

## COUNTRY UPDATE-Latvia: GDPR

Mar 22 2018 [TRRI commissioning team](#)



The [General Data Protection Regulation](#) (GDPR) comes into force across the European Union on May 25, 2018. Many of its provisions contain "opening clauses" enabling member states to introduce national laws that take GDPR requirements further.



This article provides an oversight of the relevant law in Latvia by [Sarmis Spilbergs](#) and [Ingrida Stelmane](#) of [Ellex Klavins](#).

### GDPR basics

This section briefly outlines some core GDPR provisions.

**Application:** The GDPR applies to EU-based controllers and processors of personal data. It also applies to non-EU bodies where they process an EU resident's personal data in relation to offering them goods or services or the behaviour of individuals within the EU is being monitored.

**General Principles:** Set in Article [5.1](#). Personal data must be processed "lawfully, fairly and in a transparent manner". Among additional requirements, processing must be limited to a specified, explicit and legitimate purpose, the data must be accurate and processed in a manner that ensures it appropriate security.

Article [5.2](#): The person controlling the data is responsible for, and must demonstrate compliance with the [5.1](#) requirements.

**Legal Bases:** Article [6](#). There are six legal bases for data processing. These include compliance with a legal obligation, legitimate interest and, subject to conditions in article [7](#), consent of the subject.

**Rights of data subjects:** Articles [12-23](#). These include right to be informed, to object, of data access, rectification, portability and erasure.

**Data Protection Officer (DPO):** Article [37](#). Where a data controller or processor's core activities require 'regular and systematic monitoring of data subjects on a large scale' they must appoint a DPO.

**Impact Assessments:** Article [35](#). Before a data controller conducts processing that presents a high risk to people's rights and freedoms, in particularly using new technologies, it must carry out a data protection impact assessment (a DPIA).

1. What pre-GDPR national data protection or processing legislation did Latvia have and how did it compare to the basic Data Protection Directive 95/46/EC requirements?

Data Protection Directive 95/46/EC requirements in Latvia are implemented through the Personal Data Protection Law (Fizisko personu datu aizsardzības likums), applicable until May 25, 2018. It has almost in direct wording implemented the Data Protection Directive's requirements into national legislation. Only a few deviations or national specifics can be identified.

During this firm's practice it has been identified that in terms of transparency about data processing the current law is less stringent. Namely, currently Latvian law requires that only information about controller and purpose of processing must be provided upfront to data subject, whereas all other information must be provided only with request of data subject. It is noted that in other countries across EU more information had to be provided upfront, for example, also on legal basis for processing, the right to access and rectification, right to withdraw consent, etc. Thus, in other EU countries the approach was similar to GDPR art 12 requirements, thus along with GDPR the transparency requirements in Latvia especially will need to be revised, whereas in other EU countries the notices may already have the required information in them.

Another local specific, expressly permitted by the Directive 95/46/EC, was the situations that required prior consultation/registration with local data protection authority Various approaches by each EU country to notification and registration requirements was one of the reasons to abolish such requirements all together and choose Regulation as the form for new data protection framework in EU, instead of revision of Directive.

Besides the above mentioned, substantively and in other terms the current law is almost identical to Directive 95/46/EC.

2. What will happen to existing national data law when the GDPR comes into force?

The existing Personal Data Protection Law will be abolished and replaced by another law, i.e. draft Personal data processing

### Related content

#### News by subject

- ▶ [Data protection and privacy](#)
- ▶ [Operations, systems and controls](#)
- ▶ [Regulatory oversight](#)
- ▶ [Browse all subjects](#)

#### News by country

- ▶ [Latvia](#)
- ▶ [View country guides](#)

#### Related rulebooks

- [EU Regulations](#)
- ▶ [2016/679 — General Data Protection Regulation](#)

### Search

Subject browser →

Advanced →

### Most read articles

- ▶ [Deutsche Bank tightening anti-financial crime and compliance controls, says CEO](#)
- ▶ [FCA set culture as a "hot topic" yesterday, referred to in five publications this week](#)
- ▶ [FCA makes crucial changes to supervision, enforcement but grey areas remain, say lawyers](#)
- ▶ [Singapore fines Standard Chartered entities \\$4.9 million for money laundering breaches](#)
- ▶ [SEC sets \\$83 million whistleblower record in Merrill awards; new curbs may limit future payouts](#)

### Message boards

Show all messages

**NEW** [Steward](#)  
General Discussion  
1 post – [1 new](#) (last post Mar 22, 2018)  
Very few enforcement outcomes, staff leaving in th...

[SEC Liquidity Rules Updat](#)  
General Discussion  
1 post (last post Mar 15, 2018)  
New SEC liquidity rules

[Little or no sympathy](#)  
General Discussion  
1 post (last post Mar 14, 2018)  
I have relatively little sympathy for these people...

Add a post →

More messages →

### Reference Library

- ▶ [Practitioner's Guide for Broker-Dealers](#)
- ▶ [The MLRO Handbook](#)
- ▶ [The Compliance Handbook](#)

law (Personas datu apstrādes likums).

3. Which regulator will supervise the GDPR and have there been any indications of how it will approach oversight and enforcement?

The national supervisory authority will be the Data State Inspectorate (Datu valsts inspekcija), which is the direct successor of the national supervisory institution for data protection already established. It has been noted that the Data State Inspectorate will follow the principle "consult first" at least in the year 2018, and only from 2019-2020 it will start to enforce GDPR more actively, including penalize GDPR non-compliant controllers and processors. Furthermore, it has stated that only malicious and intentional GDPR breaches will be penalized, as the main intention is to achieve a high level of GDPR requirement understanding and compliance within data controllers and processors rather than simply penalizing for every breach detected.

4. Any new national legislation that extends GDPR requirements been introduced or planned?

The text of the new draft law – Personal data processing law (Personas datu apstrādes likums) – has been made publicly available and introduced in the Meeting of State Secretaries on October 12, 2017, and further reviewed in the Committee of Cabinet of Ministers just recently – on February 27, 2018. These are the first of legislative stages – the draft law will have to be reviewed by the Cabinet of Ministers and further approved in 3 Parliament hearings.

This draft law does not extend any GDPR requirements, but mostly covers institutional changes relevant for the Data State Inspectorate functioning. It also makes use of the GDPR "opening clauses", for example, regarding child consent in relation to information society services (the minimum age a child can give his/her consent have been set to 13 years). The draft law also makes use of the typical/expressly recognized derogations, for example, for data processing for purposes of journalism, for data processing by law enforcement authorities, for historical and statistical research purposes and others.

Finally, it can also be mentioned that the draft law specifies that data subjects may request information about their data processing by the controller in relation to the last two years and also obliges controllers to store log data (i.e. information who and when has accessed the data on controllers systems) for at least 1 year. The GDPR is not as specific in this regard. Draft law also foresees that controllers, where required, may choose to appoint either a data protection officer that complies with GDPR requirements, or appoint one who has taken exam held by Data State Inspectorate. It suggests that controllers that will have DPOs who have taken the exams may be under less scrutiny than those who have not. However, only the enforcement practice will show whether such fear is founded.

5. Any other legal considerations around data processing that financial services firms should be aware of?

There are no specific rules in the draft law addresses particularly at financial services firms. Accordingly, Latvia does not take sector specific approach in implementation of GDPR.

- MIFID Survival Guide
- The Insurance Practitioner's Guide

#### Comment on this article

Subject\*

Name or pseudonym\*

Message\*

Submit Message