyer since 1986 specialised in company and business related criminal law, besides of compliance and securities law. On his client list are more than 15 of the largest Swedish public companies, some multinational foreign public companies, and foreign states. He is a litigator and has appeared in most of the public criminal cases involving listed companies as well as in the Supreme Court. He has also been involved in legislative work regarding Swedish corruption legislation and has been active in producing the Swedish Code of Conduct related to corruption for companies. He is also active in examining lawyers when becoming members of the Swedish Bar Association.

Olle Kullinger
Partner
Nordia Law
T +46 8 563 08 100
E olle.kullinger@nordialaw.com

Olle Kullinger has been with the firm since 2007 and specialises in company and business related criminal law, as well as compliance and securities law. He has worked with many of the largest listed companies in Sweden as well as a range of other companies whose businesses have been questioned. He is a litigator and has appeared in a number of cases concerning white collar crimes, representing both companies and directors. He has appeared as counsel two times before the Supreme Court. He has headed and taken part in a number of internal investigations. He has also been involved in legislative work regarding Swedish corruption legislation and has been active in producing the Code on Gifts, Rewards and other Benefits in Business.

Carl-Johan Allansson
Partner
Nordia Law
T +46 8 563 08 100
E carl-johan.allansson@nordialaw.com

Carl-Johan Allansson has been with the firm since 2007. He is specialised in company and business related criminal law and litigation. He has worked with many of the largest listed companies in Sweden as well as a range of other companies whose businesses have been questioned. He has assisted in a number of internal investigations.

Switzerland

taormina law AG

Dr. iur. Andrea
Taormina LL.M.

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	Limited	X	X	Very limited	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

In 2019 the Federal Council of Switzerland proposed a change of law to increase whistleblowing protection. This proposal was refused by Swiss parliament in 2020. Since then, no general laws for the handling of whistleblower reports and whistleblower protection have been enacted in Switzerland in the *private sector*. However, employers are subject to a general duty of care towards their employees, which might include protective measures in case of internal conflicts or mobbing triggered by a whistleblower report. In some cases, it may be advisable to suspend whistleblowers (on full pay) following their report. If whistleblowing activity is investigated internally and personal data is processed, the Federal Act on Data Protection might be applicable. It provides, for instance, that the use of personal data must be carried out in good faith, be proportionate and may only be collected for a specific purpose. If the employer collects personal data, he or she may have the duty to inform the employee in an "appropriate manner".

In the *public sector*, there are rules that have to be followed pursuant to the laws of the different cantons (e.g. in the canton of Geneva) or within the federal administration (Article 22a Federal Personnel Act). Due to the restrained territorial or material scope of application of these rules, their applicability must be evaluated from case to case.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

There are also no specific requirements referring to the structure of a reporting system for whistleblowing. As Switzerland is not a member of the EU, it is not obliged to implement the EU Whistleblower Directive (Directive (EU) 2019/1937) into its national law. Nevertheless, Swiss companies with business activity in the EU area might fall within the scope of this directive, especially if they have business offices in the EU area with more than 50 employees.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Internal investigations do not require prior disclosure to employees or to their representatives.

b) No information duty applies with regard to the data protection authorities or the company's (internal) data protection officer.

c) There are no information requirements to other local authorities.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees have a general duty of loyalty towards the employer's legitimate interests. This includes supporting an internal investigation. Disciplinary measures for non-compliance are possible in principle, provided employee personality rights are respected.

Termination on grounds of non-cooperation is not advisable in most cases, however, and might be frowned upon by authorities since employees should remain available for any subsequent official investigation.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Investigative actions do not trigger specific deadlines. Neither can they be qualified as waivers of the employer's rights.

On the other hand, a whistleblowing report might lead to the suspension of termination rights. As a general rule, termination of an employee's contract may be unlawful if said employee has asserted claims under the employment relationship in good faith prior to the termination. Thus, in cases where investigative action was triggered by a (rightful) complaint of an employee, said employee is protected from termination for a certain time afterwards.

Although no general whistleblower protection exists under Swiss law, this rule has in practice been applied to certain whistleblowers who acted in good faith and correctly followed any applicable procedures.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

Secrecy obligations, such as banking secrecy, might be applicable depending on the sector in which the company is active.

General data protection principles must also be observed. While not part of Swiss legislation, under certain circumstances (targeting criterion), the General Data Protection Regulation of 27 April 2016 (Regulation (EU) 2016/679 of the European Parliament and the Council) may have to be observed. For the most part, the requirements of this regulation have been implemented into Swiss law by the comprehensive revision of the Federal Act on Data Protection.

Further, in case of procedures by foreign authorities, proceedings before foreign courts and potentially in case of an intended disclosure to foreign authorities or courts, the mere performance of interviews on Swiss territory may qualify as an unlawful activity on behalf of a foreign state. Such activity could then constitute a

criminal offence punishable by imprisonment or monetary penalty, sometimes referred to as Swiss blocking statute). Exemptions can be requested (prior to the investigation) from the competent Swiss authority.

The presence of external counsel at the interview (in the role of conductor of the investigation or of employee counsel) is unproblematic if such counsel is subject to professional secrecy. Other third parties must not be present at interviews if secrecy obligations apply.

b) reviewing emails?

Private correspondence by employees must not be reviewed. If employees' email accounts are legitimately used for private purposes, such correspondence must be excluded from the review. Such exclusion can require time-consuming and costly triage procedures. Preventive measures (email policy, clause in employment agreement) are therefore highly recommended.

As soon as emails are disclosed to third parties, secrecy obligations may have to be observed in certain sectors.

c) collecting (electronic) documents and/or other information?

The collection of documents and other information (e.g. personal data) can be subject to the obligation to inform the person concerned by this measure following the Federal Act on Data Protection.

As is the case with performing interviews, in case of procedures by foreign authorities, proceedings before foreign courts and potentially in case of an intended disclosure to foreign authorities or courts, the mere collection of documents on Swiss territory might qualify as an unlawful activity on behalf of a foreign state. It is important to note that pre-trial discovery can also be problematic under this rule. Again, exemptions can be requested (prior to the investigation) from the competent Swiss authority.

Permanent electronic supervision of employees (by cameras or by constant monitoring of information technology use) is only permitted in exceptional circumstances.

d) analysing accounting and/or other business databases?

In this regard no secrecy/privacy obligations apply.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

Written instructions are not mandatory by law, but highly recommended. They might subsequently serve as evidence that procedural requirements have been met.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

There is no directly applicable legal duty to inform employees thereof. However, it is general practice in Switzerland that such information is given. With a view to the future use of employee statements in a criminal/civil procedure, such information is highly recommended.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

No formal requirement applies. It is, however, highly recommended to clearly explain (in writing) the circumstances of the interview to the employee.

d) be informed of their right to have their own lawyer attend the interview?

Swiss law does not grant an explicit right to the employee to request attendance of their lawyer. Nonetheless, it is general practice to allow such attendance. It is advisable (rather than mandatory) to inform the employee thereof.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

There are no such attendance rights under Swiss law.

f) be informed that data may be transferred to another country (in particular to the United States)?

Under the Federal Act on Data Protection, data may only be disclosed abroad if the foreign country in question guarantees an adequate level of protection. The Federal Council has published an official list that mentions countries in which this is the case. This list does not include the United States. The transfer of data to countries lacking an adequate level of data protection, e.g. the United States, requires specific legal justification. Employee consent is one possible form of justification. Other forms include overriding private or public interests, as well as binding corporate rules that have been approved in advance by the Federal Data Protection and Information Commissioner or by the authority responsible for data protection in a State that guarantees an adequate level of protection. The person concerned must be informed about a transfer of data abroad.

It is important to observe that the disclosure of sensitive information to a foreign recipient might be problematic in spite of explicit consent by the information owner. The provision on industrial espionage prohibits the disclosure of trade secrets to foreign agents. Since this provision protects public as well as private interests, a waiver by the information owner is not sufficient in some cases.

g) sign a data privacy waiver?

Disclosure of data requires legal justification. Employee consent is one possible form of justification. Other forms include overriding private or public interests. Under Swiss law, there is no specific obligation to sign a privacy waiver. Still, it is advisable in many cases to do so, especially if no other grounds for disclosure apply.

h) be informed that the information gathered might be passed on to authorities?

General data protection principles require the employer to specify the possible use of personal data provided by the employee. It is advisable to explain the investigation procedure to the employee.

i) be informed that written notes will be taken?

In this regard no express information requirement applies. It is, however, advisable to explain the investigation procedure to the employee.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Document hold notices are unknown in Switzerland. If issued regardless, they are without legal effect. This must not be interpreted as permission to destroy evidence. Such destruction could unfavourably influence the outcome of a trial, since it would be taken into account by the court when weighing the evidence.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Under Swiss law, attorney-client privilege exclusively applies to external counsel. If an investigation is conducted by external counsel, any work products or forms of correspondence are protected. No formal steps such as expressly marking documents as confidential are required. Nevertheless, it is advisable to use such markers, in particular if documents could potentially be disclosed abroad at a later stage.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Under Swiss law, attorney-client privilege does not apply to in-house counsel or compliance officers. Thus, any findings in investigations conducted without assistance of external counsel are outside the scope of attorney-client privilege.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

In this regard, no general rules apply. Notification requirements might be included in the terms of any specific insurance policy.

b) Business partners (e.g. banks and creditors)?

In this regard, no general rules apply. Banks and other creditors may include specific clauses in loan agreements and other contractual instruments.

c) Shareholders?

Shareholders must be informed annually about the course of business of the company at the general meeting. They are entitled to demand additional information at this opportunity. Furthermore, shareholders who represent at least 10 percent of the share capital or the votes of a not listed company can request the board of directors to provide information on company matters.

Listed companies are subject to *ad hoc* publicity requirements. Facts that are not known publicly and that (from an *ex ante* perspective) could potentially lead to a significant change in share prices must be communicated to the public. Under these rules and subject to a case-by-case analysis, serious incidents (such as big-scale bribery) which trigger investigations must be disclosed to the public.

d) Authorities?

No general information requirement applies. Even in the case of criminal acts, companies, that do not fall under the scope of sector-specific rules, have no general duty to notify the authorities. Notification might, however, have a mitigating effect in criminal or administrative procedures.

A specific leniency application programme applies to cartel investigations. The first party to report the cartel to the Swiss Competition Commission ("**COMCO**") might benefit from full immunity from fines.

Companies under supervision by sector-specific authorities might be subject to specific requirements. This applies in particular to the reporting duty towards the Swiss Financial Market Supervisory Authority ("**FINMA**") in the financial sector.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Employers are subject to a duty of care towards their employees. If the alleged conduct leads to any threat or damage to employees' interests, immediate measures to protect other employees might be required under Swiss employment law. Suspension of employment is possible at any time under Swiss law. It might be advisable to suspend certain employees on full pay.

No general duty to prevent criminal behaviour exists under Swiss law. Nonetheless, companies are under an express duty to take reasonable and sufficient preventative measures against certain offences, namely money laundering, bribery, and terrorism financing. In view of the rules on corporate criminal responsibility and general principles of corporate governance, companies are generally recommended to enact and uphold an effective compliance programme.

Regardless of the nature of the (alleged) offence, companies are recommended to take immediate measures aimed at the discontinuation of any discovered or suspected criminal conduct by employees. Specialist legal advice might be required to determine the nature and scope of such measures to prevent prejudice to the investigation's outcome (or a premature admission of employer negligence).

Measures aimed at limiting the company's financial damage might also be advisable with a view to future damage claims against perpetrators. A general duty to mitigate damages exists under Swiss law.

In the case of a limited number of offences (namely money laundering, bribery, and terrorism financing), companies can be fined regardless of any individual's responsibility if they failed to take reasonable and sufficient preventative measures.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

In general, public prosecutors and other authorities encourage and reward internal investigations. The conduct of a thorough internal investigation might lead to a considerable mitigation in case of criminal or administrative sanctions.

With a view to future criminal or civil proceedings, it is advisable to observe basic procedural requirements when conducting an internal investigation. Even then, interview transcripts will generally not suffice the strict requirements for evidence in official proceedings. They might, nonetheless, serve to give authorities indications as to how to establish the relevant facts in the course of their investigation.

As soon as a criminal or civil procedure is imminent or opened, contact with (potential) witnesses might be problematic. Complex, largely unwritten rules apply. Thus, professional advice is highly recommended in this regard.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Searches can be conducted against the will of the occupant of the premises if there is reasonable suspicion that a criminal offence has been committed, the measure is proportionate, the seriousness of the offence justifies the means and evidence or assets that must be seized or wanted persons are expected to be found. In addition, the will of the occupant of the premises is not needed if offences are being committed on the premises that are to be searched. Although search warrants must be issued in writing by the prosecutor, oral warrants are just admissible in urgent cases. Sealing of any seized items or (electronic) records can be demanded within three days after the search. The prosecutor will subsequently have to file a request for removal of the seal within 20 days.

In principle, any unlawfully obtained evidence is inadmissible. Exceptions to this rule are, however, granted routinely if the evidence could have been obtained legally and if its use considerably furthers the establishment of the truth.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Public prosecutors have limited discretion regarding the opening of an investigation against a certain subject. Nonetheless, self-reporting and maximum cooperation might be beneficial at this stage.

With regard to criminal prosecution, a guilty plea can enable an abbreviated procedure, leading to a summary judgement which is drafted by the prosecutor and approved by a court. Abbreviated procedures are only possible for penalties up to five years' imprisonment, in cases where the defendant fully acknowledges the facts of the case and recognises, in principle, any civil claims brought in connection with the offence.

Minor offences that are punished with a fine, a monetary penalty of no more than 180 daily penalty units or a custodial sentence of no more than six months can lead to a punishment order. Such cases are resolved without the involvement of a court.

FINMA and COMCO conclude their procedures with formal decisions. Self-reporting and cooperation by the subject of the investigation are taken into account when deciding upon sanctions. Prior to the opening of a formal procedure, maximum cooperation may lead to the abandonment of the investigation.

A specific leniency application procedure applies in the case of cartel investigations. COMCO may grant full immunity from fines to the leniency applicant.

Specialist legal advice regarding self-reporting and cooperation is highly recommended since detailed knowledge of the legal framework as well as experience in dealing with the authorities involved is essential when determining the best strategy for an impending official investigation.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

In Swiss criminal law, the focus lies on the responsibility of the individual. Directors, officers, or employees may face monetary penalties and imprisonment. Additionally, criminal courts can impose professional bans or issue expulsion orders for foreign nationals.

The scope of corporate criminal liability is limited. Companies cannot be convicted as perpetrators of a crime. Rather, the law penalises organisational shortfalls within the company. Thus, companies can be fined if a criminal offence by an employee or director cannot be attributed to an individual due to organisational deficiencies. In the case of a limited number of offences (namely money laundering, bribery, and terrorism financing), companies can be fined regardless of any individual's responsibility if they failed to take reasonable and sufficient preventative measures.

In COMCO proceedings, fines are imposed upon companies and/or individuals. Fines for companies can be calculated in proportion to their turnover.

In FINMA proceedings companies can be fined, and individuals can face fines or (rarely) imprisonment. Other possible sanctions include the revocation of a company's licence or occupational bans for individuals.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Penalties for companies are assessed, *inter alia*, based on the gravity of the company's lack of proper organisation. Accordingly, serious organisational deficiencies will likely increase the penalty. This rule only applies if the compliance system was implemented prior to the alleged misconduct. Thus, the introduction of adequate and effective compliance procedures can serve to protect companies from criminal liability. The upper limit for fines imposed on companies is 5 million Swiss francs. As a general rule, penalties for directors, officers, and employees are not reduced or suspended in case of an efficient compliance system.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

The EU has issued various pieces of legislation on ESG related matters, e.g. the EU-Directive 2014/95/EU regarding disclosure of non-financial and diversity information by certain large undertakings and groups and the EU-Regulation 2017/821 laying down supply chain due diligence obligations for Union importers certain metals and minerals. The rules set forth in these legislative acts are not directly part of Swiss legislation but may, nevertheless, be applicable on Swiss companies if targeting criteria are met.

Switzerland has partially adapted its regulatory framework to EU-standards regarding ESG by introducing Article 964a ff. of the Code of Obligations ("**OR**"). As of January 2022, in concert with EU-Directive 2014/95/EU, companies of public interest with more than 500 full-time equivalent positions on annual average, a balance sheet total of 20 million Swiss francs or a sales revenue of 40 million Swiss francs have to publish a report on non-financial matters (as for example CO2 goals, human rights or corruption).

Additionally, similar to EU-Regulation 2017/821, companies whose seat, head office or principal place of business is located in Switzerland, must comply with due diligence obligations in the supply chain and reporting if they deal with certain metals and minerals (Article 964j ff. OR).

Furthermore, on 1 January 2021, Switzerland has adapted its legislation regarding transparency in the sector of raw materials. Certain companies involved in the extraction of minerals, oil or natural gas or in the harvesting of timber in primary forests must, on an annual basis, publish a report on the payments above 100,000 Swiss francs they have made to state bodies (Article 964d ff. OR).

In 2020 Switzerland introduced rules concerning gender representation of the board of directors and the executive board (Article 734 f. OR). According to these rules, each gender must make up to 30 percent of the board of directors and 20 percent of the executive board. If these quotas are not met, the reasons and the measures taken to address the issue have to be indicated in the renumeration report.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Internal investigations were not traditionally part of the Swiss legal landscape. This is still apparent in the lack of specific legislation for this field. In the last decades, however, internal investigations have rapidly become a much-practiced instrument. They are being recognised and encouraged by authorities.

As of 1 January 2025, the Swiss Civil Procedure Code will allow in-house counsels of companies to refuse the collaboration in civil procedures under certain circumstances, in addition to accredited lawyers. This amendment, however, has no direct effect on criminal procedures.

CONTACT

taormina

Kanzleistrasse 127
CH-8004 Zürich
Switzerland

Tel.: +41 44 455 66 60
www.taormina-law.ch

Dr. iur. Andrea Taormina, LL.M.
Specialist Criminal Attorney, SBA
taormina law AG
T +41 44 455 66 60
E taormina@taormina-law.ch

Andrea Taormina advises clients and represents them in court, specialising in criminal law and international mutual legal assistance in criminal matters.

Andrea holds a Doctorate in Law [Dr. iur.] from Freiburg University (Switzerland) and is admitted to the bar in the Canton of Zurich. In 2002, he was awarded an LL.M. degree from the University of Chicago Law School. From 2002 to 2004, Andrea worked in the U.S. Law Group at Allen & Overy in London. From 2004 to 2005 he worked at Homburger Rechtsanwälte in Zurich, after which he set up his own independent criminal law practice in Zurich. In addition, Andrea is a member of the Commission on Legal Fees of the Zurich Bar Association.

Turkey

Cerrahoğlu Attorney Partnership

Onur Gülsaran

Yasemin Antakyalıoğlu Kastowski

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X*	X	X	X	X
No					

* Corporates cannot be criminally liable under Turkish law but may be liable under administrative law.

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

Since Turkey is not a member state of the European Union, the EU Directive has not been implemented in Turkey and there is no obligation for such implementation.

There is no specific Turkish legislation providing whistleblower protection. The whistleblower's protection is governed by general employment law principles. As such, an employee cannot be dismissed on the grounds that they have reported misconduct or suspected misconduct. However, a dismissal of the employee with immediate effect may be justified if the employee discloses trade secrets to authorities or the public without genuine suspicion or knowledge of actual misconduct (e.g. when the employee's report is untruthful and/or vexatious). Under Turkish law, companies are not obligated to investigate a whistleblower report, although it is generally considered good practice to do so. At the end of an internal investigation, if any offence is detected, the company should report it to the prosecution authorities if it is ongoing at the time of the investigation (subject to the right to avoid self-incrimination under the Turkish Constitution).

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

Please refer to our answer to question 1a.

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) Many companies in Turkey have labour unions and an associated collective bargaining agreement between management and employees. An employee representative from the labour union has the right to be informed about and/or to participate in the investigation if this was agreed in the collective bargaining agreement. In the absence of such an agreement, the employee representative body has no automatic statutory right to be involved in an investigation.

b) There is no specific provision in the applicable Turkish Data Protection legislation that gives the data protection officer or data privacy authority the right to be informed about and/or participate in the investigation.

c) Where the relevant misconduct being investigated is also an offence regulated under the Turkish Criminal Code, this Code provides that the offence must be reported to the prosecution authorities if it is ongoing at the time of the investigation. In general, even if the relevant misconduct is deemed an offence under Turkish Criminal Code, there is no reporting obligation if the offence is not being committed at the time of the investigation. However, certain cases, such as money laundering offences uncovered as a result of an internal investigation, should be reported to the relevant authority (see question 10 below).

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

In general, employees have the labour law duty to cooperate with an internal investigation as far as the facts to be investigated relate to activities conducted or matters known to them as part of their employment. They must answer work-related questions truthfully and completely. If the matters under investigation are unrelated to the employee's work or position in the company, a balancing of interests has to be performed to determine if a duty to cooperate exists.

Where an employee is required to participate, the employee's refusal may be regarded as a breach of duty and such misconduct may justify dismissal.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

The legal period under Turkish labour law for dismissal for cause is six working days following the date the employer becomes aware of the relevant misconduct giving rise to the dismissal. In case an investigation is carried out, this six working day period will, in general, not commence until the investigation is finalised and a report is provided to the relevant person/body within the company in charge of employee dismissals. If a claim for unfair dismissal is brought before the courts, the burden is on the employer to prove that the termination is justified.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The Law of Protection of Personal Data (General Data Protection Regulation is not applicable in Turkey) which entered into force on 7 April 2016 applies to the processing of data. This includes securing, collecting and reviewing data, as well as the creation of work products such as interview file notes and final reports. Therefore, it is very important to perform an early assessment of the applicable data privacy laws and to document the steps taken.

b) reviewing emails?

Private communications are protected under Turkish law. Reviewing private emails of employees may even constitute a criminal offence if data privacy requirements are not observed. Provided that a general disclaimer is provided to the employee, stating that their business-related communications (including work emails) could be monitored by the company at any time, the work emails of the employee can generally be reviewed. This disclaimer should be signed by all employees at the start of their employment contract.

c) collecting (electronic) documents and/or other information?

As with emails, all other forms of documents containing personal data or private communications will be protected by Turkish law.

d) analysing accounting and/or other business databases?

There is no specific regulation in this respect unless the relevant databases contain personal data, in which case the Law of Protection of Personal Data will apply.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no general statutory obligation that the employee to be interviewed should receive written instructions. Nevertheless, explanations are considered to be ethically required and advisable. In general, this includes a brief description of the background of the investigation and the subject matter. For documentation purposes, it is advisable to provide these instructions in written form to be countersigned by the interviewee.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

There is no legal requirement to inform the employee in this regard.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no legal requirement to inform the employee in this regard. However, an Upjohn warning would be advisable where the investigation may have a U.S. context.

d) be informed of their right to have their own lawyer attend the interview?

There is no legal requirement to inform the employee in this regard. However, should the employee request the presence of their lawyer, it is advisable to allow the lawyer to represent their client at the interview.

e) be informed that they have the right of a representative from the works council (or other employee representative body) to attend?

Where there is a labour union in the workplace and there is a provision to such purpose in the collective bargaining agreement, the employee representative would have the right to be informed about and/or to participate in the interview.

f) be informed that data may be transferred to another country (in particular to the United States)?

The employee should be informed, and their explicit consent should be requested before their data is transferred outside Turkey. Under Turkish data privacy law, transfer of data to a foreign country is permissible if explicit consent for such transfer is given.

g) sign a data privacy waiver?

According to Turkish data privacy legislation, the employee needs to consent to the company's use of their personal data. Where the personal data of the interviewee might be used for other purposes in the future (such as in possible court proceedings), a data privacy waiver signed by the interviewee can be very helpful.

h) be informed that the information gathered might be passed on to authorities?

Although there is no legal obligation in Turkey in this regard, this should be included in the interview instructions as a matter of good practice.

i) be informed that written notes will be taken?

For reasons of transparency, the fact that the information provided in the interview will be recorded (e.g. for reports and potentially for disclosure) should be explained. It is also advisable to have a copy of the written notes signed by the relevant employee and maintained in the investigation records. However, there is no such legal obligation under Turkish law.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

There is no specific law requiring that a document retention notice should be issued, but issuing such notices is advisable. Such notices should be clear, sent to all potentially relevant addressees, and issued as early as possible. Before issuing the document retention notice, the company should consider which employee's documents should be retained and what types of documents should be sought (e.g. physical documentation, emails, documents contained on hard-drives and mobile devices). The document retention notice should briefly describe the terms of reference of the investigation, bearing in mind the need to maintain confidentiality.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Attorney-client privilege exists under Turkish law, although there are no specific rules in relation to its application in internal investigations. The documents relating to the findings of an internal investigation may be subject to attorney-client privilege protection if they have been prepared by an independent attorney and to the extent, they concern the client's defence rights. Accordingly, to protect and render such documents out of the scope of the public investigation, it is recommended to mark these documents as "Confidential, Privileged, Attorney-client Privileged" and "Relating to Defence Rights".

Prosecutors may search company offices, although they will need a warrant to do so, and the search must be done in the presence of a public prosecutor. It is recommended to have a lawyer present at the company offices during a raid. During such a raid, it is important to object to the seizure of any privileged documents and to ensure that this objection is documented in the minutes of the raid. Such objections will be considered by the public prosecutor or relevant judge when assessing the claim for privilege. Where the claim for privilege is successful, the public prosecutor or judge shall return these documents to the company.

Prosecutors may also search an attorney's office, but will need a court warrant to do so, and the search must be done in the presence of a public prosecutor. In case of a raid at an attorney's office, the attorney and/or the bar representative present at the raid may claim during the raid that a document, which is about to be confiscated, is related to the client's defence rights. In this case, the document is put in a separate envelope and the envelope's flap is sealed. The evaluation of attorney-client privilege status of the document is done by the magistrate in cases of criminal investigation, and by the criminal judge in cases of prosecution, in each case within 24 hours. If it is

decided that the document falls under the scope of attorney-client privilege, it is immediately returned to the attorney and the correspondence relating to the document is destroyed. Therefore, in order to ensure privilege protection, it is advisable to keep the important documents relating to an internal investigation at the office of an outside counsel rather than on company premises, and to write "Confidential/Attorney-client correspondence" and "Relating to Defence Rights" on them.

Under the Criminal Procedure Code, upon a judge's warrant, a public prosecutor may seize computers and/or computer files. It is important to obtain a copy of the seized computer files and raise written objections with respect to potentially privileged documents during the raid. A claim for privilege may also be raised following the raid, but, where possible, it is advisable to object during the seizure proceedings since these objections may be taken into account during the search of the copies of computer files by the relevant authorities.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Attorney-client privilege does not apply to in-house counsel. A recent decision of the Turkish Competition Board held that correspondence with an independent attorney will fall within the scope of attorney-client privilege. The decision implied that, as in-house counsel are employed by the company, they are not considered independent attorneys.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

As far as circumstances arise that could give rise to a claim under an insurance policy, (for example, under a D&O policy in relation to conduct of company directors), the company should make a notification of circumstances to the insurer. Each individual policy should be reviewed to ensure notification requirements are met.

b) Business partners (e.g. banks and creditors)?

Duties to inform business partners may arise from contractual obligations between the company and the business partner, particularly where the matter under investigation may have implications for the business partner. Even if there is no explicit provision in the relevant contract, there may be an obligation to notify a business partner of an internal investigation, where that information is highly significant to the business partner and relevant to its contract with the company. The interests of the business partner need to be evaluated against the legitimate interests of the company. Therefore, it depends on the individual case whether and when the business partner needs to be notified.

c) Shareholders?

Potential reporting duties towards shareholders compete with the company's requirements to maintain business confidentiality. Such reporting duty would play an essential role in companies since certain investigations may require a mandatory disclosure under the law (for example, companies listed on the BORSA Istanbul stock exchange will be required to disclose an investigation if it is deemed a material event). In addition to statutory disclosure obligations, the company has to evaluate on a case by case basis if there is an *ad hoc* duty to report to the shareholders. An obligation to disclose exits if the internal investigation affects the market price significantly and fulfils certain criteria (e.g. relating to the risk, scope, and suspects involved in the internal investigation).

d) Authorities?

In general, there is no duty to inform the prosecutor about an internal investigation or potential misconduct within the company. However, there are exceptions where certain types of serious misconduct are uncovered during an investigation. For example, under the Regulation on Suspension of Transactions within the scope of Laundering Proceeds of Crime and Financing of Terrorism, certain companies (e.g. financial and insurance institutions, lawyers, and accountants) are required to notify the Turkish Financial Crimes

Investigation Board if a serious indication exists which shows that a suspicious transaction has been performed or attempted. Even where no statutory duty to report exists, a cooperative approach with the local prosecutor may prevent adverse and unexpected measures by the authorities.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

The company has to minimise damages, stop any ongoing misconduct and try to prevent new cases of misconduct. Additionally, the company may have to re-evaluate its compliance system, especially its compliance policies (such as its Code of Conduct) and the related training provided to the employees, in order to eliminate potential deficits and to improve its existing system. Further, the company may impose sanctions on the concerned employees, including termination, in order to show that misconduct is not tolerated inside the company. Depending on the individual investigation and the industry sector concerned, notification to certain regulators may be advisable for strategic, risk management reasons.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Internal investigations are not very common in Turkey, and usually Turkish subsidiaries of global companies conduct such investigations. As of today, the findings of such investigations are reported to the authorities in rare cases. Therefore the case law on the matter is very limited. However, where criminal misconduct is found in an internal investigation, a detailed internal investigation report of such misconduct would be helpful to the prosecution office (although there are no provisions under Turkish law relating to self-disclosure by the company to the prosecutors).

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

A search of company premises can be carried out with a judge's warrant or the prosecutor's warrant in urgent cases. The search warrant should detail the suspected criminal act to which the search relates, the person(s) to be searched, the address, the property to be searched, and the duration of the warrant. In principle, the prosecutor should be present during the search. However, where this is not possible, the search can be conducted in the presence of two aldermen or neighbours. "Aldermen" are elected government officials who act as neighbourhood representatives, and a "neighbour" is someone who lives in the same neighbourhood and who agrees to be a witness during a search.

In case of non-compliance with the rules on search warrants, the evidence gathered in the search cannot be used in court proceedings. Furthermore, anybody whose rights are violated by a non-compliant search can claim pecuniary and non-pecuniary damages.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

In principle, deals and non-prosecution or deferred prosecution agreements are not available under Turkish law except the following:

With the amendment made to the Criminal Procedural Law on 23 October 2019, a system called "serial procedure" has been adopted for certain offences to be effective commencing from 1 January 2020.

The types of offences to which this system will be applied are explicitly enumerated in the law. In summary, this system can be applied for light crimes and for crimes the proof of which require high technical nature such as fraud

in money, endangering traffic safety, deliberate jeopardy of general security, false declarations in the issuance of official documents and seal breaking.

The basic rule of the serial procedure is that the public prosecutor agrees with the suspect, who accepts the fact that they have committed the act. The public prosecutor then, without indictment, conducts a detailed trial activity, and imposes half of the amount of the punishment prescribed in the law for the offence considered to have been committed by the suspect. Instead of the indictment, the report prepared by the public prosecutor containing the prescribed provision shall be forwarded to the relevant court and shall be issued as a verdict in case the defendant declares the acceptance before the Court with the presence of their lawyer.

This system, which is a kind of agreement, has been introduced with the aim of a quick conclusion of the proceedings in respect of certain crimes. If the proposal is not accepted by the suspect, the investigation and prosecution will be carried out according to the general principles of trial.

In addition, prosecutors have discretionary powers on whether to commence criminal action under certain circumstances. For criminal acts that require the filing of a complaint and are punishable by a maximum of one year of imprisonment, if the defendant has no criminal past, the prosecutor can defer the criminal case for five years. If the suspect does not commit any crime during this five-year period, the prosecutor may decide not to commence any criminal proceedings.

Since criminal liability does not attach to companies, the deferment of prosecution would only be applicable for the company's related directors, officers, or employees.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Corporations are not subject to criminal responsibility under Turkish law. However, they can be subject to sanctions such as administrative fines, cancellation of business, and permits or expropriation (i.e. taking possession of assets). This will depend on the type of the misconduct committed by their directors or officers.

Individuals who have supervisory duties may face sanctions not only for their own misconduct but also in relation to the misconduct of other employees under their supervision. These may include imprisonment, fines, or official debarment from their profession.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

If companies (i) have an effective internal investigation mechanism in place, (ii) report the evidence obtained as a result of their investigations and the actions considered to constitute a crime to the public prosecutor's office in due time, (iii) have taken the necessary prevention measures, and/or (iv) take further measures based on the nature of the action, this shall be taken into account by the relevant judge and can be used as a defence argument.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

There is no specific requirement in Turkish legislation with respect to ESG. However, existing corporations and emerging markets are voluntarily implementing ESG-related requirements, considering the needs of consumers, market and investors.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

Since internal investigations are not common and not widely conducted in the country, precedents are very rare. As a result of the accession talks between Turkey and the European Union, there is a tendency for local corporations to follow the practices in Europe. Although the process for new legislation is slow, as long as the accession talks continue as planned, the legal environment in this regard would most probably evolve accordingly.

CONTACTS

CERRAHOĞLU
AVUKATLIK BÜROSU / LAW FIRM

Barbaros Bulvarı, Mustafa İzzet Efendi Sokak
No:11 Cerrahoğlu Binası Balmumcu - Beşiktaş
34349 İstanbul
Turkey

Tel.: +90 212 355 30 00
Fax: +90 212 266 39 00
www.cerrahoglu.av.tr

Onur Gülsaran
Partner
Cerrahoğlu Law Firm
T +90 212 355 30 00
E onur.gulsaran@cerrahoglu.av.tr

Onur Gülsaran qualified as a Partner in 2008 and is a member of the Corporate Law Department.

He provides consultancy services regarding corporate issues (i.e. incorporation, general assemblies, board meetings), anti-corruption, lease, franchise, loan and asset purchase.

He speaks English and Turkish and currently holds membership in the Istanbul Bar Association since 1996.

Yasemin Antakyalıoğlu Kastowski
Founder
Antakyalıoğlu Law Office
T +90 212 355 30 00
E yasemin@antakyalıoglu.com

Yasemin Antakyalıoğlu is the founder of Antakyalıoğlu Law Office in Istanbul.

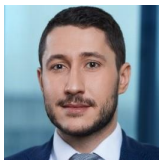
She especially focuses on criminal law and compliance issues. Ms. Antakyalıoğlu has an extensive knowledge in all ranges of white collar crimes and compliance investigations. She advises, represents, and defends her national and international clients in every step of criminal investigations and cases, such as fraud, tax fraud, custom fraud, misappropriation, forgery of documents, fraudulent bankruptcy, and defamation. She also advices and assists other prestigious law offices in criminal law matters. Before establishing her own office, she worked with a well-known criminal law Professor in Istanbul and as a Senior Associate in the criminal law department of an international law firm based in Istanbul.

She speaks English, German, and Turkish and currently holds membership in the Istanbul Bar Association since 2006.

Ukraine

ASTERS


Sergiy Grebenyuk


Orest Stasiuk


Oleksandr Volkov


Olha Yurchenko

Overview

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	
No					X

Question List

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

The Law of Ukraine on "Prevention of Corruption" ("Anti-Corruption Law") defines "whistleblower" as a person who reports corruption and corruption-related violations. It envisages provisions related to whistleblowers' protection. The EU Whistleblower Directive covers potential infringements of Union law in a broader sense the Ukrainian Anti-Corruption-law, however, Ukraine is not a member of the European Union yet. Therefore, the Ukraine is still in the process of harmonising its legislation with Union standards.

The established safeguards for a whistleblower include a right to anonymity and confidentiality, to receive information on the status of the investigation, and to obtain a reward (if a criminal corruption offence is reported and other conditions are met). Further, it is prohibited to dismiss whistleblowers because of their report and to impose disciplinary sanctions or other punitive measures on them.

In addition, the entities noted under below categories (c) and (d) should consider the Model Anti-Corruption Programme governing, *inter alia*, the conduct of internal investigations and setting forth an obligation for the officials responsible for implementation of such programme (e.g. compliance officer) to cooperate with whistleblowers and ensure the protections of their rights and guarantees.

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The Anti-Corruption Law provides for an obligation to ensure the availability of channels (including internal) to report potential violations for: (a) state and municipal bodies; (b) legal entities of public law; (c) state/municipal enterprises and companies (in which the state/municipal share exceeds 50 percentage) with the average number of employees exceeding 50, and the gross revenue exceeding UAH 70 million (circa US$1.87 million) for the financial year; (d) companies participating in public procurement for projects, equal to or exceeding UAH 20 million (circa US$534,045).

The obligation to establish a reporting system is rather general and does not address the question regarding the use of local or group-wide reporting systems. In practice, however, the implementation may vary.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) There is no obligation to inform employee representative bodies (e.g. primary trade union organisations) about internal investigations or engage them to participate in them. The only exceptions are internal investigations into accidents or occupational diseases of employees (non-compliance with the obligation to inform and engage the above bodies in such investigations may result in an insignificant fine).

b) There is no obligation to notify company's data protection officer. The data protection authority (the Ukrainian Parliament's Commissioner for Human Rights) should be notified only if sensitive data (such as health, genetic and biometric data, data on political and religious beliefs, etc.) is processed, unless such processing is necessary to exercise company's rights and obligations in terms of employment. However, as a matter of practice, such sensitive data is rarely processed within internal investigations.

c) There is no general obligation to inform other authorities about the commencement of an internal investigation or to involve them to be part of it.

However, in terms of corruption and corruption-related offences, the notification of authorities is required if such offences are identified (e.g. as a result of a preliminary review of the whistleblower report or of the internal investigation). Namely, officials of the governmental and municipal bodies and officers of legal entities of public law have an obligation to stop the offence and report it to the responsible state anti-corruption authorities within 24 hours. The Model Anti-Corruption Programme imposes a similar obligation for the companies mentioned under categories (c) and (d) in the response to question 1b above.

Non-compliance with the notification requirement by an official or officer may lead to an insignificant fine.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

There is no general duty of employees to support an internal investigation. Nevertheless, the company as an employer may establish such duty in its internal regulations (policies, programmes, etc.). Failure to comply with it may trigger imposition of disciplinary penalties. Other options to introduce the above duty and impose disciplinary penalties for its violation are also available.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

Investigative actions themselves shall not trigger the above deadlines or waive any right to sanction employees. Nevertheless, in view of Ukrainian labour law, the disciplinary penalties can be applied to an employee within a month from the date of the establishment of the elements of the disciplinary offence and in any case, within six months after commission of such offence. For the above one-month deadline, it is important to define the date when the offence can be considered as established.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The Law of Ukraine on Personal Data Protection ("**Law**") sets a general framework for data processing and protection. In 2022 its new draft was presented with the intention to bring the Law in compliance with the EU standards, including with the General Data Protection Regulation. Adoption of the draft is pending.

Conducting internal investigations, including interviews, usually involves processing of personal data. A company may process such data based on consent. Such consent must be specific and include information on: data controller, data categories, purpose of processing, its types and duration, data processors, parties to which data may be transferred/disclosed, including express permission for cross-border data transfer, data subject's rights under the Law etc.

When appropriate consent is not available, a company may apply the following grounds for personal data processing: (i) a need for the data controller to comply with an obligation established by law; (ii) a need to protect the legitimate interests of the data controller or third parties unless overridden by fundamental rights and freedoms of data subjects. The relevant requirements of anti-corruption law can potentially justify reliance on the above grounds to process such data. However, administrative sanctions may apply if the respective data processing is viewed as a breach of data protection laws in the absence of the individual's consent. It is advisable to have such consent in place before commencement of the interview.

Ukrainian law also provides for additional restrictions concerning classified information (i) relating to state and/or bank secrets; (ii) marked as "confidential" by the owning company; (iii) falling under a professional confidentiality obligation.

These restrictions shall be considered depending on the specifics of internal investigation (e.g. its subject), sphere of the company's activities, access of respective individuals to such information, and the company's contractual non-disclosure obligation in this regard.

b) reviewing emails?

Reviewing business and/or private emails without the individual's consent (even if such emails are of a business nature and were exchanged via an employer-provided account) may be considered a breach of the constitutional right for secrecy of correspondence and, therefore, trigger the risk of criminal sanctions.

To review emails, it is necessary to obtain consent from the individual as specified in the response to question 5a above. This also includes the permission to review emails by a company. Further, to avoid intrusion into the private life, respective data filtration means should be used when reviewing emails. It is also advisable to warn employees not to use employer-provided accounts for personal matters and/or have respective policies in this regard.

c) collecting (electronic) documents and/or other information?

Documents, including electronic and/or other information, may contain personal data and classified information. Therefore, the obligations and restrictions specified above may apply.

d) analysing accounting and/or other business databases?

Accounting and/or other business databases may contain personal data and classified information. Therefore, the obligations and restrictions specified above may apply.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

The company is not obliged to provide its employees with written or other instructions for the purpose of their interviews.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

The company is not obliged to inform its employees about such a right. Nevertheless, an employee may opt to rely on this right during the interview or otherwise during an internal investigation.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

The company has no such obligation. An "Upjohn warning" is alien to Ukrainian law.

d) be informed of their right to have their own lawyer attend the interview?

The company has no such obligation. An employee can be interviewed without a lawyer. Nevertheless, employees, at their own initiative, may choose to bring a lawyer to the interview.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

Generally, the company has no such obligation. Ukrainian law does not provide for a right of representatives of the employee representative body (if formed) to participate in the internal investigations (except of investigations into accidents or occupational diseases of employees who are members of such body).

f) be informed that data may be transferred to another country (in particular to the United States)?

Yes. The Law prohibits the transfer of personal data outside Ukraine unless the recipient's country ensures adequate data protection. The member-states of the EEA and the signatories of the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data are recognised as providing adequate protection. There are also exceptions on when personal data can be transferred to countries other than member-states of the EEA and signatories of the Convention. The relevant one here is the express consent of the data subject, which may be included in the general one described above.

The Law requires that the data controller notifies the data subject of the transfer of personal data to a third party within 10 business days, if required by the consent or otherwise not provided by law (except when such notification is not required, e.g. the transfer is duly requested by investigating authorities).

g) sign a data privacy waiver?

Ukrainian law does not envisage a data privacy waiver. A company may ask an individual to grant consent for conducting an interview, processing personal data, reviewing emails and/or granting access to or providing relevant (electronic) documents and other information on a voluntary basis.

h) be informed that the information gathered might be passed on to authorities?

The Law requires notification to the data subject by a data controller on the transfer of personal data to a third party within 10 business days if required by his consent or otherwise is provided by law (except when such notification is not required, e.g. the transfer is duly requested by investigating authorities).

i) be informed that written notes will be taken?

Ukrainian law does not provide for such obligation. However, if an audio or videorecording is made, it would be necessary to obtain the consent of the interview participants.

---

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

Ukrainian law does not prohibit using document hold or document retention notices or provides specific requirements for such notices. In the absence of specific requirements, it is recommended that such notice is issued by an authorised person under labour law and contains a clear description of the documents and information to be retained. It is also advisable to provide the addressees of the notice with the possibility to confirm its receipt (e.g. for the purpose of disciplinary penalties in case of non-compliance).

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

Generally, yes. The attorney-client privilege applies to any communications between the attorney and the client; any information or materials received from the client within the provision of legal advice; content of the attorney's advice or consultations; and documents drafted for the above purpose. It also covers legal advice and communications with a person who consulted with the attorney when no legal assistance agreement was subsequently concluded.

Generally, the attorneys, their assistants, and other employees shall not disclose the above communication and materials (unless there is a consent of the client or for the purpose of proceedings against the attorney initiated by their client). However, as a matter of practice, there are instances in which law enforcement authorities and courts continue to interfere with such privilege.

A legal assistance agreement with a licensed attorney/-s who works independently or with an attorney partnership shall be in place to ensure privilege protection.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Generally, the attorney-client privilege applies only to relations of licensed attorneys providing legal advice to their clients under a legal assistance agreement. Thus, if an in-house counsel does not have a licence (i.e. is not admitted to the Ukrainian bar), they cannot rely on such privilege, save for instances explicitly provided in the law (e.g. in-house counsels cannot be interrogated on matters they become aware while representing a company within the criminal proceedings).

As a matter of practice, licensed in-house counsels may conclude a legal assistance agreement with their employer in parallel with an employment agreement to cover advice given to the employer under the attorney-client privilege (e.g. to represent the company in the court). However, we are not aware of any instances where this approach was tested in courts regarding internal investigations.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

Ukrainian law does not contain such a requirement. As a matter of practice, such obligation may exist in respective insurance contracts.

b) Business partners (e.g. banks and creditors)?

Ukrainian law does not provide for such a requirement. The parties may agree on an early notification in their contracts.

c) Shareholders?

Ukrainian law does not envisage such a requirement explicitly. However, the company's bylaws (e.g. its charter) or internal regulations (e.g. governing conduct of an internal investigation) may contain the obligation to notify shareholders of the start of an internal investigation. Further, depending on the circumstances, the directors' duty to act reasonably, in good faith, and in the company's interest, may be interpreted to cover notification of shareholders before starting an internal investigation.

d) Authorities?

There is no general obligation to inform authorities of the start of an internal investigation. Please also refer to responses under question 3c.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

Generally, Ukrainian law does not require any specific immediate measures upon start of an investigation. Nevertheless, based on good faith principle and as a matter of practice, it is advisable that officials of the company and its shareholders, as applicable, take measures to stop any ongoing violations. Please also refer to response to question 3c.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

No, internal investigations in Ukraine are not subject to any specific requirements from the prosecutor's office. If criminal proceedings are anticipated, the measures to obtain and preserve evidence for such proceedings should be taken.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Searches in Ukraine can be carried out if: (1) there is a ruling of the investigative judge for it rendered within a criminal proceeding (for the period of martial law in Ukraine, the search warrant can be granted by the head of the relevant prosecutor's office in cases where the investigative judge has no objective possibility to fulfil his powers), (2) in urgent cases related to the necessity to save life, property, or capture a suspect (if such search is not followed by immediate retrospective approval of the investigative judge, all evidence gathered in its course should be inadmissible).

The searches may be initiated by the investigator upon approval of the prosecutor or by the prosecutor. A copy of the court ruling (or decision by the head of the relevant prosecutor's office) should be provided to the company.

The search can be conducted within the term of validity of the decision and the scope and purpose outlined in it. The company is entitled to have its attorney present at the search and video record the search. If the above requirements are violated, the company may argue the inadmissibility of the evidence obtained.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Ukrainian law does not provide for the possibility of companies to enter into such or other types of agreements within criminal proceeding.

At the same time, criminal liability of companies in Ukraine (in a form of measures of criminal law nature) is rather limited. Generally, it applies only to certain criminal offences committed in the interest of the company and provided that the company's directors or other authorised representatives are convicted for the respective criminal offence.

Ukrainian law provides for two types of agreements that could be entered by individuals: (1) settlement agreement between a victim and a suspect/accused and (2) plea agreement between the prosecutor and a suspect/accused; and lists criminal offences subject to such agreements, requirements to and conditions of their conclusion. Both types of agreements require the approval of the competent court.

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Generally, the criminal liability in Ukraine is of individual nature. Thus, directors or other employees of the company can be held liable if they were involved in the commission of an offence or neglected their duties falling within the scope of their responsibility.

As an example, directors, depending on the gravity of criminal offence, can face: a fine with deprivation of the right to hold specific positions for up to three years and confiscation of property (for tax evasion); a fine with deprivation of the right to hold a particular position for up to three years (for contentious insolvency); a fine or deprivation of the right to hold specific positions for up to five years, corrective labours up to two years, or arrest up to six months (for unlawful dismissal or other gross violation of employment law); fines or limitation of freedom from two to four years or imprisonment, with or without confiscation of property (for basic bribery of public officials and officials of public sector enterprises).

Directors and other officers of the company could also be subject to administrative liability (typically, minor fines) for different violations in the course of the company's activity (e.g. violations of accounting rules, unfair competition, failure to submit information related to the Ultimate Beneficial Owner to the state registrar).

Generally, companies can be held liable (in a form of measures of criminal law nature) for certain criminal offences (e.g. bribery related offences, money laundering, interference with work of the judiciary) committed by their directors, other authorised representatives on behalf and in the interests of the company (i.e. benefiting the company). However, due to a number of legislative deficiencies and practical constraints, such measures are rarely applied in practice.

The penalties include fines and liquidation of the company along with confiscation of its property. Further, private companies have an obligation to compensate for all losses and the amount of undue advantage (unlawful benefit) received, or which could have been received because of the criminal offence. However, there is no mechanism for the latter in place. The fines are calculated based on the amount of undue advantage received by the entity due to the criminal offence and doubled. If it was not received by the company or its amount cannot be calculated, the courts may apply a fine within a range of approximately UAH 85,000 (circa US$2,300) to UAH 1,275 million (circa US$34,000) depending on the gravity of the relevant criminal offence.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

Ukrainian law provides the possibility for the reduction of a potential fine if the company took measures to prevent the criminal offence (e.g. implementation of a compliance system). However, as court practice of holding companies liable is very limited and in the absence of relevant guidance, the application of such provisions remains to be seen.

Also, if a bribery related criminal offence or money laundering is committed by an employee of the company for the company's benefit, the company may be responsible for the failure of its directors or shareholders to fulfil their obligations to prevent corruption. The availability of an efficient compliance system, including a robust risk assessment, should prevent the company from being fined. However, this approach was not tested in practice yet.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

Effective Ukrainian law does not oblige Ukrainian business to ensure that social and environmental standards are observed in their supply chain or comply with any specifics ESG-related disclosure standards, although provisions with respect to ESG-related reporting are in place.

In particular, the Ministry of Finance of Ukraine recommends that large companies (above 500 employees) include information on ecological (e.g. waste management, greenhouse gas emissions; energy consumption) and social (e.g.

labour protection and safety, respect for human rights) aspects of their activities into the management reports, filed along with financial statement.

The National Securities and Stock Market Commission advises to make impact of the companies on society and the environment clear to stakeholders. It provides that companies must disclose all material information that may reasonably be expected to have an impact on the price of their shares or the decisions of shareholders and markets. Further, in the annex related to ESG issues to Code of Corporate Governance, the above Commission, *inter alia*, recommends Ukrainian companies to fully comply with the elements of IFRS that require reporting on material sustainability issues and follow relevant EU standards.

The National Bank of Ukraine ("**NBU**") also requires banks to report on the ecological and social aspects of their activities. Further, according to NBU Sustainable Finance Development Policy 2025, it is planned, *inter alia*, to (i) develop the standards on disclosure of ESG-related information by banks and NBFIs; (ii) develop the requirements on environmental and social risk management by such institutions; (iii) setting the standards for evaluation and selection criteria for the projects to be funded, depending on their role in sustainable development.

Further developments in this sphere will be shaped by several factors, including the accession negotiations with EU.

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

On 6 September 2023 the Unified Portal of Whistleblowers' Reports in Ukraine ("**Portal**") was launched. The Portal should be accessible on a 24/7 basis, accepting, *inter alia*, anonymous reports. It should contain summaries of reports, data on their status and results of consideration, and information on assignment of whistleblower status. Whistleblowers will have access to above information of the Portal.

Also, in 2023 the first reward to be paid to whistleblower at the expense of the state budget was approved by the court in the attempted bribery case of a state agency official (the case is pending cassation review presently).

Considering that in December 2023, the EU decided to open accession negotiations with Ukraine, inviting the Council to adopt the negotiation framework, further strengthening of anti-corruption institutions and harmonisation of legislation with EU laws in this sphere is anticipated.

CONTACTS

ASTERS

Tel.: +380 44 230 6000

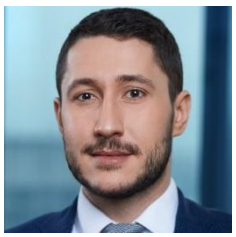
www.asterslaw.com

Sergiy Grebenyuk
Partner
Asters
E sergiy.grebenyuk@asterslaw.com

Sergiy heads Asters criminal law practice. He focuses on representing clients facing criminal cases and court procedures.

Sergiy has extensive experience in White Collar Crime cases, focuses on the management of internal corporate investigations of possible violations, anti-corruption and compliance issues.

Sergiy has deep knowledge of local anti-corruption and other compliance rules, understanding of local business environment and government's approaches, as well as broad experience in complex projects involving multinational companies and global policies.



Orest Stasiuk
Counsel
Asters
E orest.stasiuk@asterslaw.com

Orest focuses on criminal cases with international element, anti-bribery compliance work, internal investigations.

He has LLM in compliance field and practical background advising major Ukrainian and international blue chips across the wide range of industries on all types of compliance matters, internal investigations, fraud response, government investigations, enforcement actions.

Orest is Co-Head of Compliance Club at American Chamber of Commerce in Ukraine.

Oleksandr Volkov
Partner
Asters
E oleksandr.volkov@asterslaw.com

Oleksandr has over 12 years of experience in international commercial, investment and sports arbitration, cross-border litigation and corporate investigations.

He represents both state authorities and private companies and frequently advises foreign investors engaged in pre-arbitration negotiations with governments, alternative dispute resolution and fraud investigations.

Oleksandr also participated in multinational corporate internal investigations touching sensitive compliance issues, involving data privacy, anti-bribery and fraudulent practices.

Olha Yurchenko
Senior Associate
Asters
E olha.yurchenko@asterslaw.com

Olha has over 10 years of professional experience in the arears of WCC, compliance, internal investigations and regulatory issues. She has LLM in international legal studies and advices international and local clients on different anti-corruption, anti-money laundering, sanctions, and regulatory matters, with focus on criminal and compliance risks assessment.

Olha also handles complex internal investigations, assist clients with compliance due diligence. She has considerable experience across many sectors, including pharmaceuticals, media, banking and financial services, energy, real estate and construction.

United Kingdom

Hogan Lovells International LLP


Liam Naidoo


Arwen Handley


Olga Tocewicz


Reuben Vandercruyssen


Nick Roper

OVERVIEW

	Corporate Liability	Public Bribery	Commercial Bribery	Extraterritorial Applicability of Criminal Laws	Adequate Procedures Defence
Yes	X	X	X	X	X
No					

QUESTION LIST

1. Regarding the implementation of a whistleblowing system:

a) Are there any specific procedures that need to be taken into consideration once a whistleblower report triggers an internal investigation (e.g. for whistleblower protection)?

In general, English law does not require specific procedures to be followed if an internal investigation is commenced following the raising of concerns by a whistleblower. Employee protections, such as ensuring that an employee or worker who makes a protected disclosure is not subject to any detriment, and maintaining, as far as possible, confidentiality in relation to the whistleblower's identity should, as a matter of good practice, be incorporated into the firm's procedures.

However, there are specific requirements in relation to whistleblowing imposed by the UK's financial services regulators on certain regulated financial services firms, including requirements to adopt appropriate internal procedures for handling reportable concerns made by whistleblowers and to appoint a whistleblower's champion.

UK legislation (the Public Interest Disclosure Act 1998, which made changes to the Employment Rights Act 1996) provides whistleblower protection to an employee or worker who makes disclosures about a criminal offence, a failure to comply with a legal obligation, a miscarriage of justice, health and safety risks, risk or damage to the environment, or a "cover up" of any of the above matters. The employee must have a reasonable belief that the disclosure tends to show one or more of the listed concerns and is made in the public interest, and it must be made to an appropriate person (e.g. their employer, a lawyer or specified regulator).

b) Does the local law allow the use of group wide reporting systems instead of requiring local systems (e.g. in light of the interpretation of the European Commission in each group entity with more than 50 employees)?

The EU Whistleblower Directive has not been implemented in the United Kingdom. However, where companies in the United Kingdom have operations in the EU, they will need to consider whether the provisions of the Directive impact their operations in EU countries.

Where multinational companies maintain a single global whistleblowing framework, they will also need to take the provisions of the EU Whistleblower Directive into account. English law does not prevent the use of group-wide reporting systems.

---

2. Do the following persons/bodies have the right to be informed about an internal investigation before it is commenced and/or to participate in the investigation (e.g. the interviews)?

a) Employee representative bodies, such as a works council

b) Data protection officer or data privacy authority

c) Other local authorities

What would be the consequences of non-compliance?

a) In the United Kingdom, bodies such as works councils do not exist. There are, however, trade unions which depending on the industry and sector may be relevant to how an interview with an employee is planned and undertaken. Notwithstanding this, employee representative bodies such as trade unions are not automatically entitled to be informed about or participate in an internal investigation.

b) There is no specific obligation to notify the United Kingdom's data protection authority (the Information Commissioner's Office, "**ICO**"). However, the authority may need to be informed about certain internal security incidents, such as personal data breaches under the UK General Data Protection Regulation ("**UK GDPR**"). Additionally, the ICO has powers to request and obtain copies of materials created in the course of an internal investigation unless these are protected by privilege. In the event that an internal investigation relates to the processing of personal data, then the organisation's data protection officer should be made aware and involved in all relevant decisions relating to the matter. This officer is the 'relevant supervisory authority' that must be contacted within 72 hours of certain breaches of personal data. The ICO does not need to be notified of an internal investigation, subject to compliance with data privacy regulations and there being no significant risks to the protection of personal data.

c) Local authorities do not have the right to be informed about and/or to participate in an investigation. However, regulated financial services firms have certain ongoing notification obligations to relevant UK financial services regulators, and these obligations should be considered in each case.

---

3. Do employees have a duty to support the investigation, e.g. by participating in interviews? If so, is the company entitled to impose disciplinary measures if the employee refuses to cooperate?

Employees are under implied contractual obligations to follow the reasonable instructions of their employer and may also be under express obligations to cooperate with their employer and to disclose any wrongdoing. Therefore, employees could be required to participate in interviews and assist in an investigation. Failure to do so could result in disciplinary action being taken against them.

---

4. Does the taking of investigative steps potentially trigger any labour law deadlines or waive any rights to sanction employees? If so, how can this be avoided?

There is no specific timescale in which an employer must take action against an employee once an investigation has commenced. Failure to sanction an employee within a specific time will not waive the employer's rights. However, disciplinary action against an employee following an internal investigation should be commenced without undue delay. In relation to both disciplinary action and civil claims, and where appropriate, consideration can be given to whether or not further cooperation from the employee may assist the investigation.

In relation to claims arising as a result of investigative actions, the usual limitation periods under English law will apply.

---

5. Are there any relevant data privacy laws, state secret laws, or blocking statutes in your country that have to be taken into account before

a) conducting interviews?

The provision of documents before an interview may give rise to data protection issues, particularly where multiple jurisdictions are involved and other individuals' personal data is present in documents or emails being provided. It is important that personal data is only disclosed to or by an interviewee where necessary and a lawful basis for processing has been satisfied. Particular care should be taken in the disclosure of special category data, which is subject to additional protections under both UK and EU data protection laws.

b) reviewing emails?

The review of emails as part of an investigation should comply with the safeguards set out in the Data Protection Act 2018 ("**UK DPA**") and the UK GDPR. Employees' emails may typically be reviewed as part of the investigation. The collection and use of personal data in this context must be kept to the minimum amount necessary, in accordance with the principle of data minimisation.

Employee consent is likely not required to review business emails in the context of an investigation, although data protection requirements should be assessed before any material is provided to third parties. Individuals involved in an investigation generally have the right to request copies of the data collected pertaining to them.

c) collecting (electronic) documents and/or other information?

The collection of documents and/or other information is subject to data protection laws and will apply to documents collected which contain personal information or data.

d) analysing accounting and/or other business databases?

Data protection laws will apply to the extent that the databases contain personal data. If the databases do not contain personal data, obligations under the UK DPA and the UK GDPR do not arise.

Many organisations have data protection agreements in place (also known as model clauses or a Binding Corporate Rules policy) that permit the flow of information within an organisation. Specialist legal advice should be sought to assess whether such agreements are sufficient under the UK GDPR and the UK DPA.

---

6. Before conducting employee interviews in your country, does the interviewee have to

a) receive written instructions?

There is no specific legal requirement for the employee to receive written instructions about the matters the interview will cover.

b) be informed that they do not have to make statements that could potentially be self-incriminating?

There is no specific legal requirement to inform the employee that they have a right not to incriminate themselves as part of an internal investigation.

c) be informed that the lawyer attending the interview is the lawyer of the company and not the lawyer of the interviewee (so-called "Upjohn warning")?

There is no specific legal requirement to deliver an "Upjohn warning" at the start of an internal investigation interview that does not have a U.S. context. In practice, such warnings should generally be given and are frequently used in UK interviews.

d) be informed of their right to have their own lawyer attend the interview?

There is no specific legal requirement that an employee should be informed that they have the right to be accompanied by a lawyer.

e) be informed of their right to have a representative from the works council (or other employee representative body) attend the interview?

There is no specific legal requirement to allow an employee to be accompanied to an internal investigatory interview by a works council, trade union or other employee representative and it would be unusual for this to be permitted.

f) be informed that data may be transferred to another country (in particular to the United States)?

Cross-border data transfers are a complex area. Specific advice should be sought to ensure compliance with the UK GDPR. The UK is reforming data transfer rules under the Data Protection and Digital Information Bill which proposes amendments to the UK's data protection framework including the UK DPA and UK GDPR. However, the law is still in draft, and at the time of writing we do not know the final form it will take. If the transfer does not include personal data, then it will not fall within the scope of the UK GDPR and may be freely transferred subject to other laws. On 28 June 2021, the United Kingdom gained an adequacy decision from the European Economic Area, so personal data may flow freely between the United Kingdom and the European Union. International transfers of personal data outside of the European Economic Area (including to the United States) are, however, subject to certain rules under the UK GDPR and may require additional safeguards to be implemented.

In July 2023, the European Commission adopted its adequacy for the EU-U.S. Data Privacy Framework, concluding that transfers under the framework are protected with an essentially equivalent level of protection as under the EU GDPR. The UK Government then adopted their own adequacy decision to allow transfers of personal data under the DPF, creating a UK extension to the framework. However, only transfers to U.S. organisations that have self-certified under the framework will be protected. The old framework for transfers, the U.S.-EU Privacy Shield framework, was invalidated in July 2020 by the CJEU in the case of Schrems II (Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems, Case C-311/1). Standard contractual clauses and other supplementary safeguards may need to be put in place for transfer to organisations that are not signed up to the framework before exporting any data outside the European Economic Area. There may be derogations for specific situations, so legal advice must be sought.

When personal data is collected from the data subject, the data subject must be informed whether the data is being transferred to a non-European Economic Area country or international organisation. This is generally achieved through an organisation's privacy notice, which needs to be brought to the data subject's attention.

g) sign a data privacy waiver?

The tightening of data protection under the UK GDPR will likely necessitate providing an employee with a privacy notice which explains, amongst other things, the legal basis for processing their personal data, the purpose for this processing, and any related rights in relation to their data which they may possess, such as a right to access, or rectify this information. This notice is often provided by employers to staff on a general basis (rather than in relation to specific investigations).

h) be informed that the information gathered might be passed on to authorities?

There is no specific legal requirement to inform the employee that information might be passed on to authorities (unless the investigation has a U.S. context), but it would be good practice to do so.

i) be informed that written notes will be taken?

There is no specific legal requirement to inform the employee that written notes will be taken, but it would be good practice to do so.

7. Are document hold notices or document retention notices allowed in your country? Are there any specifics to be observed (point in time/form/sender/addressees etc.)?

A company should take immediate steps to preserve all relevant evidence. A document hold notice should be sent to relevant custodians identifying the categories of documents that should be preserved.

It is important that all documents identified as potentially relevant are isolated and remain secure throughout the investigation.

---

8. Can attorney-client privilege be claimed over findings of the internal investigation? What steps can be taken to ensure privilege protection?

English law recognises the concept of legal advice privilege between a lawyer and client, which broadly reflects and is comparable to that of attorney-client privilege in the United States. Legal advice privilege applies to confidential communications between a lawyer and their client for the dominant purpose of giving or obtaining legal advice. Legal advice privilege extends to documents which evidence such communications, including relating to the findings of the investigation.

When assessing legal advice privilege, the "client" is only those employees and officers charged with obtaining legal advice. Communications involving employees not expressly tasked to seek advice, and all communications with third parties (such as forensic accountants) are not protected; even where communications are necessary to inform lawyers of relevant events or information. Note that, in particular, file notes of investigation interviews may not always attract legal advice privilege, even if taken by a lawyer.

A distinct category of legal professional privilege exists through litigation privilege. Litigation privilege can be claimed over any confidential communication between a client and their lawyer, or between either of them and a third party, where the sole or dominant purpose of the communication is for use in actual, pending or contemplated litigation. Litigation privilege only applies if litigation is reasonably contemplated (i.e. there is the possibility (which is more than merely fanciful) of litigation), and communications or documents must be created for the dominant purpose of that litigation. Litigation privilege, therefore, may not apply during purely internal investigations unless and until evidence is discovered which indicates potential criminality or civil liability. Actual wrongdoing need not be established for litigation privilege to apply: the question of whether litigation privilege applies should be carefully considered in each case.

---

9. Does attorney-client privilege also apply to communication with in-house counsel in your country?

Generally, both legal advice privilege and litigation privilege apply equally to in-house and external counsel, save for competition investigations by the European Commission in which internal advice is not considered (by the Commission) to be privileged.

As a general matter, communications may not be deemed privileged where in-house counsel communications contain both legal and business/commercial information. To ensure the maintenance of privilege, communications for the purpose of obtaining legal advice should be kept entirely separate to those of a commercial or business nature. Where this is not practicable, advice should be sought on the best ways of maintaining privilege in the in-house context.

---

10. Are any early notifications to any of the parties below required when starting an investigation? E.g. to

a) Insurance companies (D&O insurance etc. to avoid losing insurance coverage)?

It is likely to be a condition of certain insurance policies that the insurer is notified of issues that may give rise to a claim, which can include issues leading to, or arising in, an internal investigation. Each individual policy should be reviewed.

b) Business partners (e.g. banks and creditors)?

It is unlikely to be a condition of agreements with business partners that they are notified of issues which have given rise to an internal investigation. However, relevant agreements should be checked, particularly if the matters under investigation could impact or involve the business partner.

c) Shareholders?

If the allegations are serious and could expose the company or directors to liability or reputational damage, the board of the company may need to be notified (depending on the escalation requirements and thresholds of the company in question) but not necessarily shareholders.

Companies whose securities are admitted to trading on a market operated by the London Stock Exchange are subject to ongoing disclosure obligations. Publicly listed companies must issue a market announcement (without delay) of any inside information, which could include, for example, a major new development (including findings in – or even, in some cases, the start of – an investigation that may lead to a substantial share price movement).

d) Authorities?

Advice should be taken before notifying any regulatory authority about an internal investigation, especially where there are concerns of money laundering or other criminal offences.

Generally, there is no positive obligation to report a crime. The main exception relates to a suspicion of money laundering, where an obligation may arise if the person or company is in the 'regulated sector' (including, for example, Financial Conduct Authority ("**FCA**") regulated firms, solicitors and accountants). Companies or persons not within the regulated sector are under less onerous obligations, but nonetheless must report money laundering if concerns exist that they are involved in an arrangement involving criminal property, for example. Individual regulators, such as the FCA, may have their own notification requirements.

---

11. Are there certain other immediate measures in your country that need to be taken or would be expected by the authorities once an investigation has started, e.g. any particular immediate reaction to the alleged misconduct?

A company should, as a first step, preserve all documents and materials that may be relevant to any criminal or regulatory investigation.

It is a criminal offence to destroy, falsify, conceal, or dispose of relevant documents when a person knows or suspects an investigation of serious or complex fraud is already being, or is likely to be, undertaken by the police or the Serious Fraud Office ("**SFO**"). If unlawful conduct has ceased and the company was aware or suspected that it possessed funds obtained from the conduct, but it failed to take any action in respect of those funds, the company could commit a money laundering offence.

Those operating in the regulated sector should also be mindful of the risk of committing a "tipping off" offence under the Proceeds of Crime Act 2002. The term refers to the act of alerting someone that they are under investigation or that their financial activities are being scrutinised by law enforcement or regulatory authorities.

---

12. Do local prosecutor offices generally have concerns about internal investigations or do they ask for specific steps to be observed?

Historically, UK authorities have not generally objected to internal investigations so long as they did not hinder a criminal investigation. However, a more formalised procedure appears to be emerging, especially following the Cooperation Guidance issued by the SFO in August 2019 (the "**Guidance**"). The Guidance sets out various factors to be adhered to by corporations hoping to receive a recommendation for a Deferred Prosecution Agreement ("**DPA**").

Expectations of the SFO in relation to privilege are one example. The Guidance states that corporations will not be penalised for choosing not to waive privilege for internal investigation documents or interviews, but will not receive

the corresponding cooperation credit towards a DPA. Further, claims to privilege should now be independently verified by counsel to ascertain that legal professional privilege has been applied properly.

The Guidance further suggests consultations with the SFO prior to undertaking interviews – a tighter and more procedural requirement than before.

The Guidance also sets out indicators of 'good practice'. These are extensive and are not considered to be exhaustive. In addition, the Guidance is not always rigorously applied by the SFO in practice. Advice should be sought prior to any investigation to understand these intricacies properly.

Other regulators may have different requirements. In some cases, for example, the FCA may wish to interview employees before the company's internal investigators do so.

---

13. Describe the legal prerequisites for search warrants or dawn raids at companies in your country. In case the prerequisites are not fulfilled, can gathered evidence still be used against the company?

Authorities that investigate corporate crime in the United Kingdom may conduct dawn raids of business or residential premises under a search warrant issued by a court. When a raid is carried out under a warrant, the authority may use reasonable force to gain entry to the premises.

Legally privileged material cannot be seized unless it was created with the intention of the furtherance of a crime (the crime-fraud exception). If legally privileged material cannot be separated from non-privileged material, it can be seized but must first be reviewed for privilege by an independent lawyer before the authority can review it.

The Competition and Markets Authority may conduct a dawn raid of business premises without a warrant where it reasonably suspects that a cartel offence has been committed.

If there are significant defects in the process of obtaining a warrant or authorising or executing a raid, the raid can be challenged by judicial review in the courts. If it is rendered unlawful, the raid may be deemed a civil or criminal trespass. Any material seized during the raid could become inadmissible.

---

14. Are deals, non-prosecution agreements, or deferred prosecution agreements available and common for companies in your jurisdiction?

Non-prosecution agreements are not available in the United Kingdom. DPAs (for certain offences) have been available in England, Wales and Northern Ireland since 2014 and must be approved by the court. They are available to the Crown Prosecution Service and the SFO.

A prosecutor may invite a suspect into DPA negotiations where it determines that the full extent of the corporate offending has been identified and the public interest is served by a DPA.

A company will be formally charged with the criminal offence, but such proceedings will be suspended for a period defined by the terms of the DPA. If there is full compliance with the DPA, the criminal proceedings will be formally discontinued at the end of the period. Criminal proceedings will resume if the DPA is breached beyond remedy. At the time of writing, there have been 12 approved SFO DPA agreements.

The Guidance notes that to secure favourable consideration, such as a DPA, a corporation must adopt a genuinely proactive approach to cooperation and may be required to have practices which go above and beyond what the law requires, such as waiving privilege (as previously outlined).

---

15. What types of penalties (e.g. fines, imprisonment, disgorgement, or debarment) may companies, their directors, officers, or employees face for misconduct of (other) individuals of the company?

Penalties for individuals in relation to criminal offences include imprisonment, fines, disgorgement, and compensation orders. Individuals can also be disqualified from being a director of a company for up to 15 years. Companies may be subject to mandatory or discretionary exclusion from public tendering for up to five years.

Certain regulatory authorities can impose additional penalties. For example, the FCA can prohibit authorised firms from undertaking specific regulated activities for up to 12 months and impose fines on firms and individuals.

---

16. Is it possible to have penalties against companies, their directors, officers, or employees reduced or suspended if the company implements an efficient compliance system following the alleged misconduct; or if the company already had an efficient compliance system in place prior to the alleged misconduct?

A corporation may benefit from a complete defence against Section 7 of the Bribery Act (for the strict liability offence of failing to prevent bribery) if it can be shown that it had 'adequate procedures' in place to prevent bribery. In practice, this requires a risk-based review to be undertaken on a regular basis to ensure that processes are efficient and proportionate to the nature of the corporate function, areas and jurisdictions of operation, and the profile and size of the corporations.

If such risk-based processes are maintained, 'adequate and sufficient' protocols will provide a complete defence to liability under Section 7.

This exemption is likely only to apply where controls and procedures are implemented prior to the alleged misconduct, although the Bribery Act doesn't provide specific guidance on this point.

An analogous regime also exists for the corporate criminal offence of failure to prevent the facilitation of tax evasion, pursuant to the Criminal Finances Act 2017. A corporate will have a complete defence if it can demonstrate that it had in place reasonable procedures to prevent the misconduct in question.

The Economic Crime and Corporate Transparency Act 2023 further created a corporate offence of failure to prevent fraud. Again, this provides corporates with a "reasonable procedures" defence. This new law is expected to come into force in 2024.

For all other criminal offences falling outside of the "failure to prevent model", the existence of an efficient compliance regime will likely be relevant to whether it is in the public interest to prosecute a corporate, and/or sentencing.

Specialist legal advice should be sought in this area due to the complexity of factors necessary to be considered on an ongoing basis.

---

17. Are there any specific Environmental, Social and Governance ("ESG") requirements in your jurisdiction? If so, which ones? Are authorities actively prosecuting ESG related cases?

The UK has a well developed and nuanced ESG legislation regime, with a number of important domestic laws and regulations, as well as those designed to mirror EU regulations and directives. This is no single defining piece of legislation, with ESG requirements for companies and individuals often contained within larger pieces of legislation. For example, the Companies Act was recently amended to mandate large corporates (over £500 million in revenue or more than 500 employees) to include sustainability and other non-financial information in their annual reports. Failure to report can result in significant fines. In 2015, the UK was the first country to enact legislation requiring companies to report on steps they have taken to prevent modern slavery and trafficking in their business and supply chains.

Further, companies incorporated, or operating in the UK can expect to be increasingly subject to legislation requiring them to conduct extensive due diligence across their supply chains for human rights abuses, bribery, pollution, and many other issues. Alongside legislation pending in the EU (The EU Corporate Sustainability Due Diligence Directive), which will create supply chain due diligence requirements for large UK companies operating in EU countries, supply chain due diligence legislation is currently under discussion in the UK, although there are currently no formal government proposals on the topic. There are a host of other, more specific pieces of legislation and other rules, such as the Modern Slavery Act (as referenced above), deforestation risk regulations made under the Environment Act, the Worker Protection Bill, and requirements with respect to corporate disclosures aligned

with the Recommendations of the Task Force on Climate Related Financial Disclosures, that will also place ESG obligations on companies operating in the UK.

The UK's common law system also allows judges to clarify legal requirements, and set precedent for future decisions. There are a number of interesting cases currently ongoing, which will likely impact and clarify the enforcement of ESG legislation in the jurisdiction.

For more information, please refer to our online guides, including the Global Vision Tool, found on Hogan Lovells dedicated ESG site (https://engagepremium.hoganlovells.com/resources/esg-global-vision).

---

18. Please briefly describe any investigations trends in your country (e.g. recent case law, upcoming legislative changes, or special public attention on certain topics)?

The last year has brought with it significant changes in the leadership teams of the UK's major law enforcement agencies. In March 2023, the FCA appointed two new executive directors to co-lead its Enforcement and Market Oversight division. In September 2023, Stephen Parkinson was announced as the new Director of Public Prosecutions and head of the Crown Prosecution Service the Attorney General. Finally also in September 2023 Nick Ephgrave QPM, a former assistant commissioner in the Metropolitan Police, replaced Lisa Osofsky as director of the SFO.

In October 2023, the Economic Crime and Corporate Transparency Act 2023 ("**ECCTA**") received Royal Assent. Most significantly, the ECCTA:

- Created a new corporate criminal offence – the "failure to prevent fraud". The new law creates a strict liability offence which makes it an offence for a large company or partnership to fail to prevent fraud by a person associated with it. The only defence available will be that a company can show it had reasonable procedures in place to prevent fraud. Guidance as to reasonable procedures is expected from the government this year, before the offence then comes into effect;
- Included a new legal test for attributing criminal liability to companies. The previous test for attribution (based on the common law "identification principle") resulted in a narrow definition that made it hard to hold companies to account. The ECCTA extends criminal attribution to the actions of "senior managers", a significantly wider group than the previous position (those deemed to be the "directing mind and will" of a company). It significantly lowers the bar for attributing corporate liability to organisations;
- Expanded the SFO's pre-investigative powers, which are no longer limited to suspected cases of international bribery and corruption. The SFO is not permitted to compel individuals and companies to provide information at the pre-investigation stage in all SFO cases.

Finally, whilst DPAs have historically been utilised exclusively by the SFO, the UK's Crown Prosecution Service's recent DPA with Entain plc has demonstrated that such disposals are being added to the arsenal of other prosecuting agencies. Notably, it was the UK's tax agency, HM Revenue & Customs ("**HMRC**") who was responsible for the investigation behind the £615 million DPA. HMRC has also reported this year that it had opened nine investigations into businesses suspected of failure to prevent the facilitation of tax evasion and was considering several more.

CONTACTS

Atlantic House
Holborn Viaduct
London EC1A 2FG
United Kingdom

Tel.: +44 20 7296 2000
Fax: +44 20 7296 2001
www.hoganlovells.com

Liam Naidoo
Partner
Hogan Lovells London
T +44 20 7296 2909
E liam.naidoo@hoganlovells.com

Liam is a Partner in Hogan Lovells' Investigations practice focusing on business crime, fraud, bribery and corruption, Liam's practice particularly focuses on the management of internal investigations following allegations of corrupt activity of employees, agents and other third parties. This experience allows him to give targeted advice to clients on anti-corruption compliance measures. In addition, Liam has significant experience in Commercial Court litigation arising out of complex fraud and bribery actions.

Arwen Handley
Partner
Hogan Lovells London
T +44 20 7296 2810
E arwen.handley@hoganlovells.com

Arwen advises financial, corporate and government clients on regulatory enforcement matters, internal investigations, and litigation, with a particular focus on complex matters. Prior to joining Hogan Lovells, Arwen worked for over 17 years in total in the in-house litigation and investigations teams at UBS, Bank of America and Morgan Stanley, including as head of the global Group Investigations Governance, Reporting and Whistleblowing Management function at UBS, Head of the EMEA Litigation group at UBS and Head of the EMEA and Asia Litigation & Regulatory Inquiries group at Bank of America. Arwen has extensive experience of handling crisis situations and the regulatory and litigation activity which often follows. Arwen has handled cases and investigations in numerous jurisdictions across the world, and has worked in London, New York, Washington D.C. and Hong Kong during her career.

Olga Tocewicz
Counsel
Hogan Lovells London
T +44 20 7296 5956
E olga.tocewicz@hoganlovells.com

Olga is an experienced criminal litigator, specialising in corporate and white collar crime investigations and defence.

Olga has extensive experience of representing both corporates and individuals, in multi-jurisdictional investigations, whether internal or with law enforcement involvement, in respect of allegations of fraud, bribery and corruption, money laundering, insider trading and other financial misconduct. Her practice also includes business integrity compliance advisory work including risk assessment and supply chain due diligence advisory work, following recent in-house experience gained as Senior Counsel - Business Integrity (Anti-Bribery) at a leading multi-national retailer.

Reuben Vandercruyssen
Senior Associate
Hogan Lovells London
T +44 20 7296 5990
E reuben.vandercruyssen@hoganlovells.com

Reuben is a Senior Associate in Hogan Lovells' Litigation Group and has wide-ranging experience of commercial disputes and internal investigations into allegations of unlawful or corrupt acts by employees, agents and third parties. Reuben advises large corporates on anti-corruption compliance, particularly in the context of mergers and acquisitions in high-risk jurisdictions. Reuben was part of the team that was successful in securing a landmark victory at the Court of Appeal for client ENRC against the UK Serious Fraud Office in a historic decision which will have lasting implications for the law of privilege in the UK. Reuben also advises clients on protective measures and policies to ensure compliance with the UK Bribery Act and other corruption legislation, with particular expertise in issues arising in the public procurement context.

Nick Roper
Associate
Hogan Lovells London
T +44 20 7296 7119
E nick.roper@hoganlovells.com

Nick is an Associate in the Corporate litigation, Fraud and Investigations group. Nick's experience includes advising BTA Bank in its long-running litigation and in relation to their international asset recovery strategy. In additional he has assisted in advising an American company in relation their international internal investigation into potential sanction breaches.

Nick has worked in house, on secondment, in the disputes resolution team at Standard Chartered Bank and a large telecommunications client. He is active in the firm's pro bono initiatives and successfully represented a client in their Employment Support Allowance appeal before the First-Tier Tribunal.

European Investigations Guide 2024

Multinationals face a variety of questions when confronted with an internal investigation. Especially in Europe, cross-border investigations can be challenging to navigate as every jurisdiction has its unique rules.

The guide covers 34 jurisdictions and has been updated to reflect new laws and trends. It is designed to provide you with a quick reference on some of the most pressing issues that arise during an internal investigation. This includes questions on whistleblower protection, data transfer, employee interviews, notification requirements, dawn raids, and attorney-client privilege.

In addition, you will find practical guidance on cross-border investigations, data privacy investigations, anti-money laundering, cartel investigations, and export and sanctions control.

With contribuitions from:

A&L Goodbody
ASTERS
Babić & Partners
BORENIUS
Camilleri Preziosi
Cerrahoğlu
Chrysses Demetriades
COBALT
Ellex
Gasser Partner
HAVEL & PARTNERS
Hogan Lovells
Kalo & Associates
Kambourov & Partners
KINSTELLAR
KNOETZL
Kromann Reumert
Lutgen + Associés
Mareş & Mareş
NORDIA
Ovvadias S. Namias
SENICA
taormina
Uría Menéndez
Wikborg Rein