Datu aizsardzības aspekti, ieviešot iekšējo trauksmes celšanas sistēmu

2019. gada 1. maijā stājies spēkā Trauksmes celšanas likums (turpmāk – likums), kura mērķis ir veicināt, lai sabiedrības interesēs tiktu celta trauksme par pārkāpumiem un vienlaikus tiktu nodrošināta trauksmes cēlēju pienācīga aizsardzība. Cita starpā likums paredz arī izveidot iekšējo trauksmes celšanas sistēmu visām publisko personu institūcijām un privāto tiesību juridiskajām personām (uzņēmumiem), kurās ir vairāk nekā 50 nodarbināto, nodrošinot iespēju nodarbinātajiem iekšēji ziņot par pārkāpumiem.

Nodrošinot iespēju ziņot par pārkāpumiem, uzņēmums vai publiskā institūcija apstrādā personas datus gan par ziņotāju, gan personu, par kuru ziņots, tādējādi kļūstot par datu pārzini Vispārīgās datu aizsardzības regulas (turpmāk – VDAR) kontekstā, kas paredz ievērot noteiktas prasības attiecībā uz datu apstrādi. Šajā rakstā apskatītas galvenās prasības, kas uzņēmumiem kā datu pārziņiem ir jāizvērtē un jāņem vērā no datu aizsardzības puses, ieviešot iekšējo trauksmes celšanas sistēmu: kāda sistēma – anonīma vai konfidenciāla – būtu jāparedz, kāda informācija ir jāsniedz datu subjektiem un kā nodrošināt ziņojumu aizsardzību.

Anonīma vai konfidenciāla ziņošana

Ieviešot iekšējo trauksmes celšanas sistēmu, viens no pirmajiem jautājumiem rodas, kā pareizāk būtu nodrošināt trauksmes cēlēja identitātes aizsardzību, lai izpildītu likuma pienākumus. Vai ieviest anonīmu iekšējo ziņošanas sistēmu vai pieprasīt, lai trauksmes cēlējs norāda savus identitātes datus? Sākotnēji var šķist, ka, lai nodrošinātu datu minimizācijas prasības, pareizāk būtu ieviest anonīmu ziņošanas sistēmu, taču šāda pieeja var ietekmēt iegūto datu kvalitāti un spēju izpildīt likuma mērķus.

Viens no likuma mērķiem ir nodrošināt pienācīgu trauksmes cēlēju aizsardzību. Lai tas būtu iespējams, ir ▶

Ilustrācija: © freshidea – stock.adobe.com

JURISTA PADOMS

nepieciešams zināt trauksmes cēlēja identitāti, tādējādi var secināt, ka likumdevējs ir paredzējis, ka trauksmes cēlēja identitāte ir zināma, un **anonīmas ziņošanas sistēmas ieviešana nebūtu ieteicama, jo tā nespētu izpildīt likumā paredzēto mērķi.** Papildus jānorāda, ka identificējams ziņojums nodrošina arī atbildību par sniegto ziņojumu (ziņotājs būs ieinteresēts sniegt tikai patiesu informāciju), kā arī sadarbošanās iespējas, lai iespējamo pārkāpumu būtu vieglāk izmeklēt.

Likums neaizliedz apstrādāt anonīmus ziņojumus. Noteiktos gadījumos trauksmes cēlējam var šķist, ka, atklājot savu identitāti, tas izjutīs negatīvas sekas, neskatoties uz likumā paredzēto aizsardzību, tādēļ tas var vēlēties sniegt ziņojumu anonīmi. Tādējādi uzņēmuma iekšējā procedūrā var paredzēt, ka ir iespēja iesniegt ziņojumu arī anonīmi, taču tad ir skaidri jānorāda, ka šo ziņojumu izskatīs atbilstoši iespējām un personai netiks nodrošinātas likumā paredzētās aizsardzības garantijas. Dažkārt uzņēmumiem rodas jautājums, vai šādu iespēju ir vērts paredzēt, ņemot vērā, ka tas varētu palielināt ziņojumu skaitu. Tas ir jāizlemj katram uzņēmumam pašam, bet jāņem vērā, ka **iekšējās trauksmes celšanas sistēmas mērķis ir pēc iespējas mēģināt risināt radušās problēmas uzņēmumā iekšēji un novērst, ka informācija par iespējamo pārkāpumu rada publiskas sekas.** Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likuma 7. pants paredz, ka kredītiestādēm, finanšu iestādēm un citiem attiecīgā likuma subjektiem ir jāizveido iekšējās kontroles sistēma, kas paredz nodrošināt anonīmu ziņošanu par attiecīgā likuma pārkāpumiem, ja, ņemot vērā likuma subjekta darbinieku skaitu, šāds ziņošanas veids ir iespējams. Šādā gadījumā attiecīgajiem uzņēmumiem nebūtu tiesības atteikt izskatīt ziņojumu tikai tādēļ, ka tas ir iesniegts anonīmi.

Pārredzamības principa izpilde

Trauksmes celšanas likums cita starpā paredz, ka par iekšējo trauksmes celšanas sistēmu nodarbinātais ir jāinformē un tam jānodrošina viegli pieejama informācija par šo sistēmu, piemēram, uzņēmuma mājaslapā, iekšējā tīklā, pie atbildīgās personas utt. Saņemot un izvērtējot trauksmes cēlēja ziņojumu, tiek apstrādāti personas dati, tāpēc ir jāievēro pienākums nodrošināt personas datu apstrādes pārredzamību jeb atbilstoši VDAR 13. pantam ir jānorāda, kā tiks apstrādāti personas dati. Šī informācija var tikt norādīta jau iepriekš veidotā uzņēmuma privātuma politikā, uzņēmuma iekšējos noteikumos, speciāli izstrādātā trauksmes celšanas sistēmas politikā vai citā dokumentā, kamēr tiek izpildīts nosacījums, ka datu subjekts tiek attiecīgi informēts par datu apstrādi, un tas vienmēr var viegli piekļūt šai informācija. **Lai nodrošinātu, ka datu subjektiem tiek sniegta informācija pārredzamā veidā, praksē būtu ieteicams veidot atsevišķu politiku, kas apraksta iekšējo trauksmes celšanas sistēmu un norāda informāciju saistībā ar attiecīgo datu apstrādi.** Attiecībā uz datu apstrādi šajā politikā būtu jāprecizē, kāda informācija ir jāsniedz trauksmes cēlēja ziņojumā, kāds ir tiesiskais pamats šādu datu apstrādei, jāprecizē mērķi datu apstrādei, jānorāda, kādām personām dati var tikt nodoti un cik ilgi tie tiek glabāti, kā arī

Mikijs Zīmecs, zvērinātu advokātu biroja *Ellex Kļaviņš* jurists, sertificēts datu aizsardzības speciālists

jāatceras norādīt informāciju par datu subjekta tiesībām atbilstoši VDAR.

Lai iegūtu precīzus datus, atbilstošajā politikā jāskaidro, ka ziņojumā ir jānorāda trauksmes cēlēja vārds, uzvārds un kontaktinformācija, informācija par personu, par kuru ziņo, pierādījumi par iespējamo pārkāpumu (dokumentu kopijas, fotogrāfijas, e–pasta sarakstes kopijas u.c.) un cita informācija, kas var palīdzēt ziņojuma izskatīšanai. Lai nodrošinātu, ka tiek sniegta visa nepieciešamā informācija, ir ieteicams iepriekš sagatavot veidlapu, ko var izmantot ziņojuma iesniegšanai. Papildus, lai nodrošinātu, ka personas dati tiek vākti adekvāti to apstrādes mērķim, ir jāprecizē, par kādiem iespējamiem pārkāpumiem nodarbinātais ir tiesīgs ziņot. Atbilstoši likumam trauksmes cēlējs ir tiesīgs ziņot par pārkāpumiem, kas var skart sabiedrības intereses, par kuriem uzzinājis, veicot darba pienākumus vai dibinot tiesiskas attiecības, kas saistītas ar darba pienākumu veikšanu, it īpaši par korupciju, krāpšanu, pārtikas drošības apdraudējumu, cilvēktiesību pārkāpumiem u.c. Šo datu apstrādes mērķis ir veikt iespējamā pārkāpuma izmeklēšanu, nodrošināt trauksmes cēlēja pienācīgu aizsardzību un nodrošināt saziņu ar trauksmes cēlēju. Ņemot vērā, ka iekšējo trauksmes celšanas sistēmas izveidi pieprasa likums, tiesiskais pamats datu apstrādei ir VDAR 6. panta 1. daļas c) apakšpunkts, kas ļauj veikt datu apstrādi, ja tā ir vajadzīga, lai izpildītu uz pārzini attiecināmu juridisku pienākumu. Jāatgādina, ka atbilstoši likumam un VDAR prasībām bez attiecīga tiesiska pamata citiem mērķiem šos personas datus izmantot nedrīkst.

Politikā arī jāparedz, ka trauksmes cēlēja personas datus bez objektīva iemesla vai bez trauksmes cēlēja piekrišanas aizliegts nodot personām, kuras nav saistītas ar ziņojuma saņemšanu un izvērtēšanu (it īpaši trauksmes cēlēja ziņojumā norādītajām personām). Atbilstoši VDAR ir nepieciešams norādīt datu saņēmējus vai to kategorijas. Lai nodrošinātu ziņotāja aizsardzību, ieteicams politikā norādīt pēc iespējas konkrētākus datu saņēmējus, lai novērstu situāciju, ka ziņojums uzreiz nonāk tās personas rokās, kas minēta ziņojumā. Ja personas datus saņem ārpakalpojumu sniedzēji, kas tiek izmantoti kā kontaktpunkts, vai personas, kas izmeklē iespējamo

Foto: Aivars Siliņš

pārkāpumu, tie būtu jānorāda specifiski vai kā saņēmēju kategorija, piemēram, advokātu vai auditoru birojs.

Viens no jautājumiem, par ko nav vienotas izpratnes, – cik ilgi jāglabā saņemtie ziņojumi un ar tiem saistītie dokumenti? No vienas puses, ir jānodrošina, ka tiek aizsargāts trauksmes cēlējs, no otras puses, pārlieku ilga dokumentu glabāšana rada risku, ka ziņojums var nokļūt trešo personu rokās. Valsts kanceleja, apspriežoties ar Valsts arhīvu, vadlīnijās par trauksmes cēlēju ziņojumu izskatīšanu valsts pārvaldes institūcijās datu glabāšanas termiņu norādījusi piecus gadus, ko var pagarināt atkarībā no ziņojuma izskatīšanas rezultāta. Jāatzīst, ka norādītais termiņš uzņēmuma vajadzībām šķiet pārmērīgs, taču to var ņemt vērā, izlemjot, cik ilgi dati tiks glabāti. Jebkurā gadījumā ir jāvērtē, vai visi dokumenti ir glabājami vienlīdz ilgi, lai uzņēmums varētu pierādīt, ka tas ir veicis visus nepieciešamos soļus, lai izskatītu ziņojumu, veiktu koriģējošās darbības un/vai nodrošinātu trauksmes cēlēja atbilstošu aizsardzību.

Papildus no VDAR izriet, ka arī personai, par kuru tiek sniegts ziņojums, ir tiesības uz datu aizsardzību, taču, ņemot vērā datu apstrādes būtību, dažas tiesības var tikt ierobežotas. Piemēram, atbilstoši VDAR 14. pantam uzņēmumam nav jāinformē šī persona, ka par viņu iesniegts ziņojums, ja tas var būtiski traucēt sasniegt attiecīgās datu apstrādes mērķus (kas izriet no likuma), kā arī šai personai nebūs tiesības saņemt informāciju, kas var norādīt uz trauksmes cēlēja identitāti. Neskatoties uz to, gan atbilstoši likumam, gan VDAR noteikumiem ir aizliegts izplatīt informāciju, kas atklāj personas, par kuru ziņojis trauksmes cēlējs, identitāti personām, kas nav iesaistītas iespējamā pārkāpuma izmeklēšanā.

Tehniskās un organizatoriskās prasības

Ne likums, ne VDAR neparedz konkrētas prasības, kā nodrošināt iekšējās trauksmes celšanas sistēmas drošību, taču skaidrs ir viens – lai spētu izpildīt likuma mērķi, ir jāspēj novērst nesankcionētu piekļuvi trauksmes celšanas ziņojumiem. Atbilstoši VDAR prasībām tehniskie un organizatoriskie pasākumi ir jāievieš atbilstoši uzņēmuma iespējām un datu apstrādes iespējamam riskam attiecībā uz fizisku personu tiesībām un brīvībām. Citiem vārdiem, ņemot vērā iespējamās informācijas raksturu, kas varētu tikt norādīts trauksmes celšanas ziņojumā, trauksmes celšanas sistēmai vajadzētu piemērot stingrākas drošības prasības, salīdzinot ar, piemēram, parastiem nodarbināto personas datiem.

No organizatoriskās puses ir jānodrošina, ka ziņojumiem var piekļūt tikai personas, kas saistītas ar ziņojuma izskatīšanu. **Noteikti ir jāieceļ atbildīgās personas, kam var sniegt ziņojumus, un šī informācija jādara zināma uzņēmumā nodarbinātajiem.** Šādām personām ir jābūt objektīvām, bez iespējama konflikta un ar tiešu piekļuvi vadībai – tās var būt specifiskas personas, uzņēmuma struktūrvienības vai pat ārpakalpojuma sniedzēji, taču jāatceras, ka pēc iespējas ir jāierobežo cilvēku skaits, kas var piekļūt ziņojumiem. Nedrīkst aizmirst arī par vienkāršo drošību, ko var atļauties jebkurš uzņēmums, – kontrolēt ziņojumu papīra kopiju izmantošanu, neatstājot ziņojumus printeros, neaizslēgtos kabinetos, skapīšos vai dokumentu kaudzītē uz atbildīgās nodaļas galdiem.

Politikā arī jāparedz, ka trauksmes cēlēja personas datus bez objektīva iemesla vai bez trauksmes cēlēja piekrišanas aizliegts nodot personām, kuras nav saistītas ar ziņojuma saņemšanu un izvērtēšanu.

Lai nodrošinātu, ka trauksmes cēlēja identitāte nenonāk trešo personu rokās, viena no iespējam, ko likums paredz, ir izmantot datu pseidonimizāciju. Atbilstoši VDAR definīcijai pseidonimizācija ir personas datu apstrāde, ko veic tāda veidā, lai personas datus vairs nav iespējas saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, piemēram, aizklājot vārdu un citu informāciju ar noteiktu ciparu virkni. **Jāatceras, ka jāaizklāj ne tikai identifikācijas dati un kontaktinformācija, bet arī cita informācija, kas var atklāt trauksmes cēlēja identitāti.** Protams, jānodrošina, ka oriģinālais ziņojums un pseidonimizētā kopija tiek glabāti atsevišķi, oriģinālam piemērojot stingrākas drošības prasības. Nedrīkst arī aizmirst, ka uzņēmumam ir jānodrošina arī tehniska aizsardzība, piemēram, datu šifrēšana, gan glabājot, gan pārsūtot datus, piekļuves kontroles un atbilstošu sistēmu drošību, lai nepieļautu, ka ziņojums un informācija par trauksmes cēlēju un par personām, kas minētas ziņojumā, nonāk atklātībā vai nepiederošu personu rokās.

Ieviešot iekšējo trauksmes celšanas sistēmu, jebkurš uzņēmums uzsāks jaunu datu apstrādes procesu, kam noteikti jāpievērš atsevišķa uzmanība arī no datu aizsardzības puses, ņemot vērā apstrādāto datu iespējami augsto risku datu subjektu tiesībām un brīvībām. Kā iepriekš minēts, ir nepieciešams nodrošināt precīzu datu ieguvi, izveidot jaunas vai papildināt esošās uzņēmuma procedūras par to, kā tiek apstrādāti personas dati, kā arī nodrošināt atbilstošus tehniskos un organizatoriskos drošības pasākumus. Jāatceras, ka arī uzņēmumam ir svarīgi sakārtot datu apstrādes procesus, jo sods par datu aizsardzības pārkāpumu attiecībā uz datu apstrādi iekšējās trauksmes celšanas sistēmā saskaņā ar Vispārīgo datu aizsardzības regulu var sasniegt 20 000 000 EUR vai 4% no apgrozījuma, atkarībā no tā, kuras summas apmērs ir lielāks. Noslēgumā ir vērts uzsvērt, ka tiesība uz personas datu aizsardzību ir atzīta kā cilvēka pamattiesība, tādēļ arī ziņošana par datu aizsardzības pārkāpumiem var tikt uzskatīta kā trauksmes celšana. BJP

JURISTA PADOMS