Pamatnostādnes 01/2021

par personas datu aizsardzības pārkāpumu paziņošanu — piemēri

Pieņemtas 2021. gada 14. decembrī

Versija 2.0

Versiju tabula

Versija 2.0	14.12.2021.	Pamatnostādņu pieņemšana pēc sabiedriskās apspriešanas
Versija 1.0	14.01.2021.	Pamatnostādņu pieņemšana sabiedriskajai apspriešanai

Saturs

EIROPAS DATU AIZSARDZĪBAS KOLĒĢIJA,

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes Regulā (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk — VDAR),

ņemot vērā EEZ līgumu, jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas 2018. gada 6. jūlija Lēmumu Nr. 154/2018[1],

ņemot vērā Reglamenta 12. un 22. punktu,

ņemot vērā Komisijas Paziņojumu Eiropas Parlamentam un Padomei "Datu aizsardzība kā iedzīvotāju tiesību nodrošināšanas un ES digitālās pārkārtošanās pīlārs — Vispārīgās datu aizsardzības regulas piemērošanas divi gadi"[2],

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

1 IEVADS

1. VDAR noteiktos gadījumos ievieš prasību paziņot par personas datu aizsardzības pārkāpumu kompetentajai valsts uzraudzības iestādei (turpmāk — UI) un personām, kuras personas datus pārkāpums ir skāris (33. un 34. pants).

2. 29. panta darba grupa jau 2017. gada oktobrī izstrādāja *vispārīgas* pamatnostādnes par personas datu aizsardzības pārkāpumu paziņošanu, analizējot attiecīgās VDAR iedaļas (Pamatnostādnes par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu 2016/679, *WP* 250) (turpmāk — Pamatnostādnes *WP* 250)[3]. Tomēr to būtības un publicēšanas laika dēļ šajās pamatnostādnēs nebija pietiekami sīki aplūkoti visi praktiskie jautājumi. Tāpēc ir radusies vajadzība pēc *konkrētām un praktiskām* vadlīnijām, kurās izmantota pieredze, ko guvušas uzraudzības iestādes kopš VDAR piemērošanas sākuma.

3. Šis dokuments ir paredzēts Pamatnostādņu *WP* 250 papildināšanai un atspoguļo EEZ uzraudzības iestāžu kopīgo pieredzi kopš VDAR piemērošanas sākuma. Tā mērķis ir palīdzēt datu pārziņiem izlemt, kā rīkoties datu aizsardzības pārkāpumu gadījumos un kādi faktori jāņem vērā, veicot riska novērtējumu.

4. Lai varētu novērst pārkāpumu, pārzinim un apstrādātājam vispirms ir jāspēj to atpazīt. VDAR 4. panta 12. punktā "personas datu aizsardzības pārkāpums" ir definēts kā "drošības pārkāpums, kura rezultātā

[1] Atsauces uz "dalībvalstīm" šajā dokumentā būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".

[2] COM(2020) 264 final, 2020. gada 24. jūnijs.

[3] G29 *WP*250 1. red., 2018. gada 6. februāris, Pamatnostādnes par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar Regulu 2016/679 — apstiprināts EDAK, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

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

5. Savā Atzinumā 03/2014 par pārkāpumu paziņošanu[4] un Pamatnostādnēs *WP* 250 DG29 paskaidroja, ka pārkāpumus var iedalīt kategorijās saskaņā ar šādiem trim labi zināmiem informācijas drošības principiem:

- "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 personas datiem vai personas datu iznīcināšana[5].

6. Pārkāpumiem var būt ievērojami nelabvēlīga ietekme uz personām, un tie var izraisīt fizisku, materiālu vai nemateriālu kaitējumu. VDAR skaidrots, ka tie var izraisīt kontroles zaudēšanu pār saviem personas datiem vai personu tiesību ierobežošanu, diskrimināciju, identitātes zādzību vai viltošanu, finansiālu zaudējumu, neatļautu pseidonimizācijas atcelšanu, kaitējumu reputācijai, ar dienesta noslēpumu aizsargātu personas datu konfidencialitātes zaudēšanu. Tie var radīt attiecīgajai fiziskajai personai arī jebkādu citu īpaši nelabvēlīgu ekonomisko vai sociālo situāciju. Viens no svarīgākajiem datu pārziņa pienākumiem ir izvērtēt šos riskus datu subjektu tiesībām un brīvībām un īstenot atbilstošus tehniskos un organizatoriskos pasākumus to novēršanai.

7. Attiecīgi VDAR uzliek pienākumu pārzinim:

- dokumentēt visus personas datu aizsardzības pārkāpumus, norādot faktus, kas saistīti ar personas datu pārkāpumu, tā sekas un veiktās koriģējošās darbības[6];
- paziņot par personas datu aizsardzības pārkāpumu uzraudzības iestādei, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām[7];
- paziņot datu subjektam par personas datu aizsardzības pārkāpumu gadījumā, ja personas datu aizsardzības pārkāpums varētu radīt augstu risku fizisku personu tiesībām un brīvībām[8].

8. Ir saprotams, ka datu aizsardzības pārkāpumi ir problēma, taču tie var norādīt arī uz nepilnīgu, iespējams, novecojušu datu drošības režīmu, kā arī uz sistēmas nepilnībām, kas jānovērš. Vispārpieņemts uzskats ir tāds, ka vienmēr labāk datu aizsardzības pārkāpumus novērst, iepriekš sagatavojoties, jo dažas to sekas pēc būtības ir neatgriezeniskas. Pirms pārzinis var *pilnībā* novērtēt risku, ko rada noteikta veida uzbrukuma izraisīts pārkāpums, ir jānosaka problēmas pamatcēlonis, lai saprastu, vai ievainojamības, kas pieļāva incidentu, joprojām pastāv un rada risku. Daudzos gadījumos pārzinis var noteikt, ka incidents var radīt

---

[4] G29 *WP*213, 2014. gada 25. marts, Atzinums 03/2014 attiecībā uz informēšanu par personas datu aizsardzības pārkāpumu, 5. lpp., https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[5] Sk. Pamatnostādnes *WP* 250, 7. lpp. Jāņem vērā, ka datu aizsardzības pārkāpums var attiekties uz vienu kategoriju vai vairākām kategorijām vienlaikus.

[6] VDAR 33. panta 5. punkts.

[7] VDAR 33. panta 1. punkts.

[8] VDAR 34. panta 1. punkts.

risku, un tāpēc par to ir jāpaziņo. Citos gadījumos paziņošana nav jāatliek līdz brīdim, kad pilnībā novērtēts ar pārkāpumu saistītais risks un ietekme, jo pilnīgs riska novērtējums var notikt vienlaicīgi ar paziņošanu, un šādi iegūtu informāciju UI var sniegt pa posmiem bez turpmākas nepamatotas kavēšanās[9].

9. Par pārkāpumu jāpaziņo, ja pārzinis uzskata, ka tas var radīt risku datu subjekta tiesībām un brīvībām. Pārziņiem šis novērtējums jāveic, tiklīdz viņi uzzina par pārkāpumu. Pārzinim nevajadzētu gaidīt detalizētu tiesu ekspertīzi un (agrīnus) risku mazinošos pasākumus, pirms sākt novērtēt, vai datu aizsardzības pārkāpums var radīt risku un vai par to būtu jāinformē.

10. Ja pārzinis pats novērtē risku kā maz ticamu, bet izrādās, ka risks materializējas, kompetentā UI var izmantot savas korektīvās pilnvaras un noteikt sankcijas.

11. Katram pārzinim un apstrādātājam ir jābūt plāniem un procedūrām iespējamo datu aizsardzības pārkāpumu novēršanai. Organizāciju rīcībā jābūt skaidrai pakļautības kārtībai un personām, kas ir atbildīgas par noteiktiem atjaunošanas procesa aspektiem.

12. Ir būtiski nodrošināt arī pārziņa un apstrādātāja darbinieku mācības un veidot izpratni par datu aizsardzības jautājumiem, galveno uzmanību pievēršot personas datu aizsardzības pārkāpumu pārvaldībai (personas datu aizsardzības pārkāpuma identificēšanai un turpmāk veicamajām darbībām, utt.). Šīs mācības ir regulāri jāatkārto atkarībā no apstrādes darbības veida un pārziņa lieluma, ņemot vērā jaunākās tendences un brīdinājumus par kiberuzbrukumiem vai citiem drošības incidentiem.

13. Pārskatatbildības un integrētās datu aizsardzības princips varētu ietvert analīzi, ko iekļauj paša datu pārziņa un datu apstrādātāja "Rokasgrāmatā par rīcību personas datu aizsardzības pārkāpumu gadījumā", kuras mērķis ir noteikt faktus attiecībā uz katru apstrādes aspektu galvenajos datu apstrādes posmos. Šāda iepriekš sagatavota rokasgrāmata būtu daudz ātrāk pieejams informācijas avots, kas ļautu datu pārziņiem un datu apstrādātājiem bez nepamatotas kavēšanās mazināt riskus un izpildīt saistības. Rezultātā būtu nodrošināts, ka personas datu aizsardzības pārkāpumu gadījumā organizācijas darbinieki zinātu, kā rīkoties, un incidents, visticamāk, tiktu atrisināts ātrāk nekā tad, ja risku mazinošu pasākumu vai plānu nebūtu.

14. Lai gan turpmāk minētie gadījumi nav īsti, tie ir pamatoti ar tipiskiem gadījumiem no uzraudzības iestāžu kolektīvās pieredzes saistībā ar paziņojumiem par datu aizsardzības pārkāpumiem. Piedāvāto gadījumu analīze attiecas uz konkrētiem pārbaudāmajiem gadījumiem, taču var palīdzēt datu pārziņiem novērtēt datu aizsardzības pārkāpumus, ar ko saskaras viņi paši. Jebkādas izmaiņas turpmāk aprakstīto gadījumu apstākļos var radīt atšķirīgus vai vēl lielākus riskus, tādējādi varētu būt nepieciešami citi vai papildu pasākumi. Šajās pamatnostādnēs gadījumi ir strukturēti atbilstoši noteiktām pārkāpumu kategorijām (piemēram, izspiedējprogrammatūras uzbrukumi). Izskatot noteiktas kategorijas pārkāpumus, katrā gadījumā ir nepieciešami noteikti riska mazināšanas pasākumi. Šie pasākumi nav obligāti jāatkārto katrā vienas un tās pašas pārkāpumu kategorijas analīzē. Attiecībā uz vienas kategorijas gadījumiem ir norādītas tikai atšķirības. Tāpēc ir jāizlasa visi attiecīgās pārkāpumu kategorijas gadījumi, lai noteiktu un atšķirtu visus atbilstošos veicamos pasākumus.

15. Pārkāpuma iekšējā dokumentēšana ir pienākums, kas nav atkarīgs no riskiem, kuri saistīti ar pārkāpumu, un ir jāveic katrā atsevišķā gadījumā. Turpmāk aprakstītie gadījumi varētu sniegt zināmu skaidrību par to, vai paziņot par pārkāpumu UI un ietekmētajiem datu subjektiem.

[9] VDAR 33. panta 4. punkts.

2 IZSPIEDĒJPROGRAMMATŪRA

16. Bieži iemesls paziņojumam par datu aizsardzības pārkāpumu ir izspiedējprogrammatūras uzbrukums, no kā cietis datu pārzinis. Šādos gadījumos ļaunkods šifrē personas datus, un pēc tam uzbrucējs pieprasa pārzinim izpirkuma maksu apmaiņā pret atšifrēšanas kodu. Šāda veida uzbrukumu parasti var klasificēt kā pieejamības pārkāpumu, taču bieži vien var rasties arī konfidencialitātes pārkāpums.

2.1 1. GADĪJUMS — izspiedējprogrammatūra ar pareizi izveidotu dublējumkopiju un bez eksfiltrācijas

Kāda neliela ražošanas uzņēmuma datorsistēmas tika pakļautas izspiedējprogrammatūras uzbrukumam, un šajās sistēmās glabātie dati tika šifrēti. Datu pārzinis bija veicis datu šifrēšanu miera stāvoklī, izmantojot modernāko šifrēšanas algoritmu, tāpēc visi dati, kuriem piekļuva izspiedējprogrammatūra, bija glabāti šifrētā veidā. Atšifrēšanas atslēga uzbrukumā netika uzlauzta, t. i., uzbrucējs nevarēja tai ne piekļūt, ne netieši to izmantot. Tādējādi uzbrucējam bija piekļuve tikai šifrētiem personas datiem. Turklāt netika ietekmēta ne uzņēmuma e-pasta sistēma, ne arī klientu sistēmas, kas tika izmantotas, lai tai piekļūtu. Uzņēmums incidenta izmeklēšanā izmanto ārēja kiberdrošības uzņēmuma palīdzību. Ir pieejami žurnāli, kas izseko visas no uzņēmuma izejošās datu plūsmas (tostarp nosūtītās e-pasta vēstules). Analizējot žurnālus un uzņēmuma izmantoto atklāšanas sistēmu apkopotos datus, iekšējā izmeklēšanā ar ārējā kiberdrošības uzņēmuma palīdzību *pārliecinoši* konstatēja, ka uzbrucējs datus tikai šifrējis, neveicot to eksfiltrāciju. Žurnāli uzbrukuma laikā neuzrāda izejošu datu plūsmu. Pārkāpums skāra uzņēmuma klientu un darbinieku — kopumā dažu desmitu personu — personas datus. Dublējumkopija bija viegli pieejama, un dati tika atjaunoti dažas stundas pēc uzbrukuma. Pārkāpums neradīja nekādas sekas pārziņa ikdienas darbībā. Netika kavēti maksājumi darbiniekiem vai klientu pieprasījumu apstrāde.

17. Šajā gadījumā tika realizēti šādi "personas datu aizsardzības pārkāpuma" definīcijā ietvertie elementi: drošības pārkāpuma rezultātā notika nelikumīga datu pārveidošana un nesankcionēta piekļuve tiem.

2.1.1 1. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

18. Tāpat kā visu citu risku gadījumos, ko rada ārējie dalībnieki, iespējamību, ka izspiedējprogrammatūras uzbrukums izdosies, var būtiski mazināt, pastiprinot datu kontroles vides drošību. Lielāko daļu no šiem pārkāpumiem var novērst, nodrošinot, ka ir veikti atbilstoši organizatoriskie, fiziskie un tehnoloģiskie drošības pasākumi. Tādi pasākumi ir, piemēram, pienācīga ielāpu pārvaldība [*patch management*] un atbilstošas ļaunatūras noteikšanas sistēmas izmantošana. Pienācīga un atsevišķa dublējumkopija palīdzēs mazināt varbūtēja sekmīga uzbrukuma sekas. Turklāt programma darbinieku izglītošanai drošības jautājumos, mācībām un izpratnes veicināšanai (*SETA*) palīdzēs novērst un atpazīt šāda veida uzbrukumus. (Ieteicamo pasākumu saraksts atrodams 2.5. iedaļā.) Pareiza ielāpu pārvaldība, kas nodrošina to, ka sistēmas ir atjauninātas un visas zināmās izvietoto sistēmu ievainojamības ir novērstas, ir viens no vissvarīgākajiem pasākumiem, jo lielākā daļa izspiedējprogrammatūras uzbrukumu izmanto labi zināmās ievainojamības.

19. Novērtējot riskus, pārzinim ir jāizmeklē pārkāpums un jāidentificē ļaunkoda veids, lai izprastu uzbrukuma iespējamās sekas. Viens no riskiem, kas jāņem vērā, ir iespēja, ka dati tika eksfiltrēti, neatstājot pēdas sistēmu žurnālos.

20. Šajā piemērā uzbrucējam bija piekļuve personas datiem un tika apdraudēta tāda kodēta teksta konfidencialitāte, kas satur personas datus šifrētā veidā. Tomēr datus, kas varētu būt eksfiltrēti, uzbrucējs vismaz pagaidām nevar nolasīt vai izmantot. Datu pārziņa izmantotā šifrēšanas tehnika atbilst modernākajām tehnoloģijām. Atšifrēšanas atslēga netika uzlauzta, un, iespējams, to nevarēja noteikt arī ar citiem līdzekļiem.

Tādējādi konfidencialitātes riski fizisko personu tiesībām un brīvībām ir samazināti līdz minimumam, liedzot kriptoanalīzes progresu, kas šifrētos datus padarītu saprotamus nākotnē.

21. Datu pārzinim būtu jāņem vērā pārkāpuma radītais risks personām[10]. Šajā gadījumā šķiet, ka riskus datu subjektu tiesībām un brīvībām rada personas datu pieejamības trūkums, bet personas datu konfidencialitāte nav apdraudēta[11]. Šajā piemērā pārkāpuma nelabvēlīgā ietekme tika mazināta diezgan drīz pēc pārkāpuma. Pienācīga dublēšanas režīma rezultātā[12] pārkāpuma sekas nav tik nopietnas, un pārzinis šajā gadījumā to efektīvi izmantoja.

22. Attiecībā uz datu subjektiem radīto seku nopietnību varēja konstatēt tikai nelielas sekas, jo ietekmētie dati tika atjaunoti dažu stundu laikā, pārkāpums neradīja nekādas sekas pārziņa ikdienas darbībā un nebija būtiskas ietekmes uz datu subjektiem (piemēram, maksājumiem darbiniekiem vai klientu pieprasījumu apstrādi).

2.1.2 1. GADĪJUMS — seku mazināšana un saistības

23. Ja nav dublējumkopijas, pārzinis var veikt tikai dažus pasākumus, lai novērstu personas datu zudumu, un dati ir jāsavāc atkārtoti. Tomēr šajā konkrētajā gadījumā uzbrukuma ietekmi varēja efektīvi ierobežot, atiestatot visas apdraudētās sistēmas tā, ka tajās nav ļaunkoda, novēršot ievainojamību un drīz pēc uzbrukuma atjaunojot skartos datus. Ja nav dublējumkopijas, dati tiek zaudēti, taču sekas var būt vēl nopietnākas, jo pieaug arī riski personām vai ietekme uz tām.

24. Galvenais mainīgais lielums, analizējot pārkāpumu, ir efektīvas datu atjaunošanas savlaicīgums, izmantojot viegli pieejamo dublējumkopiju. Atbilstoša laika perioda noteikšana apdraudēto datu atjaunošanai ir atkarīga no konkrētā pārkāpuma unikālajiem apstākļiem. VDAR noteic, ka par personas datu aizsardzības pārkāpumu jāpaziņo bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā. Tāpēc varētu teikt, ka 72 stundu termiņa pārsniegšana nekādā gadījumā nav vēlama, bet, risinot augsta riska līmeņa gadījumus, paziņošana pat šajā galējā termiņā vērtējama kā neapmierinoša.

25. Šajā gadījumā pēc detalizēta ietekmes novērtējuma un incidentu reaģēšanas procesa pārzinis konstatēja, ka pārkāpums, visticamāk, neradīs risku fizisko personu tiesībām un brīvībām, tāpēc nav nepieciešams paziņot ne datu subjektiem, ne arī UI. Tomēr, tāpat kā visi datu aizsardzības pārkāpumi, tas ir jādokumentē saskaņā

---

[10] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. A29 darba grupas "Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē", *WP* 248 01. red. — apstiprinātas EDAK, https://ec.europa.eu/newsroom/article29/items/611236, 9. lpp.

[11] Tehniskā ziņā datu šifrēšana ietvers "piekļuvi" sākotnējiem datiem, bet izspiedējprogrammatūras gadījumā — to dzēšanu, kas nozīmē, ka datiem ir jāpiekļūst ar izspiedējprogrammatūras kodu, lai tos šifrētu un izdzēstu sākotnējos datus. Pirms dzēšanas uzbrucējs var paņemt sākotnējo datu kopiju, taču personas dati ne vienmēr tiks iegūti. Izmeklēšanas laikā datu pārzinis var atklāt jaunu informāciju, kas var mainīt šo novērtējumu. Piekļuve, kuras rezultātā notiek personas datu nelikumīga iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai materializējas datu subjekta drošības risks, pat bez datu interpretācijas var būt tikpat nopietns pārkāpums kā piekļuve ar personas datu interpretāciju.

[12] Dublēšanas procedūrām būtu jābūt strukturētām, saskaņotām un atkārtojamām. Dublēšanas procedūru piemēri ir "3-2-1" metode un "vectēva-tēva-dēla" metode. Jebkura metode vienmēr būtu jāpārbauda attiecībā uz pārklājuma efektivitāti un datu atjaunošanu. Lai nodrošinātu sistēmas integritāti, testēšana arī ik pa laikam būtu jāatkārto, jo īpaši tad, ja notiek izmaiņas apstrādes darbībā vai tās apstākļos.

ar 33. panta 5. punktu. Organizācijai var būt arī nepieciešams (vai vēlāk to var pieprasīt UI) atjaunināt un sakārtot organizatoriskos un tehniskos personas datu drošības pasākumus un riska mazināšanas pasākumus un procedūras. Lai novērstu līdzīgus notikumus nākotnē, šīs atjaunināšanas un sakārtošanas ietvaros organizācijai rūpīgi jāizpēta pārkāpums un jāidentificē tā cēloņi un metodes, ko izmantojis uzbrucējs.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	X	X

2.2 2. GADĪJUMS — izspiedējprogrammatūra bez pienācīgas dublējumkopijas

Viens no kāda lauksaimniecības uzņēmuma izmantotajiem datoriem tika pakļauts izspiedējprogrammatūras uzbrukumam, un uzbrucējs šifrēja tajā esošos datus. Uzņēmums sava tīkla uzraudzībai izmanto ārēja kiberdrošības uzņēmuma palīdzību. Ir pieejami žurnāli, kas izseko visas no uzņēmuma izejošās datu plūsmas (tostarp nosūtītās e-pasta vēstules). Pēc žurnālu un uzņēmuma izmantoto atklāšanas sistēmu apkopoto datu analīzes iekšējā izmeklēšanā, ko veica ar ārējā kiberdrošības uzņēmuma palīdzību, pārliecinoši konstatēja, ka uzbrucējs datus tikai šifrējis, neveicot to eksfiltrāciju. Žurnāli neuzrāda izejošu datu plūsmu uzbrukuma laikā. Pārkāpums skāra uzņēmuma darbinieku un klientu — kopumā dažu desmitu personu — personas datus. Īpašas datu kategorijas netika ietekmētas. Dublējumkopija elektroniskā formātā nebija pieejama. Lielākā daļa datu tika atjaunoti no dublējumkopijas papīra formātā. Datu atjaunošana ilga piecas darba dienas un izraisīja nelielu pasūtījumu piegādes kavēšanos klientiem.

2.2.1 2. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

26. Datu pārzinim bija jāveic tie paši iepriekšējie pasākumi, kas minēti 2.1. un 2.9. iedaļā. Galvenā atšķirība no iepriekšējā gadījuma ir elektroniskās dublējumkopijas trūkums un šifrēšanas trūkums glabāšanas laikā. Tāpēc būs būtiskas atšķirības turpmākajās darbībās.

27. Novērtējot riskus, pārzinim ir jāizpēta infiltrācijas metode un jāidentificē ļaunkoda veids, lai izprastu iespējamās uzbrukuma sekas. Šajā piemērā izspiedējprogrammatūra šifrēja personas datus, neveicot to eksfiltrāciju. Rezultātā šķiet, ka riskus datu subjektu tiesībām un brīvībām rada personas datu pieejamības trūkums, bet personas datu konfidencialitāte nav apdraudēta. Lai noteiktu risku, ir ļoti svarīgi rūpīgi pārbaudīt ugunsmūra žurnālus un tā rādījumus. Datu pārzinim pēc pieprasījuma būtu jāiesniedz šīs izmeklēšanas faktiskie konstatējumi.

28. Datu pārzinim ir jāpatur prātā, ka gadījumā, ja uzbrukums ir sarežģītāks, ļaunatūras funkcionalitāte tai ļauj rediģēt žurnāldatnes un izdzēst pēdas. Ņemot vērā, ka žurnāli netiek pārsūtīti vai replicēti uz centrālo žurnālu serveri, pat pēc rūpīgas izmeklēšanas, kurā konstatēts, ka uzbrucējs nav eksfiltrējis personas datus, datu pārzinis nevar apgalvot, ka žurnāla ieraksta neesība pierāda, ka nav notikusi eksfiltrācija, tāpēc konfidencialitātes pārkāpuma iespējamību nevar pilnībā izslēgt.

29. Datu pārzinim ir jānovērtē šā pārkāpuma riski[13] gadījumā, ja uzbrucējs bija piekļuvis datiem. Veicot riska novērtējumu, datu pārzinim būtu jāņem vērā arī pārkāpumā skarto personas datu raksturs, sensitivitāte, apjoms un konteksts. Šajā gadījumā nav ietekmētas īpašas personas datu kategorijas, skarto datu apjoms un ietekmēto datu subjektu skaits ir neliels.

[13] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

30. Būtiski ir vākt precīzu informāciju par nesankcionēto piekļuvi, lai noteiktu riska līmeni un novērstu jaunu vai atkārtotu uzbrukumu. Ja uzbrucējs būtu nokopējis datubāzē esošos datus, tas pilnīgi noteikti būtu risku palielinošs faktors. Ja nav skaidrības par nelikumīgās piekļuves specifiku, jāapsver sliktākais scenārijs un attiecīgi jānovērtē risks.

31. Rezerves datubāzes neesamību var uzskatīt par risku palielinošu faktoru tik lielā mērā, cik nopietnas sekas datu subjektiem rada datu trūkums.

2.2.2 2. GADĪJUMS — seku mazināšana un saistības

32. Ja nav dublējumkopijas, pārzinis var veikt tikai dažus pasākumus, lai novērstu personas datu zudumu, un dati ir jāapkopo atkārtoti, ja vien nav pieejams kāds cits avots (piemēram, pasūtījuma apstiprinājuma e-pasta vēstules). Ja nav dublējumkopijas, dati var būt zaudēti un tas, cik nopietnas būs sekas, būs atkarīgs no ietekmes uz personām.

33. Datu atjaunošanai nevajadzētu būt pārlieku problemātiskai[14], ja vien dati ir pieejami papīra formātā, taču, ņemot vērā elektroniskās rezerves datubāzes neesamību, ir nepieciešams paziņot UI, jo datu atjaunošana prasīja zināmu laiku un varēja aizkavēt pasūtījumu piegādi klientiem, kā arī var izrādīties neiespējami atgūt ievērojamu daudzumu metadatu (piemēram, žurnālus, laika zīmogus).

34. Datu subjektu informēšana par pārkāpumu var būt atkarīga arī no tā, cik ilgi personas dati nav bijuši pieejami un kādas grūtības tas var radīt pārziņa darbībā (piemēram, kavēti maksājumu pārskaitījumi darbiniekiem). Tā kā šie maksājumu un piegādes kavējumi var radīt finansiālus zaudējumus personām, kuru dati tika apdraudēti, varētu arī apgalvot, ka pārkāpums var radīt augstu risku. Tāpat, iespējams, būs jāinformē datu subjekti, ja šifrēto datu atjaunošanā būs nepieciešama viņu līdzdalība.

35. Šis gadījums ir tāda izspiedējprogrammatūras uzbrukuma piemērs, kas apdraud datu subjektu tiesības un brīvības, bet nerada augstu risku. Tas būtu jādokumentē saskaņā ar 33. panta 5. punktu un jāpaziņo UI saskaņā ar 33. panta 1. punktu. Organizācijai var būt arī nepieciešams (vai arī to var pieprasīt UI) atjaunināt un sakārtot organizatoriskos un tehniskos personas datu drošības pasākumus un riska mazināšanas pasākumus un procedūras.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	X

2.3 3. GADĪJUMS — izspiedējprogrammatūra ar dublējumkopiju un bez eksfiltrācijas slimnīcā

[14] Tas būs atkarīgs no personas datu sarežģītības un struktūras. Sarežģītākajos gadījumos datu integritātes un saskanības ar metadatiem atjaunošana, pareizu attiecību nodrošināšana datu struktūrās un datu precizitātes pārbaude var prasīt ievērojamus resursus un pūles.

Kādas slimnīcas / veselības aprūpes centra informācijas sistēma tika pakļauta izspiedējprogrammatūras uzbrukumam, un uzbrucējs šifrēja ievērojamu daļu tajā esošo datu. Uzņēmums sava tīkla uzraudzībai izmanto ārēja kiberdrošības uzņēmuma palīdzību. Ir pieejami žurnāli, kas izseko visas no uzņēmuma izejošās datu plūsmas (t. sk. nosūtītās e-pasta vēstules). Pēc žurnālu un citu noteikšanas sistēmu apkopoto datu analīzes iekšējā izmeklēšanā, ko veica ar ārējā kiberdrošības uzņēmuma palīdzību, pārliecinoši konstatēja, ka uzbrucējs datus tikai šifrējis, neveicot to eksfiltrāciju. Žurnāli neuzrāda izejošu datu plūsmu uzbrukuma laikā. Pārkāpums skāra darbinieku un pacientu — kopumā vairāku tūkstošu personu — personas datus. Dublējumkopijas bija pieejamas elektroniskā formātā. Lielākā daļa datu tika atjaunota, taču tas prasīja divas darba dienas un izraisīja ievērojamu kavēšanos pacientu aprūpē un operāciju atcelšanu/atlikšanu, kā arī pakalpojumu līmeņa pazemināšanos sistēmu nepieejamības dēļ.

2.3.1 3. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

36. Datu pārzinim bija jāveic tie paši iepriekšējie pasākumi, kas minēti 2.1. un 2.5. iedaļā. Galvenā atšķirība no iepriekšējā gadījuma ir augstā seku nopietnības pakāpe ievērojamai datu subjektu daļai[15].

37. Skarto datu apjoms un ietekmēto datu subjektu skaits ir liels, jo slimnīcas parasti apstrādā lielu datu apjomu. Datu nepieejamībai ir liela ietekme uz būtisku datu subjektu daļu. Turklāt pastāv atlikušais risks par augstu nopietnības pakāpi attiecībā uz pacienta datu konfidencialitāti.

38. Svarīgs ir pārkāpuma veids, būtība, sensitivitāte un pārkāpuma rezultātā ietekmēto personas datu apjoms. Lai gan dati tika dublēti un tos varēja atjaunot dažu dienu laikā, joprojām pastāv augsts risks, jo datu subjektiem ir iestājušās nopietnas sekas tādēļ, ka uzbrukuma brīdī un nākamajās dienās dati nebija pieejami.

2.3.2 3. GADĪJUMS — seku mazināšana un saistības

39. Nepieciešams paziņot UI, jo ir iesaistītas īpašas personas datu kategorijas un datu atjaunošana varēja ieilgt, kā rezultātā tika būtiski kavēta pacientu aprūpe. Nepieciešams informēt datu subjektus par pārkāpumu, ņemot vērā ietekmi uz pacientiem, arī pēc šifrēto datu atjaunošanas. Lai gan dati par visiem pēdējos gados slimnīcā ārstētajiem pacientiem tika šifrēti, tika ietekmēti tikai tie pacienti, kuriem bija paredzēts ārstēties slimnīcā laikā, kad datorsistēma nebija pieejama. Pārzinim būtu tieši jāpaziņo šiem pacientiem par datu aizsardzības pārkāpumu. Tieša saziņa ar citiem pacientiem, no kuriem daži, iespējams, nav bijuši slimnīcā vairāk nekā divdesmit gadus, nebūtu nepieciešama saskaņā ar 34. panta 3. punkta c) apakšpunktā minēto izņēmumu. Šādā gadījumā tās vietā var izmantot publisku saziņu[16] vai līdzīgu pasākumu, ar ko datu subjekti tiek informēti vienlīdz efektīvi. Šajā gadījumā slimnīcai ir jāpublisko informācija par izspiedējprogrammatūras uzbrukumu un tā sekām.

40. Šis gadījums ir tāda izspiedējprogrammatūras uzbrukuma piemērs, kas rada augstu risku datu subjektu tiesībām un brīvībām. Tas būtu jādokumentē saskaņā ar 33. panta 5. punktu, jāpaziņo UI saskaņā ar 33. panta 1. punktu un datu subjektiem saskaņā ar 34. panta 1. punktu Organizācijai arī nepieciešams atjaunināt un

[15] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

[16] VDAR 86. apsvērumā paskaidrots, ka "*[š]āda 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*".

sakārtot organizatoriskos un tehniskos personas datu drošības pasākumus un riska mazināšanas pasākumus un procedūras.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	✓

2.4 4. GADĪJUMS — izspiedējprogrammatūra bez dublējumkopijas un ar eksfiltrāciju

Kāda sabiedriskā transporta uzņēmuma serveris tika pakļauts izspiedējprogrammatūras uzbrukumam, un uzbrucējs šifrēja tajā esošos datus. Kā liecina iekšējās izmeklēšanas konstatējumi, uzbrucējs ne tikai šifrēja datus, bet tos arī eksfiltrēja. Tika skarti klientu un darbinieku, kā arī to vairāku tūkstošu cilvēku personas dati, kuri izmanto uzņēmuma pakalpojumus (piemēram, pērk biļetes tiešsaistē). Pārkāpumā tika skarti ne tikai identitātes pamatdati, bet arī personas apliecību numuri un finanšu dati, piemēram, kredītkartes informācija. Pastāvēja rezerves datubāze, taču uzbrucējs šifrēja arī to.

2.4.1 4. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

41. Datu pārzinim bija jāveic tie paši iepriekšējie pasākumi, kas minēti 2.1. un 2.5. iedaļā. Lai gan bija dublējumkopija, arī to skāra uzbrukums. Šis aspekts vien rada jautājumus par pārziņa iepriekš veikto IT drošības pasākumu kvalitāti un izmeklēšanā būtu rūpīgi jāpārbauda, jo labi izstrādātā dublēšanas režīmā vairākas dublējumkopijas ir jāglabā droši, lai tām nevarētu piekļūt no galvenās sistēmas, pretējā gadījumā tās var tikt apdraudētas tajā pašā uzbrukumā. Turklāt izspiedējprogrammatūras uzbrukumi var netikt atklāti vairākas dienas, un pa to laiku tikt lēnām šifrēti reti izmantotie dati. Tādējādi vairākas dublējumkopijas var kļūt nelietojamas, tāpēc periodiski būt arī jāveido dublējumkopijas un tās jāizolē. Tas palielinātu datu atjaunošanas iespēju, lai gan palielinātos zaudēto datu apjoms.

42. Šis pārkāpums attiecas ne tikai uz datu pieejamību, bet arī uz konfidencialitāti, jo uzbrucējs, iespējams, ir modificējis un/vai kopējis datus no servera. Tāpēc šis pārkāpuma veids rada augstu risku[17].

43. Personas datu raksturs, sensitivitāte un apjoms vēl vairāk palielina riskus, jo ietekmēto personu skaits un kopējais skarto datu apjoms ir liels. Pārkāpumā tika skarti ne tikai identitātes pamatdati, bet arī personu apliecinoši dokumenti un finanšu dati, piemēram, kredītkartes informācija. Datu aizsardzības pārkāpums attiecībā uz šāda veida datiem pats par sevi rada augstu risku, un, ja tos apstrādā kopā, tos cita starpā var izmantot identitātes zādzībai vai viltošanai.

44. Nepilnīgas servera loģikas vai organizatoriskās vadības dēļ izspiedējprogrammatūra ietekmēja dublējuma datnes, traucējot datu atjaunošanu un palielinot risku.

45. Šis datu aizsardzības pārkāpums rada lielu risku personu tiesībām un brīvībām, jo tas varētu radīt gan materiālu kaitējumu (piemēram, finansiālus zaudējumus, jo tika ietekmēti kredītkartes dati), gan nemateriālu kaitējumu (piemēram, identitātes zādzību vai viltošanu, jo tika skarti personas apliecību dati).

[17] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

2.4.2 4. GADĪJUMS — seku mazināšana un saistības

46. Paziņot datu subjektiem ir būtiski, lai viņi varētu veikt nepieciešamos pasākumus (piemēram, bloķēt savas kredītkartes) un izvairītos no materiāla kaitējuma.

47. Papildus pārkāpuma dokumentēšanai saskaņā ar 33. panta 5. punktu šajā gadījumā ir obligāti jāpaziņo arī UI (33. panta 1. punkts), un pārzinim ir arī pienākums paziņot par pārkāpumu datu subjektiem (34. panta 1. punkts). Pēdējo var veikt individuāli, bet attiecībā uz personām, kuru kontaktinformācija nav pieejama, pārzinim jāsniedz publisks paziņojums, vienlaikus nodrošinot, ka šāda paziņošana neizraisīs papildu negatīvas sekas datu subjektiem, piemēram, jāpaziņo savā tīmekļvietnē. Pēdējā gadījumā ir nepieciešams precīzs un skaidrs paziņojums, kas ir labi redzams pārziņa tīmekļvietnē un sniedz precīzas atsauces uz attiecīgajiem VDAR noteikumiem. Organizācijai arī nepieciešams atjaunināt un sakārtot organizatoriskos un tehniskos personas datu drošības pasākumus un riska mazināšanas pasākumus un procedūras.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	✓

2.5 Organizatoriskie un tehniskie pasākumi izspiedējprogrammatūras uzbrukumu novēršanai / seku mazināšanai

48. Iespējamība, ka varētu būt noticis izspiedējprogrammatūras uzbrukums, parasti liecina par vienu vai vairākām ievainojamībām pārziņa sistēmā. Tas attiecas arī uz izspiedējprogrammatūras uzbrukumiem, kuros personas datus šifrē, bet neveic eksfiltrāciju. Neatkarīgi no uzbrukuma iznākuma un sekām nav iespējams pārvērtēt datu drošības sistēmas visaptveroša novērtējuma nozīmīgumu, bet īpaša uzmanība ir jāpievērš IT drošībai. Konstatētās nepilnības un drošības nepilnības ir jādokumentē un nekavējoties jānovērš.

49. Ieteicamie pasākumi:

(Turpmāk minēto pasākumu saraksts nekādā ziņā nav uzskatāms par pilnīgu vai visaptverošu. Drīzāk mērķis ir sniegt idejas profilaksei un iespējamos risinājumus. Katra apstrādes darbība ir atšķirīga, tāpēc pārzinim ir jāpieņem lēmums par to, kuri pasākumi ir vispiemērotākie konkrētajā situācijā.)

- aparātprogrammatūras, operētājsistēmas un lietojumprogrammatūras atjaunināšana serveros, klientu iekārtās, aktīvajos tīkla komponentos un visās citās iekārtās tajā pašā lokālajā tīklā jeb *LAN* (tostarp bezvadu interneta jeb *Wi-Fi* ierīcēs); atbilstošu IT drošības pasākumu ieviešana, pārliecināšanās, ka tie ir efektīvi, un, apstrādei vai apstākļiem mainoties vai attīstoties, regulāra to atjaunināšana. Tas nozīmē arī saglabāt detalizētus žurnālus par to, kuri ielāpi tiek lietoti un ar kādu laika zīmogu;

- apstrādes sistēmu un infrastruktūras projektēšana un organizēšana tā, lai segmentētu vai izolētu datu sistēmas un tīklus un tādējādi izvairītos no ļaunatūras izplatīšanās organizācijā un ārējās sistēmās;

- mūsdienīgas, drošas un pārbaudītas dublēšanas procedūras esība. Vidēja un ilgtermiņa dublēšanas datu nesēji ir jāglabā atsevišķi no operatīvo datu krātuves un trešajāmm pusēm nepieejamā vietā pat veiksmīga uzbrukuma gadījumā (piemēram, ikdienas inkrementālā dublēšana un iknedēļas pilnīgā dublēšana);

- atbilstošas, atjauninātas, efektīvas un integrētas pretļaunatūras programmatūras esība/nodrošināšana;

- atbilstoša, mūsdienīga, efektīva un integrēta ugunsmūra un ielaušanās atklāšanas un novēršanas sistēmas esība; tīkla datu plūsmas virzīšana caur ugunsmūri / ielaušanās detektoru, pat strādājot no

mājām vai mobilā darba gadījumā (piemēram, kad izmanto *VPN* savienojumus ar organizācijas drošības mehānismiem, piekļūstot internetam);

- darbinieku mācības par IT uzbrukumu atpazīšanas un novēršanas metodēm. Pārzinim būtu jānodrošina līdzekļi, lai varētu noteikt, vai e-pasta vēstules un ziņojumi, kas iegūti, izmantojot citus saziņas līdzekļus, ir autentiski un uzticami. Darbinieki būtu jāmāca atpazīt, kad šāds uzbrukums ir noticis, kā atvienot beigupunktu no tīkla, un darbiniekiem būtu jāatgādina par pienākumu nekavējoties ziņot par uzbrukumu drošības speciālistam;
- būtu jāuzsver nepieciešamība identificēt ļaunkoda veidu, lai saprastu uzbrukuma sekas un spētu atrast pareizos pasākumus riska mazināšanai. Ja izspiedējprogrammatūras uzbrukums ir izdevies un nav veikts dublējums, datu izgūšanai var tikt izmantoti tādi rīki kā projekta "nē izspiešanai" (*nomoreransom.org*) rīki. Tomēr, ja ir pieejams droša dublējumkopija, ieteicams datus atjaunot no tā;
- visu žurnālu pārsūtīšana vai replicēšana uz centrālo žurnālu serveri (iespējams, parakstot žurnāla ierakstus vai uzliekot kriptogrāfisko laika zīmogu);
- droša šifrēšana un vairākfaktoru autentifikācija, jo īpaši administratīvai piekļuvei IT sistēmām, atbilstoša atslēgu un paroļu pārvaldība;
- regulāra ievainojamības un ielaušanās testēšana;
- datordrošības incidentu reaģēšanas vienības (*CSIRT*) vai datorapdraudējumu reaģēšanas vienības (*CERT*) izveidošana organizācijā vai pievienošanās kolektīvai *CSIRT/CERT*; ārkārtas rīcības plāna, negadījuma seku novēršanas plāna un darbības nepārtrauktības plāna izveidošana un pārliecināšanās, ka tie ir rūpīgi pārbaudīti;
- riska analīzes pārskatīšana, pārbaude un atjaunināšana, novērtējot pretpasākumus.

3 UZBRUKUMI AR DATU EKSFILTRĀCIJU

50. Uzbrukumi, kuros tiek izmantotas dažādas ievainojamības pakalpojumos, ko pārzinis piedāvā trešajāmm personām internetā, piemēram, tādi, kas veikti, izmantojot iespraudzbrukumus (piemēram, *SQL* iespraudzbrukums, direktoriju šķērsošana), tīmekļvietņu uzlaušanu un līdzīgas metodes, var līdzināties izspiedējprogrammatūras uzbrukumiem, jo risku rada nesankcionētas trešās puses darbība, taču šo uzbrukumu mērķis parasti ir personas datu kopēšana, eksfiltrācija un ļaunprātīga izmantošana. Tādējādi tie galvenokārt ir konfidencialitātes un, iespējams, arī datu integritātes pārkāpumi. Taču, ja pārzinis spēj atpazīt šāda veida pārkāpumu pazīmes, viņam ir pieejami daudzi pasākumi, kas var būtiski mazināt uzbrukuma veiksmīgas izpildes risku.

3.1 5. GADĪJUMS — darba pieteikuma datu eksfiltrācija no tīmekļvietnes

Pret kādu nodarbinātības aģentūru tika veikts kiberuzbrukums, kura laikā tās tīmekļvietnē tika ievietots ļaunkods. Šis ļaunkods padarīja nepiederošām personām pieejamus personas datus, kas tika iesniegti, izmantojot tiešsaistes darba pieteikuma veidlapas, un glabāti tīmekļa serverī. Iespējams, tika ietekmētas 213 šādas veidlapas, bet pēc skarto datu pārbaudes tika konstatēts, ka pārkāpumā nav skartas īpašas datu kategorijas. Konkrētajā uzstādītajā ļaunatūras rīkkopā bija funkcijas, kas ļāva uzbrucējam izdzēst jebkādu eksfiltrācijas vēsturi, kā arī pārraudzīt apstrādi serverī un iegūt personas datus. Rīkkopu atklāja tikai mēnesi pēc tās uzstādīšanas.

3.1.1 5. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

51. Datu pārziņa vides drošība ir ārkārtīgi svarīga, jo lielāko daļu no šiem pārkāpumiem var novērst, nodrošinot, ka visas sistēmas tiek pastāvīgi atjauninātas, sensitīvie dati tiek šifrēti un lietojumprogrammas tiek izstrādātas atbilstoši augstiem drošības standartiem, piemēram, droša autentificēšana, pasākumi pret pārlases uzbrukumiem, "izvairīšanās" no lietotāju ievaddarbībām vai to "attīrīšanas"[18] utt. Lai iepriekš atklātu un labotu šāda veida ievainojamības, ir nepieciešami arī periodiski IT drošības auditi, ievainojamības novērtējumi un ielaušanās testi. Šajā konkrētajā gadījumā datņu integritātes uzraudzības rīki ražošanas vidē būtu palīdzējuši pamanīt koda iespraušanu. (Ieteicamo pasākumu saraksts atrodams 3.7. iedaļā).

52. Pārzinim vienmēr ir jāsāk pārkāpuma izmeklēšana ar uzbrukuma veida un metodes noteikšanu, lai novērtētu, kādi pasākumi ir jāveic. Šādu novērtējumu var veikt ātri un efektīvi, ja datu pārzinim ir izstrādāts incidentu reaģēšanas plāns, kurā norādīti nepieciešamie un ātri veicamie pasākumi, kas ļaus pārņemt kontroli pār incidentu. Šajā konkrētajā gadījumā pārkāpuma veids bija risku palielinošs faktors, jo ne vien tika pārkāpta datu konfidencialitāte, bet iebrucējam arī bija līdzekļi, kas ļāva veikt izmaiņas sistēmā, tāpēc tika apdraudēta arī datu integritāte.

53. Būtu jānovērtē pārkāpumā skarto personas datu raksturs, sensitivitāte un apjoms, lai noteiktu, cik lielā mērā pārkāpums ir ietekmējis datu subjektus. Lai gan netika ietekmētas īpašas personas datu kategorijas, tiešsaistes veidlapās esošie dati satur būtisku informāciju par personām, un šādus datus var ļaunprātīgi izmantot vairākos veidos (adresējot nevēlamas reklāmas, veicot identitātes zādzības utt.), tāpēc šādu seku nopietnība palielina risku datu subjektu tiesībām un brīvībām[19].

3.1.2 5. GADĪJUMS — seku mazināšana un saistības

54. Ja iespējams, pēc problēmas atrisināšanas datubāze jāsalīdzina ar drošā dublējumkopijā saglabāto. Pārkāpuma rezultātā gūtā pieredze būtu jāizmanto IT infrastruktūras atjaunināšanai. Datu pārzinim būtu jāatjauno visas ietekmētās IT sistēmas drošā un tīrā stāvoklī, jānovērš ievainojamība un jāievieš jauni drošības pasākumi, lai izvairītos no līdzīgiem datu aizsardzības pārkāpumiem nākotnē, piemēram, jāveic datņu integritātes pārbaudes un drošības auditi. Ja personas dati tika ne tikai eksfiltrēti, bet arī dzēsti, pārzinim ir jāveic sistemātiskas darbības, lai atgūtu personas datus tādā stāvoklī, kādā tie bija pirms pārkāpuma. Var būt nepieciešams veidot pilnīgās dublējumkopijas, ieviest inkrementālās izmaiņas un pēc tam, iespējams, atkārtot apstrādi kopš pēdējās inkrementālās dublējumkopijas, kas nozīmē, ka pārzinim jāspēj replicēt kopš pēdējās dublējumkopijas veiktās izmaiņas. Pārzinim jābūt sistēmai, kas izstrādāta, lai saglabātu ikdienas ievades datnes gadījumā, ja tās būtu atkārtoti jāapstrādā, kā arī stabilai datu uzglabāšanas metodei un piemērotai datu saglabāšanas politikai.

55. Ņemot vērā iepriekš minēto, tā kā pārkāpuma rezultātā var tikt apdraudētas fizisko personu tiesības un brīvības, datu subjekti noteikti par to būtu jāinformē (34. panta 1. punkts), kas, protams, nozīmē, ka par datu aizsardzības pārkāpumu būtu jāpaziņo arī attiecīgajām UI. Pārkāpuma dokumentēšana ir obligāta saskaņā ar VDAR 33. panta 5. punktu un atvieglo situācijas novērtēšanu.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	✓

[18] Izvairīšanās no lietotāju ievaddarbībām vai to attīrīšana ir ievades validācijas veids, kas nodrošina, ka informācijas sistēmā tiek ievadīti tikai pienācīgi formatēti dati.

[19] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

3.2 6. GADĪJUMS — jauktas paroles eksfiltrācija no tīmekļvietnes

Tika izmantota ievainojamība pret *SQL* iesprauduzbrukumu, lai piekļūtu kādas kulinārijas tīmekļvietnes servera datubāzei. Lietotāji kā lietotājvārdus drīkstēja izvēlēties tikai brīvi izvēlētus pseidonīmus. Tika ieteikts šim nolūkam neizmantot e-pasta adreses. Datubāzē saglabātās paroles ar droša algoritma palīdzību tika sajauktas, un iekaisītie algoritmi netika apdraudēti. Skartie dati — 1200 lietotāju jauktās paroles. Drošības apsvērumu dēļ pārzinis paziņoja datu subjektiem par pārkāpumu e-pasta vēstulē un lūdza nomainīt paroles, jo īpaši tad, ja tā pati parole tika izmantota

3.2.1 6. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

56. Konkrētajā gadījumā tika apdraudēta datu konfidencialitāte, taču datubāzē esošās paroles tika sajauktas ar mūsdienīgas metodes palīdzību, kam vajadzētu mazināt risku attiecībā uz personas datu raksturu, sensitivitāti un apjomu. Šajā gadījumā nav apdraudētas datu subjektu tiesības un brīvības.

57. Turklāt netika apdraudēta nekāda datu subjektu kontaktinformācija (piemēram, e-pasta adreses vai tālruņu numuri), kas nozīmē, ka datu subjektiem nepastāv būtisks risks piedzīvot krāpšanas mēģinājumus (piemēram, pikšķerēšanas e-pasta vēstules, krāpnieciskas īsziņas un tālruņa zvanus). Īpašas personas datu kategorijas netika ietekmētas.

58. Daži lietotājvārdi var tikt uzskatīti par personas datiem, taču tīmekļvietnes tematika nepieļauj negatīvas konotācijas. Tomēr jāņem vērā, ka riska novērtējums var mainīties[20], ja tīmekļvietnes veids un dati, kam piekļuva, varētu atklāt īpašas personas datu kategorijas (piemēram, politiskās partijas vai arodbiedrības tīmekļvietne). Modernas šifrēšanas izmantošana varēja mazināt pārkāpuma nelabvēlīgo ietekmi. Nodrošinot, ka ir atļauts ierobežots pieteikšanās mēģinājumu skaits, tiks novērsti pieteikšanās pārlases uzbrukumi, tādējādi lielā mērā samazinot riskus, ko rada uzbrucēji, kuri jau zina lietotājvārdus.

3.2.2 6. GADĪJUMS — seku mazināšana un saistības

59. Datu subjektu informēšanu dažos gadījumos varētu uzskatīt par seku mazināšanas faktoru, jo datu subjekti arī var veikt nepieciešamos pasākumus, lai izvairītos no turpmāka pārkāpuma radītā kaitējuma, piemēram, nomainot paroli. Šajā gadījumā paziņošana nebija obligāta, taču daudzos gadījumos to var uzskatīt par labu praksi.

60. Datu pārzinim būtu jānovērš ievainojamība un jāievieš jauni drošības pasākumi, lai izvairītos no līdzīgiem datu aizsardzības pārkāpumiem nākotnē, piemēram, jāveic sistemātiski tīmekļvietnes drošības auditi.

61. Pārkāpums būtu jādokumentē saskaņā ar 33. panta 5. punktu, taču nav nepieciešama paziņošana vai informēšana.

62. Jebkurā gadījumā ļoti ieteicams paziņot datu subjektiem par pārkāpumiem, kas saistīti ar parolēm, pat ja paroles tika glabātas, izmantojot jaucējkodu iekaisīšanu ar algoritmu, kas atbilst modernākajām tehnoloģijām. Vēlams izmantot autentificēšanas metodes, kas novērš nepieciešamību apstrādāt paroles

[20] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

servera pusē. Datu subjektiem būtu jādod iespēja izvēlēties veikt atbilstošus pasākumus attiecībā uz savām parolēm.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	X	X

3.3 7. GADĪJUMS — akreditācijas datu pārpildīšanas uzbrukums bankas tīmekļvietnei

Kādas bankas tiešsaistes bankas tīmekļvietne piedzīvoja kiberuzbrukumu. Uzbrukuma mērķis bija uzskaitīt visus iespējamos pieteikšanās lietotāju identifikatorus, izmantojot fiksētu triviālu paroli. Paroles sastāv no astoņiem cipariem. Vietnes ievainojamības dēļ atsevišķos gadījumos uzbrucējam tika nopludināta informācija par datu subjektiem (vārds, uzvārds, dzimums, dzimšanas datums un vieta, nodokļu maksātāja reģistrācijas numurs, lietotāja identifikācijas kods), arī ja izmantotā parole nebija pareiza vai bankas konts vairs nebija aktīvs. Tas ietekmēja aptuveni 100 000 datu subjektu. Tostarp uzbrucējs veiksmīgi pieteicās aptuveni 2000 kontos, kuros tika izmantota uzbrucēja izmēģinātā triviālā parole. Pēc uzbrukuma pārzinis varēja identificēt visus nelikumīgos pieteikšanās mēģinājumus. Datu pārzinis varēja apstiprināt, ka saskaņā ar krāpšanas apkarošanas pārbaudēm uzbrukuma laikā šajos kontos netika veikti nekādi darījumi. Banka bija informēta par datu aizsardzības pārkāpumu, jo tās drošības operāciju centrs bija konstatējis lielu skaitu pieteikšanās pieprasījumu, kas vērsti uz šo tīmekļvietni. Reaģējot uz šo uzbrukumu, pārzinis atslēdza iespēju pieteikties tīmekļvietnē, un lika atiestatīt uzlauzto kontu paroles. Pārzinis par pārkāpumu informēja tikai uzlauzto kontu lietotājus, t. i., lietotājus, kuru paroles tika uzlauztas vai kuru dati tika izpausti.

3.3.1 7. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

63. Svarīgi pieminēt, ka pārziņiem, kas apstrādā ļoti personiskus datus[21], ir lielāka atbildība attiecībā uz adekvātas datu drošības nodrošināšanu, piemēram, jābūt drošības operācijas centram un citiem incidentu novēršanas, atklāšanas un reaģēšanas pasākumiem. Šo augstāko standartu neievērošana noteikti liks piemērot nopietnākus pasākumus UI izmeklēšanas laikā.

64. Pārkāpums attiecas ne vien uz finanšu datiem, bet arī uz identitātes un lietotāja identifikatora informāciju, tādēļ tas ir īpaši nopietns pārkāpums. Ietekmēto personu skaits ir liels.

65. Fakts, ka pārkāpums varēja notikt tik sensitīvā vidē, norāda uz būtiskiem datu drošības trūkumiem pārziņa sistēmā un var liecināt par laiku, kad ietekmēto pasākumu pārskatīšana un atjaunināšana bija "nepieciešama" saskaņā ar VDAR 24. panta 1. punktu, 25. panta 1. punktu un 32. panta 1. punktu. Skartie dati ļauj unikāli identificēt datu subjektus un satur citu informāciju par tiem (t. sk. dzimumu, dzimšanas datumu un vietu), turklāt uzbrucējs tos var izmantot, lai uzminētu klientu paroles vai rīkotu uz bankas klientiem vērstu pikšķerēšanas kampaņu.

[21] Piemēram, informācija par datu subjektiem, kas attiecas uz maksājumu metodēm, t. sk., karšu numuri, bankas konti, tiešsaistes maksājumi, algu saraksti, bankas izraksti, ekonomiskie pētījumi vai jebkura cita informācija, kas var atklāt ar datu subjektiem saistītu ekonomisko informāciju.

66. Šo iemeslu dēļ tika uzskatīts, ka datu aizsardzības pārkāpums var radīt lielu risku visu attiecīgo datu subjektu tiesībām un brīvībām[22]. Tāpēc var pieņemt, ka tā rezultātā var rasties materiāls kaitējums (piemēram, finansiāls zaudējums) un nemateriāls kaitējums (piemēram, identitātes zādzība vai viltošana).

3.3.2 7. GADĪJUMS — seku mazināšana un saistības

67. Gadījuma aprakstā minētie pārziņa veiktie pasākumi ir atbilstoši. Pēc pārkāpuma tas arī novērsa tīmekļvietnes ievainojamību un veica citus pasākumus, lai novērstu līdzīgus datu aizsardzības pārkāpumus nākotnē, piemēram, attiecīgajai tīmekļvietnei pievienoja divfaktoru autentifikāciju, tādējādi ieviešot drošu klientu autentifikāciju.

68. Pārkāpuma dokumentēšana saskaņā ar VDAR 33. panta 5. punktu un paziņošana par to UI šajā gadījumā ir obligāta. Turklāt pārzinim saskaņā ar VDAR 34. pantu būtu jāpaziņo visiem 100 000 datu subjektu (tostarp datu subjektiem, kuru konti netika apdraudēti).

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	✓

3.4 Organizatoriskie un tehniskie pasākumi hakeru uzbrukumu novēršanai / seku mazināšanai

69. Tāpat kā izspiedējprogrammatūras uzbrukumu gadījumā, neatkarīgi no uzbrukuma iznākuma un sekām līdzīgos gadījumos pārzinim obligāti jāveic atkārtota IT drošības novērtēšana.

70. Ieteicamie pasākumi:[23]

(Turpmāk minēto pasākumu saraksts nekādā ziņā nav uzskatāms par pilnīgu vai visaptverošu. Drīzāk mērķis ir sniegt idejas profilaksei un iespējamos risinājumus. Katra apstrādes darbība ir atšķirīga, tāpēc pārzinim ir jāpieņem lēmums par to, kuri pasākumi ir vispiemērotākie konkrētajā situācijā.)

- modernākā šifrēšana un atslēgu pārvaldība, jo īpaši, ja tiek apstrādātas paroles, sensitīvi vai finanšu dati. Slepenas informācijas (paroļu) kriptogrāfiska jaukšana un iekaisīšana vienmēr ir ieteicamāka par paroļu šifrēšanu. Vēlams izmantot autentifikācijas metodes, kas novērš nepieciešamību apstrādāt paroles servera pusē;
- regulāra sistēmas atjaunināšana (programmatūra un aparātprogrammatūra). Jānodrošina, ka ir ieviesti visi IT drošības pasākumi, jāpārliecinās, ka tie ir efektīvi, un, apstrādei vai apstākļiem mainoties vai attīstoties, tie regulāri jāatjaunina. Lai uzskatāmi parādītu atbilstību VDAR 5. panta 1. punkta f) apakšpunktam saskaņā ar VDAR 5. panta 2. punktu, pārzinim būtu jāsaglabā visu veikto atjauninājumu uzskaite, tostarp arī to veikšanas laika reģistrācija;
- drošas autentifikācijas metožu, piemēram, divfaktoru autentifikācijas un autentifikācijas serveru, izmantošana, ko papildina moderna paroļu politika;
- drošas izstrādes standartos ietilpst lietotāja ievaddarbību filtrēšanas (cik vien iespējams izmantojot t. s. balto sarakstu), izvairīšanās no lietotāja ievaddarbībām un pārlases uzbrukumu novēršanas pasākumi

[22] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

[23] Informāciju par drošu tīmekļa lietojumprogrammu izstrādi sk. arī vietnē https://www.owasp.org/index.php/Main_Page .

(piemēram, maksimālā atkārtoto mēģinājumu skaita ierobežošana). "Tīmekļa lietojumprogrammu ugunsmūri" var palīdzēt efektīvi izmantot šo paņēmienu;

- drošas lietotāju privilēģiju un piekļuves kontroles pārvaldības politika;
- piemērotu, modernu, efektīvu un integrētu ugunsmūra, ielaušanās atklāšanas un citu perimetra aizsardzības sistēmu izmantošana;
- sistemātiski IT drošības auditi un ievainojamības novērtēšana (ielaušanās testēšana);
- regulāra dublējumkopiju pārskatīšana un testēšana ar mērķi nodrošināt, ka tās var izmantot, lai atjaunotu datus, kuru integritāte vai pieejamība ir ietekmēta;
- vienotajā resursu vietrādī jeb *URL* nenorādīt sesijas identifikatoru vienkāršā tekstā.

4 IEKŠĒJAIS CILVĒCISKĀ RISKA AVOTS

71. Īpaša uzmanība jāpievērš cilvēka kļūdas izraisītiem personas datu aizsardzības pārkāpumiem, jo tādi gadās bieži. Tā kā šāda veida pārkāpumi var būt gan tīši, gan netīši, datu pārziņiem ir ļoti grūti noteikt ievainojamības un pielāgot pasākumus, lai tās novērstu. Starptautiskajā datu aizsardzības un privātuma komisāru konferencē tika atzīts, ka ir svarīgi izslēgt šos cilvēciskos faktorus, un 2019. gada oktobrī tika pieņemta rezolūcija par to, kā izvairīties no cilvēka kļūdu izraisītiem personas datu aizsardzības pārkāpumiem[24]. Šajā rezolūcijā uzsvērts, ka būtu jāveic atbilstoši aizsardzības pasākumi, lai novērstu cilvēku kļūdas, un sniegts arvien papildināms šādu aizsardzības pasākumu un risinājumu saraksts.

4.1 8. GADĪJUMS — komercdatu eksfiltrācija, ko veicis darbinieks

Uzteikuma termiņa laikā uzņēmuma darbinieks no uzņēmuma datubāzes izkopē komercdatus. Darbinieks ir tiesīgs piekļūt datiem tikai savu darba uzdevumu veikšanai. Vairākus mēnešus pēc aiziešanas no darba viņš izmanto iegūtos datus (pamata kontaktinformāciju), lai sāktu jaunu datu apstrādi, kuras pārzinis viņš ir, un lai sazinātos ar uzņēmuma klientiem un piesaistītu viņus savam jaunajam uzņēmumam.

4.1.1 8. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

72. Konkrētajā gadījumā netika veikti nekādi iepriekšēji pasākumi, lai neļautu darbiniekam nokopēt uzņēmuma klientūras kontaktinformāciju, jo viņam šī informācija bija nepieciešama un bija likumīga piekļuve tai darba pienākumu veikšanai. Tā kā, veicot vairumu darba pienākumu, kas saistīti ar klientu attiecību nodrošināšanu, darbiniekiem ir nepieciešama noteikta līmeņa piekļuve personas datiem, šādus datu aizsardzības pārkāpumus novērst ir visgrūtāk. Piekļuves ierobežojumi var ierobežot konkrētā darbinieka veicamo darbu. Tomēr labi pārdomātas piekļuves politikas un pastāvīga kontrole var palīdzēt novērst šādus pārkāpumus.

73. Kā parasti, riska novērtēšanā ir jāņem vērā pārkāpuma veids un skarto personas datu raksturs, sensitivitāte un apjoms. Šāda veida pārkāpumi parasti ir konfidencialitātes pārkāpumi, jo datubāze parasti tiek atstāta neskarta, tās saturs tiek "tikai" kopēts turpmākai lietošanai. Skarto datu apjoms parasti arī ir neliels vai vidēji liels. Šajā konkrētajā gadījumā netika ietekmētas īpašas personas datu kategorijas, darbiniekam bija

[24] http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf.

nepieciešama tikai klientu kontaktinformācija, lai viņš varētu ar tiem sazināties pēc aiziešanas no uzņēmuma. Tāpēc attiecīgie dati nav sensitīvi.

74. Lai gan bijušajam darbiniekam, kurš ļaunprātīgi nokopējis datus, vienīgais mērķis varētu būt uzņēmuma klientu kontaktinformācijas iegūšana komerciālos nolūkos, pārzinis nevar uzskatīt, ka riska līmenis attiecībā uz ietekmētajiem datu subjektiem ir zems, jo pārzinim nav skaidras pārliecības par darbinieka nodomiem. Tādējādi, lai gan pārkāpuma sekas var aprobežoties ar to, ka datu subjekti tiks pakļauti bijušā darbinieka nepieprasītai pašreklāmai, nav izslēgta turpmāka un bīstamāka nozagto datu ļaunprātīga izmantošana atkarībā no bijušā darbinieka uzsāktās apstrādes mērķa[25].

4.1.2 8. GADĪJUMS — seku mazināšana un saistības

75. Iepriekš minētajā gadījumā pārkāpuma nelabvēlīgās ietekmes mazināšana ir sarežģīta. Iespējams, nepieciešama tūlītēja juridiska darbība, lai novērstu to, ka bijušais darbinieks turpmāk ļaunprātīgi izmanto un izplata datus. Papildus tam jānodrošina, ka līdzīgas situācijas neatkārtojas nākotnē. Pārzinis var likt bijušajam darbiniekam pārtraukt datu izmantošanu, taču šīs darbības panākumi labākajā gadījumā ir apšaubāmi. Var līdzēt atbilstoši tehniskie pasākumi, piemēram, padarīt neiespējamu datu kopēšanu vai lejupielādēšanu noņemamās ierīcēs.

76. Šāda veida gadījumiem nav viena universāla risinājuma, taču sistemātiska pieeja var palīdzēt tos novērst. Piemēram, uzņēmums var apsvērt iespēju atsaukt noteiktus piekļuves veidus darbiniekiem, kuri paziņojuši par savu nodomu pārtraukt darba attiecības, vai ieviest piekļuves žurnālus, lai nevēlamu piekļuvi varētu reģistrēt un atzīmēt. Līgumā, kas noslēgts ar darbiniekiem, jāiekļauj noteikumi, kas aizliedz šādas darbības.

77. Tā kā konkrētais pārkāpums neradīs augstu risku fizisko personu tiesībām un brīvībām, kopumā pietiks ar paziņojumu UI. Tomēr informēt datu subjektus varētu būt noderīgi arī pašam datu pārzinim, jo labāk, ka viņi par datu noplūdi uzzina no uzņēmuma, nevis no bijušā darbinieka, kurš mēģinās ar viņiem sazināties. Datu aizsardzības pārkāpuma dokumentēšana saskaņā ar 33. panta 5. punktu ir juridisks pienākums.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	X

[25] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

4.2 9. GADĪJUMS — nejauša datu pārsūtīšana uzticamai trešaja pusei

Apdrošināšanas aģents pamanīja, ka kļūdaini e-pastā saņemtas *Excel* datnes iestatījumi ļauj viņam piekļūt informācijai, kas saistīta ar divdesmit klientiem, kuri neietilpst viņa darbības jomā. Viņam ir pienākums neizpaust dienesta noslēpumu, un viņš bija vienīgais e-pasta vēstules saņēmējs. Vienošanās starp datu pārzini un apdrošināšanas aģentu uzliek aģentam pienākumu bez nepamatotas kavēšanās ziņot datu pārzinim par personas datu aizsardzības pārkāpumu. Tāpēc aģents par kļūdu nekavējoties informēja pārzini, kas datni izlaboja un nosūtīja vēlreiz, lūdzot aģentu dzēst iepriekšējo ziņojumu. Saskaņā ar iepriekš minēto vienošanos aģentam rakstveida paziņojumā ir jāapstiprina izdzēšanas fakts, ko viņš arī izdarīja. Iegūtajā informācijā nav iekļautas īpašas personas datu kategorijas, ir tikai kontaktinformācija un dati par apdrošināšanu (apdrošināšanas veids, summa). Pēc pārkāpumā skarto personas datu analīzes datu pārzinis nekonstatēja īpašas pazīmes attiecībā uz personām vai datu pārzini, kas varētu ietekmēt pārkāpuma ietekmes līmeni.

4.2.1 9. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

78. Šajā gadījumā pārkāpumu nav izraisījusi darbinieka tīša darbība, bet gan neuzmanības radīta netīša cilvēka kļūda. Šāda veida pārkāpumus var novērst vai to biežumu var samazināt, a) īstenojot mācības, izglītošanas un izpratnes veidošanas programmas, kurās darbinieki gūst labāku izpratni par personas datu aizsardzības nozīmi, b) samazinot datņu apmaiņu ar e-pasta starpniecību, tā vietā izmantojot, piemēram, īpašas sistēmas klientu datu apstrādē, c) veicot datņu divkāršu pārbaudi pirms nosūtīšanas, d) nodalot datņu izveidi un nosūtīšanu.

79. Šis datu aizsardzības pārkāpums attiecas tikai uz datu konfidencialitāti, un to integritāte un pieejamība palika neskarta. Datu aizsardzības pārkāpums ietekmēja tikai divdesmit klientus, tāpēc skarto datu daudzumu var uzskatīt par nelielu. Turklāt skartie personas dati nesatur sensitīvus datus. Par risku mazinošu faktoru var uzskatīt to, ka datu apstrādātājs pēc tam, kad uzzināja par datu aizsardzības pārkāpumu, nekavējoties sazinājās ar datu pārzini. (Jāizvērtē arī, vai iespējams, ka dati tika nosūtīti citiem apdrošināšanas aģentiem, un, ja tas apstiprināsies, jāveic atbilstoši pasākumi.) Tā kā pēc datu aizsardzības pārkāpuma tika veikti atbilstoši pasākumi, tas, visticamāk, neietekmēs datu subjektu tiesības un brīvības.

80. Nelielais ietekmēto personu skaits, pārkāpuma tūlītēja atklāšana un pasākumi, kas veikti, lai samazinātu tā sekas, ļauj uzskatīt šo konkrēto gadījumu par tādu, kas nerada risku.

4.2.2 9. GADĪJUMS — seku mazināšana un saistības

81. Turklāt pastāv arī citi risku mazinoši apstākļi: aģentam ir pienākums neizpaust dienesta noslēpumu; viņš pats ziņoja par problēmu pārzinim, un viņš pēc pieprasījuma izdzēsa datni. Informētības palielināšana un, iespējams, papildu darbību iekļaušana tādu dokumentu pārbaudē, kas ietver personas datus, palīdzētu izvairīties no līdzīgiem gadījumiem nākotnē.

82. Papildus pārkāpuma dokumentēšanai saskaņā ar 33. panta 5. punktu nav jāveic citas darbības.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	X	X

4.3 Organizatoriskie un tehniskie pasākumi, lai novērstu/mazinātu iekšējo cilvēciskā riska avotu radītās sekas

83. Turpmāk minēto pasākumu kombinācijai, ko piemēro atkarībā no gadījuma unikālajām iezīmēm, būtu jāpalīdz mazināt līdzīga pārkāpuma atkārtošanās iespējamību.

84. Ieteicamie pasākumi:

(Turpmāk minēto pasākumu saraksts nekādā ziņā nav uzskatāms par pilnīgu vai visaptverošu. Drīzāk mērķis ir sniegt idejas profilaksei un iespējamos risinājumus. Katra apstrādes darbība ir atšķirīga, tāpēc pārzinim ir jāpieņem lēmums par to, kuri pasākumi ir vispiemērotākie konkrētajā situācijā.)

- periodiska mācību, izglītošanas un izpratnes veidošanas programmu organizēšana darbiniekiem par viņu pienākumiem attiecībā uz privātumu un drošību un personas datu drošības apdraudējumu atklāšanu un ziņošanu par tiem[26]; izpratnes veidošanas programmu izstrāde, lai atgādinātu darbiniekiem par visbiežāk pieļautajām kļūdām, kas izraisa personas datu aizsardzības pārkāpumus, un to, kā no tām izvairīties;
- drošas un efektīvas datu aizsardzības un privātuma prakses, procedūru un sistēmu izveide[27];
- privātuma prakses, procedūru un sistēmu novērtējums, kas palīdz nodrošināt nepārtrauktu efektivitāti[28];
- pienācīgas piekļuves kontroles politikas veidošana un nodrošināšana, ka lietotāji ievēro noteikumus;
- tādu metožu ieviešana, kas liek autentificēt lietotāju, kad tiek piekļūts sensitīviem personas datiem;
- ar uzņēmumu saistītā lietotāja konta atspējošana, tiklīdz persona atstāj uzņēmumu;
- neparastas datu plūsmas kontrole starp datņu serveri un darbinieku darbstacijām;
- *I/O* saskarnes drošības iestatīšana *BIOS* vai izmantojot programmatūru, kas kontrolē datora saskarņu lietošanu (bloķēt vai atbloķēt, piemēram, *USB/CD/DVD* utt.);
- darbinieku piekļuves politikas pārskatīšana (piemēram, piekļuves sensitīviem datiem reģistrēšana un pieprasīšana lietotājam ievadīt uzņēmējdarbības iemeslu, lai tas būtu pieejams auditiem);
- atvērto mākoņpakalpojumu atspējošana;
- aizliegums un neļaušana piekļūt zināmiem atvērtā pasta pakalpojumiem;
- ekrāna drukāšanas funkcijas atspējošana operētājsistēmā;
- tīra galda politikas īstenošana;
- automātiska visu datoru bloķēšana pēc noteikta bezdarbības laika;
- tādu mehānismu (piemēram, (bezvadu) marķieru, kas ļauj pieteikties bloķētiem kontiem vai atvērt tos) izmantošana, kas nodrošina lietotāju ātru pārslēgšanu koplietotās vidēs;

[26] Rezolūcijas par to, kā izvairīties no cilvēka kļūdu izraisītiem personas datu aizsardzības pārkāpumiem, 2. sadaļas i) apakšpunkts.

[27] Rezolūcijas par to, kā izvairīties no cilvēka kļūdu izraisītiem personas datu aizsardzības pārkāpumiem, 2. sadaļas ii) apakšpunkts.

[28] Rezolūcijas par to, kā izvairīties no cilvēka kļūdu izraisītiem personas datu aizsardzības pārkāpumiem, 2. sadaļas iii) apakšpunkts.

- speciālu sistēmu izmantošana personas datu pārvaldībai, kam ir atbilstoši piekļuves kontroles mehānismi un kas novērš cilvēka kļūdas, piemēram, ziņojumu nosūtīšanu nepareizam subjektam. Izklājlapu un citu biroja dokumentu izmantošana nav piemērots līdzeklis klientu datu pārvaldībai.

5 PAZAUDĒTAS VAI NOZAGTAS IERĪCES UN DOKUMENTI PAPĪRA FORMĀTĀ

85. Bieži gadās, ka tiek nozaudētas vai nozagtas portatīvās ierīces. Šādos gadījumos pārzinim ir jāņem vērā apstrādes darbības apstākļi, piemēram, ierīcē glabāto datu veids, kā arī palīglīdzekļi un pasākumi, kas veikti pirms pārkāpuma, lai nodrošinātu atbilstošu apstrādes drošības līmeni. Visi šie elementi nosaka datu aizsardzības pārkāpuma iespējamo ietekmi. Veikt riska novērtējumu ir sarežģīti, jo ierīce vairs nav pieejama.

86. Šāda veida pārkāpumus vienmēr var klasificēt kā konfidencialitātes pārkāpumus. Tomēr, ja nozagtajai datubāzei nav dublējumkopijas, pārkāpumu var klasificēt arī kā pieejamības un integritātes pārkāpumu.

87. Turpmāk minētie scenāriji parāda, kā iepriekš minētie apstākļi ietekmē datu aizsardzības pārkāpuma iespējamību un nopietnības pakāpi.

5.1 10. GADĪJUMS — nozagta ierīce, kurā glabājas šifrēti personas dati

Ielaužoties kādā bērnu dienas aprūpes centrā, nozagti divi planšetdatori. Planšetdatoros bija lietotne, kurā bija personas dati par bērniem, kas apmeklē dienas aprūpes centru. Skartie dati bija vārds, dzimšanas datums, personas dati par bērnu izglītību. Gan šifrētie planšetdatori, kas ielaušanās brīdī bija izslēgti, gan lietotne bija aizsargāti ar drošu paroli. Dublējuma dati pārzinim bija ātri un viegli pieejami. Uzzinot par ielaušanos, dienas aprūpes iestāde neilgi pēc ielaušanās atklāšanas attālināti izdzēsa informāciju no planšetdatoriem.

5.1.1 10. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

88. Šajā konkrētajā gadījumā datu pārzinis veica atbilstošus pasākumus, lai novērstu un mazinātu iespējamā datu aizsardzības pārkāpuma sekas, izmantojot ierīces šifrēšanu, ieviešot atbilstošu paroles aizsardzību un nodrošinot planšetdatoros glabāto datu dublēšanu. (Ieteicamo pasākumu saraksts atrodams 5.7. iedaļā).

89. Uzzinot par pārkāpumu, datu pārzinim jānovērtē riska avots, datu apstrādes atbalsta sistēmas, skarto personas datu veids un datu aizsardzības pārkāpuma iespējamā ietekme uz attiecīgajām personām. Iepriekš aprakstītais datu aizsardzības pārkāpums varētu tikt klasificēts kā attiecīgo datu konfidencialitātes, pieejamības un integritātes pārkāpums, taču, pateicoties datu pārziņa veiktajām atbilstošajām procedūrām pirms un pēc datu aizsardzības pārkāpuma, neviens no tiem neīstenojās.

5.1.2 10. GADĪJUMS — seku mazināšana un saistības

90. Ierīcēs esošo personas datu konfidencialitāte netika apdraudēta, pateicoties drošas paroles aizsardzībai gan planšetdatoros, gan lietotnēs. Planšetdatori tika iestatīti tā, ka paroles iestatīšana nozīmē arī to, ka ierīcē esošie dati tiek šifrēti. To vēl vairāk uzlaboja pārziņa rīcība, mēģinot attālināti izdzēst visu informāciju no nozagtajām ierīcēm.

91. Pateicoties veiktajiem pasākumiem, tika saglabāta arī datu konfidencialitāte. Turklāt dublēšana nodrošināja nepārtrauktu personas datu pieejamību, tāpēc nevarēja rasties iespējamā negatīvā ietekme.

92. Ņemot vērā šos faktus, visticamāk, iepriekš aprakstītais datu aizsardzības pārkāpums nerada augstu risku datu subjektu tiesībām un brīvībām, tāpēc nav jāpaziņo UI vai attiecīgajiem datu subjektiem. Tomēr šis datu aizsardzības pārkāpums ir jādokumentē saskaņā ar 33. panta 5. punktu.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	X	X

5.2 11. GADĪJUMS — nozagta ierīce, kurā glabājas nešifrēti personas dati

Kāda pakalpojumu sniedzēja uzņēmuma darbiniekam nozagts piezīmjdators. Nozagtajā piezīmjdatorā vairāk nekā 100 000 klientu vārdi, uzvārdi, dzimums, adrese un dzimšanas datums. Tā kā nozagtā ierīce vairs nebija pieejama, nebija iespējams noteikt, vai ir skartas arī citas personas datu kategorijas. Piekļuve piezīmjdatora cietajam diskam nebija aizsargāta ar paroli. Personas datus varēja atjaunot no pieejamajām ikdienas dublējumkopijām.

5.2.1 11. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

93. Datu pārzinis iepriekš nebija veicis nekādus drošības pasākumus, tāpēc nozagtajā piezīmjdatorā glabātie personas dati bija viegli pieejami zaglim vai jebkurai citai personai, kuras rīcībā ierīce nonāca.

94. Šis datu aizsardzības pārkāpums attiecas uz nozagtajā ierīcē glabāto datu konfidencialitāti.

95. Šajā gadījumā piezīmjdators, kurā bija personas dati, bija ievainojams, jo tam nebija nekādas paroles aizsardzības vai šifrēšanas. Pamata drošības pasākumu trūkums paaugstina ietekmēto datu subjektu riska līmeni. Turklāt problemātiska ir arī attiecīgo datu subjektu identificēšana, kas arī paaugstina pārkāpuma nopietnības pakāpi. Ievērojamais iesaistīto personu skaits palielina risku, tomēr datu aizsardzības pārkāpumā netika ietekmētas īpašas personas datu kategorijas.

96. Veicot riska novērtējumu[29], pārzinim būtu jāņem vērā konfidencialitātes pārkāpuma iespējamā nelabvēlīgā ietekme. Pārkāpuma rezultātā attiecīgie datu subjekti var tikt pakļauti identitātes viltošanai, pamatojoties uz nozagtajā ierīcē pieejamajiem datiem, tāpēc tiek uzskatīts, ka risks ir augsts.

5.2.2 11. GADĪJUMS — seku mazināšana un saistības

97. Ierīces šifrēšanas aktivizēšana un drošas paroles aizsardzības izmantošana glabājamajai datubāzei varēja novērst datu aizsardzības pārkāpuma risku datu subjektu tiesībām un brīvībām.

98. Šo apstākļu dēļ ir nepieciešams paziņot UI, kā arī attiecīgajiem datu subjektiem.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem

[29] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

✓	✓	✓

5.3 12. GADĪJUMS — nozagti dokumenti papīra formātā, kuros ir sensitīvi dati

Kādā no narkotikām atkarīgo personu rehabilitācijas iestādē tika nozagts papīra formāta reģistrācijas žurnāls. Žurnālā bija reģistrēti rehabilitācijas iestādē uzņemto pacientu identitātes pamatdati un veselības dati. Dati tika glabāti tikai papīra formātā, un pacientus ārstējošajiem ārstiem nebija pieejama dublējumkopija. Žurnāls netika glabāts slēgtā atvilktnē vai telpā, datu pārzinim nebija ne piekļuves kontroles režīma, ne citu papīra dokumentācijas aizsardzības pasākumu.

5.3.1 12. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

99. Datu pārzinis iepriekš nebija veicis nekādus drošības pasākumus, tāpēc nozagtajā žurnālā glabātie personas dati bija viegli pieejami personai, kuras rīcībā žurnāls nonāca. Turklāt žurnālā glabāto personas datu raksturs padara datu dublējumkopijas trūkumu par ļoti nopietna riska faktoru.

100. Šis gadījums ir augsta riska datu aizsardzības pārkāpuma piemērs. Tā kā netika veikti atbilstoši drošības pasākumi, tika zaudēti sensitīvi veselības dati, kas noteikti VDAR 9. panta 1. punktā. Šajā gadījumā ir ietekmēta īpaša personas datu kategorija, tāpēc potenciālie riski attiecīgajiem datu subjektiem pieaug, kas jāņem vērā arī pārzinim, izvērtējot risku[30].

101. Šis pārkāpums attiecas uz skarto personas datu konfidencialitāti, pieejamību un integritāti. Pārkāpuma rezultātā tiek izpausts medicīniskais noslēpums un nesankcionētas trešās puses var piekļūt pacienta privātajai medicīniskajai informācijai, kas var nopietni ietekmēt pacienta personisko dzīvi. Pieejamības pārkāpums var arī traucēt pacientu ārstēšanas nepārtrauktību. Tā kā nevar izslēgt žurnāla satura daļēju pārveidošanu/iznīcināšanu, tiek apdraudēta arī personas datu integritāte.

5.3.2 12. GADĪJUMS — seku mazināšana un saistības

102. Aizsardzības pasākumu izvērtēšanas laikā jāņem vērā arī atbalsta līdzekļa veids. Tā kā pacienta žurnāls bija fizisks dokuments, tā aizsardzība bija jāorganizē citādi nekā elektroniskās ierīces aizsardzība. Pacientu vārdu pseidonimizācija, žurnāla glabāšana apsargātās telpās un slēgtā atvilktnē vai telpā, kā arī atbilstoša piekļuves kontrole ar autentifikāciju varēja novērst datu aizsardzības pārkāpumu.

103. Iepriekš aprakstītais datu aizsardzības pārkāpums var nopietni ietekmēt attiecīgos datu subjektus, tāpēc par pārkāpumu obligāti jāpaziņo UI un attiecīgajiem datu subjektiem.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	✓

5.4 Organizatoriskie un tehniskie pasākumi, lai novērstu/mazinātu ierīču nozaudēšanas vai zādzības sekas

104. Turpmāk minēto pasākumu kombinācijai, ko piemēro atkarībā no gadījuma unikālajām iezīmēm, būtu jāpalīdz mazināt līdzīga pārkāpuma atkārtošanās iespējamību.

105. Ieteicamie pasākumi:

[30] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

(Turpmāk minēto pasākumu saraksts nekādā ziņā nav uzskatāms par pilnīgu vai visaptverošu. Drīzāk mērķis ir sniegt idejas profilaksei un iespējamos risinājumus. Katra apstrādes darbība ir atšķirīga, tāpēc pārzinim ir jāpieņem lēmums par to, kuri pasākumi ir vispiemērotākie konkrētajā situācijā.)

- ierīces šifrēšanas (piemēram, *Bitlocker*, *Veracrypt* vai *DM-Crypt*) aktivizēšana;
- piekļuves koda/paroles izmantošana visās ierīcēs; visas mobilās elektroniskās ierīces tiek šifrētas tā, lai atšifrēšanai būtu jāievada sarežģīta parole;
- vairākfaktoru autentifikācijas izmantošana;
- viedierīcēs tādas funkcijas aktivizēšana, kas ļauj noteikt ierīču atrašanās vietu pazaudēšanas vai nepareizas novietošanas gadījumā;
- *MDM* (mobilo ierīču pārvaldības) programmatūras/lietotnes un lokalizācijas izmantošana; pretatspīduma filtru izmantošana; bez uzraudzības atstātu ierīču aizvēršana;
- ja iespējams un atbilstoši attiecīgajai datu apstrādei, personas datu saglabāšana nevis mobilajā ierīcē, bet gan centrālajā aizmugurserverī;
- ja darbstacija ir pieslēgta korporatīvajam *LAN*, automātiskas dublēšanas nodrošināšana no darba mapēm, ja absolūti nepieciešams tur glabāt personas datus;
- drošu virtuālo privāto tīklu jeb *VPN* (piemēram, kam nepieciešama atsevišķa otrā faktora autentifikācijas atslēga droša savienojuma izveidei) izmantošana, lai savienotu mobilās ierīces ar aizmugurserveriem;
- fiziskas slēdzenes nodrošināšana darbiniekiem, lai viņi varētu fiziski aizsargāt mobilās ierīces, ko izmanto, kamēr tās paliek bez uzraudzības;
- atbilstoša regulējuma ieviešana ierīces lietošanai ārpus uzņēmuma;
- atbilstoša regulējuma ieviešana ierīces lietošanai uzņēmuma iekšienē;
- *MDM* (mobilo ierīču pārvaldības) programmatūras/lietotnes izmantošana un attālās dzēšanas funkcijas iespējošana;
- centralizētas ierīču pārvaldības izmantošana ar minimālām tiesībām galalietotājiem instalēt programmatūru;
- fiziskās piekļuves vadīklas instalēšana;
- izvairīšanās no sensitīvas informācijas glabāšanas mobilajās ierīcēs vai cietajos diskos. Ja rodas nepieciešamība piekļūt uzņēmuma iekšējai sistēmai, būtu jāizmanto droši kanāli, kā minēts iepriekš.

6 KĻŪDAINA PASTA PIEGĀDE

106. Arī šajā gadījumā riska avots ir iekšēja cilvēka kļūda, taču pārkāpumu nav izraisījusi ļaunprātīga darbība. Tās ir neuzmanības sekas. Pārzinis pēc notikušā neko daudz nevar izdarīt, tāpēc šādos gadījumos profilakse ir vēl svarīgāka nekā cita veida pārkāpumu gadījumos.

6.1 13. GADĪJUMS — kļūdaina pasta piegāde

Kāds mazumtirdzniecības uzņēmums iesaiņoja divus apavu pasūtījumus. Cilvēka kļūdas rezultātā tika sajauktas divas pavadzīmes, kā rezultātā abas preces un attiecīgās pavadzīmes tika nosūtītas nepareizai personai. Tas nozīmē, ka divi klienti saņēma viens otra pasūtījumu, arī pavadzīmes, kurās bija personas dati. Uzzinājis par pārkāpumu, datu pārzinis atsauca pasūtījumus un nosūtīja tos pareizajiem adresātiem.

6.1.1 13. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

107. Pavadzīmēs bija norādīti personas dati, kas nepieciešami veiksmīgai piegādei (vārds, adrese, kā arī iegādātā prece un tās cena). Ir svarīgi noteikt, kā cilvēka kļūda vispār varēja notikt un, ja iespējams, kā to varēja novērst. Konkrētajā gadījumā risks nav liels, jo netika ietekmētas īpašas personas datu kategorijas vai citi dati, kuru ļaunprātīga izmantošana varētu radīt būtiskas negatīvas sekas, pārkāpums nav noticis pārziņa sistēmiskas kļūdas dēļ un ir ietekmētas tikai divas personas. Netika konstatēta negatīva ietekme uz personām.

6.1.2 13. GADĪJUMS — seku mazināšana un saistības

108. Pārzinim būtu jānodrošina preču un attiecīgo pavadzīmju bezmaksas atgriešana, kā arī jāprasa, lai saņēmēji, kas kļūdaini saņēma sūtījumu, iznīcinātu/dzēstu visas iespējamās pavadzīmju kopijas, kurās ir ietverti citas personas dati.

109. Pat ja pārkāpums pats par sevi nerada lielu risku ietekmēto personu tiesībām un brīvībām un tādējādi paziņošana datu subjektiem nav obligāta atbilstoši VDAR 34. pantam, nevar izvairīties no paziņošanas par pārkāpumu, jo ir nepieciešama viņu sadarbība riska mazināšanā.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	X	X

6.2 14. GADĪJUMS — īpaši konfidenciāli personas dati, kas kļūdaini nosūtīti pa pastu

Valsts pārvaldes biroja nodarbinātības nodaļa nosūtīja e-pasta ziņojumu par gaidāmajām mācībām personām, kas tās sistēmā reģistrētas kā darba meklētāji. Šim e-pastam kļūdaini tika pievienots dokuments, kurā bija visi šo darba meklētāju personas dati (vārds, e-pasta adrese, pasta adrese, sociālās apdrošināšanas numurs). Ietekmēto personu skaits pārsniedz 60 000. Pēc notikušā birojs sazinājās ar visiem adresātiem un lūdza dzēst iepriekšējo ziņojumu un neizmantot tajā esošo informāciju.

6.2.1 14. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

110. Šādu ziņojumu sūtīšanai vajadzēja ieviest stingrākus noteikumus. Jāapsver papildu kontroles mehānismu ieviešana.

111. Ietekmēto personu skaits ir ievērojams, un risku paaugstina tas, ka kopā ar citiem pamatdatiem tika nosūtīts arī viņu sociālās apdrošināšanas numurs, tāpēc risku var kvalificēt kā augstu[31]. Pārzinis nevar novērst to, ka kāds no saņēmējiem datus varētu izplatīt tālāk.

[31] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

6.2.2 14. GADĪJUMS — seku mazināšana un saistības

112. Kā minēts iepriekš, līdzekļi, kas efektīvi mazinātu līdzīgu pārkāpumu risku, ir ierobežoti. Lai gan pārzinis lūdza dzēst ziņojumu, tas nevar piespiest adresātus to izdarīt un tādējādi arī nevar būt pārliecināts, ka viņi izpilda šo lūgumu.

113. Šādā gadījumā būtu jāveic visas trīs turpmāk norādītās darbības.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	✓

6.3 15. GADĪJUMS — personas dati, kas kļūdaini nosūtīti pa pastu

Juridiskās angļu valodas kursu dalībnieku saraksts kļūdaini nosūtīts 15 bijušajiem kursu dalībniekiem, nevis viesnīcai, kurā piecas dienas norisināsies kursi. Sarakstā ir 15 dalībnieku vārdi, e-pasta adreses un informācija par izvēlētajiem ēdieniem. Tikai divi dalībnieki ir ierakstījuši savu izvēli attiecībā uz ēdienu, norādot, ka viņiem ir laktozes nepanesība. Neviena dalībnieka identitāte nav aizsargāta. Pārzinis atklāj kļūdu uzreiz pēc saraksta nosūtīšanas, informē par kļūdu saņēmējus un lūdz sarakstu dzēst.

6.3.1 15. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

114. Personas datus saturošu ziņojumu sūtīšanai vajadzēja ieviest stingrākus noteikumus. Jāapsver papildu kontroles mehānismu ieviešana.

115. Riski, kas izriet no personas datu rakstura, sensitivitātes, apjoma un konteksta, ir zemi. Personas datos ir iekļauti sensitīvi dati par divu dalībnieku izvēli attiecībā uz ēdienu. Kaut arī informācija par to, ka personai ir laktozes nepanesība, ir veselības dati, risks, ka šie dati tiks izmantoti ļaunprātīgā veidā, būtu jāuzskata par salīdzinoši zemu. Lai gan attiecībā uz datiem par veselību parasti tiek pieņemts, ka pārkāpums datu subjektam var radīt augstu risku[32], tomēr šajā konkrētajā gadījumā nevar identificēt risku, ka pārkāpums radīs fiziskus, materiālus vai nemateriālus zaudējumus datu subjektam sakarā ar informācijas par laktozes nepanesību neatļautu izpaušanu. Pretēji dažiem citiem aspektiem attiecībā uz pārtikas izvēli laktozes nepanesību parasti nevar saistīt ar reliģiskiem vai filozofiskiem uzskatiem. Arī skarto datu apjoms un ietekmēto datu subjektu skaits ir ļoti neliels.

6.3.2 15. GADĪJUMS — seku mazināšana un saistības

116. Rezumējot var konstatēt, ka pārkāpumam nebija būtiskas ietekmes uz datu subjektiem. Par risku mazinošu faktoru var uzskatīt to, ka pārzinis pēc kļūdas pamanīšanas nekavējoties sazinājās ar saņēmējiem.

117. Ja e-pasta ziņojums tiek nosūtīts nepareiziem/neautorizētiem adresātiem, datu pārzinim ieteicams nosūtīt viņiem papildu e-pasta ziņojumu kā diskrēto kopiju (*Bcc*), kurā tas atvainojas, norāda, ka kļūdainais e-pasta ziņojums ir jāizdzēš, un informē adresātus, ka viņiem nav tiesību izmantotu e-pasta adreses, kuras kļūdas pēc ir uzzinājuši.

118. Ņemot vērā šos faktus, visticamāk, šis datu aizsardzības pārkāpums nerada augstu risku datu subjektu tiesībām un brīvībām, tāpēc nav jāpaziņo UI vai attiecīgajiem datu subjektiem. Tomēr šis datu aizsardzības pārkāpums ir jādokumentē saskaņā ar 33. panta 5. punktu.

[32] Sk. Pamatnostādnes *WP* 250, 23. lpp.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	X	X

6.4 16. GADĪJUMS — kļūdaina pasta piegāde

Kāda apdrošināšanas grupa piedāvā automobiļu apdrošināšanu. Šim mērķim tā pa pastu regulāri nosūta pielāgotas apdrošināšanas polises. Vēstulē papildus apdrošinājuma ņēmēja vārdam un adresei ir norādīts transportlīdzekļa reģistrācijas numurs bez maskētiem cipariem, kārtējā un nākamā apdrošināšanas gada apdrošināšanas tarifa likmes, aptuvenais gada nobraukums un apdrošinājuma ņēmēja dzimšanas datums. Nav iekļauti veselības dati, kas norādīti VDAR 9. pantā, maksājumu dati (bankas dati), ekonomiskie un finanšu dati.

Vēstules iesaiņo automatizētas aplokšņošanas iekārtas. Mehāniskas kļūdas dēļ divas vēstules dažādiem apdrošinājuma ņēmējiem ievietotas vienā aploksnē un pa pastu nosūtītas vienam apdrošinājuma ņēmējam. Apdrošinājuma ņēmējs, saņemot un atverot aploksni, redz gan sev adresēto vēstuli, gan nepareizi piegādāto cita apdrošinājuma ņēmēja vēstuli.

6.4.1 16. GADĪJUMS — iepriekš veiktie pasākumi un riska novērtēšana

119. Nepareizi piegādātajā vēstulē ir norādīts vārds, uzvārds, adrese, dzimšanas datums, nemaskēts transportlīdzekļa reģistrācijas numurs un kārtējā un nākamā gada apdrošināšanas tarifa likmes klasifikācija. Ietekme uz skarto personu ir uzskatāma par vidēju, jo neautorizētam saņēmējam tiek atklāta informācija, kas nav publiski pieejama, piemēram, dzimšanas datums vai nemaskēti transportlīdzekļa reģistrācijas numuri, kā arī informācija par apdrošināšanas tarifa likmes pieaugumu. Šo datu ļaunprātīgas izmantošanas iespējamība ir novērtēta kā zema un vidēja. Lai gan daudzi adresāti, iespējams, nepareizi saņemto vēstuli izmetīs atkritumos, tomēr atsevišķos gadījumos nevar pilnībā izslēgt, ka vēstule tiks ievietota sociālajos tīklos vai kāds sazināsies ar apdrošinājuma ņēmēju.

6.4.2 16. GADĪJUMS — seku mazināšana un saistības

120. Pārzinim par saviem līdzekļiem būtu jāpanāk dokumenta oriģināla atgriešana. Nepareizais adresāts arī būtu jāinformē, ka viņš/viņa nedrīkst ļaunprātīgi izmantot izlasīto informāciju.

121. Visticamāk, nekad nebūs iespējams pilnībā novērst pasta piegādes kļūdu masveida sūtījumos, kur izmanto pilnībā automatizētas iekārtas. Taču gadījumā, ja šādu kļūdu skaits pieaug, ir jāpārbauda, vai aplokšņošanas iekārtas ir pietiekami pareizi iestatītas un uzturētas un vai šādu pārkāpumu neizraisa kāda cita sistēmiska problēma.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	X

6.5 Organizatoriskie un tehniskie pasākumi kļūdainas pasta piegādes novēršanai / seku mazināšanai

122. Turpmāk minēto pasākumu kombinācijai, ko piemēro atkarībā no gadījuma unikālajām iezīmēm, būtu jāpalīdz mazināt līdzīga pārkāpuma atkārtošanās iespējamību.

123. Ieteicamie pasākumi:

(*Turpmāk minēto pasākumu saraksts nekādā ziņā nav uzskatāms par pilnīgu vai visaptverošu. Drīzāk mērķis ir sniegt idejas profilaksei un iespējamos risinājumus. Katra apstrādes darbība ir atšķirīga, tāpēc pārzinim ir jāpieņem lēmums par to, kuri pasākumi ir vispiemērotākie konkrētajā situācijā.*)

- precīzu standartu noteikšana vēstuļu / e-pasta ziņojumu sūtīšanai, nepieļaujot interpretācijas;

- atbilstošas personāla mācības par to, kā nosūtāmas vēstules / e-pasta ziņojumi;
- sūtot e-pasta ziņojumus vairākiem adresātiem, tie pēc noklusējuma jānorāda laukā "diskrētā kopija" (*Bcc*);
- sūtot e-pasta ziņojumu vairākiem adresātiem, ja tie nav norādīti laukā "diskrētā kopija", ir nepieciešams papildu apstiprinājums;
- "četru acu" principa piemērošana;
- automātiska, nevis manuāla adresēšana, izmantojot datus, kas iegūti no pieejamas un atjauninātas datubāzes; automātiskās adresēšanas sistēma būtu regulāri jāpārskata, lai pārbaudītu, vai nav slēptu kļūdu un nepareizu iestatījumu;
- ziņojuma aizkaves izmantošana (piemēram, ziņojumu var dzēst/rediģēt noteiktā laikā pēc nosūtīšanas pogas nospiešanas);
- automātiskās pabeigšanas atspējošana, ievadot e-pasta adreses;
- izpratnes veicināšanas mācības par biežāk pieļautajām kļūdām, kas izraisa personas datu aizsardzības pārkāpumu;
- mācības un rokasgrāmatas par to, kā rīkoties gadījumos, kuri izraisa personas datu aizsardzības pārkāpumu, un kam jāpaziņo (iesaistīt datu aizsardzības speciālistu jeb DAS).

7 CITI GADĪJUMI — SOCIĀLĀ INŽENIERIJA

7.1 17. GADĪJUMS — identitātes zādzība

Kāda telekomunikāciju uzņēmuma kontaktu centrs saņem tālruņa zvanu no kāda, kas uzdodas par klientu. Iespējamais klients pieprasa uzņēmumam mainīt e-pasta adresi, uz kuru turpmāk jānosūta norēķinu informācija. Kontaktu centra darbinieks pārbauda klienta identitāti, pieprasot noteiktus personas datus saskaņā ar uzņēmuma procedūrām. Zvanītājs norāda pareizu pieprasīto klienta nodokļu maksātāja reģistrācijas numuru un pasta adresi (jo viņam bija piekļuve šiem datiem). Pēc apstiprināšanas operators veic pieprasītās izmaiņas, un turpmāk norēķinu informācija tiek sūtīta uz jauno e-pasta adresi. Procedūra neparedz paziņojuma nosūtīšanu uz iepriekšējo e-pasta adresi. Nākamajā mēnesī likumīgais klients sazinās ar uzņēmumu un jautā, kāpēc viņš nesaņem rēķinu uz savu e-pasta adresi, kā arī noliedz, ka būtu zvanījis un prasījis mainīt e-pasta adresi. Vēlāk uzņēmums saprot, ka informācija ir nosūtīta nelikumīgam lietotājam, un atsauc izmaiņas.

7.1.1 17. GADĪJUMS — risku novērtēšana, seku mazināšana un saistības

124. Šis gadījums parāda, cik liela nozīme ir iepriekš veiktajiem pasākumiem. Pārkāpumam ir augsts riska līmenis33, jo norēķinu dati var sniegt informāciju par datu subjekta privāto dzīvi (piemēram, ieradumiem, kontaktiem) un radīt materiālu kaitējumu (piemēram, vajāšanu, fiziskās neaizskaramības risku). Šajā uzbrukumā iegūtos personas datus var izmantot arī, lai īstenotu konta pārņemšanu šajā organizācijā vai īstenotu turpmākus autentifikācijas pasākumus citās organizācijās. Ņemot vērā šos riskus, "atbilstošam" autentifikācijas pasākumam ir jāpiemēro augstas prasības atkarībā no tā, kādus personas datus autentifikācijas rezultātā var apstrādāt.

125. Šajā gadījumā pārzinim ir jāpaziņo gan UI, gan datu subjektam.

126. Iepriekšējās klienta apstiprināšanas process noteikti ir jāpilnveido, ņemot vērā šo gadījumu. Autentifikācijai izmantotās metodes nebija pietiekamas. Ļaunprātīgā persona varēja uzdoties par īsto lietotāju, izmantojot publiski un citādi pieejamu informāciju.

127. Nav ieteicams izmantot šāda veida statisku, uz zināšanām pamatotu autentifikāciju (tādu, kur atbilde nemainās un informācija nav "slepena", pretēji tam, kā tas būtu, piemēram, paroles gadījumā).

128. Organizācijai būtu jāizmanto tāds autentifikācijas veids, kas sniegtu drošu pārliecību, ka autentificētais lietotājs ir īstā persona, nevis kāds cits. Ārpusjoslas vairākfaktoru autentifikācijas metodes ieviešana atrisinātu šo problēmu, piemēram, ļautu pārbaudīt izmaiņu pieprasījumu, nosūtot apstiprinājuma pieprasījumu uz iepriekšējo adresi vai pievienojot papildu jautājumus un pieprasot informāciju, kas ir redzama tikai iepriekšējos rēķinos. Pārziņa pienākums ir izlemt, kādus pasākumus ieviest, jo viņš vislabāk pārzina savas iekšējās darbības nianses un prasības.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	✓

7.2 18. GADĪJUMS — e-pasta eksfiltrācija

[33] Norādes par to, kad apstrādes darbība "*varētu radīt augstu risku*", sk. iepriekš 10. zemsvītras piezīmē.

Kāda lielveikalu ķēde trīs mēnešus pēc konfigurācijas konstatēja, ka daži e-pasta konti ir mainīti un noteikumi izveidoti tā, lai katrs e-pasta ziņojums, kas ietver noteiktus izteicienus (piemēram, "rēķins", "maksājums", "bankas savienojums", "kredītkartes autentifikācija", "bankas konta dati"), tiktu pārvietots uz neizmantotu mapi un pārsūtīts uz ārēju e-pasta adresi. Iepriekš bija arī veikts sociālās inženierijas uzbrukums, t. i., uzbrucējs, uzdodoties par piegādātāju, bija nomainījis šā piegādātāja bankas konta rekvizītus uz saviem. Visbeidzot, iepriekš bija nosūtīti vairāki viltoti rēķini, kuros bija iekļauta jaunā bankas konta informācija. Rezultātā e-pasta platformas uzraudzības sistēma brīdināja par mapēm. Uzņēmums nevarēja noteikt, kā uzbrucējs sākotnēji varēja piekļūt e-pasta kontiem, taču pieļāva, ka vainīgs varēja būt inficēts e-pasta ziņojums, kas nodrošināja piekļuvi par maksājumiem atbildīgai lietotāju grupai.

Tā kā e-pasta ziņojumu pārsūtīšanas pamatā bija atslēgvārdu izmantošana, uzbrucējs saņēma šādu informāciju par 99 darbiniekiem: 89 datu subjektu vārdu un konkrētā mēneša darba algas apmēru; 10 darbinieku, kuru līgums tika izbeigts, vārdu, ģimenes stāvokli, bērnu skaitu, darba algas apmēru, darba laiku un pārējo informāciju par algas saņemšanu. Pārzinis paziņoja tikai šiem pēdējiem 10 darbiniekiem.

7.2.1 18. GADĪJUMS — risku novērtēšana, seku mazināšana un saistības

129. Pat ja uzbrucēja mērķis, iespējams, nebija personas datu vākšana, pārkāpums tomēr var radīt gan materiālu kaitējumu (piemēram, finansiālus zaudējumus), gan nemateriālu kaitējumu (piemēram, identitātes zādzību vai viltošanu), kā arī datus var izmantot, lai īstenotu citus uzbrukumus (piemēram, pikšķerēšanu), tādējādi personas datu aizsardzības pārkāpums ir saistīts ar lielu risku fizisko personu tiesībām un brīvībām. Tāpēc par pārkāpumu būtu jāpaziņo visiem 99 darbiniekiem, nevis tikai 10 darbiniekiem, kuru algas informācija tika nopludināta.

130. Uzzinājis par pārkāpumu, pārzinis lika nomainīt uzlauztajiem kontiem paroli, bloķēja e-pasta ziņojumu sūtīšanu uz uzbrucēja e-pasta kontu, paziņoja uzbrucēja izmantotā e-pasta pakalpojumu sniedzējam par veikto uzbrukumu, noņēma uzbrucēja noteiktos noteikumus un uzlaboja uzraudzības sistēmas brīdinājumu iestatījumus tā, lai sistēma brīdinātu, tiklīdz tiek izveidots automātisks noteikums. Alternatīvi pārzinis varēja noņemt tiesības lietotājiem iestatīt pārsūtīšanas noteikumus, uzdodot IT pakalpojumu komandai to darīt tikai pēc pieprasījuma, vai arī ieviest tādu kārtību, ka lietotājiem reizi nedēļā vai biežāk būtu jāpārbauda savos kontos iestatītie noteikumi saistībā ar finanšu datu apstrādi un jāziņo par tiem.

131. Tas, ka pārkāpums varēja notikt un palikt nepamanīts tik ilgi, kā arī tas, ka ilgākā laika posmā sociālo inženieriju varēja izmantot, lai mainītu arī citus datus, liecina par būtiskām problēmām pārziņa IT drošības sistēmā. Tās ir jārisina nekavējoties, piemēram, liekot uzsvaru uz automatizācijas pārskatīšanu un izmaiņu vadīklām, incidentu noteikšanu un reaģēšanas pasākumiem. Pārziņiem, kas apstrādā sensitīvus datus, finanšu informāciju utt., ir lielāka atbildība attiecībā uz atbilstošas datu drošības nodrošināšanu.

Nepieciešamās darbības, pamatojoties uz identificētajiem riskiem		
Iekšējā dokumentācija	Paziņojums UI	Paziņojums datu subjektiem
✓	✓	✓