**18/LV**

**WP250rev.01**

# Pamatnostādnes par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu 2016/679

**Pieņemtas 2017. gada 3. oktobrī**

**Pēdējo reizi pārskatītas un pieņemtas 2018. gada 6. februārī**

Šī darba grupa izveidota saskaņā ar Direktīvas 95/46/EK 29. pantu. Tā ir neatkarīga Eiropas padomdevēja struktūra datu aizsardzības un privātuma jautājumos. Tās uzdevumi aprakstīti Direktīvas 95/46/EK 30. pantā un Direktīvas 2002/58/EK 15. pantā.

Sekretariāta pakalpojumus nodrošina Eiropas Komisijas Tiesiskuma, brīvības un drošības ģenerāldirektorāta C direktorāts (Pamattiesības un Savienības pilsonība), B-1049, Brisele, Beļģija, birojs nr. MO-59 02/013.

Tīmekļa vietne: http://ec.europa.eu/justice/data-protection/index_en.htm

**DARBA GRUPA PERSONU AIZSARDZĪBAI ATTIECĪBĀ UZ PERSONAS DATU APSTRĀDI,**

kas izveidota ar Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK,

ņemot vērā minētās direktīvas 29. un 30. pantu,

ņemot vērā darba grupas reglamentu,

**IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.**

# SATURA RĀDĪTĀJS

## IEVADS

Vispārīgajā datu aizsardzības regulā (VDAR) ir ieviesta prasība paziņot par personas datu aizsardzības pārkāpumu (turpmāk tekstā saukts "pārkāpums") kompetentajai valsts uzraudzības iestādei[1] (vai pārrobežu pārkāpuma gadījumā — vadošajai iestādei) un noteiktos gadījumos informēt par pārkāpumu personas, kuru personas datus šīs pārkāpums ietekmējis.

Pienākumi paziņot pārkāpumu gadījumos pašlaik attiecas uz dažām organizācijām, piemēram, publiski pieejamu elektroniskās komunikācijas pakalpojumu sniedzējiem (kā noteikts Direktīvā 2009/136/EK un Regulā (ES) Nr. 611/2013)[2]. Dažās ES dalībvalstīs jau pastāv arī savi valsts pārkāpumu paziņošanas pienākumi. Tie var ietvert pienākumu paziņot par pārkāpumiem, kas skar noteiktas pārziņu kategorijas, ne tikai publiski pieejamu elektroniskās komunikācijas pakalpojumu sniedzējus (piemēram, Vācijā un Itālijā), vai pienākumu ziņot par visiem pārkāpumiem, kas saistīti ar personas datiem (piemēram, Nīderlandē). Citās dalībvalstīs var būt attiecīgi Prakses kodeksi (piemēram, Īrijā[3]). Lai gan vairākas ES datu aizsardzības iestādes pašlaik mudina pārziņus ziņot par pārkāpumiem, Datu aizsardzības direktīvā 95/46/EK[4], kuru aizstāj ar VDAR, nav noteikts īpašs pārkāpumu paziņošanas pienākums, un tādēļ šāda prasība daudzām organizācijām būs jauna. Saskaņā ar VDAR tagad visiem pārziņiem ir noteikts obligāts paziņošanas pienākums, izņemot gadījumus, kad ir maz ticams, ka šis pārkāpums varētu radīt risku personu tiesībām un brīvībām[5]. Apstrādātājiem arī ir svarīga loma, un viņiem ir jāpaziņo par jebkuru pārkāpumu savam pārzinim[6].

29. panta darba grupa (DG29) uzskata, ka jaunā paziņošanas prasība sniedz vairākus ieguvumus. Informējot uzraudzības iestādi, pārziņi var saņemt padomu par to, vai ir nepieciešams informēt skartās personas. Faktiski uzraudzības iestāde var uzdot pārzinim informēt šīs personas par pārkāpumu[7]. Personas informēšana par pārkāpumu ļauj pārzinim sniegt informāciju par pārkāpuma rezultātā radītajiem riskiem un pasākumiem, kādus šīs personas var veikt, lai pasargātu sevi no iespējamām sekām. Jebkurā pārkāpuma reaģēšanas plānā uzmanība būtu jāpievērš personu un to personas datu aizsardzībai. Tādējādi pārkāpuma paziņojums būtu jāuzskata par instrumentu, ar ko uzlabo atbilstību personas datu aizsardzības prasībām. Tajā pašā laikā būtu jāatzīmē, ka personas vai uzraudzības iestādes neinformēšana par pārkāpumu var nozīmēt, ka saskaņā ar 83. pantu pārzinim var tikt piemērota sankcija.

---

[1] Skatīt VDAR 4. panta 21. punktu

[2] Skatīt https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex:32009L0136 unhttps://eur-lex.europa.eu/legal-content/lv/TXT/?uri=CELEX%3A32013R0611

[3] Skatīt https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Skatīt http://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex:31995L0046

[5] Tiesības, kas nostiprinātas ES Pamattiesību hartā, pieejama tīmekļa vietnē http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[6] Skatīt 33. panta 2. punktu. Tas ir konceptuāli līdzīgs Regulas (ES) Nr. 611/2013 5. pantam, kurā teikts, ka pakalpojuma sniedzējam, ar kuru ir noslēgts līgums par daļu elektroniskās komunikācijas pakalpojumu sniegšanu (nenodibinot tiešas līgumattiecības ar abonentiem), ir pienākums paziņot to nolīgušajam pakalpojumu sniedzējam personas datu aizsardzības pārkāpuma gadījumā.

[7] Skatīt 34. panta 4. punktu un 58. panta 2. punkta e) apakšpunktu.

Tādēļ pārziņiem un apstrādātājiem ir ieteicams iepriekš izplānot un ieviest procesus, lai varētu atklāt un nekavējoties apturēt pārkāpumu, novērtēt personām radīto risku[8] un pēc tam noteikt, vai ir nepieciešams paziņot kompetentajai uzraudzības iestādei un attiecīgā gadījumā informēt par pārkāpumu attiecīgās personas. Paziņojumam uzraudzības iestādei vajadzētu būt attiecīgā incidenta reaģēšanas plāna sastāvdaļai.

VDAR ir ietverti noteikumi par to, kad un kam ir nepieciešams paziņot par pārkāpumu, kā arī, kāda informācija būtu jāiesniedz paziņojuma ietvaros. Paziņojumam nepieciešamo informāciju var sniegt pa posmiem, taču jebkurā gadījumā pārziņiem būtu jāreaģē uz jebkādu pārkāpumu savlaicīgi.

Atzinumā 03/2014 attiecībā uz informēšanu par personas datu aizsardzības pārkāpumu[9] 29. panta darba grupa sniedza pārziņiem norādījumus, kas palīdzētu viņiem izlemt, vai informēt datu subjektus "personas datu aizsardzības pārkāpuma" gadījumā. Atzinumā ņemts vērā elektroniskās komunikācijas pakalpojumu sniedzēju pienākums atbilstīgi Direktīvai 2002/58/EK un sniegti piemēri no daudzām nozarēm saistībā ar tobrīd VDAR projektu, un ieteikta laba prakse visiem pārziņiem.

Šajās pamatnostādnēs ir izskaidrotas VDAR ietvertās obligātās pārkāpuma paziņošanas un informēšanas prasības un daži soļi, kurus pārziņi un apstrādātāji var veikt, lai izpildītu šos jaunos pienākumus. Šeit sniegti arī dažādu pārkāpumu veidu piemēri, kā arī norādīts, kuram atšķirīgos scenārijos būtu jāsniedz paziņojums.

## I. Personas datu aizsardzības pārkāpuma paziņošana saskaņā ar VDAR

### A. Pamata drošības apsvērumi

Viena no VDAR prasībām ir tāda, ka, izmantojot atbilstošus tehniskos un organizatoriskos pasākumus, personas dati tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu[10].

Tādēļ VDAR prasīts, lai gan pārziņi, gan apstrādātāji ieviestu atbilstošus tehniskos un organizatoriskos pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam, kas saistīts ar apstrādātājiem personas datiem. Tajos būtu jāņem vērā tehnikas līmenis, īstenošanas izmaksas un apstrādes raksturs, apmērs, konteksts un nolūki, kā arī dažādas iespējamības un nopietnības pakāpes risks attiecībā uz fizisku personu tiesībām un brīvībām[11]. Tāpat VDAR prasa visu atbilstošu tehnisko un organizatorisko pasākumu īstenošanu, lai varētu nekavējoties noteikt, vai ir noticis pārkāpums, un pēc tam noteikt, vai uz to attiecas paziņošanas pienākums[12].

Līdz ar to datu drošības politikas galvenais elements, ja iespējams, spēj novērst pārkāpumu un, ja tas tomēr ir radies, reaģēt uz to savlaicīgi.

---

[8] To var nodrošināt DAIN uzraudzības un pārbaudes prasības ietvaros, kas ir obligāta apstrādes darbībām, kuras var radīt augustu risku fizisku personu tiesībām un brīvībām (35. panta 1. un 11. punkts).

[9] Skatīt Atzinumu 03/2014 attiecībā uz informēšanu par personas datu aizsardzības pārkāpumu http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] Skatīt 5. panta 1. punkta f) apakšpunktu un 32. pantu.

[11] Regulas 32. pants; skatīt arī 83. apsvērumu.

[12] Skatīt 87. apsvērumu.

## B. Kas ir personas datu aizsardzības pārkāpums?

### 1. Definīcija

Jebkādu mēģinājumu novērst pārkāpumu ietvaros pārzinim vispirms būtu jāspēj šo pārkāpumu atpazīt. VDAR 4. panta 12. punktā "personas datu aizsardzības pārkāpums" ir definēts šādi:

> "drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem."

Vajadzētu būt pietiekami skaidram, kas ir domāts ar personas datu "iznīcināšanu": ja dati vairs nepastāv vai vairs nepastāv tādā formā, kādā pārzinis tos var izmantot. Jēdzienam "sabojāšana" arī vajadzētu būt samērā skaidram: ja personas dati tiek pārveidoti, bojāti vai vairs nav pilnīgi. Runājot par personas datu "nozaudēšanu", tā jāinterpretē tādējādi, ka dati joprojām var pastāvēt, bet pārzinis ir zaudējis kontroli vai piekļuvi tiem, vai arī tie vairs nav pārziņa rīcībā. Visbeidzot, neatļauta vai nelikumīga apstrāde var ietvert personas datu izpaušanu (vai piekļuvi tiem) saņēmējiem, kuriem nav tiesību saņemt datus (vai piekļūt tiem), vai jebkuru citu apstrādes veidu, kas ir VDAR pārkāpums.

**Piemērs**

Personas datu nozaudēšanas piemērs var būt gadījums, kad ir nozaudēta vai nozagta ierīce, kas satur pārziņa klientu datu bāzes kopiju. Vēl viens nozaudēšanas piemērs var būt, kad personas datu kopuma vienīgā kopija ir šifrēta, izmantojot ļaunprātīgu programmatūru, vai pārzinis to ir šifrējis, izmantojot atslēgu, kas vairs nav viņa rīcībā.

Būtu jāsaprot, ka pārkāpums ir informācijas drošības incidenta veids. Tomēr, kā norādīts 4. panta 12. punktā, VDAR attiecas tikai uz *personas datu* aizsardzības pārkāpumu. Šāda pārkāpuma sekas ir tādas, ka pārzinis nespēs nodrošināt atbilstību VDAR 5. pantā izklāstītajiem principiem, kas attiecas uz personas datu apstrādi. Tas norāda atšķirību starp informācijas drošības incidentu un personas datu pārkāpumu — būtībā, lai gan visi personas datu pārkāpumi ir informācijas drošības incidenti, ne visi informācijas drošības incidenti vienmēr ir personas datu pārkāpumi[13].

Turpmāk aplūkota pārkāpuma iespējamās nelabvēlīgās sekas personām.

### 2. Personas datu aizsardzības pārkāpumu veidi

Savā Atzinumā 03/2014 attiecībā uz informēšanu par pārkāpumu DG29 skaidroja, ka pārkāpumus var klasificēt saskaņā ar šādiem trim labi zināmiem informācijas drošības principiem[14]:

- "konfidencialitātes pārkāpums" — neatļauta vai nejauša personas datu izpaušana vai piekļuve tiem.
- "integritātes pārkāpums" — neatļauta vai nejauša personas datu modifikācija.
- "pieejamības pārkāpums" — nejauša vai neatļauta piekļuves zaudēšana[15] personas datiem vai personas datu iznīcināšana.

[13] Jāatzīmē, ka informācijas drošības incidents neaprobežojas tikai ar tādiem draudu modeļiem, kuros uzbrukums organizācijai nāk no ārēja avota, bet attiecas arī uz iekšējās apstrādes incidentiem.

[14] Skatīt Atzinumu 03/2014.

[15] Ir labi zināms, ka "piekļuve" būtībā ir daļa no "pieejamības". Skatīt, piemēram, NIST SP800-53rev4, kurā "pieejamība" definēta šādi: "Savlaicīgas un uzticamas piekļuves informācijai un tās izmantošanas

Jāatzīmē, ka atkarībā no apstākļiem pārkāpums var attiekties uz personas datu konfidencialitāti, integritāti un pieejamību vienlaikus, kā arī jebkuru šo elementu kombināciju.

Konfidencialitātes vai integritātes pārkāpuma noteikšana ir samērā skaidra, savukārt tas, vai ir bijis pieejamības pārkāpums, var būt mazāk acīmredzams. Par pieejamības pārkāpumu vienmēr tiks uzskatīts tāds pārkāpums, kad personas dati ir neatgriezeniski zaudēti vai iznīcināti.

**Piemērs**

Pieejamības zudumu piemēri ir gadījumi, kad dati ir izdzēsti nejauši vai tos ir izdzēsusi nepiederoša persona, vai arī droši šifrētu datu gadījumā — zudusi šifrēšanas atslēga. Gadījumā, kad pārzinis nevar atjaunot piekļuvi datiem, piemēram, izmantojot rezerves kopiju, tas tiek uzskatīts par neatgriezenisku pieejamības zudumu.

Pieejamības zudums var rasties arī tad, ja ir bijuši būtiski traucējumi organizācijas parastajā pakalpojuma sniegšanā, piemēram, tiek traucēta elektroenerģijas padeve vai pakalpojuma atteikuma uzbrukums, kā rezultātā personas dati nav pieejami.

Varētu jautāt, vai īslaicīgs personas datu pieejamības zudums būtu jāuzskata par pārkāpumu un — apstiprinošas atbildes gadījumā — vai par to ir jāpaziņo. VDAR 32. pantā ar "apstrādes drošību" paskaidrots, ka, ieviešot tehniskus un organizatoriskus pasākumus, lai nodrošinātu riskam atbilstošu drošības līmeni, cita starpā būtu jāņem vērā "spēja nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību" un "spēja laicīgi atjaunot personas datu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums".

Tādēļ informācijas drošības incidents, kura rezultātā personas dati tiek padarīti nepieejami uz noteiktu laiku, ir arī pārkāpuma veids, jo piekļuves trūkums datiem var būtiski ietekmēt fizisko personu tiesības un brīvības. Skaidrības labad, ja personas dati nav pieejami plānotas sistēmas uzturēšanas dēļ, tas nav "drošības pārkāpums" atbilstīgi 4. panta 12. punktam.

Tāpat kā personas datu neatgriezeniskas nozaudēšanas vai iznīcināšanas (vai arī faktiski jebkāda cita veida pārkāpuma) gadījumā, pārkāpums, kas saistīts ar īslaicīgu pieejamības zudumu, būtu jādokumentē saskaņā ar 33. panta 5. punktu. Tas palīdz pārzinim uzskatāmi parādīt viņa atbilstību pārskatatbildības prasībām uzraudzības iestādei, kas var pieprasīt apskatīt šos ierakstus[16]. Tomēr atkarībā no pārkāpuma apstākļiem var būt nepieciešams sniegt paziņojumu uzraudzības iestādei vai arī informēt skartās personas. Pārzinim vajadzēs pārbaudīt fizisko personu tiesību un brīvību ietekmes iespējamība un nopietnība personas datu pieejamības trūkuma dēļ. Saskaņā ar 33. pantu pārzinim būs nepieciešams paziņot, izņemot gadījumus, kad ir maz ticams, ka pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām. Tas, protams, jāizvērtē katrā atsevišķā gadījumā.

**Piemēri**

Slimnīcas kontekstā, ja pat īslaicīgi nav pieejami būtiski medicīniskie dati par pacientiem, var rasties riski personas tiesībām un brīvībām; piemēram, var tikt atceltas operācijas un apdraudētas dzīvības.

---

nodrošināšana", pieejams tīmekļa vietnē http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 atsaucas arī uz: "Timely, reliable access to data and information services for authorized users" (Savlaicīga un uzticama piekļuve datiem un informācijas pakalpojumiem pilnvarotiem lietotājiem). Skatīt https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 "pieejamība" definēta arī kā "Iespēja piekļūt un izmantot pēc pilnvarotas iestādes pieprasījuma": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

[16] Skatīt 33. panta 5. punktu.

Turpretim, ja plašsaziņas līdzekļu uzņēmuma sistēmas nav pieejamas vairākas stundas (piemēram, saistībā ar strāvas padeves pārtraukumu) un šī sabiedrība tādā gadījumā nevar nosūtīt saviem abonentiem reklāmas prospektus, tas, visticamāk, neradīs risku personas tiesībām un brīvībām.

Jāatzīmē, ka, lai gan pārziņa sistēmu pieejamības zudums varētu būt tikai īslaicīgs un tā rezultātā var netikt skartas personas, pārzinim ir svarīgi ņemt vērā visas iespējamās pārkāpuma sekas, jo uz viņu joprojām var attiekties paziņošanas pienākums citu iemeslu dēļ.

**Piemērs**

Inficēšana ar ļaunprātīgu programmatūru (ļaunprogrammatūra, kas šifrē pārziņa datus līdz izpirkuma maksas saņemšanai), var radīt īslaicīgu pieejamības zudumu, ja datus var atjaunot, izmantojot rezerves kopijas. Tomēr joprojām ir notikusi ielaušanās tīklā, un paziņojuma sniegšana var būt obligāta, ja incidents tiek kvalificēts kā konfidencialitātes pārkāpums (t. i., uzbrucējs piekļūst personas datiem) un tas rada risku fizisku personu tiesībām un brīvībām.

## 3. Personas datu aizsardzības pārkāpuma iespējamās sekas

Pārkāpums potenciāli var radīt ievērojamas nelabvēlīgas sekas personām, kā rezultātā var tikt nodarīts fizisks, materiāls vai nemateriāls kaitējums. VDAR paskaidrots, ka tas var būt kontroles zudums pār saviem personas datiem, tiesību ierobežošana, diskriminācija, identitātes zādzība vai viltošana, finansiālie zaudējumi, neatļauta pseidonimizācijas atcelšana, kaitējums reputācijai un ar dienesta noslēpumu aizsargātu personas datu konfidencialitātes zaudēšana. Tas var ietvert arī citu ievērojamu nelabvēlīgu ekonomisko vai sociālo situāciju šīm personām[17].

Attiecīgi VDAR prasīts, lai pārzinis kompetentajai uzraudzības iestādei paziņotu par pārkāpumu, izņemot gadījumus, kad ir maz ticams, ka tas radīs šādu nelabvēlīgas ietekmes risku. Ja pastāv liela šādu nelabvēlīgu seku riska iespējamība, VDAR prasīts, lai pārzinis informētu par pārkāpumu skartās personas, tiklīdz tas ir praktiski iespējams[18].

VDAR 87. apsvērumā uzsvērts, ka ir svarīgi identificēt pārkāpumu, novērtēt personām radīto risku un, nepieciešamības gadījumā, par to paziņot.

"Būtu jāpārliecinās, vai ir īstenoti visi attiecīgie tehniskie un organizatoriskie aizsardzības pasākumi, lai nekavējoties konstatētu, vai ir noticis personas datu aizsardzības pārkāpums, un ātri informētu uzraudzības iestādi un datu subjektu. Paziņošana bez nepamatotas kavēšanās būtu jānosaka, jo īpaši, ņemot vērā personas datu aizsardzības pārkāpuma raksturu un smagumu, kā arī tā sekas un nelabvēlīgo ietekmi uz datu subjektu. Šāda paziņošana var izraisīt uzraudzības iestādes iejaukšanos atbilstīgi tās uzdevumiem un pilnvarām, kas noteiktas šajā regulā."

Papildu pamatnostādnes, kā novērtēt personām radītu nelabvēlīgu seku risku, ir sniegtas IV iedaļā.

Ja pārziņi nepaziņo uzraudzības iestādei vai datu subjektiem, vai abiem par datu aizsardzības pārkāpumu, lai gan ir izpildītas 33. un/vai 34. panta prasības, tad uzraudzības iestādei ir izvēle, kurā jāapsver visi tās rīcībā esošie korektīvie pasākumi, kas ietvertu atbilstoša administratīvā naudas soda piemērošanas izskatīšanu[19], kopā ar korektīvo pasākumu saskaņā ar 58. panta 2. punktu vai arī

[17] Skatīt arī 85. un 75. apsvērumu.

[18] Skatīt arī 86. apsvērumu.

[19] Papildu informāciju skatīt DG29 Pamatnostādnēs par administratīvo sodu piemērošanu un noteikšanu, kas pieejamas tīmekļa vietnē: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

atsevišķi. Ja tiek nolemts piemērot administratīvu naudas sodu saskaņā ar VDAR 83. panta 4. punkta a) apakšpunktu, tā apmērs var būt līdz 10 000 000 EUR vai līdz 2 % no uzņēmuma kopējā visā pasaulē gūtā gada apgrozījuma. Ir svarīgi arī atcerēties, ka dažos gadījumos nepaziņošana par pārkāpumu var atklāt vai nu esošo drošības pasākumu trūkumu, vai arī esošo drošības pasākumu nepietiekamību. DG29 pamatnostādnēs par administratīvajiem sodiem ir noteikts: "Vairāku pārkāpumu izdarīšana vienā vai vairākos atsevišķos gadījumos nozīmē to, ka uzraudzības iestāde var piemērot administratīvos naudas sodus tādā apmērā, kas ir efektīvs, proporcionāls un preventīvs vissmagākā pārkāpuma robežās". Tādā gadījumā uzraudzības iestādei būs arī iespēja piemērot sankcijas par pārkāpuma nepaziņošanu vai informācijas nesniegšanu (33. un 34. pants), no vienas puses, un par (atbilstīgu) drošības pasākumu (32. pants) trūkumu, no otras puses, jo tie ir divi atsevišķi pārkāpumi.

## II. Regulas 33. pants — paziņošana uzraudzības iestādei

### A. Kad ir jāiesniedz paziņojums?

#### 1. Regulas 33. panta prasības

Regulas 33. panta 1. punktā noteikts:

> "Personas datu aizsardzības pārkāpuma gadījumā pārzinis bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms, paziņo par personas datu aizsardzības pārkāpumu uzraudzības iestādei, kas ir kompetenta saskaņā ar 55. pantu, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām. Ja paziņošana uzraudzības iestādei nav notikusi 72 stundu laikā, paziņojumam pievieno kavēšanās iemeslus."

Regulas 87. apsvērumā norādīts, ka[20]:

> "Jāpārliecinās, vai ir īstenoti visi attiecīgie tehniskie un organizatoriskie aizsardzības pasākumi, lai nekavējoties konstatētu, vai ir noticis personas datu aizsardzības pārkāpums, un ātri informētu uzraudzības iestādi un datu subjektu. Paziņošana bez nepamatotas kavēšanās būtu jānosaka, jo īpaši, ņemot vērā personas datu aizsardzības pārkāpuma raksturu un smagumu, kā arī tā sekas un nelabvēlīgo ietekmi uz datu subjektu. Šāda paziņošana var izraisīt uzraudzības iestādes iejaukšanos atbilstīgi tās uzdevumiem un pilnvarām, kas noteiktas šajā regulā."

#### 2. Kad pārzinim kļūst "zināms"?

Kā minēts iepriekš, VDAR prasīts, lai pārkāpuma gadījumā pārzinis bez nepamatotas kavēšanās paziņotu par pārkāpumu un, ja iespējams, ne vēlāk kā 72 stundas pēc tam, kad pārzinim tas kļuvis zināms. Tas var radīt jautājumu par to, kad var uzskatīt, ka pārzinim ir kļuvis "zināms" par pārkāpumu. DG29 viedoklis ir šāds: uzskatāms, ka pārzinim ir kļuvis "zināms", ja šim pārzinim ir pietiekama pārliecība, ka ir radies informācijas drošības incidents, kura rezultātā tiek apdraudēti personas dati.

Tomēr, kā norādīts iepriekš, VDAR prasa, lai pārzinis īstenotu visus attiecīgos tehniskās aizsardzības un organizatoriskos pasākumus, lai nekavējoties konstatētu pārkāpumu un ātri informētu par to uzraudzības iestādi un datu subjektus. Tajā noteikts arī, ka fakts, vai paziņošana izdarīta bez

[20] Šajā gadījumā ir svarīgs arī 85. apsvērums.

nepamatotas kavēšanās, būtu jānosaka, jo īpaši ņemot vērā pārkāpuma raksturu un smagumu, kā arī tā sekas un nelabvēlīgo ietekmi uz datu subjektu[21]. Tas uzliek pienākumu pārzinim nodrošināt, ka viņam savlaicīgi kļūs "zināmi" visi pārkāpumi, ļaujot viņam veikt atbilstošus pasākumus.

Kad tieši var uzskatīt, ka pārzinim ir "zināms" konkrētais pārkāpums, tas būs atkarīgs no konkrētā pārkāpuma apstākļiem. Dažos gadījumos jau no sākuma būs samērā skaidrs, ka ir noticis pārkāpums, bet citos gadījumos var būt nepieciešams zināms laiks, lai noteiktu, vai personas dati ir apdraudēti. Tomēr uzsvars būtu jāliek uz tūlītēju rīcību incidenta izmeklēšanā, lai noteiktu, vai tiešām ir noticis personas datu aizsardzības pārkāpums, un, ja tā ir, veikt koriģējošas darbības un paziņot, ja nepieciešams.

**Piemēri**

1. *USB* zibatmiņas nozaudēšanas gadījumā bieži vien nav iespējams noskaidrot, vai nepiederošām personām ir bijusi piekļuve nešifrētiem personas datiem. Tomēr, lai arī pārzinis, iespējams, nevar konstatēt, vai ir noticis konfidencialitātes pārkāpums, par šādu gadījumu ir jāpaziņo, jo ir pietiekami ticams, ka ir noticis pieejamības pārkāpums; varētu uzskatīt, ka pārzinim ir kļuvis "zināms" par pārkāpumu brīdī, kad viņš konstatējis *USB* zibatmiņas nozaudēšanu.

2. Trešā persona informē pārzini, ka tā ir nejauši saņēmusi kāda viņa klienta personas datus, un sniedz neatļautas izpaušanas pierādījumus. Tā kā pārzinim ir iesniegti nepārprotami pierādījumi par konfidencialitātes pārkāpumu, tad nav šaubu, ka pārzinim tas ir kļuvis "zināms".

3. Pārzinis atklāj iespējamu ielaušanos viņa tīklā. Pārzinis pārbauda savas sistēmas, lai noteiktu, vai šajā sistēmā esošie personas dati ir apdraudēti, un apstiprina, ka tas tā ir. Turklāt, tā kā pārzinim ir iesniegti nepārprotami pierādījumi par pārkāpumu, tad nav šaubu, ka pārzinim tas ir kļuvis "zināms".

4. Ar pārzini sazinās kibernoziedznieks, kurš uzlauzis viņa sistēmu ar mērķi pieprasīt izpirkuma maksu. Tādā gadījumā, pārbaudot savu sistēmu, lai apstiprinātu uzbrukumu tai, pārzinim ir nepārprotami pierādījumi, ka pārkāpums ir noticis un nav šaubu, ka viņam šis pārkāpums ir kļuvis zināms.

Ja par iespējamo pārkāpumu pārzini vispirms informē persona, plašsaziņas līdzekļu organizācija vai cits avots, vai pārzinis pats ir atklājis informācijas drošības incidentu, viņš var veikt īsu izmeklēšanu, lai noteiktu, vai pārkāpums ir faktiski noticis. Šajā izmeklēšanas periodā nevar uzskatīt, ka pārzinim ir bijis "zināms" pārkāpums. Tomēr tiek sagaidīts, ka sākotnējā izmeklēšana būtu jāuzsāk pēc iespējas ātrāk un pietiekami precīzi jānosaka, vai pārkāpums ir noticis; pēc tam var veikt detalizētāku izmeklēšanu.

Tiklīdz pārzinim ir kļuvis zināms, par paziņojuma pārkāpumu ir jāziņo bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā. Šajā periodā pārzinim būtu jānovērtē iespējamais risks personām, lai noteiktu, vai stājas spēkā prasība par paziņošanu, kā arī nepieciešamā(-s) darbība(-s), kas veicama(-s) pārkāpuma novēršanai. Tomēr pārzinis jau sākotnēji var veikt potenciālā riska, kas varētu rasties pārkāpuma rezultātā, novērtējumu datu aizsardzības ietekmes novērtējuma (DAIN)[22] ietvaros, kas veikts pirms attiecīgās apstrādes darbības uzsākšanas. Tomēr DAIN var būt daudz vispārinātāks salīdzinājumā ar faktiskā pārkāpuma konkrētajiem apstākļiem, un tādēļ jebkurā gadījumā vajadzēs veikt papildu novērtējumu, ņemot vērā attiecīgos apstākļus. Vairāk informācijas par riska novērtēšanu skatīt IV iedaļā.

[21] Skatīt 87. apsvērumu.

[22] DG29 Pamatnostādnes par DAIN pieejamas šeit: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Lielākajā daļā gadījumu šīs iepriekšējās darbības būtu jāpabeidz drīz pēc sākotnējā brīdinājuma (t. i., kad pārzinim vai apstrādātājam ir aizdomas, ka ir noticis informācijas drošības incidents, kas var skart personas datus) – tikai ārkārtas gadījumos pabeigšana var aizņemt ilgāku laiku.

**Piemērs**

Persona informē pārzini par to, ka šķietami no pārziņa ir saņemts e-pasta ziņojums, kurā ietverti personas dati saistībā ar personas (faktisko) pārziņa pakalpojuma izmantošanu, tādējādi vedinot domāt, ka ir pārkāpta pārziņa drošība sistēma. Pārzinis veic īsu izmeklēšanu un konstatē iejaukšanos viņu tīklā un pierādījumus par nesankcionētu piekļuvi personas datiem. Tagad uzskatāms, ka pārzinim ir "zināms" par pārkāpumu, un ir jāpaziņo par to uzraudzības iestādei, izņemot gadījumus, kad ir maz ticams, ka pārkāpums radīs risku fizisku personu tiesībām un brīvībām. Pārzinim vajadzēs veikt attiecīgas koriģējošās darbības, lai novērstu pārkāpumu.

Tāpēc pārzinim vajadzētu būt iekšējiem procesiem, lai varētu atklāt un novērst pārkāpumu. Piemēram, lai konstatētu dažus datu apstrādes pārkāpumus, pārzinis vai apstrādātājs var izmantot noteiktus tehniskos pasākumus, piemēram, datu plūsmas un reģistrācijas analizatorus, no kuru iegūtajiem datiem var definēt notikumus un brīdinājumus, korelējot jebkādus reģistrācijas datus[23]. Ir svarīgi, ka, atklājot pārkāpumu, par to tiek ziņots attiecīgajam augstākstāvošajam vadības līmenim, lai to varētu novērst un vajadzības gadījumā paziņot saskaņā ar 33. pantu un nepieciešamības gadījumā — 34. pantu. Šādi pasākumi un ziņošanas mehānismi varētu būt sīki izklāstīti pārziņa incidentu reaģēšanas plānos un/vai pārvaldības pasākumos. Tie palīdzēs pārzinim efektīvi plānot un noteikt, kam organizācijā ir operatīvā atbildība par pārkāpuma pārvaldību un kā un vai saasināt incidentu attiecīgā gadījumā.

Pārzinim arī būtu jāvienojas ar visiem apstrādātājiem, ko pārzinis izmanto, kuriem pašiem ir pienākums paziņot pārzinim pārkāpuma gadījumā (skatīt turpmāk).

Kaut arī pārziņiem un apstrādātājiem ir pienākums ieviest piemērotus pasākumus, lai varētu novērst un risināt pārkāpumus un reaģēt uz tiem, ir daži praktiski pasākumi, kas būtu jāveic visos gadījumos.

- Informācija par visiem ar drošību saistītajiem notikumiem būtu jānosūta atbildīgajai personai vai personām, kuru uzdevums ir risināt incidentus, konstatēt pārkāpumu un novērtēt risku.
- Tad būtu jānovērtē pārkāpuma rezultātā personām radītais risks (riska neesības, riska esības vai augsta riska iespējamība), informējot par to attiecīgās organizācijas nodaļas.
- Vajadzības gadījumā būtu jāpaziņo uzraudzības iestādei un, iespējams, par pārkāpumu būtu jāinformē skartās personas.
- Tajā pašā laikā pārzinim būtu jārīkojas tā, lai apturētu pārkāpumu un atgūtos no tā.
- Pārkāpuma dokumentācija būtu jāsagatavo tā norises gaitā.

Attiecīgi būtu jāsaprot, ka pārzinim ir pienākums rīkoties saskaņā ar jebkuru sākotnējo brīdinājumu un konstatēt, vai pārkāpums faktiski ir noticis. Šis īsais periods ļauj veikt nelielu izmeklēšanu, un pārzinis var apkopot pierādījumus un citus svarīgus datus. Tomēr, ja pārzinis pietiekami droši ir konstatējis, ka pārkāpums ir noticis, un ja ir izpildīti 33. panta 1. punkta nosacījumi, viņam jāpaziņo uzraudzības iestādei bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā[24]. Ja

[23] Jāatzīmē, ka reģistrācijas datus, kas atvieglo, piem., saglabāšanas, izmaiņu vai dzēšanas pārbaudāmību, arī var uzskatīt par personas datiem attiecībā uz personu, kura uzsākusi attiecīgo apstrādes darbību.

[24] Skatīt Regulu Nr. 1182/71, ar ko nosaka laikposmiem, datumiem un termiņiem piemērojamus noteikumus, pieejama tīmekļa vietnē: http://eur-lex.europa.eu/legal-content/lv/TXT/HTML/?uri=CELEX:31971R1182&from=EN

pārzinis nerīkoties savlaicīgi un kļūst skaidrs, ka pārkāpums ir noticis, to var uzskatīt par paziņojuma nesniegšanu atbilstīgi 33. pantam.

Regulas 32. pantā ir skaidri noteikts, ka pārzinim un apstrādātājam jābūt atbilstīgiem tehniskiem un organizatoriskiem pasākumiem, lai nodrošinātu atbilstošu personas datu drošības līmeni: spēja savlaicīgi atklāt, novērst un ziņot par pārkāpumu būtu jāuzskata par būtiskiem šo pasākumu elementiem.

### 3. Kopīgi pārziņi

Regulas 26. pants attiecas uz kopīgiem pārziņiem, un tajā noteikts, ka kopīgie pārziņi nosaka savus attiecīgos pienākumus attiecībā uz VDAR prasību izpildi[25]. Tas nozīmē, ka ir jānosaka, kura puse būs atbildīga par pienākumu izpildi saskaņā ar 33. un 34. pantu. DG29 iesaka līgumos starp kopīgiem pārziņiem iekļaut noteikumus, kuros nosaka, kurš pārzinis uzņemsies vadību vai būs atbildīgs par VDAR noteikto pārkāpumu paziņošanas pienākumu ievērošanu.

### 4. Apstrādātāja pienākumi

Pārzinim joprojām ir vispārējā atbildība par personas datu aizsardzību, taču apstrādātājam ir svarīga loma, lai pārzinis varētu izpildīt savus pienākumus; un tas ietver arī paziņošanu par pārkāpumu. Faktiski 28. panta 3. punktā tiek precizēts, ka apstrādātājs veic apstrādi, pamatojoties uz līgumu vai citu tiesību aktu. Regulas 28. panta 3. punkta f) apakšpunktā noteikts, ka līgums vai cits juridiskais akts paredz, ka apstrādātājs "palīdz pārzinim nodrošināt 32. līdz 36. pantā minēto pienākumu izpildi, ņemot vērā apstrādes veidu un apstrādātājam pieejamo informāciju".

Regulas 33. panta 2. punktā ir skaidri noteikts, ka, ja pārzinis izmanto apstrādātāju un apstrādātājam ir kļuvis zināms tādu personas datu pārkāpums, ko tas apstrādā pārziņa vārdā, viņam jāpaziņo par to pārzinim "bez nepamatotas kavēšanās". Jānorāda, ka pirms šādas paziņošanas apstrādātājam nevajag novērtēt pārkāpuma izraisītā riska iespējamību; šo novērtējumu veic pārzinis, tiklīdz viņam ir kļuvis zināms pārkāpums. Apstrādātājam vienkārši vajag konstatēt, vai ir noticis pārkāpums, un pēc tam par to paziņot pārzinim. Pārzinis izmanto apstrādātāju savu nolūku īstenošanai; tādēļ principā būtu jāuzskata, ka pārzinim pārkāpums ir kļuvis "zināms" brīdī, kad apstrādātājs viņu ir informējis par pārkāpumu. Apstrādātāja pienākums paziņot pārzinim ļauj pārzinim novērst pārkāpumu un noteikt, vai viņam jāpaziņo uzraudzības iestādei atbilstīgi 33. panta 1. punktam un skartajām personām atbilstīgi 34. panta 1. punktam. Pārzinis var arī vēlēties izmeklēt pārkāpumu, jo apstrādātājs var nezināt visus būtiskos faktus, kas saistīti ar šo jautājumu, piemēram, vai pārzinis joprojām ir saglabājis apstrādātāja iznīcināto vai nozaudēto personas datu kopiju vai rezerves kopiju. Tam var būt ietekme uz jautājumu, vai pārzinim pēc tam vajadzētu par to paziņot.

VDAR nav noteikts precīzs termiņš, kādā apstrādātājam ir jābrīdina pārzinis, izņemot to, ka tas jādara "bez nepamatotas kavēšanās". Tāpēc DG29 iesaka apstrādātājam nekavējoties informēt pārzini, sniedzot papildu informāciju par pārkāpumu pa posmiem, tiklīdz kļūst pieejama plašāka informācija. Tas ir svarīgi, lai pārzinim palīdzētu izpildīt prasību paziņot uzraudzības iestādei 72 stundu laikā.

Kā paskaidrots iepriekš, līgumā starp pārzini un apstrādātāju būtu jāprecizē, kā pildāmas 33. panta 2. punktā noteiktās prasības papildus citiem VDAR noteikumiem. Tas var ietvert prasības par apstrādātāja veiktu agrīno paziņošanu, kas savukārt ļautu pārzinim izpildīt pienākumu ziņot uzraudzības iestādei 72 stundu laikā.

Ja apstrādātājs sniedz pakalpojumus vairākiem pārziņiem, kurus skar viens un tas pats incidents, apstrādātājam informācija par incidentu būs jāsniedz katram pārzinim.

[25] Skatīt arī 79. apsvērumu.

Apstrādātājs varētu iesniegt paziņojumu pārziņa vārdā, ja pārzinis apstrādātājam ir piešķīris atbilstošu atļauju un tas ir paredzēts līgumā starp pārzini un apstrādātāju. Šāda paziņošana veicama saskaņā ar 33. un 34. pantu. Tomēr ir svarīgi atzīmēt, ka pārzinim saglabājas juridiskā atbildība par paziņošanu.

B. Informācijas sniegšana uzraudzības iestādei

1. Sniedzamā informācija

Kad pārzinis paziņo uzraudzības iestādei par pārkāpumu, 33. panta 3. punktā noteikts, ka paziņojumā vismaz:

"a) apraksta personas datu aizsardzības pārkāpuma raksturu, tostarp, ja iespējams, attiecīgo datu subjektu kategorijas un aptuveno skaitu un attiecīgo personas datu ierakstu kategorijas un aptuveno skaitu;

b) paziņo datu aizsardzības speciālista vārdu un uzvārdu un kontaktinformāciju vai norāda citu kontaktpunktu, kur var iegūt papildu informāciju;

c) apraksta personas datu aizsardzības pārkāpuma iespējamās sekas;

d) apraksta pasākumus, ko pārzinis veicis vai ierosinājis veikt, lai novērstu personas datu aizsardzības pārkāpumu, tostarp attiecīgā gadījumā — pasākumus, lai mazinātu tā iespējamās nelabvēlīgās sekas."

VDAR nav definētas datu subjektu vai personas datu ierakstu kategorijas. Tomēr DG29 ierosina datu subjektu kategorijas piesaistīt dažādiem to personu veidiem, kuru personas datus ir skāris pārkāpums: atkarībā no izmantotajiem deskriptoriem tie cita starpā varētu būt bērni un citas neaizsargātas grupas, personas ar invaliditāti, darbinieki vai klienti. Tāpat personas datu ierakstu kategorijas var attiekties uz dažādiem ierakstu veidiem, kādus pārzinis var apstrādāt, piemēram, dati par veselību, ieraksti par izglītību, informācija par sociālo aprūpi, finanšu informācija, bankas kontu numuri, pasu numuri, utt.

Regulas 85. apsvērumā ir skaidri noteikts, ka viens no paziņošanas mērķiem ierobežot personām nodarīto kaitējumu. Attiecīgi, ja datu subjektu veidi vai personas datu veidi norāda uz konkrēta kaitējuma risku pārkāpuma rezultātā (piemēram, identitātes zādzība, viltošana, finansiālie zaudējumi, draudi dienesta noslēpumam), tad ir svarīgi, lai paziņojumā būtu norādītas šīs kategorijas. Šādā veidā tas ir saistīts ar prasību aprakstīt pārkāpuma iespējamās sekas.

Precīzas informācijas trūkums (piemēram, precīzs skarto datu subjektu skaits) nedrīkstētu būt šķērslis savlaicīgai paziņošanai par pārkāpumu. VDAR ļauj noteikt aptuvenu skarto personu skaitu un attiecīgo personas datu skaitu. Galvenā uzmanība būtu jāpievērš pārkāpuma nelabvēlīgās ietekmes novēršanai, nevis precīzu datu sniegšanai. Tādējādi, kad kļūst skaidrs, ka ir noticis pārkāpums, bet tā apjoms vēl nav zināms, paziņojuma sniegšana pa posmiem (skatīt turpmāk) ir drošs veids, kā izpildīt paziņošanas pienākumus.

Regulas 33. panta 3. punktā noteikts, ka pārzinis paziņojumā sniedz "vismaz" šādu informāciju, tādēļ pārzinis vajadzības gadījumā var sniegt papildu informāciju. Dažādiem pārkāpumu veidiem (konfidencialitāte, integritāte vai pieejamība) var būt nepieciešama papildu informācija, lai pilnībā izskaidrotu katra gadījuma apstākļus.

**Piemērs**

Uzraudzības iestādes paziņojuma ietvaros pārzinis var uzskatīt par lietderīgu nosaukt savu apstrādātāju, ja tas ir pārkāpuma galvenais cēlonis, jo īpaši, ja tas ir izraisījis incidentu, kas skar daudzu citu pārziņu, kuri izmanto to pašu apstrādātāju, personas datu ierakstus.

Jebkurā gadījumā uzraudzības iestāde ir tiesīga pieprasīt papildu informāciju pārkāpuma izmeklēšanas ietvaros.

2. Paziņošana pa posmiem

Atkarībā no pārkāpuma būtības, lai konstatētu visus ar incidentu saistītos faktus, var būt nepieciešama pārziņa veikta papildu izmeklēšana. Tādēļ 33. panta 4. punktā noteikts, ka:

> "Ja un ciktāl informāciju nav iespējams sniegt vienlaikus, informāciju var sniegt pa posmiem bez turpmākas nepamatotas kavēšanās."

Tas nozīmē, ka VDAR ir atzīts, ka pārziņa rīcībā ne vienmēr būs visa nepieciešamā informācija par pārkāpumu 72 stundu laikā pēc tam, kad par to ir kļuvis zināms, jo pilnīga un visaptveroša informācija par incidentu šajā sākotnējā periodā var nebūt pieejama. Tādējādi ir atļauts paziņot pa posmiem. Visticamāk, tas būs sarežģītāku pārkāpumu gadījumā, piemēram, dažos ar kiberdrošību saistītos gadījumos, kad, piemēram, var būt nepieciešama padziļināta krimināltehniska izmeklēšana, lai pilnībā noteiktu pārkāpuma būtību un to, cik lielā mērā personas dati ir apdraudēti. Līdz ar to daudzos gadījumos pārzinim būs jāveic vēl plašāka izmeklēšana un jāiesniedz papildu informācija vēlāk. Tas ir pieļaujams ar nosacījumu, ka pārzinis norāda kavēšanās iemeslus atbilstīgi 33. panta 1. punktam. DG29 iesaka, ka gadījumos, kad pārzinis sniedz pirmo paziņojumu uzraudzības iestādei, viņam uzraudzības iestāde būtu arī jāinformē, ka viņa rīcībā vēl nav visa nepieciešamā informācija un ka sīkāka informācija tiks sniegta vēlāk. Uzraudzības iestādei būtu jāvienojas par to, kādā veidā un kad jāsniedz papildu informācija. Tas neliedz pārzinim sniegt papildu informāciju jebkurā citā posmā, ja viņam kļūst zināmas papildu būtiskas ziņas par pārkāpumu, kuras vajag iesniegt uzraudzības iestādei.

Paziņošanas prasības galvenais mērķis ir rosināt pārziņus nekavējoties rīkoties saistībā ar pārkāpumu, apturēt to un, ja iespējams, atgūt apdraudētos personas datus, kā arī lūgt uzraudzības iestādei atbilstošu padomu. Paziņošana uzraudzības iestādei pirmajās 72 stundās var ļaut pārzinim pārliecināties, vai lēmumi par paziņošanu vai nepaziņošanu personām ir pareizi.

Tomēr paziņojuma sniegšanas uzraudzības iestādei mērķis nav vienīgi iegūt norādījumus par to, vai paziņot skartām personām. Dažos gadījumos būs skaidrs, ka pārkāpuma būtības un riska nopietnības dēļ pārzinim vajadzēs nekavējoties paziņot skartajām personām. Piemēram, ja pastāv tūlītēji identitātes zādzības draudi vai ja īpašās personas datu kategorijas[26] tiek izpaustas tiešsaistē, pārziņiem būtu jārīkojas bez nepamatotas kavēšanās, lai apturētu pārkāpumu un informētu par to attiecīgās personas (skatīt III iedaļu). Ārkārtas apstākļos to varētu darīt pat pirms paziņošanas uzraudzības iestādei. Vispārīgāk runājot, paziņojums uzraudzības iestādei nedrīkst kalpot par attaisnojumu tam, ka datu subjekts nav informēts par pārkāpumu, ja tas ir nepieciešams.

Jāsaprot arī, ka pēc sākotnējā paziņojuma iesniegšanas pārzinis varētu sniegt uzraudzības iestādei atjauninātu informāciju, ja pēcpārbaudes izmeklēšanā tiek gūti pierādījumi, ka informācijas drošības incidents ticis apturēts un nekāda pārkāpuma faktiski nav. Pēc tam šo informāciju varētu papildināt ar informāciju, kas jau ir sniegta uzraudzības iestādei, un attiecīgi reģistrēt, ka šis incidentu nav pārkāpums. Netiek piemērots sods par incidenta ziņošanu, ja galu galā izrādās, ka tas nav pārkāpums.

**Piemērs**

Pārzinis 72 stundu laikā pēc pārkāpuma atklāšanas paziņo uzraudzības iestādei, ka ir nozaudējis *USB* zibatmiņu, kurā ir dažu viņa klientu personas datu kopija. *USB* zibatmiņa vēlāk tiek atrasta nolikta

[26] Skatīt 9. pantu.

nepareizā vietā pārziņa telpās un atgūta. Pārzinis sniedz uzraudzības iestādei atjauninātu informāciju un lūdz grozīt paziņojumu.

Jāatzīmē, ka pakāpeniska pieeja paziņošanai jau notiek saskaņā ar spēkā esošajiem Direktīvas 2002/58/EK, Regulas 611/2013 un citu pašu ziņotu incidentu pienākumiem.

3. Novēloti paziņojumi

Regulas 33. panta 1. punktā skaidri norādīts, ka gadījumos, kad uzraudzības iestādei nav paziņots 72 stundu laikā, paziņojumam pievieno kavēšanās iemeslus. Kopā ar paziņojuma sniegšanas pa posmiem jēdzienu šeit tiek atzīts, ka pārzinis ne vienmēr var sniegt paziņojumu par pārkāpumu šajā laika periodā un ka novēloti paziņojumi var būt pieļaujami.

Šāds scenārijs varētu būt, ja, piemēram, pārzinim īsā laika periodā rodas vairāki līdzīgi konfidencialitātes pārkāpumi, kas vienādi ietekmē lielu datu subjektu skaitu. Pārzinim varētu kļūt zināms par pārkāpumu un, uzsācis izmeklēšanu vēl pirms paziņošanas, viņš varētu atklāt papildu līdzīgus pārkāpumus, kuriem ir dažādi iemesli. Atkarībā no apstākļiem pārzinim var būt nepieciešams zināms laiks, lai noteiktu pārkāpumu apmēru, un, tā vietā, lai paziņotu par katru pārkāpumu atsevišķi, pārzinis sniedz jēgpilnu paziņojumu, kurā ir ietverti vairāki ļoti līdzīgi pārkāpumi ar iespējami atšķirīgiem iemesliem. Tā rezultātā uzraudzības iestādei paziņojums var tikt iesniegts ar novēlošanos, kas pārsniedz 72 stundas no brīža, kad pārzinim pirmo reizi ir kļuvuši zināmi šie pārkāpumi.

Stingri ņemot, katrs atsevišķs pārkāpums ir incidents, par kuru jāziņo. Tomēr, lai izvairītos no pārlieku apgrūtinošām darbībām, pārzinis var iesniegt "saistītu" paziņojumu, kurā norādīti visi šie pārkāpumi, ja vien tie attiecas uz viena un tā paša veida pārkāpumiem vienā un tajā pašā veidā salīdzinoši īsā laikā. Ja rodas virkne pārkāpumu, kas attiecas uz dažādiem personas datu veidiem, kuru aizsardzība tiek pārkāpta dažādos veidos, tad paziņojums sniedzams parastajā veidā, par katru pārkāpumu ziņojot saskaņā ar 33. pantu.

Kaut arī VDAR zināmā mērā ir pieļauti novēloti paziņojumi, nevajadzētu uzskatīt to par regulāru praksi. Ir vērts uzsvērt, ka saistīto paziņojumu var iesniegt arī par vairākiem līdzīgiem pārkāpumiem, par kuriem ir ziņots 72 stundu laikā.

C. Pārrobežu pārkāpumi un pārkāpumi ārpus ES esošās uzņēmējdarbības vietās

1. Pārrobežu pārkāpumi

Ja tiek veikta personas datu pārrobežu apstrāde[27], pārkāpums var ietekmēt datu subjektus vairāk nekā vienā dalībvalstī. Regulas 33. panta 1. punktā skaidri noteikts, ka pārkāpuma gadījumā pārziņiem būtu jāpaziņo kompetentajai uzraudzības iestādei atbilstīgi VDAR 55. pantam[28]. Regulas 55. panta 1. punktā noteikts:

"Katra uzraudzības iestāde savas dalībvalsts teritorijā ir kompetenta pildīt uzticētos uzdevumus un īstenot pilnvaras, ko tai piešķir saskaņā ar šo regulu."

Tomēr 56. panta 1. punktā noteikts:

[27] Skatīt 4. panta 23. punktu.

[28] Skatīt arī 122. apsvērumu.

"Neskarot 55. pantu, galvenās uzņēmējdarbības vietas vai pārziņa vai apstrādātāja darbības vietas uzraudzības iestāde ir kompetenta rīkoties kā vadošā uzraudzības iestāde attiecībā uz minētā pārziņa vai apstrādātāja veiktu pārrobežu apstrādi saskaņā ar 60. pantā paredzēto procedūru."

Turklāt 56. panta 6. punktā noteikts:

"Vadošā uzraudzības iestāde ir vienīgais pārziņa vai apstrādātāja partneris saistībā ar minētā pārziņa vai apstrādātāja veiktu pārrobežu apstrādi."

Tas nozīmē, ka ikreiz, kad tiek izdarīts pārkāpums pārrobežu apstrādes un paziņošanas kontekstā, pārzinim vajadzēs paziņot vadošajai uzraudzības iestādei[29]. Tāpēc, izstrādājot pārkāpuma reaģēšanas plānu, pārzinim ir jāizvērtē, kura uzraudzības iestāde ir vadošā uzraudzības iestāde, kam vajadzēs paziņot[30]. Tādējādi pārzinis var nekavējoties reaģēt uz pārkāpumu un pildīt savus pienākumus atbilstīgi 33. pantam. Jāsaprot, ka ar pārrobežu apstrādi saistīta pārkāpuma gadījumā ir jāiesniedz paziņojums vadošajai uzraudzības iestādei, kas ne vienmēr atrodas tur, kur atrodas attiecīgie datu subjekti vai kur faktiski ir izdarīts pārkāpums. Informējot vadošo iestādi, pārzinim attiecīgā gadījumā būtu jānorāda, vai pārkāpums attiecas uz uzņēmējdarbības vietām, kas atrodas citās dalībvalstīs, un kuru dalībvalstu datu subjektus šis pārkāpums varētu skart. Ja pārzinim ir šaubas par vadošās uzraudzības iestādes identitāti, tam vismaz būtu jāpaziņo vietējai uzraudzības iestādei vietā, kurā pārkāpums ir izdarīts.

### 2. Pārkāpumi ārpus ES esošās uzņēmējdarbības vietās

Regulas 3. pants attiecas uz VDAR teritoriālo piemērošanas jomu, tostarp, ja to piemēro personas datu apstrādei, ko veic pārzinis vai apstrādātājs, kas neveic uzņēmējdarbību ES. Jo īpaši 3. panta 2. punktā noteikts[31]:

"Šo regulu piemēro Savienībā esošu datu subjektu personas datu apstrādei, ko veic pārzinis vai apstrādātājs, kas neveic uzņēmējdarbību Savienībā, ja apstrādes darbības ir saistītas ar:

a) preču vai pakalpojumu piedāvāšanu šādiem datu subjektiem Savienībā, neatkarīgi no tā, vai no datu subjekta tiek prasīta samaksa; vai

b) viņu uzvedības novērošanu, ciktāl viņu uzvedība notiek Savienībā."

Būtisks ir arī 3. panta 3. punkts, kurā noteikts[32]:

"Šo regulu piemēro personas datu apstrādei, ko veic pārzinis, kas neveic uzņēmējdarbību Savienībā, bet vietā, kur saskaņā ar starptautiskajām publiskajām tiesībām ir piemērojamas dalībvalsts tiesības."

Ja pārzinim, kas neveic uzņēmējdarbību ES, piemēro 3. panta 2. punktu vai 3. panta 3. punktu, un tam ir noticis pārkāpums, šim pārzinim joprojām ir saistoši 33. un 34. pantā ietvertie paziņošanas

[29] Skatīt DG29 Pamatnostādnes pārziņa vai apstrādātāja vadošās uzraudzības iestādes noteikšanai, pieejamas tīmekļa vietnē http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] Visu Eiropas valstu datu aizsardzības iestāžu kontaktinformācija pieejama tīmekļa vietnē: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] Skatīt arī 23. un 24. apsvērumu.

[32] Skatīt arī 25. apsvērumu.

pienākumi. Regulas 27. pantā noteikts, ka gadījumos, kad piemērojams 3. panta 2. punkts, pārzinis (un apstrādātājs) ieceļ pārstāvi ES. Šādos gadījumos DG29 iesaka iesniegt paziņojumu uzraudzības iestādei tajā dalībvalstī, kurā pārziņa pārstāvis ES veic uzņēmējdarbību[33]. Tāpat, ja apstrādātājam piemēro 3. panta 2. punktu, tam būs saistoši apstrādātāju pienākumi, jo īpaši pienākums paziņot pārzinim par pārkāpumu saskaņā ar 33. panta 2. punktu.

D. Nosacījumi, kad paziņošana nav obligāta

Regulas 33. panta 1. punktā skaidri noteikts, ka uzraudzības iestādei nav jāpaziņo par pārkāpumiem, kas "maz ticams (..) varētu radīt risku fizisku personu tiesībām un brīvībām". Kā piemēru varētu minēt situāciju, kad personas dati jau ir publiski pieejami un šādu datu izpaušana nerada iespējamu risku personai. Tas ir pretstatā spēkā esošajām Direktīvas 2009/136/EK prasībām paziņot par pārkāpumiem, kas attiecas uz publiski pieejamu elektroniskās komunikācijas pakalpojumu sniedzējiem, kur nosaka, ka par visiem attiecīgajiem pārkāpumiem ir jāpaziņo kompetentajai iestādei.

Savā Atzinumā 03/2014 attiecībā uz informēšanu par pārkāpumu[34] DG29 skaidroja, ka konfidencialitātes pārkāpums attiecībā uz personas datiem, kuri šifrēti ar modernu algoritmu, tik un tā ir personas datu aizsardzības pārkāpums, un par to ir jāziņo. Tomēr, ja atslēgas konfidencialitāte ir neskarta, t. i., atslēgu neapdraudēja nekāds drošības pārkāpums, un tā tika ģenerēta tā, ka tos nevar pārbaudīt neviena persona, kurai nav atļauta piekļuve tiem, izmantojot pieejamos tehniskos līdzekļus, tādā gadījumā dati ir praktiski nesaprotami. Tādējādi maz ticams, ka pārkāpumam būs nelabvēlīgas sekas attiecībā uz personām un līdz ar to šīs personas nav jāinformē[35]. Taču pat tad, ja dati ir šifrēti, to nozaudēšana vai pārveidošana var radīt nelabvēlīgas sekas datu subjektiem, ja pārziņa rīcībā nav atbilstošu rezerves kopiju. Šajā gadījumā datu subjekti būtu jāinformē, pat ja datiem būtu piemēroti atbilstoši šifrēšanas pasākumi.

DG29 arī paskaidroja, ka līdzīgi būtu arī gadījumā, kad personas dati, piemēram, paroles, ir droši sajaukti un tiem pievienota kriptogrāfiskā jaucējvērtība "*salt*", jaucējvērtība ir aprēķināta ar modernu kriptogrāfisku jaucējfunkciju ar atslēgu, datu jaukšanas atslēgu nav skāris nekāds pārkāpums un datu jaukšanas atslēga ir ģenerēta tā, ka to ar pieejamiem tehniskajiem līdzekļiem nevar noskaidrot neviens, kam nav pilnvaru piekļūt atslēgai.

Tādējādi, ja personas dati būtībā ir nesaprotami personām, kurām nav atļauts tiem piekļūt, un, ja datiem ir kopija vai rezerves kopija, par konfidencialitātes pārkāpumu, kas skar pareizi šifrētus personas datus, nav jāpaziņo uzraudzības iestādei. Tas ir tādēļ, ka maz ticams, ka šāds pārkāpums radīs risku personas tiesībām un brīvībām. Tas, protams, nozīmē, ka nebūtu arī jāsniedz informācija personām, jo augsts risks ir maz ticams. Tomēr jāpatur prātā, ka, lai gan paziņošana sākotnēji var nebūt nepieciešama, jo nav iespējamo risku personas tiesībām un brīvībām, laika gaitā tas var mainīties un risks būtu jāpārvērtē. Piemēram, ja vēlāk tiek konstatēts, ka šī atslēga ir bojāta vai tiek konstatēta šifrēšanas programmatūras ievainojamība, paziņojums joprojām var būt jāsniedz.

Turklāt jāatzīmē, ka gadījumā, ja ir noticis pārkāpums un nav šifrētu personas datu rezerves kopiju, tad tas būs pieejamības pārkāpums, kas varētu radīt risku personām, un tādēļ var būt nepieciešams sniegt paziņojumu. Tāpat, ja notiek pārkāpums, kas saistīts ar šifrētu datu nozaudēšanu, pat ja pastāv personas datu rezerves kopijas, tas joprojām var būt pārkāpums, par kuru jāziņo – atkarībā no tā, cik ilgs laiks ir nepieciešams, lai atjaunotu datus no šīm rezerves kopijām, un sekām, kādas pieejamības

[33] Skatīt 80. apsvērumu un 27. pantu.

[34] DG29, Atzinums 03/2014 attiecībā uz informēšanu par pārkāpumu, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] Skatīt Regulas 611/2013 4. panta 1. un 2. punktu.

trūkums rada personām. Kā noteikts 32. panta 1. punkta c) apakšpunktā, svarīgs drošības faktors ir "spēja laicīgi atjaunot personas datu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums".

**Piemērs**

Pārkāpuma, par kuru nav jāpaziņo uzraudzības iestādei, piemērs būtu tādas droši šifrētas mobilās ierīces nozaudēšana, kuru izmanto pārzinis un viņa darbinieki. Ja šifrēšanas atslēga paliek pārziņa drošā valdījumā un tā nav vienīgā personas datu kopija, tad personas dati uzbrucējam nebūtu pieejami. Tas nozīmē, ka ir maz ticams, ka pārkāpums radīs risku attiecīgo datu subjektu tiesībām un brīvībām. Ja vēlāk kļūst skaidrs, ka šifrēšanas atslēga ir bojāta vai šifrēšanas programmatūra vai algoritms ir ievainojami, risks fizisku personu tiesībām un brīvībām mainīsies, un tādā gadījumā var būt nepieciešams sniegt paziņojumu.

Tomēr 33. panta prasību neievērošana būs tādā gadījumā, kad pārzinis neinformē uzraudzības iestādi par situāciju, kurā dati faktiski nav bijuši droši šifrēti. Tādēļ, izvēloties šifrēšanas programmatūru, pārziņiem rūpīgi jāizvērtē piedāvātā šifrēšanas kvalitāte un pienācīga ieviešana un jāsaprot, kādu aizsardzības līmeni tā faktiski nodrošina un vai tas atbilst norādītajiem riskiem. Pārziņiem būtu arī jāzina, kā darbojas šifrēšanas produkts. Piemēram, ierīce var tikt šifrēta, tiklīdz tā ir izslēgta, bet ne gaidīšanas režīmā. Dažiem produktiem, kuriem izmanto šifrēšanu, ir "noklusējuma atslēgas", kuras katram klientam ir jāmaina, lai tās darbotos. Var arī gadīties, ka drošības eksperti šifrēšanu šobrīd uzskata par piemērotu, bet pēc dažiem gadiem tā var būt novecojusi, t. i., apšaubāms, vai dati būtu pietiekami šifrēti, izmantojot šo produktu, un būtu nodrošināts atbilstošs aizsardzības līmenis.

## III. Regulas 34. pants — datu subjekta informēšana

### A. Personu informēšana

Noteiktos gadījumos papildus paziņojuma iesniegšanai uzraudzības iestādei pārzinim ir jāinformē par pārkāpumu arī skartās personas.

Regulas 34. panta 1. punktā noteikts:

"Gadījumā, ja personas datu aizsardzības pārkāpums varētu radīt augstu risku fizisku personu tiesībām un brīvībām, pārzinis bez nepamatotas kavēšanās paziņo datu subjektam par personas datu aizsardzības pārkāpumu."

Pārzinim būtu jāatceras, ka paziņojums uzraudzības iestādei ir obligāts, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām. Turklāt gadījumos, kad pārkāpuma rezultātā pastāv augsts risks personas tiesībām un brīvībām, ir jāinformē arī šīs personas. Tādējādi slieksnis personu informēšanai par pārkāpumiem ir augstāks nekā paziņošanai uzraudzības iestādēm, un ne par visiem pārkāpumiem ir jāinformē personas, tādējādi pasargājot tās no nevajadzīgas informēšanas mazsvarīgos gadījumos.

VDAR norādīts, ka personas jāinformē par pārkāpumiem "bez nepamatotas kavēšanās", kas nozīmē — cik drīz vien iespējams. Galvenais personu informēšanas mērķis ir sniegt konkrētu informāciju par pasākumiem, kas tām jāveic, lai sevi aizsargātu[36]. Kā jau minēts iepriekš, atkarībā no

[36] Skatīt arī 86. apsvērumu.

pārkāpuma rakstura un riska, laicīga informēšana ļaus personām veikt pasākumus, lai pasargātu sevi no pārkāpuma nelabvēlīgajām sekām.

Šo pamatnostādņu B pielikumā ir sniegts neizsmeļošs to piemēru saraksts, kuros pārkāpums var radīt augtu risku personām, un attiecīgi gadījumi, kad pārzinim ir jāpaziņo skartām personām par pārkāpumu.

B. Sniedzamā informācija

Attiecībā uz paziņošanu personām 34. panta 2. punktā noteikts:

> "Paziņojumā datu subjektam, kas minēts šā panta 1. punktā, izmantojot skaidru un vienkāršu valodu, apraksta personas datu aizsardzības pārkāpuma raksturu un ietver vismaz 33. panta 3. punkta b), c) un d) apakšpunktā paredzēto informāciju un pasākumus."

Atbilstīgi šim noteikumam pārzinim būtu jāsniedz vismaz šāda informācija:

- pārkāpuma rakstura apraksts;
- datu aizsardzības speciālista vārds un uzvārds un kontaktinformācija vai cits kontaktpunkts;
- pārkāpuma iespējamo seku apraksts un
- apraksts par pasākumiem, ko pārzinis veicis vai ierosinājis pārkāpumu novēršanai, tostarp — attiecīgā gadījumā — pasākumiem, lai mazinātu tā iespējamās nelabvēlīgās sekas.

Kā piemēru pasākumiem, kas veikti, lai novērstu pārkāpumu un mazinātu tā iespējamās nelabvēlīgās sekas, pārzinis varētu norādīt, ka pēc pārkāpuma paziņošanas attiecīgajai uzraudzības iestādei pārzinis ir saņēmis padomu par pārkāpuma novēršanu un tā ietekmes mazināšanu. Pārzinim vajadzības gadījumā būtu arī jāsniedz konkrēti padomi personām, lai tās pasargātu sevi no pārkāpuma iespējamām nelabvēlīgām sekām, piemēram, veikt paroles atiestatīšanu, ja to piekļuves akreditācijas dati ir bijuši apdraudēti. Turklāt pārzinis var izvēlēties sniegt informāciju papildus šeit prasītajam.

C. Saziņa ar personām

Principā par attiecīgajiem pārkāpumiem ir tieši jāinformē skartie datu subjekti, izņemot gadījumus, kad tas prasa nesamērīgas pūles. Šādā gadījumā tā vietā izmanto publisku saziņu vai līdzīgu pasākumu, ar ko datu subjekti tiek informēti vienlīdz efektīvā veidā (34. panta 3. punkta c) apakšpunkts).

Informējot datu subjektus par pārkāpumu, jāizmanto īpaši tam paredzēti ziņojumi, un šo informāciju nedrīkst nosūtīt kopā ar citu informāciju, piemēram, regulāriem atjauninājumiem, informatīviem biļeteniem vai standarta ziņojumiem. Tas palīdz paziņojumu par pārkāpumu padarīt skaidru un pārredzamu.

Piemēri pārredzamām saziņas metodēm ietver tiešu ziņojumapmaiņu (piemēram, e-pastu, SMS, tiešo ziņojumu), labi redzamas tīmekļa vietņu reklāmjoslas vai paziņojumus, saziņu par pastu un uzskatāmas reklāmas drukātajos plašsaziņas līdzekļos. Paziņojums, kas sniegts tikai kā paziņojums presei vai korporatīvais emuārs, nav uzskatāms par efektīvu veidu, kā informēt personu par pārkāpumu. DG29 iesaka pārziņiem izvēlēties līdzekļus, kas maksimāli palielina iespēju pienācīgi informēt visas skartās personas. Atkarībā no apstākļiem tas var nozīmēt, ka pārzinis izmanto vairākas saziņas metodes, nevis vienu saziņas kanālu.

Pārziņiem var arī būt jānodrošina, lai saziņa būtu pieejama atbilstošos alternatīvos formātos un attiecīgajās valodās, nodrošinot, ka personas spēj izprast tām sniegto informāciju. Piemēram, ja persona tiek informēta par pārkāpumu, parasti piemērotā saziņas valoda būs tā, kuru saņēmējs izmantojis agrākajā parastajā uzņēmējdarbības gaitā. Tomēr, ja pārkāpums ietekmē datu subjektus, ar kuriem pārzinis pirms tam nav saskāries, vai jo īpaši tos, kuri dzīvo citā dalībvalstī vai ārpus ES esošā

valstī, kas nav pārziņa uzņēmējdarbības vieta, saziņa vietējā valsts valodā varētu būt pieņemama, ņemot vērā nepieciešamos resursus. Galvenais ir palīdzēt datu subjektiem saprast pārkāpuma būtību un pasākumus, kurus viņi var veikt, lai sevi aizsargātu.

Pārziņi vislabāk var noteikt piemērotāko saziņas kanālu, lai informētu personas par pārkāpumu, jo īpaši ja tiem ir bieža saskare ar saviem klientiem. Tomēr nepārprotami pārzinim būtu jāatturas izmantot tādu saziņas kanālu, kuru skāris pārkāpums, jo šo kanālu varētu izmantot arī uzbrucēji, kas uzdodas par pārzini.

Tajā pašā laikā 86. apsvērumā paskaidrots:

> "Šāda paziņošana datu subjektam būtu jāveic cik vien iespējams ātri un ciešā sadarbībā ar uzraudzības iestādi, ievērojot tās vai citas attiecīgas iestādes, piemēram, tiesībaizsardzības iestādes, sniegtos norādījumus. Piemēram, ja nepieciešams mazināt tūlītēju kaitējuma risku, būtu ātri jāsniedz paziņojums datu subjektam, taču nepieciešamība īstenot piemērotus pasākumus, lai novērstu datu aizsardzības pārkāpuma turpināšanos vai līdzīgus personas datu pārkāpumus, var attaisnot vēlāku paziņošanu."

Tādēļ pārzinis varētu sazināties un konsultēties ar uzraudzības iestādi ne tikai, lai lūgtu padomu par datu subjektu informēšanu par pārkāpumu saskaņā ar 34. pantu, bet arī par atbilstošiem ziņojumiem, kas jānosūta, un par piemērotāko veidu saziņai ar personām.

Ar to ir saistīts 88. apsvērumā sniegtais ieteikums, ka paziņojumā par pārkāpumu būtu "jāņem vērā tiesībaizsardzības iestāžu leģitīmās intereses, ja priekšlaicīga informācijas atklāšana varētu nevajadzīgi kavēt personas datu pārkāpuma apstākļu izmeklēšanu". Tas var nozīmēt, ka noteiktos apstākļos, ja tas ir pamatoti, un pēc tiesībaizsardzības iestāžu ieteikuma pārzinis var aizkavēt skarto personu informēšanu par pārkāpumu līdz brīdim, kad tā neietekmēs šādu izmeklēšanu. Tomēr pēc šī perioda datu subjektus joprojām vajadzētu informēt nekavējoties.

Ikreiz, kad pārzinim nav iespējams informēt personu par pārkāpumu, jo viņa rīcībā nav pietiekami daudz datu saziņai ar personu, minētajos konkrētajos apstākļos pārzinim būtu jāinformē persona, tiklīdz tas ir pamatoti iespējams (piemēram, ja persona īsteno savas 15. pantā paredzētās tiesības piekļūt personas datiem un sniedz pārzinim saziņai nepieciešamo papildu informāciju).

### D. Nosacījumi, kad informēšana nav obligāta

Regulas 34. panta 3. punktā ir norādīti trīs nosacījumi, kad pārkāpuma gadījumā paziņojums personām nav jāsniedz. Tie ir šādi:

- pārzinis pirms pārkāpuma personas datu aizsardzībai ir piemērojis atbilstīgus tehniskus un organizatoriskus aizsardzības pasākumus, jo īpaši tādus pasākumus, kas personas datus padara nesaprotamus personām, kurām nav pilnvaru piekļūt datiem. Tas varētu, piemēram, ietvert personas datu aizsardzību, izmantojot vismodernāko šifrēšanu vai sadalīšanu daļiņās.
- Tūlīt pēc pārkāpuma pārzinis ir veicis pasākumus, ar ko nodrošina, lai, visticamāk, vairs nevarētu materializēties augstais risks attiecībā uz personu tiesībām un brīvībām. Piemēram, atkarībā no lietas apstākļiem pārzinis varēja nekavējoties identificēt un rīkoties attiecībā uz personu, kura ir piekļuvusi personas datiem, pirms tā ir spējusi kaut ko ar šiem datiem izdarīt. Joprojām ir jāpievērš pienācīga uzmanība iespējamām konfidencialitātes pārkāpumu sekām atkarībā no attiecīgo datu veida.

- Saziņa ar personām prasītu nesamērīgi lielas pūles[37], ja, iespējams, to kontaktinformācija ir zudusi pārkāpuma rezultātā vai vispār nav bijusi zināma. Piemēram, statistikas biroja noliktava ir applūdusi, un personas datus saturošie dokumenti tika glabāti tikai papīra formā. Tā vietā pārzinim ir jāsniedz publisks paziņojums vai jāveic līdzīgs pasākums, ar ko personas tiek informētas vienlīdz efektīvā veidā. Gadījumā, ja ir jāpieliek nesamērīgi lielas pūles, var arī paredzēt tehniskus pasākumus, lai informāciju par pārkāpumu varētu saņemt pēc pieprasījuma, kas var izrādīties noderīgi personām, kuras pārkāpums var būt skāris, bet pārzinim nav iespēju citādi sazināties.

Saskaņā ar pārskatatbildības principu pārziņiem būtu jāspēj uzskatāmi parādīt uzraudzības iestādei, ka viņi atbilst vienam vai vairākiem no šiem nosacījumiem[38]. Jāpatur prātā, ka, lai gan paziņošana sākotnēji var nebūt nepieciešama, jo nav riska fiziskas personas tiesībām un brīvībām, laika gaitā tas var mainīties un risks būtu jāpārvērtē.

Ja pārzinis nolemj neinformēt personu par pārkāpumu, 34. panta 4. punktā ir paskaidrots, ka uzraudzības iestāde to var pieprasīt, ja tā uzskata, ka pārkāpums var radīt augstu risku personām. Alternatīvi, iestāde var uzskatīt, ka ir izpildīti 34. panta 3. punkta nosacījumi, un tādā gadījumā nav jāpaziņo personām. Ja uzraudzības iestāde konstatē, ka lēmums nepaziņot datu subjektiem nav pamatots, tā var apsvērt iespēju izmantot savas pilnvaras un sankcijas.

## IV. **Riska un augsta riska novērtēšana**

### A. Risks kā paziņošanas pienākuma ierosinātājs

Lai gan VDAR ieviests pienākums paziņot par pārkāpumu, nav prasības to darīt visos gadījumos:

- Paziņojums kompetentajai uzraudzības iestādei ir obligāts, izņemot gadījumus, kad ir maz ticams, ka pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām.
- Personas informēšana par pārkāpumu ir veicama tikai tad, ja šis pārkāpums, visticamāk, radīs augstu risku personas tiesībām un brīvībām.

Tas nozīmē, ka nekavējoties, tiklīdz pārzinim ir kļuvis zināms par pārkāpumu, viņam ir būtiski svarīgi ne tikai censties apturēt incidentu, bet arī novērtēt risku, kuru tas varētu radīt. Tam ir divi svarīgi iemesli: pirmkārt, zinot ietekmes uz personu iespējamību un potenciālo nopietnību, pārzinis var veikt efektīvus pasākumus pārkāpuma apturēšanai un novēršanai; otrkārt, tas palīdzēs noteikt, vai ir jāsniedz paziņojums uzraudzības iestādei un vajadzības gadījumā jāinformē attiecīgās personas.

Kā paskaidrots iepriekš, paziņojums par pārkāpumu ir obligāts, izņemot gadījumus, kad ir maz ticams, ka tas radīs risku personu tiesībām un brīvībām, un galvenais iemesls, kāpēc datu subjektu informēšana par pārkāpumu kļūst obligātā, ir iespējamība, ka tas var radīt *augstu* risku personas tiesībām un brīvībām. Šis risks pastāv, ja pārkāpums var radīt fizisku, materiālu vai nemateriālu kaitējumu personām, kuru datu aizsardzības pārkāpums ir noticis. Šāda kaitējuma piemēri ir diskriminācija, identitātes zādzība vai viltošana, finansiālie zaudējumi un kaitējums reputācijai. Ja pārkāpums skar personas datus, kas atklāj rases vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, vai satur ģenētiskos datus, datus par veselību vai

[37] Skatīt DG29 Pamatnostādnes par pārredzamību, kurās tiks izskatīts jautājums par nesamērīgām pūlēm, pieejamas tīmekļa vietnē http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] Skatīt 5. panta 2. punktu.

seksuālo dzīvi, vai sodāmību un noziedzīgiem nodarījumiem, vai ar tiem saistītiem drošības pasākumiem, uzskata, ka šāds kaitējums, visticamāk, radīsies[39].

B. Faktori, kas jāņem vērā, novērtējot risku

VDAR 75. un 76. apsvērumā ir norādīts, ka, novērtējot risku, parasti ir jāņem vērā gan riska iespējamība attiecībā uz datu subjektu tiesībām un brīvībām, gan tā nopietnība. Tajos arī norādīts, ka risks jānovērtē, pamatojoties uz objektīvu novērtējumu.

Jāatzīmē, ka, novērtējot pārkāpuma rezultātā radīto risku cilvēku tiesībām un brīvībām, tiek savādāk aplūkots risks, kas tiek ņemts vērā DAIN)[40]. DAIN tiek apskatīti gan saskaņā ar plānu veiktās datu apstrādes riski, gan riski pārkāpuma gadījumā. Apsverot iespējamo pārkāpumu, vispārīgi tiek izskatīta tā rašanās iespēja, tā rezultātā datu subjektam radītais iespējamais kaitējums; citiem vārdiem sakot, tas ir teorētiska notikuma izvērtējums. Faktiska pārkāpuma gadījumā šis notikums jau ir iestājies, un tāpēc uzmanība tiek pievērsta tikai tam, kāds ir tā rezultātā personām radītās ietekmes risks.

**Piemērs**

DAIN norādīts, ka konkrētā drošības programmatūras produkta ierosinātā izmantošana personas datu aizsardzībai ir piemērots pasākums, lai nodrošinātu drošības līmeni, kas atbilst riskam, kādu apstrāde citos apstākļos radītu personai. Tomēr, ja vēlāk kļūst zināms, ka pastāv ievainojamība, programmatūras piemērotība riska aizsargātajiem personas datiem ierobežošanai mainītos, tādēļ tā būtu jāpārvērtē esošā DAIN ietvaros.

Produkta ievainojamība vēlāk tiek izmantota, un notiek pārkāpums. Pārzinim būtu jānovērtē pārkāpuma konkrētie apstākļi, skartie dati un iespējamās ietekmes līmenis uz personām, kā arī tas, kāda ir šī riska materializācijas iespējamība.

Attiecīgi, novērtējot pārkāpuma radīto risku personām, pārzinim būtu jāņem vērā pārkāpuma konkrētie apstākļi, tostarp iespējamās ietekmes nopietnība un tā iestāšanās iespējamība. Tādēļ DG29 iesaka novērtējumā ņemt vērā šādus kritērijus[41].

- Pārkāpuma veids

Notikušā pārkāpuma veids var ietekmēt personām radītā riska līmeni. Piemēram, konfidencialitātes pārkāpums, saskaņā ar kuru medicīniska informācija ir atklāta nepiederošām personām, var radīt atšķirīgas sekas personai nekā pārkāpums, kura rezultātā personas medicīniskie dati ir nozaudēti un vairs nav pieejami.

- Personas datu raksturs, sensitivitāte un apjoms

Protams, novērtējot risku, galvenais faktors ir to personas datu veids un sensitivitāte, kurus ir skāris pārkāpums. Parasti, jo sensitīvāki dati, jo lielāks kaitējuma risks skartajām personām, taču jāapsver arī citi personas dati, kas jau var būt pieejami par datu subjektu. Piemēram, personas vārda un adreses

[39] Skatīt 75. un 85. apsvērumu.

[40] Skatīt DG Pamatnostādnes par DAIN šeit: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[41] Regulas 611/2013 3. panta 2. punktā sniegti norādījumi par faktoriem, kas jāņem vērā saistībā ar paziņojumu par pārkāpumiem elektroniskās komunikācijas pakalpojumu nozarē, kas var būt noderīgi VDAR paziņojuma kontekstā. Skatīt http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:lv:PDF

izpaušana parastajos apstākļos nevarētu radīt būtisku kaitējumu. Tomēr, ja adoptētāja vecāku vārds un adrese tiek atklāti bioloģiskajam vecākam, sekas var būt ļoti smagas gan adoptētājam, gan bērnam.

Pārkāpumi, kas saistīti ar informāciju par veselības stāvokli, personu apliecinošiem dokumentiem vai finanšu datiem, piemēram, kredītkartes datiem, var radīt kaitējumu paši par sevi, bet kopā tos var izmantot identitātes zādzībai. Personas datu kombinācija parasti ir sensitīvāka nekā atsevišķa personas datu daļa.

Sākotnēji šķiet, ka dažu veidu personas dati var būt salīdzinoši nekaitīgi, tomēr būtu rūpīgi jāapsver, ko šie dati var atklāt par skarto personu. To klientu saraksts, kuri saņem regulāras piegādes, var nebūt īpaši sensitīvs, taču tāda pati informācija par klientiem, kuri pieprasījuši viņu piegādes apturēt atvaļinājuma periodā, būtu noderīga informācija noziedzniekiem.

Tāpat nelielam apjomam ļoti sensitīvu personas datu var būt liela ietekme uz personu, un plašs informācijas spektrs var atklāt vēl plašāku informāciju par šo personu. Arī pārkāpums, kas skar lielu personas datu apjomu par daudziem datu subjektiem, var ietekmēt attiecīgu lielu personu skaitu.

- Personu vienkārša identificēšana

Svarīgs faktors, kas jāņem vērā, ir tas, cik viegli personai, kurai ir piekļuve apdraudētajiem personas datiem, ir identificēt konkrētas personas vai arī datus salāgot ar citu informāciju personu identificēšanas nolūkā. Atkarībā no apstākļiem identifikācija var būt iespējama tieši, izmantojot pārkāpuma skartos personas datus, bez īpašas izpētes atklājot personas identitāti, taču personas datu salāgošana ar konkrētu personu var būt ļoti sarežģīta, taču iespējama noteiktos apstākļos. Identifikācija var būt tieši vai netieši iespējama, izmantojot pārkāpumā iesaistītos datus, taču tā var būt atkarīga arī no konkrētā pārkāpuma konteksta un saistīto personas datu publiskās pieejamības. Tas varētu būt būtiskāk konfidencialitātes un pieejamības pārkāpumu gadījumā.

Kā minēts iepriekš, personas dati, kas tiek aizsargāti, izmantojot atbilstošu šifrēšanas līmeni, bez šifrēšanas atslēgas ir nesaprotami personām, kurām nav pilnvaru piekļūt šādiem datiem. Turklāt pienācīgi īstenota pseidonimizācija (definēta 4. panta 5. punktā kā "personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nav iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu") var arī mazināt personu identificēšanas iespēju pārkāpuma gadījumā. Tomēr nevar uzskatīt, ka tikai ar pseidonimizācijas paņēmieniem datus var padarīt nesaprotamus.

- Seku nopietnība personām.

Atkarībā no pārkāpumā iesaistīto personas datu veida, piemēram, īpašām datu kategorijām, iespējamais personām radītais kaitējums var būt īpaši nopietns, jo īpaši, ja pārkāpums var izraisīt identitātes zādzību vai viltošanu, fizisku kaitējumu, psiholoģisku krīzi, pazemojumu vai kaitējumu reputācijai. Ja pārkāpums attiecas uz neaizsargātu personu personas datiem, kaitējuma risks var būt vēl lielāks.

Fakts, vai pārzinim ir zināms, ka personas dati atrodas tādu cilvēku rokās, kuru nodomi nav zināmi vai, iespējams, ir ļaunprātīgi, var ietekmēt potenciālā riska līmeni. Var būt konfidencialitātes pārkāpums, ar kuru personas dati tiek izpausti trešai personai atbilstīgi 4. panta 10. punktam vai citam kļūdainam adresātam. Tā var notikt, piemēram, ja personas dati tiek nejauši nosūtīti nepareizai organizācijas nodaļai vai plaši izmantotai piegādātāju organizācijai. Pārzinis var pieprasīt saņēmējam atdot vai droši iznīcināt datus, ko tas ir saņēmis. Abos gadījumos, ņemot vērā to, ka pārzinim ir pastāvīgas attiecības ar viņiem, un pārzinim var būt zināmas viņu procedūras, vēsture un cita būtiska informācija, saņēmēju var tikt uzskatīts par "uzticamu". Citiem vārdiem sakot, pārzinis var būt zināmā mērā pārliecināts par saņēmēju un pamatoti sagaidīt, ka šī persona nelasīs vai nepiekļūs

kļūdaini nosūtītajiem datiem, kā arī izpildīs pārziņa norādījumus atdot datus. Pat tad, ja datiem ir piekļūts, pārzinis joprojām varētu uzticēties, ka saņēmējs neveiks nekādas turpmākās darbības un nekavējoties atdos datus pārzinim, kā arī sadarbosies to atgūšanai. Šādos gadījumos to var ņemt vērā riska novērtējumā, kuru pārzinis veic pēc pārkāpuma, — fakts, ka saņēmējs ir uzticams, var novērst pārkāpuma seku nopietnību, bet tas nenozīmē, ka pārkāpums nav noticis. Tomēr tādā gadījumā var tikt likvidēta personām sagādātā riska iespējamība, kā rezultātā nav nepieciešams sniegt paziņojumu ne uzraudzības iestādei, ne skartajām personām. Atkal tas būt jāizvērtē katrā atsevišķā gadījumā. Tomēr pārzinim joprojām ir jāsaglabā informācija par pārkāpumu vispārējā pienākuma veikt pārkāpumu uzskaiti ietvaros (skatīt V iedaļu turpmāk).

Būtu jāņem vērā arī personām radīto seku pastāvīgums, jo ietekme var tikt uzskatīta par plašāku, ja tā ir ilglaicīga.

- Personas īpašas pazīmes

Pārkāpums var skart bērnu vai citu neaizsargātu personu personas datus, kā rezultātā šīs personas var tikt pakļautas augstākam apdraudējumu riskam. Var būt citi ar personu saistītie faktori, kas var skart pārkāpuma ietekmes līmeni uz tām.

- Datu pārziņa īpašās pazīmes

Pārziņa raksturs un loma, kā arī tā darbības var ietekmēt pārkāpuma rezultātā personām radītā riska līmeni. Piemēram, medicīniska organizācija apstrādās īpašas personas datu kategorijas, kas nozīmē, ka, salīdzinot ar laikraksta adresātu sarakstu, personas datu pārkāpuma gadījumā šīs personas tiek pakļautas lielākam apdraudējumam.

- Skarto personu skaits

Pārkāpums var ietekmēt tikai vienu vai dažas personas, vai vairākus tūkstošus vai vēl vairāk. Parasti, jo lielāks ir skarto personu skaits, jo lielāka var būt pārkāpuma ietekme. Tomēr pārkāpums var smagi ietekmēt pat vienu personu atkarībā no personas datu veida un apdraudējuma konteksta. Tādēļ galvenais ir apsvērt ietekmes iespējamību un nopietnību attiecībā uz skartajām personām.

- Vispārīgie aspekti

Tāpēc, novērtējot pārkāpuma rezultātā radīto iespējamo risku, pārzinim būtu jāapsver iespējamās ietekmes uz personu tiesībām un brīvībām nopietnības pakāpe un iespējamība. Nepārprotami: jo nopietnākas ir pārkāpuma sekas, jo augstāks ir risks, tāpat, jo šo seku iespējamība ir lielāka, jo paaugstinās arī risks. Ja rodas šaubas, pārzinim būtu jāievēro piesardzība un jāsniedz paziņojums. B pielikumā sniegti daži noderīgi dažāda veida tādu pārkāpumu piemēri, kas saistīti ar risku vai augstu risku personām.

Eiropas Savienības Tīklu un informācijas drošības aģentūra (*ENISA*) ir izstrādājusi ieteikumus pārkāpuma nopietnības novērtēšanas metodikai, kas var būt noderīgi pārziņiem un apstrādātājiem, izstrādājot pārkāpumu pārvaldības reaģēšanas plānu[42].

## V. Pārskatatbildība un uzskaite

### A. Pārkāpumu dokumentēšana

[42] *ENISA*, Ieteikumi metodikai, kā novērtēt personas datu aizsardzības pārkāpumu smagumu, https://www.enisa.europa.eu/publications/dbn-severity

Neatkarīgi no tā, vai par pārkāpumu jāpaziņo uzraudzības iestādei, pārzinim ir jāglabā dokumentācija par visiem pārkāpumiem, kā paskaidrots 33. panta 5. punktā:

> "Pārzinis dokumentē visus personas datu aizsardzības pārkāpumus, norādot faktus, kas saistīti ar personas datu pārkāpumu, tā sekas un veiktās koriģējošās darbības. Minētā dokumentācija ļauj uzraudzības iestādei pārbaudīt šā panta ievērošanu."

Tas ir saistīts ar VDAR pārskatatbildības principu, kas ietverts 5. panta 2. punktā. Pārkāpumu, par kuriem nav jāziņo, un pārkāpumu, par kuriem jāpaziņo, reģistrācijas mērķis ir arī saistīts ar pārziņa 24. pantā noteiktajiem pienākumiem, un uzraudzības iestāde var pieprasīt šos ierakstus apskatīt. Tādēļ pārziņiem ir ieteikts izveidot iekšēju pārkāpumu reģistru neatkarīgi no tā, vai par šiem pārkāpumiem ir jāpaziņo[43].

Lai gan pārzinim ir pienākums noteikt, kādu metodi un struktūru izmantot pārkāpumu dokumentēšanai, ir galvenie elementi attiecībā uz reģistrējamo informāciju, kas būtu jāiekļauj visos gadījumos. Kā prasīts 33. panta 5. punktā, pārzinim vajag reģistrēt informāciju par pārkāpumu, norādot iemeslus, to, kas noticis, un skartos personas datus. Informācijā būtu arī jāietver pārkāpuma sekas un ietekme, kā arī pārziņa veiktās koriģējošās darbības.

VDAR nav noteikts šādu dokumentu saglabāšanas periods. Ja šādos ierakstos ir ietverti personas dati, pārzinim būs pienākums noteikt atbilstošu saglabāšanas periodu saskaņā ar personas datu apstrādei piemērojamajiem principiem[44] un izpildīt apstrādes likumīga pamatojuma prasības[45]. Pārzinim vajadzēs saglabāt dokumentāciju saskaņā ar 33. panta 5. punktu tiktāl, ciktāl to var pieprasīt, lai pierādītu uzraudzības iestādei atbilstību šī panta prasībām vai vispārīgāk — pārskatatbildības principam. Protams, ja paši ieraksti nesatur personas datus, VDAR noteiktais glabāšanas ierobežojuma princips[46] nav piemērojams.

Papildus šai informācijai DG29 iesaka pārzinim arī dokumentēt, reaģējot uz pārkāpumu, pieņemto lēmumu pamatojumu. Jo īpaši šāds lēmuma pamatojums būtu jādokumentē, ja par pārkāpumu netiek paziņots. Tajā ir jāiekļauj iemesli, kādēļ pārzinis uzskata, ka ir maz ticams, ka šis pārkāpums radīs risku fizisku personu tiesībām un brīvībām[47]. Alternatīvi, ja pārzinis uzskata, ka kāds no 34. panta 3. punkta nosacījumiem ir izpildīts, viņam būtu jāspēj sniegt to pamatojošus atbilstošus pierādījumus.

Ja pārzinis paziņo uzraudzības iestādei par pārkāpumu, bet paziņojums ir sniegts ar nokavēšanos, pārzinim jāspēj pamatot šī kavēšanās; ar to saistītā dokumentācija varētu palīdzēt uzskatāmi parādīt, ka ziņojuma iesniegšanas aizkavēšanās ir pamatota, ne pārmērīga.

Informējot skartās personas par pārkāpumu, pārziņa sniegtajai informācijai par pārkāpumu ir jāatbilst pārredzamības principiem un tai jābūt sniegtai efektīvi un savlaicīgi. Pārzinim būtu vieglāk uzskatāmi parādīt pārskatatbildību un atbilstības nodrošināšanu, saglabājot pierādījumus par šādu saziņu.

---

[43] Pārzinis var izvēlēties dokumentēt pārkāpumus atbilstīgi 30. panta prasībām uzturētā apstrādes darbību reģistra ietvaros. Nav nepieciešams uzturēt atsevišķu reģistru, ja informācija, kas attiecas uz pārkāpumu, ir skaidri identificējama pati par sevi un to var iegūt pēc pieprasījuma.

[44] Skatīt 5. pantu.

[45] Skatīt 6., kā arī 9. pantu.

[46] Skatīt 5. panta 1. punkta e) apakš□punktu.

[47] Skatīt 85. apsvērumu.

Lai palīdzētu nodrošināt atbilstību 33. un 34. pantam, gan pārziņiem, gan apstrādātājiem būtu lietderīgi sagatavot dokumentētu paziņošanas procedūru, norādot procesu, kas jāievēro, tiklīdz ir atklāts pārkāpums, tostarp, kā apturēt, pārvaldīt incidentu un atgūties no tā, kā arī novērtēt risku un paziņot par pārkāpumu. Šajā sakarā, lai pierādītu atbilstību VDAR prasībām, var arī būt noderīgi uzskatāmi parādīt, ka darbinieki ir informēti par šādu procedūru un mehānismu pastāvēšanu un zina, kā reaģēt uz pārkāpumiem.

Jāatzīmē, ka nepareizas pārkāpuma dokumentēšanas rezultātā uzraudzības iestāde var īstenot savas pilnvaras saskaņā ar 58. pantu un/vai piemērot administratīvu sodu saskaņā ar 83. pantu.

### B. Datu aizsardzības speciālista loma

Pārzinim vai apstrādātājam var būt datu aizsardzības speciālists (DAS)[48] saskaņā ar 37. pantu vai pēc brīvprātības principa, pamatojoties uz labo praksi. VDAR 39. pantā DAS noteikti vairāki obligāti uzdevumi, bet tas neaizliedz pārzinim vajadzības gadījumā noteikt papildu uzdevumus.

Īpaši svarīgi paziņošanas par pārkāpumu pienākuma kontekstā DAS obligātie uzdevumi cita starpā ietver pienākumus sniegt datu aizsardzības padomus un informāciju pārzinim vai apstrādātājam, uzraudzīt atbilstību VDAR un sniegt padomus saistībā ar DAIN. DAS arī jāsadarbojas ar uzraudzības iestādi un jādarbojas kā uzraudzības iestādes un datu subjektu kontaktpunktam. Jāatzīmē, ka, paziņojot uzraudzības iestādei par pārkāpumu, 33. panta 3. punkta b) apakšpunktā noteikts, ka pārzinim ir jānorāda sava DAS vai cita kontaktpunkta vārds un kontaktinformācija.

Attiecībā uz pārkāpumu dokumentēšanu pārzinis vai apstrādātājs, iespējams, vēlēsies saņemt sava DAS viedokli par šādas dokumentācijas struktūru, izveidi un pārvaldīšanu. DAS var tikt uzdots papildu uzdevums uzturēt šādus ierakstus.

Šie faktori nozīmē, ka DAS būtu jāuzņemas būtiska loma, palīdzot novērst pārkāpumu vai sagatavoties tam, sniedzot padomus un uzraugot atbilstību, kā arī pārkāpuma laikā (t. i., paziņojot uzraudzības iestādei) un jebkuras turpmākas uzraudzības iestādes veiktas izmeklēšanas laikā. Ņemot to vērā, DG29 iesaka, ka DAS tiek nekavējoties informēts par pārkāpuma esību un iesaistīts visā pārkāpumu pārvaldības un paziņošanas procesā.

## VI. Pienākums paziņot saskaņā ar citiem juridiskajiem instrumentiem

Papildus paziņošanai un informēšanai par pārkāpumiem un atsevišķi no šiem pienākumiem saskaņā ar VDAR pārziņiem vajadzētu arī būt informētiem par jebkuru prasību paziņot par informācijas drošības incidentiem saskaņā ar citiem saistītiem tiesību aktiem, kas uz viņiem var attiekties, un par to, vai viņiem par personas datu aizsardzības pārkāpumu vienlaikus ir arī jāpaziņo uzraudzības iestādei. Šādas prasības dalībvalstīs var atšķirties, taču citos juridiskajos instrumentos norādīto paziņošanas prasību piemēri un to savstarpējās attiecības ar VDAR ietver šo:

- Regula (ES) Nr. 910/2014 par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū (*eIDAS* regula)[49].

Saskaņā ar *eIDAS* regulas 19. panta 2. punktu uzticamības pakalpojumu sniedzējiem jāpaziņo savai uzraudzības iestādei par drošības pārkāpumu vai integritātes zudumu, kas būtiski ietekmē sniegto uzticamības pakalpojumu vai tajā uzturētos personas datus. Attiecīgā gadījumā, t. i., ja šāds

[48] Skatīt DG Pamatnostādnes par DAS šeit: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[49] Skatīt https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:32014R0910&from=LV

pārkāpums vai zaudējums ir arī personas datu aizsardzības pārkāpums saskaņā ar VDAR, uzticamības pakalpojuma sniedzējam būtu arī jāpaziņo uzraudzības iestādei.

- Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (TID direktīva)[50].

TID direktīvas 14. un 16. pants prasa, lai pamatpakalpojumu sniedzēji un digitālie pakalpojumu sniedzēji paziņotu par informācijas drošības incidentiem savai kompetentajai iestādei. Kā atzīts TID 63. apsvērumā[51], informācijas drošības incidentos bieži vien var tikt apdraudēti personas dati. Kaut arī TID prasīts kompetentajām un uzraudzības iestādēm sadarboties un apmainīties ar informāciju šajā kontekstā, joprojām gadījumos, kad šādi incidenti ir vai kļūst par personas datu pārkāpumiem saskaņā ar VDAR, attiecīgajiem operatoriem un/vai pakalpojumu sniedzējiem ir jāpaziņo uzraudzības iestādei neatkarīgi no TID ietvertajām prasībām par paziņošanu par incidentiem.

**Piemērs**

Mākoņpakalpojumu sniedzējam, kas paziņo par pārkāpumu saskaņā ar TID direktīvu, var būt arī japaziņo pārzinim, ja tas skar personas datu aizsardzības pārkāpumu. Tāpat uzticamības pakalpojuma sniedzējam, kas sniedz paziņojumu saskaņā *eIDAS*, pārkāpuma gadījumā var arī būt pienākums paziņot attiecīgajai datu aizsardzības iestādei.

- Direktīva 2009/136/EK (Pilsoņu tiesību direktīva) un Regula 611/2013 (Regula par pārkāpumu paziņošanu).

Publiski pieejamu elektroniskās komunikācijas pakalpojumu sniedzējiem Direktīvas 2002/58/EK[52] kontekstā jāpaziņo par pārkāpumiem kompetentajām valsts iestādēm.

Pārziņiem būtu arī jāapzinās visi papildu juridiskie, medicīniskie vai profesionālie paziņošanas pienākumi saskaņā ar citiem piemērojamiem režīmiem.

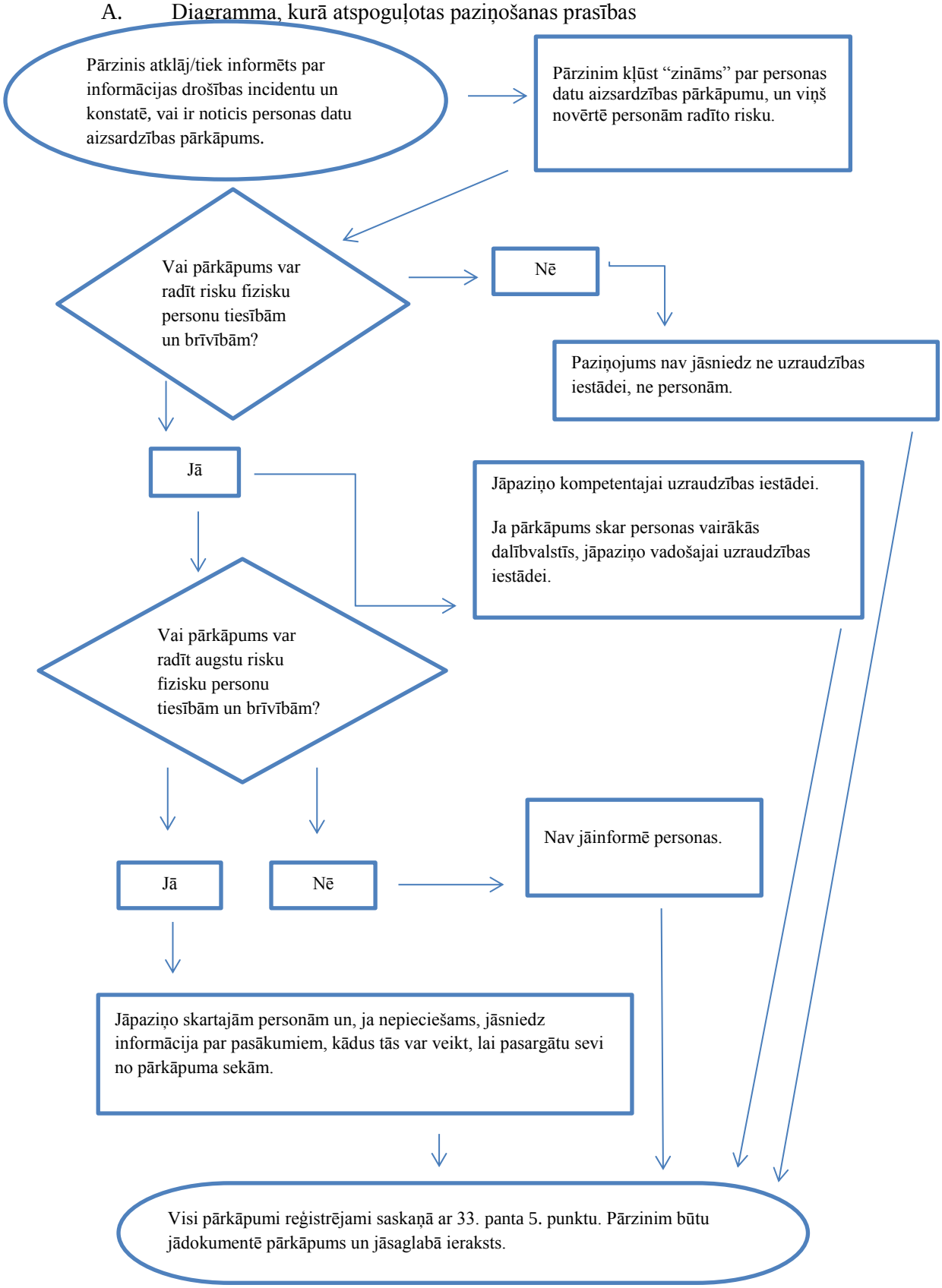
[50] Skatīt https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:32016L1148&from=EN

51 Regulas 63. apsvērums: *"Incidentu dēļ daudzos gadījumos tiek kompromitēti personas dati. Šajā sakarā kompetentajām iestādēm un datu aizsardzības iestādēm būtu jāsadarbojas un jāapmainās ar informāciju visos attiecīgos jautājumos, lai novērstu jebkurus personas datu aizsardzības pārkāpumus, kas rodas incidentu dēļ."*

[52] Eiropas Komisija 2017. gada 10. janvārī ierosināja Privātuma un elektronisko sakaru regulu, ar ko aizstās Direktīvu 2009/136/EK un atcels paziņošanas prasības. Tomēr, kamēr šis priekšlikums nav apstiprināts Eiropas Parlamentā, spēkā esošā paziņošanas prasība paliek spēkā, skatīt https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

## VII. **Pielikums**

### A. Diagramma, kurā atspoguļotas paziņošanas prasības



B. Personas datu aizsardzības pārkāpumu piemēri, un kam par tiem jāpaziņo

Turpmāk sniegtais neizsmeļošais piemēru saraksts palīdzēs pārziņiem noteikt, vai viņiem vajag sniegt paziņojumu dažādos personas datu aizsardzības pārkāpumu scenārijos. Šie piemēri var arī palīdzēt atšķirt risku un augstu risku personas tiesībām un brīvībām.

| **Piemērs** | **Vai jāpaziņo uzraudzības iestādei?** | **Vai jāpaziņo datu subjektam?** | **Piezīmes/ieteikumi** |
|---|---|---|---|
| i) Pārzinis glabāja *USB* zibatmiņā šifrētu personas datu arhīva rezerves kopiju. Ielaušanās laikā atslēga tiek nozagta. | Nē. | Nē. | Kamēr dati tiek šifrēti, izmantojot modernu algoritmu, datu rezerves kopijas pastāv, unikāla atslēga nav bojāta un datus iespējams savlaicīgi atjaunot, tas var nebūt pārkāpums, par kuru ir jāziņo. Tomēr, ja atslēga vēlāk tiek bojāta, paziņošana ir obligāta. |
| ii) Pārzinis uztur tiešsaistes pakalpojumu. Kiberuzbrukuma šim pakalpojumam rezultātā personu personas dati tiek izfiltrēti.<br><br>Pārzinim ir klienti vienā dalībvalstī. | Jā, ziņot uzraudzības iestādei, ja ir iespējamas sekas personām. | Jā, ziņot personām atkarībā no skarto personas datu veida un ja iespējamo seku nopietnības pakāpe personām ir augsta. | |
| iii) Īss strāvas padeves pārtraukums, kas ilgst vairākas minūtes pārziņa zvanu centrā, kā rezultātā klienti nespēj sazvanīt pārzini un piekļūt saviem ierakstiem. | Nē. | Nē. | Tas nav pārkāpums, par kuru jāpaziņo, bet joprojām ir reģistrējams incidents saskaņā ar 33. panta 5. punktu.<br><br>Pārzinim būtu jāuztur atbilstoši ieraksti. |
| iv) Pārzinis cieš no ļaunprātīgas programmatūras uzbrukuma, kā rezultātā visi dati tiek šifrēti. Nav pieejamas rezerves kopijas, un datus nav iespējams atjaunot. Izmeklēšanas laikā kļūst skaidrs, ka ļaunprātīgās programmatūras | Jā, ziņot uzraudzības iestādei, ja ir iespējamas sekas personām, jo šis ir pieejamības zudums. | Jā, ziņot personām atkarībā no skarto personas datu rakstura un šo datu nepieejamības iespējamās ietekmes, kā arī citām iespējamām sekām. | Ja būtu pieejama rezerves kopija un datus būtu iespējams atjaunot savlaicīgi, par to nevajadzētu ziņot uzraudzības iestādei un personām, jo nebūtu neatgriezeniskas pieejamības vai konfidencialitātes zuduma. Tomēr, ja uzraudzības iestādei kļūtu |

| | | | |
|---|---|---|---|
| vienīgā funkcija bija datu šifrēšana un ka sistēmā nebija citas ļaunprogrammatūras. | | | zināms par incidentu citā veidā, tā varētu apsvērt izmeklēšanu, lai novērtētu atbilstību 32. pantā minētajām plašākajām drošības prasībām. |
| v) Persona zvana bankas zvanu centram, lai ziņotu par datu aizsardzības pārkāpumu. Persona ir saņēmusi citas personas ikmēneša pārskatu.<br><br>Pārzinis veic īsu izmeklēšanu (t. i., to pabeidz 24 stundu laikā) un pamatoti droši konstatē, ka ir noticis personas datu aizsardzības pārkāpums un vai šis ir sistēmisks trūkums, kas var nozīmēt, ka varētu būt skartas arī citas personas. | Jā. | Tiek informētas tikai skartās personas, ja pastāv augsts risks un ir skaidrs, ka citas personas nav skartas. | Ja papildu izmeklēšanas gaitā tiek konstatēts, ka skartas vairākas personas, uzraudzības iestādei jāsniedz atjaunināta informācija, un pārzinis papildus informē citas personas, ja pastāv augsts risks attiecībā uz tām. |
| vi) Pārzinis vada tiešsaistes tirgu, un viņam ir klienti vairākās dalībvalstīs. Tirgus cieš no kiberuzbrukuma, un uzbrucējs tiešsaistē publicē lietotājvārdus, paroles un pirkumu vēsturi. | Jā, jāziņo vadošajai uzraudzības iestādei, ja ir ietverta pārrobežu apstrāde. | Jā, jo varētu radīt augstu risku. | Pārzinim būtu jārīkojas, piemēram, panākot skarto kontu paroļu piespiedu nomaiņu, kā arī jāveic citi pasākumi riska mazināšanai.<br><br>Pārzinim būtu jāapsver arī jebkādi citi paziņošanas pienākumi, piemēram, saskaņā ar TID direktīvu kā digitālo pakalpojumu sniedzējam. |
| vii) Tīmekļa vietnes mitināšanas uzņēmums, kas darbojas kā datu apstrādātājs, identificē kļūdu kodā, ar kuru kontrolē lietotāja autorizāciju. Kļūdas sekas nozīmē to, ka | Tīmekļa vietnes mitināšanas uzņēmumam kā apstrādātājam jāpaziņo saviem skartajiem klientiem (pārziņiem) bez nepamatotas kavēšanās. | Ja nav augsta riska attiecībā uz personām, tām nav jāpaziņo. | Tīmekļa vietnes mitināšanas uzņēmumam (apstrādātājam) jāapsver jebkādi citi paziņošanas pienākumi (piemēram, saskaņā ar TID direktīvu kā digitālo pakalpojumu sniedzējam). |

| | | | |
|---|---|---|---|
| jebkuram lietotājam ir pieeja konta informācijai par jebkuru citu lietotāju. | Pieņemot, ka tīmekļa vietnes mitināšanas uzņēmums ir veicis savu izmeklēšanu, skartajiem pārziņiem vajadzētu būt pamatoti pārliecinātiem par to, vai viņus ir skāris pārkāpums un, visticamāk, tiks uzskatīts, ka viņiem pārkāpums ir "kļuvis zināms", tiklīdz viņi ir saņēmuši informāciju no mitināšanas uzņēmuma (apstrādātāja). Pēc tam pārzinim jāpaziņo uzraudzības iestādei. | | Ja netiek konstatēts, ka šī ievainojamība tiek izmantota attiecībā uz kādu no tā pārziņiem, iespējams, nav noticis pārkāpums, par kuru jāpaziņo, bet tas, visticamāk, ir reģistrējams vai norāda uz neatbilstību saskaņā ar 32. pantu. |
| viii) Kiberuzbrukuma dēļ slimnīcā 30 stundas nav pieejamas medicīniskās kartes. | Jā, slimnīcai ir pienākums paziņot, jo pastāv augsta riska iespēja pacientu labklājībai un privātumam. | Jā, ziņot skartām personām. | |
| ix) Ļoti daudzu studentu personas dati kļūdaini tiek nosūtīti uz nepareizu adresātu sarakstu ar vairāk nekā 1000 saņēmējiem. | Jā, ziņot uzraudzības iestādei. | Jā, ziņot personām atkarībā no skarto personas datu apjoma un veida un iespējamo seku nopietnības. | |
| x) Tiešās tirgvedības e-pasts tiek nosūtīts adresātiem, kas norādīti laukos "kam" vai "kopija", tādējādi ļaujot visiem adresātiem redzēt citu adresātu e-pasta adresi. | Jā, paziņojuma sniegšana uzraudzības iestādei var būt obligāta, ja tiek skarts liels personu skaits, ja tiek izpausti sensitīvi dati (piem., psihoterapeita adresātu saraksts) vai citi faktori rada augsta risku (piem., pastā ir ietvertas sākotnējās paroles). | Jā, ziņot personām atkarībā no skarto personas datu apjoma un veida un iespējamo seku nopietnības. | Paziņojuma sniegšana var nebūt obligāta, ja nav izpausti sensitīvi dati un ja tiek atklāts tikai neliels e-pasta adrešu skaits. |