Pamatnostādnes

Pamatnostādnes 4/2019 par 25. pantu

Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma

Versija 2.0

Pieņemtas 2020. gada 20. oktobrī

Versiju vēsture

Versija 1.0.	2019. gada 13. novembris	Pamatnostādņu pieņemšana sabiedriskai apspriešanai
Versija 2.0	2020. gada 20. oktobris	Pamatnostādņu pieņemšana EDAK pēc sabiedriskās apspriešanas

Satura rādītājs

1 Darbības joma 5

2 Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma — 25. panta 1. un 2. punkta analīze 5

2.1 25. panta 1. punkts — Integrēta datu aizsardzība 6

2.1.1 Pārziņa pienākums apstrādē īstenot atbilstošus tehniskus un organizatoriskus pasākumus un vajadzīgās garantijas 6

2.1.2 Efektīva datu aizsardzības principu īstenošana un datu subjektu tiesību un brīvību aizsardzība 6

2.1.3 Elementi, kas jāņem vērā 7

2.1.4 Laika aspekts 10

2.2 25. panta 2. punkts — Datu aizsardzība pēc noklusējuma 10

2.2.1 Pēc noklusējuma tiek apstrādāti tikai tādi persondati, kas ir nepieciešami katram konkrētajam apstrādes nolūkam. 10

2.2.2 Datu minimizēšanas pienākuma aspekti 12

3 Datu aizsardzības principu īstenošana persondatu apstrādē, izmantojot integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma 13

3.1 Pārredzamība 14

3.2 Likumība 15

3.3 Godprātība 17

3.4 Nolūka ierobežojums 19

3.5 Datu minimizēšana 20

3.6 Precizitāte 22

3.7 Glabāšanas ierobežojums 24

3.8 Integritāte un konfidencialitāte 25

3.9 Pārskatatbildība 27

4 VDAR 25. panta 3. punkts — Sertifikācija 27

5 25. panta izpilde un sekas 28

6 Ieteikumi 28

Eiropas Datu aizsardzības kolēģija,

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulā (ES) 2016/679 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 un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas 2018. gada 6. jūlija Lēmumu Nr. 154/2018,

ņemot vērā tās Reglamenta 12. un 22. pantu,

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

<u>Kopsavilkums</u>

Pieaugot digitalizācijai, prasību ievērošanai attiecībā uz integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma ir būtiska nozīme privātuma un datu aizsardzības veicināšanā sabiedrībā. Tāpēc ir svarīgi pārziņiem nopietni attiekties pret šo pienākumu un izpildīt no VDAR izrietošās saistības, plānojot apstrādes darbības.

Šajās pamatnostādnēs ir sniegti vispārīgi norādījumi par pienākumu ievērot integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma (turpmāk "IDADAN"), kā noteikts VDAR 25. pantā. IDADAN pienākums ir saistošs visiem pārziņiem neatkarīgi no apstrādes apmēra un sarežģītības pakāpes. Lai varētu īstenot IDADAN prasības, ir būtiski, lai pārzinis izprastu datu aizsardzības principus un datu subjekta tiesības un brīvības.

Galvenais pienākums ir īstenot *atbilstīgus* pasākumus un vajadzīgās garantijas, kas nodrošina *datu aizsardzības principu efektīvu īstenošanu* un tādējādi arī *datu subjektu tiesības un brīvības integrēti un pēc noklusējuma.* VDAR 25. pantā ir noteikti gan integrācijas, gan noklusējuma elementi, kas būtu jāņem vērā. Šie elementi tiks sīkāk izklāstīti šajās pamatnostādnēs.

VDAR 25. panta 1. punktā ir noteikts, ka pārziņiem IDADAN būtu jāapsver agrīnā posmā, kad tie plāno jaunu apstrādes darbību. Pārziņi īsteno IDADAN *pirms* apstrādes, kā arī *pastāvīgi* apstrādes laikā, regulāri pārskatot izvēlēto pasākumu un garantiju efektivitāti. IDADAN attiecas arī uz esošajām sistēmām, kas apstrādā persondatus.

Pamatnostādnēs ir ietverti arī norādījumi par to, kā efektīvi īstenot 5. pantā ietvertos datu aizsardzības principus, kur uzskaitīti galvenie integrētas datu aizsardzības un noklusējuma elementi, kā arī praktiski piemēri, kas to ilustrē. Pārzinim būtu jāapsver ierosināto pasākumu piemērotība saistībā ar konkrēto apstrādi.

EDAK sniedz ieteikumus par to, kā pārziņi, apstrādātāji un ražotāji var sadarboties, lai sasniegtu IDADAN. Tā mudina nozares pārziņus, apstrādātājus un ražotājus izmantot IDADAN kā līdzekli, lai iegūtu konkurences priekšrocības, pārdodot savus produktus pārziņiem un datu subjektiem. Tā arī mudina visus pārziņus izmantot sertifikātus un rīcības kodeksus.

1 DARBĪBAS JOMA

1. Pamatnostādnēs galvenā uzmanība ir pievērsta IDADAN īstenošanai, ko veic pārziņi, pamatojoties uz VDAR 25. pantā noteikto pienākumu.[1] Šīs pamatnostādnes var būt noderīgas arī citiem dalībniekiem, uz kuriem 25. pants tieši neattiecas, piemēram, apstrādātājiem un produktu, pakalpojumu un lietojumprogrammu ražotājiem (turpmāk "ražotāji"), kad tie veido VDAR atbilstošus produktus un pakalpojumus, kas pārziņiem ļauj izpildīt savus datu aizsardzības pienākumus.[2] VDAR 78. apsvērumā ir arī norādīts, ka IDADAN būtu jāņem vērā publiskā iepirkuma konkursos. Lai gan visiem pārziņiem ir pienākums integrēt IDADAN savās apstrādes darbībās, šis noteikums veicina datu aizsardzības principu pieņemšanu gadījumos, kad valsts pārvaldes iestādēm būtu jārāda piemērs. Pārzinis ir atbildīgs par IDADAN pienākumu izpildi attiecībā uz apstrādi, ko veic tā apstrādātāji un apakšapstrādātāji, tāpēc tiem tas būtu jāņem vērā, slēdzot līgumus ar šīm personām.

2. Regulas 25. pantā ir noteikta prasība, ka pārziņiem datu aizsardzība ir jāintegrē persondatu apstrādē un kā noklusējuma iestatījums, un tas attiecas uz visu apstrādes ciklu. IDADAN ir arī prasība attiecībā uz apstrādes sistēmām, kas pastāvēja pirms VDAR stāšanās spēkā. Pārziņiem apstrāde ir pastāvīgi jāatjaunina saskaņā ar VDAR. Sīkāku informāciju par to, kā uzturēt esošu sistēmu saskaņā ar IDADAN, skatīt šo pamatnostādņu 2.1.4. apakšnodaļā. Šā noteikuma būtība ir nodrošināt *piemērotu* un *efektīvu* datu aizsardzību gan *integrētā* veidā, gan pēc *noklusējuma*, kas nozīmē, ka pārziņiem būtu jāspēj pierādīt, ka apstrādē tiek īstenoti atbilstošie pasākumi un garantijas, lai nodrošinātu datu aizsardzības principu un datu subjektu tiesību un brīvību efektivitāti.

3. Pamatnostādņu otrajā nodaļā galvenā uzmanība tiek pievērsta 25. pantā noteikto prasību interpretācijai un tiek pētītas ar šo noteikumu ieviestās juridiskās saistības. Trešajā nodaļā ir sniegti piemēri, kā piemērot IDADAN konkrētu datu aizsardzības principu kontekstā.

4. Pamatnostādņu ceturtajā nodaļā uzmanība tiek pievērsta iespējai izveidot sertifikācijas mehānismu, lai pierādītu atbilstību 25. pantam, savukārt piektajā nodaļā — tam, kā uzraudzības iestādes var panākt šā panta izpildi. Visbeidzot, pamatnostādnēs ir sniegti plašāki ieteikumi ieinteresētajām personām par to, kā veiksmīgi īstenot IDADAN. EDAK atzīst, ka mazajiem un vidējiem uzņēmumiem (turpmāk "MVU") ir grūtības pilnībā izpildīt IDADAN pienākumus, un sestajā nodaļā sniedz papildu ieteikumus konkrēti MVU.

2 INTEGRĒTA DATU AIZSARDZĪBA UN DATU AIZSARDZĪBA PĒC NOKLUSĒJUMA — 25. PANTA 1. UN 2. PUNKTA ANALĪZE

5. Šīs nodaļas mērķis ir pētīt un sniegt norādījumus par integrētas datu aizsardzības prasībām saskaņā ar 25. panta 1. punktu un datu aizsardzības pēc noklusējuma prasībām saskaņā ar 25. panta 2. punktu. Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma ir savstarpēji papildinoši jēdzieni, kas

[1] Šeit sniegtās interpretācijas ir vienādi piemērojamas Direktīvas (ES) 2016/680 20. pantam un Regulas (ES) 2018/1725 27. pantam.

[2] VDAR 78. apsvērumā šī vajadzība ir skaidri izteikta: "*Attīstot, izstrādājot, atlasot un izmantojot lietojumprogrammas, pakalpojumus un preces, kas balstās uz persondatu apstrādi vai apstrādā persondatus savu pienākumu veikšanai, preču, pakalpojumu un lietojumprogrammu ražotāji būtu jāmudina ņemt vērā tiesības uz datu aizsardzību, kad attīsta un izstrādā šādas preces, pakalpojumus un lietojumprogrammas, un pienācīgi ņemt vērā tehnikas līmeni, lai nodrošinātu, ka pārziņi un apstrādātāji spēj izpildīt savus datu aizsardzības pienākumus.*"

viens otru nostiprina. Datu subjekti gūs lielāku labumu no datu aizsardzības pēc noklusējuma, ja vienlaikus tiks īstenota integrēta datu aizsardzība, un otrādi.

6. IDADAN ir prasība visiem pārziņiem, tostarp kā maziem uzņēmumiem, tā arī starptautiskiem uzņēmumiem. To ņemot vērā, IDADAN īstenošanas sarežģītība var atšķirties atkarībā no individuālās apstrādes darbības. Tomēr neatkarīgi no uzņēmuma lieluma jebkurā gadījumā, ieviešot IDADAN, var panākt pozitīvus ieguvumus pārzinim un datu subjektam.

2.1 25. panta 1. punkts — Integrēta datu aizsardzība

2.1.1 Pārziņa pienākums apstrādē īstenot atbilstošus tehniskus un organizatoriskus pasākumus un vajadzīgās garantijas

7. Saskaņā ar 25. panta 1. punktu pārzinis īsteno *atbilstošus* tehniskus un organizatoriskus *pasākumus*, kas ir paredzēti, lai īstenotu datu aizsardzības principus un lai apstrādē integrētu *vajadzīgās garantijas* nolūkā izpildīt prasības un aizsargāt datu subjektu tiesības un brīvības. Gan atbilstoši pasākumi, gan vajadzīgās garantijas ir paredzēti vienam un tam pašam mērķim — aizsargāt datu subjektu tiesības un nodrošināt viņu persondatu aizsardzības integrēšanu apstrādes procesā.

8. *Tehniskus un organizatoriskus pasākumus* un vajadzīgās garantijas plašā nozīmē var saprast kā jebkuru metodi vai līdzekli, ko pārzinis var izmantot apstrādē. *Atbilstība* nozīmē, ka pasākumiem un vajadzīgajām garantijām vajadzētu būt piemērotiem, lai sasniegtu paredzēto mērķi, t. i., tiem *efektīvi* jāīsteno datu aizsardzības principi[3]. Tādējādi atbilstības prasība ir cieši saistīta ar efektivitātes prasību.

9. Tehnisks vai organizatorisks pasākums un garantija var būt jebkas, sākot ar progresīvu tehnisko risinājumu izmantošanu un beidzot ar personāla pamatapmācību. Piemēri, kas var būt atbilstoši, atkarībā no konteksta un ar attiecīgo apstrādi saistītajiem riskiem ietver persondatu pseidonimizāciju[4]; persondatu uzglabāšanu strukturētā, plaši izmantotā mašīnlasāmā formātā; iespēju sniegšanu datu subjektiem iejaukties apstrādē; informācijas sniegšanu par persondatu uzglabāšanu; ļaunprogrammatūras atklāšanas sistēmu ieviešanu; darbinieku apmācību par "kiberhigiēnas" pamatiem; privātuma un informācijas drošības pārvaldības sistēmu izveidi; līgumisku pienākumu noteikšanu apstrādātājiem īstenot konkrētu datu minimizēšanas praksi utt.

10. Atbilstošu pasākumu noteikšanā var noderēt standarti, paraugprakse un rīcības kodeksi, ko atzīst apvienības un citas struktūras, kuras pārstāv pārziņu kategorijas. Tomēr pārzinim ir jāpārbauda pasākumu atbilstība attiecībā uz konkrēto apstrādi.

2.1.2 Efektīva datu aizsardzības principu īstenošana un datu subjektu tiesību un brīvību aizsardzība

11. *Datu aizsardzības principi* ir noteikti 5. pantā (turpmāk "principi"); *datu subjektu tiesības un brīvības* ir fizisku personu pamattiesības un pamatbrīvības un jo īpaši viņu tiesības uz persondatu aizsardzību, kas 1. panta 2. punktā ir minēta kā VDAR mērķis (turpmāk "tiesības")[5]. To precīzs formulējums ir atrodams ES Pamattiesību hartā. Ir svarīgi, lai pārzinis saprastu *principu* un *tiesību* nozīmi kā pamatu aizsardzībai, ko piedāvā VDAR, jo īpaši IDADAN pienākums.

[3] "Efektivitāte" turpmāk ir aplūkota 2.1.2. apakšnodaļā.
[4] Definēta VDAR 4. panta 5. punktā.
[5] Sk. VDAR 4. apsvērumu.

12. Īstenojot atbilstošus tehniskus un organizatoriskus pasākumus, pasākumi un garantijas būtu *jāizstrādā*, ņemot vērā katra iepriekš minētā principa efektīvu īstenošanu un no tās izrietošo tiesību aizsardzību.

Efektivitātes jautājums

13. Efektivitāte ir integrētas datu aizsardzības jēdziena pamatā. Prasība efektīvi īstenot principus nozīmē, ka pārziņiem ir jāīsteno vajadzīgie pasākumi un garantijas šo principu aizsardzībai, lai aizsargātu datu subjektu tiesības. Katram īstenotajam pasākumam būtu jāsniedz plānotie rezultāti pārziņa paredzētajai apstrādei. Šim apsvērumam ir divas sekas.

14. Pirmkārt, tas nozīmē, ka 25. pantā nav prasīts īstenot konkrētus tehniskus un organizatoriskus pasākumus, bet tas paredz, ka izvēlētajiem pasākumiem un garantijām ir jābūt specifiskiem, lai īstenotu datu aizsardzības principus konkrētajā apstrādē. To darot, pasākumi un garantijas būtu jāizstrādā tā, lai tie būtu stingri, un pārzinim būtu jāspēj īstenot turpmākus pasākumus, lai pielāgotos jebkādam riska pieaugumam[6]. Tāpēc tas, vai pasākumi ir efektīvi, būs atkarīgs no konkrētās apstrādes konteksta un konkrētu elementu novērtējuma, kas būtu jāņem vērā, nosakot apstrādes veidus. Iepriekš minētie elementi turpmāk ir aplūkoti 2.1.3. apakšnodaļā.

15. Otrkārt, pārziņiem būtu jāspēj pierādīt, ka principi ir ievēroti.

16. Īstenotajiem pasākumiem un garantijām būtu jāsasniedz vēlamais rezultāts attiecībā uz datu aizsardzību, un pārzinim vajadzētu būt dokumentācijai par īstenotajiem tehniskajiem un organizatoriskajiem pasākumiem[7]. Lai to izdarītu, pārzinis var noteikt attiecīgus galvenos darbības rādītājus (GDR) efektivitātes pierādīšanai. GDR ir pārziņa izvēlēta izmērāma vērtība, kas parāda, cik efektīvi pārzinis sasniedz savu datu aizsardzības mērķi. GDR var būt *kvantitatīvi*, piemēram, aplamu pozitīvo vai aplamu negatīvo vērtību īpatsvars, sūdzību samazināšanās, reaģēšanas laika samazināšanās, datu subjektiem īstenojot savas tiesības, vai *kvalitatīvi*, piemēram, veiktspējas novērtējumi, vērtēšanas skalu izmantošana vai ekspertu novērtējumi. Kā alternatīva GDR pārziņiem var būt iespēja pierādīt principu efektīvu īstenošanu, sniedzot pamatojumu savam izvēlēto pasākumu un garantiju efektivitātes novērtējumam.

2.1.3 Elementi, kas jāņem vērā

17. Elementi, kas pārzinim ir jāņem vērā, nosakot konkrētas apstrādes darbības pasākumus, ir uzskaitīti 25. panta 1. punktā. Turpmāk mēs sniegsim norādījumus par to, kā šos elementus izmantot plānošanas procesā, kas ietver noklusējuma iestatījumu plānošanu. Visi šie elementi palīdz noteikt, vai pasākums ir atbilstošs, lai efektīvi īstenotu principus. Tādējādi katrs no šiem elementiem nav pašmērķis — tie ir faktori, kas jāaplūko kopumā, lai sasniegtu mērķi.

[6] "Pārziņiem piemērojamajiem pamatprincipiem (t. i., leģitimitātei, datu minimizēšanai, nolūka ierobežojumam, pārredzamībai, datu integritātei, datu precizitātei) vajadzētu būt vienādiem neatkarīgi no apstrādes un datu subjektiem radītā riska. Tomēr šādas apstrādes raksturs un apjoms vienmēr ir bijis pienācīgi jāņem vērā, piemērojot šos principus, lai tie pēc būtības būtu mērogojami." 29. panta darba grupa, paziņojums "Uz risku balstītas pieejas nozīme attiecībā uz datu aizsardzības tiesisko regulējumu", WP 218, 2014. gada 30. maijs, 3. lpp., ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[7] Sk. 74. un 78. apsvērumu.

2.1.3.1 "tehnikas līmenis"

18. Jēdziens "tehnikas līmenis" ir ietverts dažādos ES *acquis*, piemēram, vides aizsardzības un produktu drošības jomā. VDAR atsauce uz "tehnikas līmeni"[8] ir izdarīta ne tikai 32. pantā attiecībā uz drošības pasākumiem,[9] [10] bet arī 25. pantā, tādējādi attiecinot šo kritēriju uz visiem tehniskajiem un organizatoriskajiem pasākumiem, kas integrēti apstrādes procesā.

19. Atsauce uz "tehnikas līmeni" 25. panta kontekstā uzliek pārziņiem pienākumu atbilstošu tehnisko un organizatorisko pasākumu noteikšanā **ņemt vērā** tirgū pieejamo **tehnoloģiju šā brīža progresu**. Pārziņiem ir jābūt zināšanām un jābūt pastāvīgi informētiem par tehnoloģiju attīstību, to, kā tehnoloģijas var radīt datu aizsardzības riskus vai iespējas apstrādes darbībai, un to, kā īstenot un atjaunināt pasākumus un garantijas, kas *nodrošina* datu subjektu principu un tiesību *efektīvu īstenošanu*, ņemot vērā mainīgo tehnoloģiju vidi.

20. "Tehnikas līmenis" ir dinamisks jēdziens, ko nevar statiski definēt noteiktā brīdī; tas būtu *pastāvīgi* jāizvērtē tehnoloģiskā progresa kontekstā. Ņemot vērā tehnoloģiskos sasniegumus, pārzinis var konstatēt, ka pasākums, kas reiz nodrošināja pietiekamu aizsardzības līmeni, vairs to nespēj. Tādējādi tehnoloģisko izmaiņu neņemšana vērā var novest pie neatbilstības 25. pantam.

21. Kritērijs "tehnikas līmenis" attiecas ne tikai uz tehnoloģiskiem, bet arī uz organizatoriskiem pasākumiem. Atbilstošu organizatorisko pasākumu trūkums var pazemināt vai pat pilnībā apdraudēt izvēlētās tehnoloģijas efektivitāti. Organizatorisku pasākumu piemēri var būt iekšējās politikas pieņemšana, aktuāla apmācība par tehnoloģiju, drošību un datu aizsardzību un IT drošības un pārvaldības politika.

22. Esošajām un atzītajām sistēmām, standartiem, sertifikātiem, rīcības kodeksiem utt. dažādās jomās var būt nozīme, lai norādītu pašreizējo "tehnikas līmeni" attiecīgajā izmantošanas jomā. Ja šādi standarti pastāv un nodrošina augstu aizsardzības līmeni datu subjektam, izpildot vai pārsniedzot juridiskās prasības, pārziņiem tie būtu jāņem vērā, izstrādājot un īstenojot datu aizsardzības pasākumus.

2.1.3.2 "īstenošanas izmaksas"

23. Pārzinis var ņemt vērā īstenošanas izmaksas, kad tas izvēlas un piemēro atbilstošus tehniskus un organizatoriskus pasākumus un vajadzīgās garantijas, ar kurām efektīvi īsteno principus, lai aizsargātu datu subjektu tiesības. Izmaksas attiecas uz resursiem kopumā, tostarp laika resursiem un cilvēkresursiem.

24. Izmaksu elements nenosaka, ka pārzinim ir jātērē nesamērīgs resursu apjoms, ja pastāv alternatīvi, mazāk resursietilpīgi, bet efektīvi pasākumi. Tomēr īstenošanas izmaksas ir faktors, kas jāņem vērā, lai īstenotu integrētu datu aizsardzību, nevis iemesls to neīstenot.

---

[8] Sk. Vācijas Federālās Konstitucionālās tiesas 1978. gada nolēmumu lietā *Kalkar*: https://germanlawarchive.iuscomp.org/?p=67, kas var sniegt pamatu jēdziena objektīvas definēšanas metodikai. Pamatojoties uz to, "tehnikas līmenis" var tikt identificēts starp "esošo zinātnisko zināšanu un izpētes" tehnikas līmeni un vairāk vispāratzītiem "vispārpieņemtiem tehnikas noteikumiem". Tādējādi "tehnikas līmeni" var identificēt kā tāda pakalpojuma vai tehnoloģijas, vai produkta tehnikas līmeni, kāds pastāv tirgū un ir visefektīvākais noteikto mērķu sasniegšanai.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

25. Tādējādi izvēlētie pasākumi nodrošina, ka pārziņa paredzētajā apstrādes darbībā neapstrādā persondatus, pārkāpjot principus, neatkarīgi no izmaksām. Pārziņiem būtu jāspēj pārvaldīt kopējās izmaksas, lai varētu efektīvi īstenot visus principus un attiecīgi aizsargāt tiesības.

2.1.3.3 "apstrādes raksturs, apmērs, konteksts un nolūks"

26. Nosakot vajadzīgos pasākumus, pārziņiem jāņem vērā apstrādes raksturs, apmērs, konteksts un nolūks.

27. Šie faktori būtu jāinterpretē atbilstīgi to lomai citos VDAR noteikumos, piemēram, 24., 32. un 35. pantā, lai datu aizsardzības principus integrētu apstrādē.

28. Īsāk sakot, **raksturu** var saprast kā apstrādes raksturīgās[11] īpašības. **Apmērs** attiecas uz apstrādes lielumu un diapazonu. **Konteksts** attiecas uz apstrādes apstākļiem, kas var ietekmēt datu subjekta gaidas, savukārt **nolūks** attiecas uz apstrādes mērķiem.

2.1.3.4 "dažādas iespējamības un nopietnības pakāpes riski attiecībā uz fizisku personu tiesībām un brīvībām, kurus rada apstrāde"

29. Ar VDAR ir pieņemta saskaņota, uz risku balstīta pieeja daudzos tās noteikumos — 24., 25., 32. un 35. pantā —, lai noteiktu atbilstošus tehniskus un organizatoriskus pasākumus nolūkā aizsargāt personas, viņu persondatus un nodrošinātu atbilstību VDAR prasībām. Aizsargājamie aktīvi vienmēr ir vienādi (indivīdi, izmantojot savu persondatu aizsardzību), aizsargājami pret vieniem un tiem pašiem riskiem (riskiem indivīdu tiesībām), ņemot vērā tos pašus nosacījumus (apstrādes raksturu, apmēru, kontekstu un nolūku).

30. Veicot riska analīzi attiecībā uz atbilstību 25. pantam, pārzinim ir jāapzina datu subjektu tiesību riski, ko rada principu pārkāpums, un jānosaka to iespējamība un smagums, lai īstenotu pasākumus apzināto risku efektīvai mazināšanai. Veicot riska novērtējumus, būtiska nozīme ir sistemātiskam un rūpīgam apstrādes novērtējumam. Piemēram, pārzinis novērtē konkrētos riskus, kuri saistīti ar brīvi sniegtas piekrišanas trūkumu, kas ir likumības principa pārkāpums, bērnu un jauniešu, kas jaunāki par 18 gadiem, kā neaizsargātas grupas persondatu apstrādes laikā, ja nav cita juridiska pamata, un īsteno atbilstošus pasākumus, lai novērstu un efektīvi mazinātu apzinātos riskus, kas saistīti ar šo datu subjektu grupu.

31. EDAK pamatnostādnēs par datu aizsardzības ietekmes novērtējumu (NIDA)[12], kurās galvenā uzmanība pievērsta tam, lai noteiktu, vai apstrādes darbība var radīt augstu risku datu subjektam, ir sniegti arī norādījumi par to, kā novērtēt datu aizsardzības riskus un kā veikt datu aizsardzības riska novērtējumu. Šīs pamatnostādnes var būt noderīgas arī risku novērtēšanā visos iepriekšminētajos pantos, ieskaitot 25. pantu.

32. Uz risku balstīta pieeja neizslēdz bāzes līniju, paraugprakses un standartu izmantošanu. Tie varētu būt pārziņiem noderīgs instrumentu kopums, lai novērstu līdzīgus riskus līdzīgās situācijās (apstrādes raksturs, apmērs, konteksts un nolūks). Tomēr joprojām saglabājas 25. pantā (kā arī 24. un 32. pantā un 35. panta 7. punkta c) apakšpunktā) noteiktais pienākums ņemt vērā "*dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, kurus rada apstrāde*".

[11] Piemēri ir īpašu kategoriju persondati, automātiska lēmumu pieņemšana, nenoteiktas attiecības ar varu, neprognozējama apstrāde, grūtības datu subjektam īstenot tiesības utt.

[12] 29. panta darba grupa, "Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē", WP 248 vers. 01, 2017. gada 4. oktobris, ec.europa.eu/newsroom/document.cfm?doc_id=47711 — apstiprinājusi EDAK.

Tāpēc pārziņiem, lai arī viņi izmanto šādus rīkus, katrā individuālā gadījumā ir jāveic datu apstrādes risku novērtēšana attiecīgajai apstrādes darbībai un jāpārbauda ierosināto atbilstošo pasākumu un garantiju efektivitāte. Tādā gadījumā papildus var būt nepieciešams NIDA vai esoša NIDA atjauninājums.

2.1.4 Laika aspekts

2.1.4.1 Apstrādes līdzekļu noteikšanas laikā

33. Integrēta datu aizsardzība ir jāīsteno "*apstrādes līdzekļu noteikšanas laikā*".

34. "*Apstrādes līdzekļi*" ir gan vispārīgi, gan sīki izstrādāti apstrādes plānošanas elementi, tostarp arhitektūra, procedūras, protokoli, izkārtojums un izskats.

35. "*Apstrādes līdzekļu noteikšanas laiks*" attiecas uz laikposmu, kurā pārzinis pieņem lēmumu par to, kā tiks veikta apstrāde un kā notiks apstrāde, un mehānismiem, kas tiks izmantoti šādas apstrādes veikšanai. Šādu lēmumu pieņemšanas procesā pārzinim ir jāizvērtē atbilstošie pasākumi un garantijas, lai efektīvi īstenotu principus un datu subjektu tiesības apstrādes procesā, un jāņem vērā tādi elementi kā tehnikas līmenis, īstenošanas izmaksas, raksturs, apmērs, konteksts un nolūks, kā arī riski. Tas ietver datu apstrādes programmatūras, aparatūras un pakalpojumu iegādes un ieviešanas laiku.

36. IDADAN agrīnai apsvēršanai ir izšķiroša nozīme, lai sekmīgi īstenotu datu subjektu tiesību principus un aizsardzību. Turklāt, raugoties no izmaksu un ieguvumu viedokļa, pārziņu interesēs ir arī ņemt vērā IDADAN pēc iespējas agrāk, jo jau izdotu plānu un izstrādātu apstrādes darbību izmaiņu veikšana vēlāk var būt problemātiska un dārga.

2.1.4.2 Pašas apstrādes laikā (datu aizsardzības prasību uzturēšana un pārskatīšana)

37. Tiklīdz apstrāde ir sākusies, pārzinim joprojām ir pienākums uzturēt IDADAN, t. i., turpināt efektīvi īstenot principus, lai aizsargātu tiesības, ievērojot tehnikas līmeni, atkārtoti vērtējot riska līmeni utt. Apstrādes darbību raksturs, apmērs un konteksts, kā arī risks var mainīties apstrādes gaitā, kas nozīmē, ka pārzinim ir atkārtoti jāizvērtē savas apstrādes darbības, regulāri pārskatot un novērtējot tā izvēlēto pasākumu un garantiju efektivitāti.

38. Pienākums pēc vajadzības uzturēt, pārskatīt un atjaunināt apstrādes darbību attiecas arī uz iepriekš pastāvošām sistēmām. Tas nozīmē, ka mantotās sistēmas, kas izstrādātas pirms VDAR stāšanās spēkā, ir jāpārskata un jāuztur, lai nodrošinātu tādu pasākumu un garantiju īstenošanu, ar kuriem efektīvi īsteno datu subjektu principus un tiesības, kā izklāstīts šajās pamatnostādnēs.

39. Šis pienākums attiecas arī uz jebkuru apstrādi, ko veic datu apstrādātāji. Pārziņiem ir regulāri jāpārskata un jānovērtē apstrādātāju darbības, lai pārliecinātos, ka tās nodrošina pastāvīgu atbilstību principiem un ļauj datu pārzinim izpildīt tā attiecīgos pienākumus.

2.2 25. panta 2. punkts — Datu aizsardzība pēc noklusējuma

2.2.1 Pēc noklusējuma tiek apstrādāti tikai tādi persondati, kas ir nepieciešami katram konkrētajam apstrādes nolūkam.

40. "Noklusējums", kā to parasti definē datorzinātnēs, attiecas uz iepriekš pastāvošu vai iepriekš atlasītu konfigurējama iestatījuma vērtību, kas tiek piešķirta programmatūras lietojumprogrammai, datorprogrammai vai ierīcei. Šādus iestatījumus sauc arī par "sākotnējiem iestatījumiem" vai "rūpnīcas iestatījumiem", jo īpaši attiecībā uz elektroniskām ierīcēm.

41. Tādējādi termins “pēc noklusējuma”, apstrādājot persondatus, nozīmē izvēles izdarīšanu attiecībā uz konfigurācijas vērtībām vai apstrādes iespējām, kas ir noteiktas vai paredzētas apstrādes sistēmā, piemēram, programmatūras lietojumprogramma, pakalpojums vai ierīce, vai manuālas apstrādes procedūra, kas ietekmē savākto persondatu apjomu, to apstrādes apmēru, glabāšanas ilgumu un pieejamību.

42. Pārzinim vajadzētu izvēlēties un būt atbildīgam par noklusējuma apstrādes iestatījumu un iespēju īstenošanu tādā veidā, ka pēc noklusējuma tiek veikta tikai apstrāde, kas ir absolūti nepieciešama, lai sasniegtu noteikto likumīgo mērķi. Pārziņiem šajā gadījumā būtu jāpaļaujas uz apstrādes nepieciešamības novērtējumu attiecībā uz 6. panta 1. punkta juridisko pamatu. Tas nozīmē, ka pēc noklusējuma pārzinis nevāc vairāk datu, nekā tas ir nepieciešams, tas neapstrādā savāktos datus vairāk, nekā tas ir nepieciešams to nolūkiem, kā arī neglabā datus ilgāk, nekā tas ir nepieciešams. Pamatprasība ir tāda, ka datu aizsardzība tiek integrēta datu apstrādē pēc noklusējuma.

43. Pārzinim ir pienākums iepriekš noteikt, kādiem konkrētiem, skaidriem un likumīgiem nolūkiem persondati tiek vākti un apstrādāti.[13] Pasākumiem pēc noklusējuma jābūt atbilstošiem, lai nodrošinātu, ka tiek apstrādāti tikai tādi persondati, kas nepieciešami katram konkrētam apstrādes nolūkam. EDAU “Pamatnostādnes, lai novērtētu to pasākumu nepieciešamību un samērīgumu, kas ierobežo tiesības uz persondatu aizsardzību” var būt noderīgas arī, lai izlemtu, kādi dati ir jāapstrādā, lai sasniegtu konkrētu mērķi[14] [15] [16].

44. Ja pārzinis izmanto trešās personas programmatūru vai plašpatēriņa programmatūru, pārzinim būtu jāveic produkta riska novērtējums un jāpārliecinās, ka tiek izslēgtas funkcijas, kam nav juridiska pamata vai kas nav saderīgas ar paredzētajiem apstrādes nolūkiem.

45. Tie paši apsvērumi attiecas uz organizatoriskiem pasākumiem, ar kuriem atbalsta apstrādes darbības. Tie ir jāplāno tā, lai visupirms tiktu apstrādāts tikai minimālais persondatu apjoms, kas nepieciešams konkrētajām darbībām. Tas jo īpaši ir jāņem vērā, piešķirot piekļuvi datiem darbiniekiem ar dažādām funkcijām un dažādām piekļuves vajadzībām.

46. Atbilstošus “tehniskus un organizatoriskus pasākumus” datu aizsardzības pēc noklusējuma kontekstā tādējādi saprot tādā pašā veidā, kā aprakstīts iepriekš 2.1.1. apakšnodaļā, bet tos īpaši piemēro datu minimizēšanas principa īstenošanai.

47. Iepriekš minētais pienākums apstrādāt tikai tos persondatus, kas nepieciešami katram konkrētajam nolūkam, attiecas uz turpmāk aprakstītajiem elementiem.

[13] VDAR 5. panta 1. punkta b), c), d) un e) apakšpunkts.

[14] EDAU, “Pamatnostādnes, lai novērtētu to pasākumu nepieciešamību un samērīgumu, kas ierobežo tiesības uz datu aizsardzību”, 2019. gada 25. februāris, edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[15] Sk. arī EDAU, “To pasākumu nepieciešamības novērtēšana, kas ierobežo pamattiesības uz persondatu aizsardzību — Rīkkopa”, https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en.

[16] Sīkāku informāciju par nepieciešamību sk.: 29. panta darba grupa, “Atzinums 06/2014 par persondatu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu”, WP 217, 2014. gada 9. aprīlis, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lv.pdf.

2.2.2 Datu minimizēšanas pienākuma aspekti

48. VDAR 25. panta 2. punktā ir uzskaitīti datu minimizēšanas pienākuma aspekti attiecībā uz apstrādi pēc noklusējuma, nosakot, ka šis pienākums attiecas uz savākto persondatu apjomu, to apstrādes apmēru, glabāšanas ilgumu un pieejamību.

2.2.2.1 "vākto persondatu apjoms"

49. Pārziņiem būtu jāņem vērā gan persondatu apjoms, gan apstrādes nolūkiem vajadzīgo persondatu veidi, kategorijas un detalizācijas pakāpe. Plānošanas izvēlēs būtu jāņem vērā paaugstināts risks integritātes un konfidencialitātes principiem, datu minimizēšana un glabāšanas ierobežojums, vācot lielu daudzumu detalizētu persondatu, un tas ir jāsalīdzina ar samazinātu risku, kas saistīts ar mazāka apjoma un/vai mazāk detalizētas informācijas vākšanu par datu subjektiem. Jebkurā gadījumā noklusējuma iestatījumā neiekļauj tādu persondatu vākšanu, kas nav nepieciešami konkrētajam apstrādes nolūkam. Citiem vārdiem sakot, ja atsevišķas persondatu kategorijas nav nepieciešamas vai arī nav nepieciešami detalizēti dati, jo pietiek ar mazāk detalizētiem datiem, tad papildu persondati netiek vākti.

50. Tādas pašas noklusējuma prasības attiecas uz pakalpojumiem neatkarīgi no tā, kāda platforma vai ierīce tiek izmantota, — var vākt tikai attiecīgajam nolūkam nepieciešamos persondatus.

2.2.2.2 "to apstrādes pakāpe"

51. Persondatu apstrādes[17] darbības aprobežojas ar to, kas ir nepieciešams. Daudzas apstrādes darbības var veicināt apstrādes nolūku. Tomēr tas, ka noteikti persondati ir nepieciešami, lai sasniegtu kādu mērķi, nenozīmē, ka ar šiem datiem var veikt visa veida un biežuma apstrādes darbības. Pārziņiem arī vajadzētu būt piesardzīgiem, lai nepaplašinātu "saderīgu nolūku" robežas, kas noteikts 6. panta 4. punktā, un jāpatur prātā, kādu apstrādi pamatoti sagaida datu subjekti.

2.2.2.3 "glabāšanas laikposms"

52. Savāktos persondatus neglabā, ja tie nav nepieciešami apstrādes nolūkā un ja nav cita saderīga mērķa un juridiska pamata saskaņā ar 6. panta 4. punktu. Datu pārzinim būtu pēc nepieciešamības objektīvi jāpamato jebkura datu glabāšana saskaņā ar pārskatatbildības principu.

53. Pārzinis ierobežo glabāšanas periodu līdz tam, kas ir nepieciešams konkrētajam nolūkam. Ja persondati vairs nav nepieciešami apstrādes nolūkā, tos pēc noklusējuma dzēš vai anonimizē. Tādējādi glabāšanas ilgums ir atkarīgs no attiecīgās apstrādes nolūka. Šis pienākums ir tieši saistīts ar glabāšanas ierobežojuma principu, kas noteikts 5. panta 1. punkta e) apakšpunktā, un to īsteno pēc noklusējuma, t. i., pārzinim apstrādē ir jābūt integrētām sistemātiskām procedūrām datu dzēšanai vai anonimizēšanai.

[17] Saskaņā ar VDAR 4. panta 2. punktu tas ietver vākšanu, reģistrēšanu, organizēšanu, strukturēšanu, uzglabāšanu, pielāgošanu vai pārveidošanu, izguvi, aplūkošanu, izmantošanu, izpaušanu, izmantojot pārsūtīšanu, izplatīšanu vai citādi darot to pieejamu, saskaņošanu vai kombinēšanu, ierobežošanu, dzēšanu vai iznīcināšanu.

54. Persondatu anonimizēšana[18] ir alternatīva dzēšanai, ar nosacījumu, ka tiek ņemti vērā visi attiecīgie kontekstuālie elementi un regulāri tiek novērtēta riska iespējamības un nopietnības pakāpe, ieskaitot atkārtotas identifikācijas risku[19].

2.2.2.4 "to pieejamība"

55. Pārzinim būtu jāierobežo to personu loks, kuras var piekļūt persondatiem, un tas, kādos veidos var piekļūt persondatiem, pamatojoties uz nepieciešamības novērtējumu, kā arī jāpārliecinās, ka persondati faktiski ir pieejami tiem, kuriem tie vajadzīgi nepieciešamības gadījumā, piemēram, kritiskās situācijās. Apstrādes laikā būtu jānodrošina piekļuves kontrole visai datu plūsmai.

56. Turklāt 25. panta 2. punktā noteikts, ka persondatus bez personas līdzdalības nedara pieejamus nenoteiktam fizisku personu skaitam. Pārzinim pēc noklusējuma jāierobežo pieejamība un jāsniedz datu subjektam iespēja iejaukties, pirms tas publicē vai citādi dara pieejamus datu subjekta persondatus neierobežotam fizisku personu skaitam.

57. Persondatu nodošana nenoteiktam personu skaitam var izraisīt vēl lielāku datu izplatīšanu, nekā sākotnēji paredzēts. Tas ir īpaši svarīgi interneta un meklētājprogrammu kontekstā. Tas nozīmē, ka pārziņiem pēc noklusējuma būtu jāsniedz datu subjektiem iespēja iejaukties, pirms persondati tiek darīti pieejami atvērtā internetā. Tas ir īpaši svarīgi attiecībā uz bērniem un neaizsargātām grupām.

58. Atkarībā no apstrādes juridiskā pamata iespēja iejaukties var atšķirties atkarībā no apstrādes konteksta. Piemēram, var lūgt piekrišanu padarīt persondatus publiski pieejamus vai noteikt privātuma iestatījumus, lai datu subjekti paši varētu kontrolēt publisku piekļuvi.

59. Pat ja persondati tiek darīti publiski pieejami ar datu subjekta atļauju un sapratni, tas nenozīmē, ka jebkurš cits pārzinis ar piekļuvi persondatiem var tos brīvi apstrādāt saviem nolūkiem — tiem ir vajadzīgs atsevišķs juridiskais pamats[20].

3 DATU AIZSARDZĪBAS PRINCIPU ĪSTENOŠANA PERSONDATU APSTRĀDĒ, IZMANTOJOT INTEGRĒTU DATU AIZSARDZĪBU UN DATU AIZSARDZĪBU PĒC NOKLUSĒJUMA

60. Visos apstrādes darbību plānošanas posmos, tostarp iepirkumos, konkursos, ārpakalpojumos, izstrādē, atbalstā, uzturēšanā, testēšanā, uzglabāšanā, dzēšanā utt., pārzinim būtu jāņem vērā un jāapsver

[18] 29. panta darba grupa, "Atzinums 05/2014 par anonimizācijas metodēm", WP 216, 2014. gada 10. aprīlis, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lv.pdf.
[19] Sk. VDAR 4. panta 1. punktu, 26. apsvērumu un 29. panta darba grupas "Atzinumu 05/2014 par anonimizācijas metodēm". Lūdzu skatīt arī šā dokumenta 3. iedaļas apakšiedaļu par "glabāšanas ierobežojumu", kurā ir atsauce uz vajadzību pārzinim nodrošināt ieviestās(-o) anonimizācijas metodes(-žu) efektivitāti.
[20] Sk. lietu *Satakunnan Markkinapörssi Oy* un *Satamedia Oy* pret Somiju, Nr. 931/13.

dažādi IDADAN elementi, kas principu īstenošanas kontekstā tiks ilustrēti ar piemēriem šajā nodaļā[21] [22] [23].

61. Pārziņiem ir jāīsteno principi, lai sasniegtu IDADAN. Šie principi cita starpā ir pārredzamība, likumība, godprātība, nolūka ierobežošana, datu minimizēšana, precizitāte, uzglabāšanas ierobežojumi, integritāte un konfidencialitāte, un pārskatatbildība. Šie principi ir izklāstīti VDAR 5. pantā un 39. apsvērumā. Lai gūtu pilnīgu izpratni par to, kā īstenot IDADAN, tiek uzsvērts, cik svarīgi ir izprast katra principa nozīmi.

62. Sniedzot piemērus par to, kā IDADAN īstenot praksē, par katru principu ir sagatavots **galveno IDADAN elementu** saraksts. Kaut arī piemēros ir izcelts konkrētais datu aizsardzības princips, tie var pārklāties arī ar citiem cieši saistītiem principiem. EDAK uzsver, ka turpmāk izklāstītie galvenie elementi un piemēri nav ne izsmeļoši, ne saistoši, bet ir paredzēti kā katra principa vadošie elementi. Pārziņiem ir jānovērtē, kā garantēt principu ievērošanu konkrētās apstrādes darbības kontekstā.

63. Lai gan šajā sadaļā galvenā uzmanība ir pievērsta principu īstenošanai, pārzinim būtu arī jāīsteno *atbilstoši* un *efektīvi* veidi, kā aizsargāt datu subjektu tiesības, arī saskaņā ar VDAR III nodaļu, ja tas jau nav noteikts pašos principos.

64. Pārskatatbildības princips ir visaptverošs — tas nosaka, ka pārzinim jābūt atbildīgam, izvēloties nepieciešamos tehniskos un organizatoriskos pasākumus.

3.1 Pārredzamība[24]

65. Pārzinim ir jābūt godīgam un atklātam pret datu subjektu attiecībā uz to, kā viņš vāks, izmantos un kopīgos persondatus. Pārredzamība nozīmē iespēju datu subjektiem saprast un vajadzības gadījumā īstenot savas 15.–22. pantā noteiktās tiesības. Šis princips ir integrēts 12., 13., 14. un 34. pantā. Pasākumiem un garantijām, kas īstenoti, lai nodrošinātu pārredzamības principa ievērošanu, ir arī jāpalīdz šo pantu īstenošanā.

66. Pārredzamības principa galvenie integrācijas un noklusējuma elementi var būt šādi:

- skaidrība — informācija tiek sniegta skaidrā un saprotamā valodā, ir kodolīga un saprotama;
- semantika — komunikācijai vajadzētu būt skaidri saprotamai attiecīgajai auditorijai;
- pieejamība — informācijai ir viegli pieejama datu subjektam;
- konteksts — informācija būtu jāsniedz piemērotā laikā un atbilstošā formā;
- atbilstība — informācijai vajadzētu būt atbilstošai un piemērojamai attiecībā uz konkrēto datu subjektu;
- universāls plānojums — informācija ir pieejama visiem datu subjektiem un ietver mašīnlasāmu valodu lietošanu, lai atvieglotu un automatizētu lasāmību un skaidrību;
- saprotamība — datu subjektiem vajadzētu būt skaidrai izpratnei par to, ko viņi var sagaidīt no viņu persondatu apstrādes, jo īpaši, ja datu subjekti ir bērni vai citas neaizsargātas grupas;

[21] Vairāk piemēru sk.: Norvēģijas Datu aizsardzības iestāde, "Programmatūru izstrāde, ņemot vērā integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma", 2017. gada 28. novembris, www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729.

[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers

[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

[24] Papildu informācija par pārredzamības jēdziena izpratni ir atrodama 29. panta darba grupas "Pārredzamības pamatnostādnēs saskaņā ar Regulu 2016/679", WP 260 vers. 01, 2018. gada 11. aprīlis, ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 — apstiprinājusi EDAK.

- daudzkanālu informācija — informācija būtu jāsniedz dažādos kanālos un plašsaziņas līdzekļos, ne tikai teksta formātā, lai palielinātu iespējamību, ka informācija efektīvi sasniegs datu subjektu;
- slāņainība — informācija vajadzētu būt slāņotai tādā veidā, lai novērstu spriedzi starp pilnīgumu un izpratni, vienlaikus ņemot vērā datu subjektu pamatotās cerības.

Piemērs[25]

Pārzinis izstrādā privātuma politiku savā tīmekļa vietnē, lai nodrošinātu atbilstību pārredzamības prasībām. Privātuma politikā nebūtu jāietver garš informācijas izklāsts, kurā vidusmēra datu subjektam ir grūti iedziļināties un kuru ir grūti saprast. To raksta skaidrā un kodolīgā valodā, tā, lai tīmekļa vietnes lietotājam būtu viegli saprast, kā tiek apstrādāti viņa persondati. Tāpēc pārzinis sniedz informāciju slāņos, izceļot vissvarīgākos punktus. Sīkāka informācija ir viegli pieejama. Lai sīkāk izskaidrotu dažādos elementus un jēdzienus, kas lietoti politikā, tiek piedāvātas nolaižamās izvēlnes un saites uz citām lapām. Pārzinis arī pārliecinās, ka informācija tiek sniegta vairākos kanālos, nodrošinot videoklipus, lai izskaidrotu rakstiskās informācijas svarīgākos punktus. Būtiska ir sinerģija starp dažādām lapām, lai nodrošinātu, ka slāņu pieeja nepalielina apjukumu, bet drīzāk to samazina.

Privātuma politikai nevajadzētu būt datu subjektam grūti sasniedzamai. Tādējādi konfidencialitātes politika ir pieejama un redzama attiecīgās vietnes visās tīmekļa lapās, lai datu subjekts vienmēr varētu tikai ar vienu klikšķi piekļūt informācijai. Sniegtā informācija ir izstrādāta arī saskaņā ar paraugpraksi un universāla plānojuma standartiem, nodrošinot tās pieejamību visiem.

Turklāt nepieciešamā informācija būtu arī jāsniedz arī pareizajā kontekstā un atbilstošā laikā. Tā kā pārzinis veic daudzas apstrādes darbības, izmantojot tīmekļa vietnē savāktos datus, vispārīga privātuma politika tikai tīmekļa vietnē nav pietiekama, lai pārzinis izpildītu pārredzamības prasības. Tādēļ pārzinis plāno informācijas plūsmu, sniedzot datu subjektam atbilstošu informāciju attiecīgajā kontekstā, izmantojot, piemēram, informācijas fragmentus vai uznirstošos logus. Piemēram, lūdzot datu subjektam ievadīt persondatus, pārzinis informē datu subjektu par to, kā persondati tiks apstrādāti un kāpēc šie persondati ir nepieciešami apstrādei.

3.2 Likumība

67. Pārzinim jānorāda spēkā esošs persondatu apstrādes juridiskais pamats. Ar pasākumiem un garantijām būtu jāatbalsta prasība nodrošināt visa apstrādes dzīves cikla atbilstību attiecīgajiem apstrādes juridiskajiem pamatiem.

68. Likumības galvenie integrācijas un noklusējuma elementi var būt šādi:
    - atbilstība — apstrādei piemēro pareizo juridisko pamatu;
    - diferencēšana[26] — juridisko pamatu, ko izmanto katrai apstrādes darbībai, diferencē;
    - konkrēts nolūks — attiecīgajam juridiskajam pamatam jābūt nepārprotami saistītam ar apstrādes konkrēto nolūku[27];

[25] Francijas Datu aizsardzības iestāde ir publicējusi vairākus piemērus ar lietotāju informēšanas paraugpraksi, kā arī citiem pārredzamības principiem: https://design.cnil.fr/en/.
[26] EDAK, "Pamatnostādnes 2/2019 par persondatu apstrādi saskaņā ar VDAR 6. panta 1. punkta b) apakšpunktu, sniedzot tiešsaistes pakalpojumus datu subjektiem", versija 2.0, 2019. gada 8. oktobris, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_lv.pdf.
[27] Skatīt turpmāk sadaļu par nolūka ierobežojumu.

- nepieciešamība — apstrādei jābūt nepieciešamai un bez nosacījumiem, lai nolūks būtu likumīgs;
- autonomija — datu subjektam būtu jāpiešķir pēc iespējas augstāka autonomijas pakāpe attiecībā uz persondatu kontroli juridiskā pamata ietvaros;
- piekrišanas iegūšana — piekrišanai jābūt brīvi sniegtai un jābūt konkrētai, apzinātai un nepārprotamai.[28] Īpaša uzmanība būtu jāpievērš bērnu un jauniešu spējai sniegt apzinātu piekrišanu;
- piekrišanas atsaukšana — ja piekrišana ir juridiskais pamats, apstrādei būtu jāatvieglo piekrišanas atsaukšana. Piekrišanas atsaukšanai jābūt tikpat vienkāršai kā piekrišanas sniegšanai. Ja tā nav, tad pārziņa piekrišanas mehānisms neatbilst VDAR[29];
- interešu izsvēršana — ja likumīgas intereses ir juridiskais pamats, pārzinim ir jāveic interešu izsvēršana, īpašu uzmanību pievēršot varas nelīdzsvarotībai, jo īpaši bērniem, kuri jaunāki par 18 gadiem, un citām neaizsargātām grupām. Ir paredzēti pasākumi un garantijas, lai mazinātu negatīvo ietekmi uz datu subjektiem;
- iepriekšēja noteikšana — juridisko pamatu nosaka pirms apstrādes veikšanas;
- izbeigšana — ja juridisko pamatu vairs nepiemēro, attiecīgi izbeidz arī apstrādi;
- pielāgošana — ja notiek pamatotas apstrādes juridiskā pamata izmaiņas, faktiskā apstrāde ir jāpielāgo atbilstoši jaunajam juridiskajam pamatam[30].
- atbildības sadalījums — ja ir paredzēta kopīga kontrole, pusēm skaidri un pārredzami jāsadala savi attiecīgie pienākumi attiecībā pret datu subjektu un jāplāno apstrādes pasākumi saskaņā ar šo sadalījumu.

Piemērs

Banka plāno piedāvāt pakalpojumu, lai uzlabotu aizdevumu pieteikumu pārvaldības efektivitāti. Pakalpojuma pamatā ir ideja, ka banka, pieprasot atļauju no klienta, var izgūt datus par klientu tieši no valsts nodokļu iestādēm. Šajā piemērā nav aplūkota no citiem avotiem iegūtu persondatu apstrāde.

Persondatu iegūšana par datu subjekta finansiālo stāvokli ir nepieciešama, lai veiktu pasākumus pēc datu subjekta pieprasījuma pirms aizdevuma līguma noslēgšanas[31]. Tomēr persondatu vākšana tieši no nodokļu administrācijas netiek uzskatīta par nepieciešamu, jo klients var noslēgt līgumu, pats sniedzot informāciju no nodokļu administrācijas. Lai gan bankai var būt likumīgas intereses iegūt dokumentus tieši no nodokļu iestādēm, piemēram, lai nodrošinātu aizdevumu apstrādes efektivitāti, šāda banku tieša piekļuve pieteikuma iesniedzēju persondatiem rada risku, kas saistīts ar piekļuves tiesību izmantošanu vai iespējamu ļaunprātīgu izmantošanu.

Īstenojot likumības principu, pārzinis apzinās, ka šajā kontekstā tas nevar izmantot "nepieciešamību līguma noslēgšanai" kā pamatu apstrādei, kas ietver persondatu vākšanu tieši no nodokļu iestādēm. Fakts, ka šī konkrētā apstrāde rada risku, ka datu subjekts mazāk iesaistīsies viņa datu apstrādē, ir būtisks faktors arī pašas apstrādes likumības novērtēšanā. Banka secina, ka šai apstrādes daļai jābalstās uz citu apstrādes juridisko pamatu. Konkrētajā dalībvalstī, kurā atrodas pārzinis, pastāv valsts tiesību

[28] Sk. Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
[29] Sk. Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679, 24. lpp., https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
[30] Ja sākotnējais juridiskais pamats ir piekrišana, skatīt Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en.
[31] Sk. VDAR 6. panta 1. punkta b) apakšpunktu.

akti, kas ļauj bankai iegūt informāciju tieši no valsts nodokļu iestādēm, ja datu subjekts tam iepriekš ir piekritis.

Tāpēc banka tiešsaistes lietojumprogrammu platformā sniedz informāciju par apstrādi veidā, kas datu subjektiem ļauj viegli saprast, kura apstrāde ir un kura nav obligāta. Apstrādes iespējas pēc noklusējuma neļauj izgūt datus tieši no citiem avotiem, izņemot pašu datu subjektu, un tiešas informācijas izgūšanas iespēja ir parādīta veidā, kas neliedz datu subjektam atturēties. Jebkura piekrišana, kas dota datu vākšanai tieši no citiem pārziņiem, nozīmē pagaidu piekļuves tiesības konkrētam informācijas kopumam.

Jebkura sniegtā piekrišana tiek apstrādāta elektroniski un dokumentējamā veidā, un datu subjektiem tiek parādīts vienkāršs veids, kā kontrolēt to, kam viņi ir devuši piekrišanu, un atsaukt piekrišanu.

Pārzinis ir iepriekš izvērtējis šīs IDADAN prasības un visus šos kritērijus iekļauj savā platformas iepirkuma konkursa prasību specifikācijā. Pārzinis apzinās, ka, ja iepirkumā neiekļauj IDADAN prasības, datu aizsardzības īstenošana pēc tam var būt novēlota vai ļoti dārga.

3.3 Godprātība

69. Godprātība ir visaptverošs princips, kas nosaka, ka persondati nedrīkst tikt apstrādāti veidā, kas nepamatoti kaitē, ir nelikumīgi diskriminējošs, neparedzams vai maldina datu subjektu. Ar pasākumiem un garantijām godprātības principa īstenošanai nodrošina arī datu subjektu tiesības un brīvības, jo īpaši tiesības uz informāciju (pārredzamību), tiesības iejaukties (piekļuvi, dzēšanu, datu pārnesamību, labošanu) un tiesības ierobežot apstrādi (tiesības netikt pakļautam automatizētai individuālu lēmumu pieņemšanai un datu subjektu nediskriminēšanu šādos procesos).

70. Godprātības galvenie integrācijas un noklusējuma elementi var būt šādi:
- autonomija — datu subjektiem būtu jāpiešķir visaugstākā iespējamā autonomija, lai noteiktu viņu persondatu izmantošanu, kā arī šīs izmantošanas vai apstrādes apmēru un nosacījumus;
- mijiedarbība — datu subjektiem jāspēj sazināties un īstenot savas tiesības attiecībā uz pārziņa apstrādātajiem persondatiem;
- gaidas — apstrādei būtu jāatbilst datu subjektu saprātīgām gaidām;
- nediskriminācija — pārzinis netaisnīgi nediskriminē datu subjektus;
- neizmantošana — pārzinis nedrīkstētu izmantot datu subjektu vajadzības vai ievainojamību;
- patērētāja izvēle — pārzinis nedrīkstētu netaisnīgi norobežot savus lietotājus. Ja pakalpojums, kas apstrādā persondatus, ir patentēts, tas var radīt pakalpojuma norobežošanu, kas var nebūt taisnīga, ja tā mazina datu subjektu iespēju izmantot savas tiesības uz datu pārnesamību saskaņā ar 20. pantu;
- varas līdzsvars — varas līdzsvaram vajadzētu būt vienam no galvenajiem pārziņa un datu subjekta attiecību mērķiem. Būtu jāizvairās no varas nelīdzsvarotības. Ja tas nav iespējams, tā jāatzīst un jāpārvalda, veicot atbilstošus pretpasākumus;
- riska nenodošana — pārziņi nedrīkstētu nodot uzņēmuma riskus datu subjektiem;
- nemaldināšana — datu apstrādes informācija un iespējas būtu jāsniedz objektīvā un neitrālā veidā, izvairoties no jebkādas maldinošas vai manipulatīvas valodas vai izstrādes;
- tiesību ievērošana — pārzinim ir jāievēro datu subjektu pamattiesības un jāīsteno atbilstoši pasākumi un garantijas, un tas nedrīkst iejaukties šajās tiesībās, ja vien tas nav skaidri pamatots ar likumu;
- ētika — pārzinim būtu jāsaprot apstrādes plašāka ietekme uz indivīdu tiesībām un cieņu;

- patiesums — pārzinim ir jādara pieejama informācija par to, kā tas apstrādā persondatus, tam ir jārīkojas tā, kā tas ir teicis, un tas nedrīkst maldināt datu subjektus;
- cilvēka iejaukšanās — pārzinim ir jāiekļauj tāda *kvalificēta* cilvēka iejaukšanās, kurš spēj atklāt mašīnas radītas noslieces saskaņā ar tiesībām netikt pakļautiem automatizētai individuālai lēmumu pieņemšanai atbilstoši 22. pantam[32];
- taisnīgi algoritmi — regulāri novērtē, vai algoritmi darbojas saskaņā ar mērķiem, un pielāgo algoritmus, lai mazinātu neatklātās noslieces un nodrošinātu apstrādes taisnīgumu. Datu subjekti būtu jāinformē par persondatu apstrādes norisi, pamatojoties uz algoritmiem, kas datus analizē vai prognozē, piemēram, par darba veiktspēju, ekonomisko situāciju, veselību, personīgām vēlmēm, uzticamību vai uzvedību, atrašanās vietu vai pārvietošanos[33].

1. piemērs

Pārzinis pārvalda meklētājprogrammu, ar ko apstrādā galvenokārt lietotāja ģenerētus persondatus. Pārzinis gūst labumu, saņemot lielu daudzumu persondatu, kas ļauj izmantot šos persondatus mērķtiecīgai reklāmai. Tādēļ pārzinis vēlas ietekmēt datu subjektus, lai varētu vākt un izmantot to persondatus plašākā mērogā. Piekrišana ir jāiegūst, piedāvājot datu subjektam apstrādes iespējas.

Īstenojot godprātības principu, ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūku, pārzinis apzinās, ka iespējas nevar tikt piedāvātas tādā veidā, kas datu subjektu mudinātu atļaut pārzinim vākt vairāk persondatu nekā tad, ja iespējas tiktu piedāvātas vienlīdzīgi un neitrāli. Tas nozīmē, ka pārzinis nevar apstrādes iespējas piedāvāt tādā veidā, kas apgrūtina datu subjektus atturēties no dalīšanās ar saviem datiem vai apgrūtina datu subjektiem to privātuma iestatījumu pielāgošanu un apstrādes ierobežošanu. Šie ir "tumšās" ietekmēšanas piemēri, kas ir pretrunā 25. panta garam. Apstrādes noklusējuma iespējas nedrīkstētu būt invazīvas, un turpmākās apstrādes izvēle būtu jāiesniedz tā, lai neliktu datu subjektam dot piekrišanu. Tāpēc pārzinis piedāvā iespējas dot piekrišanu vai atturēties kā divas vienlīdz redzamas izvēles, precīzi atspoguļojot katras izvēles sekas datu subjektam.

2. piemērs

Cits pārzinis apstrādā persondatus straumēšanas pakalpojuma sniegšanai, kur lietotāji var izvēlēties starp parasto standarta kvalitātes abonementu vai augstākas kvalitātes *premium* līmeņa abonementu. Kā daļu no *premium* abonementa abonenti saņem prioritāru klientu apkalpošanu.

Attiecībā uz godprātības principu prioritāra klientu apkalpošana, kas tiek sniegta *premium* līmeņa abonentiem, nedrīkst diskriminēt parasto abonentu piekļuvi to tiesību īstenošanai saskaņā ar VDAR 12. pantu. Tas nozīmē, ka, lai arī *premium* līmeņa abonenti saņem prioritāru apkalpošanu, šādu priekšrocību rezultātā nevar rasties attiecīgu pasākumu trūkums, lai atbildētu uz parasto abonentu pieprasījumiem bez nepamatotas kavēšanās un katrā ziņā viena mēneša laikā no pieprasījumu saņemšanas.

[32] Sk. Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826.
[33] Sk. VDAR 71. apsvērumu.

Prioritārie klienti var maksāt, lai saņemtu labāku apkalpošanu, taču visiem datu subjektiem ir jābūt vienlīdzīgai un nediskriminētai piekļuvei, lai īstenotu savas tiesības un brīvības, kā noteikts 12. pantā.

3.4 Nolūka ierobežojums[34]

71. Pārzinim ir jāvāc dati konkrētiem, skaidriem un likumīgiem nolūkiem, un tos nedrīkst turpmāk apstrādāt tādā veidā, kas nav saderīgs ar nolūkiem, kuriem tie tika savākti[35]. Tāpēc apstrāde būtu jāplāno, pamatojoties uz to, kas ir nepieciešams nolūku sasniegšanai. Ja ir jāveic jebkāda turpmāka apstrāde, pārzinim vispirms ir jāpārliecinās, vai šīs apstrādes nolūki ir saderīgi ar sākotnējiem nolūkiem, un attiecīgi jāplāno šāda apstrāde. To, vai jauns nolūks ir saderīgs, vērtē atbilstoši 6. panta 4. punkta kritērijiem.

72. Nolūka ierobežojuma galvenie integrācijas un noklusējuma elementi var būt šādi:
- iepriekšēja noteikšana — pirms apstrādes plānošanas nosaka likumīgos nolūkus;
- specifiskums — nolūkus precizē, skaidri norādot, kāpēc persondati tiek apstrādāti;
- nolūka orientācija — atkarībā no apstrādes nolūka būtu jāvirza apstrādes plānošana un jānosaka apstrādes robežas;
- nepieciešamība — pamatojoties uz nolūku, nosaka, kādi persondati ir nepieciešami apstrādei;
- saderīgums — jebkuram jaunam nolūkam jābūt saderīgam ar sākotnējo nolūku, kādam dati tika vākti, un, vadoties no tā, jānosaka attiecīgās plānošanas izmaiņas;
- turpmākas apstrādes ierobežošana — pārzinis nedrīkst savienot datu kopas vai veikt jebkādu turpmāku apstrādi jauniem nesaderīgiem nolūkiem;
- atkārtotas izmantošanas ierobežojumi — pārzinim būtu jāizmanto tehniski pasākumi, tostarp jaukšana un šifrēšana, lai ierobežotu persondatu atkārtotas izmantošanas iespēju citam nolūkam. Pārzinim vajadzētu būt arī organizatoriskiem pasākumiem, piemēram, politikai un līgumsaistībām, kas ierobežo persondatu atkalizmantošanu;
- pārskatīšana — pārzinim būtu regulāri jāpārskata, vai apstrāde ir nepieciešama nolūkiem, kādiem dati tika vākti, un jāpārbauda plānošana attiecībā uz nolūka ierobežojumu.

Piemērs

Pārzinis apstrādā savu klientu persondatus. Apstrādes mērķis ir izpildīt līgumsaistības, t. i., spēt piegādāt preces uz pareizo adresi un saņemt apmaksu. Saglabātie persondati ir pirkumu vēsture, vārds, adrese, e-pasta adrese un tālruņa numurs.

Pārzinis apsver iespēju iegādāties klientu attiecību pārvaldības (*CRM*) produktu, kas vienuviet apkopo visus datus par klientiem, piemēram, pārdošanu, tirgvedību un klientu apkalpošanu. Produkts dod iespēju glabāt visus tālruņa zvanus, darbības, dokumentus, e-pastus un tirgdarbības kampaņas, sniedzot pilnīgu priekšstatu par klientu. Turklāt *CRM* spēj automātiski analizēt klientu pirktspēju, izmantojot publisku informāciju. Analīzes mērķis ir labāk orientēt reklāmas darbības. Šīs darbības neietilpst sākotnējā likumīgajā apstrādes nolūkā.

[34] Nolūka ierobežojuma principa izpratnei saskaņā ar Direktīvu 95/46/EK norādījumus sniedza 29. panta darba grupa. Lai gan konkrēto atzinumu nav pieņēmusi EDAK, tas tik un tā var būt nozīmīgs, jo principa formulējums ir tāds pats kā VDAR. 29. panta darba grupa, "Atzinums 03/2013 par nolūka ierobežojumu", WP 203, 2013. gada 2. aprīlis, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[35] VDAR 5. panta 1. punkta b) apakšpunkts.

Lai nodrošinātu atbilstību nolūka ierobežojuma principam, pārzinis pieprasa produkta piegādātājam kartēt dažādās apstrādes darbības, izmantojot persondatus ar pārziņa vajadzībām atbilstošiem nolūkiem.

Pēc kartēšanas rezultātu saņemšanas pārzinis novērtē, vai jaunais tirgvedības nolūks un mērķtiecīgais reklāmas nolūks ir saderīgi ar sākotnējiem nolūkiem, kas noteikti, vācot datus, un vai attiecīgajai apstrādei ir pietiekams juridiskais pamats. Ja novērtējums nesniedz pozitīvu atbildi, pārzinis neizmanto attiecīgās funkcijas. Pārzinis var arī izvēlēties neveikt novērtējumu un vienkārši neizmantot aprakstītās produkta funkcijas.

3.5 Datu minimizēšana

73. Apstrādā tikai tos persondatus, kas ir adekvāti, atbilstīgi un ietver tikai to, kas **nepieciešams** to apstrādes nolūkam[36]. Tādējādi pārzinim ir iepriekš jānosaka, kuras apstrādes sistēmu funkcijas un parametri, kā arī to atbalsta funkcijas ir pieļaujamas. Ar datu minimizēšanu pamato un operacionalizē nepieciešamības principu. Turpmākajā apstrādē pārzinim būtu periodiski jāapsver, vai apstrādātie persondati joprojām ir adekvāti, atbilstīgi un nepieciešami, vai arī dati tiek dzēsti vai anonimizēti.

74. Pārzinim būtu vispirms ir jānosaka, vai persondatu apstrāde vispār ir vajadzīga attiecīgajiem nolūkiem. Pārzinim būtu jāpārbauda, vai attiecīgos nolūkus var sasniegt, apstrādājot mazāk persondatu, iegūstot mazāk detalizētus vai apkopotus persondatus vai vispār neapstrādājot persondatus[37]. Šādai pārbaudei būtu jānotiek pirms jebkādas apstrādes, bet to var veikt arī jebkurā apstrādes aprites cikla brīdī. Tas arī ir atbilstīgi 11. pantam.

75. Minimizēšana var attiekties arī uz identifikācijas pakāpi. Ja apstrādes nolūkam nav nepieciešams, lai galīgajā datu kopā būtu atsauce uz identificētu vai identificējamu personu (piemēram, statistikā), bet sākotnējai apstrādei tas ir nepieciešams (piemēram, pirms datu apkopošanas), pārzinis persondatus dzēš vai anonimizē, tiklīdz identifikācija vairs nav vajadzīga. Vai arī, ja citām apstrādes darbībām ir vajadzīga pastāvīga identifikācija, persondatus vajadzētu pseidonimizēt, lai mazinātu riskus datu subjektu tiesībām.

76. Datu minimizēšanas galvenie integrācijas un noklusējuma elementi var būt šādi:
    - Izvairīšanās no datiem — pilnīga izvairīšanās no persondatu apstrādes, ja tas ir iespējams attiecīgajam nolūkam;
    - ierobežojumi — vākto persondatu apjoma ierobežošana līdz nolūkam nepieciešamajam;
    - piekļuves ierobežošana — datu apstrādi veic tā, lai minimālam cilvēku skaitam būtu vajadzīga piekļuve persondatiem savu pienākumu veikšanai, un attiecīgi ierobežo piekļuvi;
    - atbilstība — persondatiem vajadzētu būt atbilstīgiem attiecīgajai apstrādei, un pārzinim būtu jāspēj to pierādīt;
    - nepieciešamība — katra persondatu kategorija ir nepieciešama noteiktajiem nolūkiem un būtu jāapstrādā tikai tad, ja nolūku nav iespējams sasniegt ar citiem līdzekļiem;
    - apkopošana — pēc iespējas apkopotu datu izmantošana;
    - pseidonimizācija — persondatus pseidonimizē, tiklīdz tieši identificējami persondati vairs nav nepieciešami, un identifikācijas atslēgu glabā atsevišķi;

[36] VDAR 5. panta 1. punkta c) apakšpunkts.
[37] VDAR 39. apsvērumā ir noteikts: "(..) Persondati būtu jāapstrādā tikai tad, ja apstrādes nolūku nav iespējams pienācīgi sasniegt citiem līdzekļiem."

- anonimizācija un dzēšana — ja persondati nav vai vairs nav nepieciešami konkrētajam nolūkam, persondatus anonimizē vai dzēš;
- datu plūsma — datu plūsmai vajadzētu būt pietiekami efektīvai, lai neveidotu vairāk kopiju, nekā nepieciešams;
- "tehnikas līmenis" — pārzinim būtu jāizmanto pieejamās un atbilstošās tehnoloģijas, lai izvairītos no datu apstrādes un minimizētu to.

1. piemērs

Grāmatu veikals vēlas palielināt savus ieņēmumus, pārdodot grāmatas tiešsaistē. Grāmatu veikala īpašnieks vēlas izveidot standartizētu veidlapu pasūtījumu veikšanai. Lai nodrošinātu, ka klienti aizpilda visu nepieciešamo informāciju, grāmatu veikala īpašnieks norāda, ka visi lauki veidlapā ir obligāti (neaizpildot visus laukus, klients nevar veikt pasūtījumu). Interneta veikala īpašnieks sākotnēji izmanto standarta saziņas veidlapu, kurā papildus citai informācijai jānorāda klienta dzimšanas datums, tālruņa numurs un mājas adrese. Tomēr ne visi veidlapas lauki ir obligāti nepieciešami grāmatu pirkšanai un piegādei. Šajā konkrētajā gadījumā, ja datu subjekts par produktu maksā iepriekš, datu subjekta dzimšanas datums un tālruņa numurs nav nepieciešami produkta iegādei. Tas nozīmē, ka tie nevar būt obligāti aizpildāmi lauki tīmekļa veidlapā, lai pasūtītu produktu, ja vien pārzinis nevar skaidri pierādīt, ka tas ir citādi nepieciešams un kāpēc lauki ir vajadzīgi. Turklāt ir situācijas, kad adrese nebūs nepieciešama. Piemēram, pasūtot e-grāmatu, klients var lejupielādēt produktu tieši savā ierīcē.

Tāpēc interneta veikala īpašnieks nolemj izveidot divas tīmekļa veidlapas — vienu grāmatu pasūtīšanai, iekļaujot lauku klienta adresei, un vienu tīmekļa veidlapu e-grāmatu pasūtīšanai, bez klienta adreses lauka.

2. piemērs

Sabiedriskā transporta uzņēmums vēlas apkopot statistikas informāciju par braucēju maršrutiem. Tas ir noderīgi, lai izdarītu pareizu izvēli attiecībā uz izmaiņām sabiedriskā transporta grafikos un vilcienu kustībā. Pasažieriem, katru reizi iekāpjot transportlīdzeklī vai izkāpjot no tā, ir jāreģistrē biļete lasītājā. Veicot riska novērtējumu saistībā ar pasažieru tiesībām un brīvībām attiecībā uz pasažieru braucienu maršrutu apkopošanu, pārzinis konstatē, ka pasažierus ir iespējams identificēt apstākļos, ja tie dzīvo vai strādā reti apdzīvotās teritorijās, pamatojoties uz atsevišķu maršrutu identifikāciju, ko nodrošina biļešu identifikators. Tādēļ, tā kā tas nav nepieciešams sabiedriskā transporta grafiku un vilcienu maršrutu optimizācijai, pārzinis nesaglabā biļešu identifikatoru. Pēc brauciena beigām pārzinis saglabā tikai atsevišķos brauciena maršrutus, lai nevarētu identificēt braucienus, kas piesaistīti vienai biļetei, bet tikai saglabā informāciju par atsevišķiem brauciena maršrutiem.

Gadījumos, kad joprojām pastāv risks identificēt personu tikai pēc viņas sabiedriskā transporta maršruta, pārzinis īsteno statistikas pasākumus, lai samazinātu risku, piemēram, izgriežot maršruta sākumu un beigas.

3. piemērs

Kurjera mērķis ir novērtēt piegādes efektivitāti attiecībā uz piegādes termiņiem, darba slodzes plānošanu un degvielas patēriņu. Lai sasniegtu šo mērķi, kurjeram ir jāapstrādā noteikts daudzums persondatu attiecībā gan uz darbiniekiem (autovadītājiem), gan klientiem (adreses, piegādājamās preces u. tml.). Šī apstrādes darbība ietver gan darbinieku uzraudzības risku, kam vajadzīgas īpašas tiesiskās garantijas, gan klientu ieradumu izsekošanas risku, kas rodas, apzinot piegādātās preces laika gaitā. Šos riskus var ievērojami mazināt ar darbinieku un klientu attiecīgu pseidonimizāciju. Jo īpaši, ja notiek bieža pseidonimizācijas atslēgu rotācija un detalizētu adrešu vietā tiek ņemti vērā makro apgabali, veic efektīvu datu minimizēšanu, un pārzinis var koncentrēties tikai uz piegādes procesu un resursu optimizācijas nolūku, nepārsniedzot indivīdu (klientu vai darbinieku) uzvedības uzraudzības robežu.

4. piemērs

Slimnīca vāc datus par saviem pacientiem slimnīcas informācijas sistēmā (elektroniskā veselības karte). Slimnīcas personālam ir jāpiekļūst pacientu lietām, lai varētu pieņemt lēmumus par pacientu aprūpi un ārstēšanu, kā arī dokumentēt visus veiktos diagnostikas, aprūpes un ārstēšanas pasākumus. Pēc noklusējuma piekļuve tiek piešķirta tikai tiem medicīnas darbiniekiem, kam ir uzdots ārstēt attiecīgo pacientu specialitātes nodaļā, kurā viņš ir norīkots. To personu grupu, kam ir piekļuve pacienta lietai, paplašina, ja ārstēšanā ir iesaistītas citas struktūrvienības vai diagnostikas vienības. Pēc pacienta izrakstīšanas un rēķinu sagatavošanas pabeigšanas piekļuve tiek ierobežota līdz nelielai tādu darbinieku grupai katrā specialitātes nodaļā, kuri atbild uz medicīniskās informācijas pieprasījumiem vai konsultāciju, ko veic vai pieprasa citi medicīnas pakalpojumu sniedzēji pēc attiecīgā pacienta atļaujas saņemšanas.

3.6 Precizitāte

77. Persondati ir precīzi un atjaunināti, un veic visus saprātīgos pasākumus, lai nodrošinātu, ka neprecīzi persondati, ņemot vērā nolūkus, kādos tie tiek apstrādāti, bez kavēšanās tiktu dzēsti vai laboti[38].

78. Šīs prasības būtu jāskata saistībā ar riskiem un sekām, ko rada konkrētais datu izmantojums. Neprecīzi persondati varētu būt risks datu subjektu tiesībām un brīvībām, piemēram, novedot pie kļūdainas diagnozes vai nepareizas veselības protokola apstrādes, vai nepareiza personas attēla rezultātā var tikt pieņemti nepareizi lēmumi gan manuāli, gan izmantojot automatizētu lēmumu pieņemšanu vai mākslīgo intelektu.

79. Precizitātes galvenie integrācijas un noklusējuma elementi var būt šādi:
- datu avots — datu avotiem vajadzētu būt uzticamiem datu precizitātes ziņā;
- precizitātes pakāpe — katram persondatu elementam vajadzētu būt tik precīzam, cik nepieciešams noteiktajiem nolūkiem;
- izmērāma precizitāte — samazina viltus pozitīvo/negatīvo rezultātu skaitu, piemēram, automatizēto lēmumu un mākslīgā intelekta neobjektivitāti;
- pārbaude — atkarībā no datu rakstura, attiecībā uz to, cik bieži tie var mainīties, pārzinim būtu jāpārbauda persondatu pareizība, sazinoties ar datu subjektu pirms apstrādes un dažādos apstrādes posmos (piemēram, ņemot vērā vecuma prasības);

[38] VDAR 5. panta 1. punkta d) apakšpunkts.

- dzēšana/labošana — pārzinis nekavējoties dzēš vai labo neprecīzus datus. Pārzinis to jo īpaši veicina gadījumos, kad datu subjekti ir vai bija bērni un vēlāk vēlas dzēst šādus persondatus[39];
- izvairīšanās no kļūdas izplatīšanās — pārzinim būtu jāsamazina uzkrātas kļūdas ietekme apstrādes ķēdē;
- piekļuve — būtu jāsniedz datu subjektiem informācija par persondatiem un efektīva piekļuve tiem saskaņā ar VDAR 12.–15. pantu, lai kontrolētu to precizitāti un vajadzības gadījumā tos labotu;
- nepārtraukta precizitāte — persondatiem vajadzētu būt precīziem visos apstrādes posmos, un kritiskos posmos būtu jāveic precizitātes testi;
- aktualitāte — ja nepieciešams konkrētajam nolūkam, persondatus atjaunina;
- datu struktūra — tehnoloģiskās un organizatoriskās struktūras iezīmju izmantošana, lai samazinātu neprecizitāti, piemēram, piedāvā kodolīgas, iepriekš noteiktas izvēles brīvā teksta lauku vietā.

1. piemērs

Apdrošināšanas sabiedrība vēlas izmantot mākslīgo intelektu (MI), lai raksturotu klientus, kas pērk apdrošināšanu, lai to izmantotu par pamatu lēmumu pieņemšanai, aprēķinot apdrošināšanas risku. Nosakot, kā būtu jāizstrādā tās MI risinājumi, tā nosaka apstrādes veidus, un, izvēloties MI lietojumprogrammu no piegādātāja un lemjot par to, kā apmācīt MI, ņem vērā integrētu datu aizsardzību.

Nosakot, kā apmācīt MI, pārzinim vajadzētu būt precīziem datiem, lai sasniegtu precīzus rezultātus. Tādēļ pārzinim būtu jāpārliecinās par MI apmācībā izmantoto datu precizitāti.

Ja ir juridisks pamats MI apmācībai, izmantojot persondatus no liela esošo klientu apakškopuma, pārzinis izvēlas klientu reprezentatīvu kopumu, arī lai izvairītos no novirzēm.

Tad klientu datus vāc no attiecīgās datu apstrādes sistēmas, tostarp datus par apdrošināšanas veidu, piemēram, veselības apdrošināšanu, mājokļa apdrošināšanu, ceļojumu apdrošināšanu utt., kā arī datus no publiskiem reģistriem, kuriem tiem ir likumīga piekļuve. Visi dati tiek pseidonimizēti pirms nosūtīšanas uz sistēmu, kas paredzēta MI modeļa apmācībai.

Lai nodrošinātu MI apmācībā izmantoto datu pēc iespējas lielāku precizitāti, pārzinis no datu avotiem vāc tikai datus, kas satur pareizu un aktualizētu informāciju.

Apdrošināšanas sabiedrība pārbauda, vai MI ir uzticams un sniedz nediskriminējošus rezultātus gan tā izstrādes laikā, gan, visbeidzot, pirms produkta izlaides. Kad MI ir pilnībā apmācīts un darbojas, apdrošināšanas sabiedrība izmanto rezultātus, lai atbalstītu apdrošināšanas riska novērtējumus, tomēr nepaļaujoties tikai uz MI, lai izlemtu, vai piešķirt apdrošināšanu, ja vien lēmums netiek pieņemts saskaņā ar VDAR 22. panta 2. punktā minētajiem izņēmumiem.

Apdrošināšanas sabiedrība arī regulāri pārskatīs MI radītos rezultātus, lai saglabātu uzticamību un vajadzības gadījumā pielāgotu algoritmu.

2. piemērs

[39] Sal. ar 65. apsvērumu.

Pārzinis ir veselības iestāde, kas vēlas atrast metodes, kā nodrošināt persondatu integritāti un precizitāti tās klientu datu reģistros.

Situācijās, kad divas personas vienlaikus ierodas iestādē un saņem vienādu ārstēšanu, pastāv risks viņas sajaukt, ja vienīgais parametrs, pēc kā tās atšķir, ir vārds. Lai nodrošinātu precizitāti, pārzinim ir vajadzīgs katras personas unikāls identifikators, līdz ar to vairāk informācijas nekā tikai klienta vārds.

Iestāde izmanto vairākas sistēmas, kas satur klientu persondatus, un tai ir jāpārliecinās, ka ar klientu saistītā informācija ir pareiza, precīza un konsekventa visās sistēmās jebkurā brīdī. Iestāde ir identificējusi vairākus riskus, kas var rasties, ja informācija tiek izmainīta vienā sistēmā, bet ne pārējās.

Pārzinis nolemj mazināt risku, pielietojot jaukšanas metodi, ko var izmantot, lai nodrošinātu datu integritāti ārstēšanas žurnālā. Reģistrācijas žurnālu ierakstiem un ar tiem saistītajam klientam tiek izveidoti nemaināmi kriptogrāfiski laika zīmogi, lai vajadzības gadījumā varētu atpazīt, korelēt un izsekot jebkādas izmaiņas.

3.7 Glabāšanas ierobežojums

80. Pārzinim ir jānodrošina persondatu glabāšana tādā formā, kas ļauj identificēt datu subjektus ne ilgāk, kā tas nepieciešams nolūkiem, kam persondati tiek apstrādāti[40].
Ir svarīgi, lai pārzinis precīzi zinātu, kādus persondatus uzņēmums apstrādā un kāpēc. Apstrādes nolūks ir galvenais kritērijs, lemjot, cik ilgi glabāt persondatus.

81. Pasākumi un garantijas, ar ko īsteno glabāšanas ierobežojuma principu, papildina datu subjektu tiesības un brīvības, jo īpaši tiesības uz dzēšanu un tiesības iebilst.

82. Glabāšanas ierobežojuma galvenie integrācijas un noklusējuma elementi var būt šādi:
- Dzēšana un anonimizācija — pārzinim vajadzētu būt skaidrām iekšējām procedūrām un funkcijām dzēšanai un/vai anonimizācijai;
- anonimizācijas/dzēšanas efektivitāte — pārzinis nodrošina, ka nav iespējams atkārtoti identificēt anonimizētus datus vai atgūt izdzēstos datus, kā arī viņam būtu jāpārbauda, vai tas ir iespējams;
- automatizācija — noteiktu persondatu dzēšanai vajadzētu būt automatizētai;
- glabāšanas kritēriji — pārzinis nosaka, kādi dati un glabāšanas ilgums ir nepieciešami konkrētajam nolūkam;
- pamatojums — pārzinis spēj pamatot, kāpēc glabāšanas ilgums ir nepieciešams konkrētajam nolūkam un persondatiem, un spēj atklāt glabāšanas perioda pamatojumu un juridisko pamatojumu;
- glabāšanas politikas izpilde — pārzinim būtu jāievieš iekšējā glabāšanas politika un jāpārbauda, vai organizācijā šī politika tiek ievērota;
- rezerves kopijas/žurnāli — pārzinis nosaka, kādi persondati un glabāšanas ilgums ir nepieciešami rezerves kopijām un žurnāliem;
- datu plūsma — pārziņiem būtu jāpārzina persondatu plūsma un to kopiju glabāšana un jācenšas ierobežot to "pagaidu" glabāšanu.

Piemērs

[40] VDAR 5. panta 1. punkta c) apakšpunkts.

Pārzinis vāc persondatus, kur apstrādes mērķis ir pārvaldīt datu subjekta dalību. Persondatus dzēš, kad dalība tiek izbeigta un nav juridiska pamata datu turpmākai glabāšanai.

Pārzinis vispirms izstrādā iekšēju datu saglabāšanas un dzēšanas procedūru. Saskaņā ar to darbinieki pēc glabāšanas perioda beigām manuāli dzēš persondatus. Darbinieks ievēro procedūru, regulāri izdzēšot un labojot datus visās ierīcēs, rezerves kopijās, žurnālos, e-pastos un citos attiecīgos datu nesējos.

Tad, lai dzēšana būtu efektīvāka un mazāk pakļauta kļūdām, pārzinis ievieš automatizētu sistēmu, lai datus dzēstu automātiski, uzticami un regulārāk. Sistēma ir konfigurēta tā, lai izpildītu norādīto datu dzēšanas procedūru, kas tiek veikta iepriekš noteiktos regulāros intervālos, lai noņemtu persondatus no visiem uzņēmuma datu nesējiem. Pārzinis regulāri pārskata un pārbauda glabāšanas procedūru un nodrošina, ka tā atbilst atjauninātajai saglabāšanas politikai.

3.8 Integritāte un konfidencialitāte

83. Integritātes un konfidencialitātes princips ietver aizsardzību pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskus vai organizatoriskus pasākumus. Persondatu drošībai ir vajadzīgi atbilstoši pasākumi, kas paredzēti, lai novērstu un pārvaldītu datu aizsardzības pārkāpumu incidentus, garantētu datu apstrādes uzdevumu pienācīgu izpildi un atbilstību pārējiem principiem un veicinātu indivīdu tiesību efektīvu īstenošanu.

84. Kā noteikts 78. apsvērumā, viens no IDADAN pasākumiem varētu ietvert iespēju pārzinim "*izveidot un uzlabot drošības pasākumus*". Papildus citiem IDADAN pasākumiem 78. apsvērumā ir ierosināts noteikt pārziņiem pienākumu pastāvīgi novērtēt, vai vienmēr izmantoti attiecīgie apstrādes līdzekļi, un novērtēt, vai izvēlētie pasākumi faktiski novērš esošo neaizsargātību. Turklāt pārziņiem būtu regulāri jāpārskata informācijas drošības pasākumi, kas aptver un aizsargā persondatus, kā arī procedūra datu aizsardzības pārkāpumu novēršanai.

85. Integritātes un konfidencialitātes galvenie integritātes un noklusējuma elementi var būt šādi:
    - informācijas drošības pārvaldības sistēma (IDPS) — pastāv operatīvs līdzeklis informācijas drošības politikas un procedūru pārvaldībai;
    - riska analīze — novērtē riskus persondatu drošībai, ņemot vērā ietekmi uz indivīdu tiesībām, un novērš konstatētos riskus. Izmantošanai riska novērtējumā izstrādā un uztur visaptverošu, sistemātisku un reālistisku "draudu modelēšanu" un izstrādātās programmatūras uzbrukumu tvēruma analīzi, lai samazinātu uzbrukuma vektorus un iespējas izmantot vājās vietas un neaizsargātību;
    - integrēta drošība — apsver drošības prasības pēc iespējas agrīnākā sistēmas projektēšanas un izstrādes posmā un pastāvīgi integrē un veic attiecīgus testus;
    - uzturēšana — regulāri pārskata un testē programmatūru, aparatūru, sistēmas un pakalpojumus, utt., lai atklātu apstrādes atbalsta sistēmu vājās vietas;
    - piekļuves kontroles pārvaldība — tikai pilnvarotajiem darbiniekiem, kuriem tas vajadzīgs, vajadzētu būt piekļuvei persondatiem, kas nepieciešami viņu apstrādes uzdevumu veikšanai, un pārzinim būtu jānošķir pilnvarotā personāla piekļuves tiesības;
        - piekļuves ierobežošana (aģenti) — datu apstrādi veic tā, lai minimālam cilvēku skaitam būtu vajadzīgs piekļūt persondatiem savu pienākumu veikšanai, un attiecīgi ierobežo piekļuvi;
        - piekļuves ierobežošana (saturs) — saistībā ar katru apstrādes darbību piekļuvi ierobežo tikai līdz tiem datu kopas atribūtiem, kas ir vajadzīgi konkrētās darbības

veikšanai. Turklāt ierobežo piekļuvi datiem, kas attiecas uz tiem datu subjektiem, kuri ir attiecīgā darbinieka kompetencē;
    - piekļuves nošķiršana — datu apstrādi veic tā, lai nevienai personai nebūtu vajadzīga visaptveroša piekļuve visiem datiem, kas savākti par datu subjektu, un vēl jo mazāk — visiem konkrētas datu subjektu kategorijas persondatiem;
- droša pārsūtīšana — datu pārsūtīšana ir aizsargāta pret nesankcionētu un nejaušu piekļuvi un izmaiņām;
- droša glabāšana — datu glabāšana ir aizsargāta pret nesankcionētu piekļuvi un izmaiņām. Vajadzētu būt procedūrām, lai novērtētu centralizētas vai decentralizētas glabāšanas risku un to, uz kādām persondatu kategorijām tas attiecas. Attiecībā uz dažiem datiem var būt vajadzīgi papildu drošības pasākumi salīdzinājumā ar citiem datiem vai nošķirtība no citiem datiem;
- pseidonimizācija — persondatiem un rezerves kopijām/žurnāliem būtu jāpiemēro pseidonimizācija kā drošības līdzeklis, lai mazinātu iespējamos datu aizsardzības pārkāpumu riskus, piemēram, izmantojot jaukšanu vai šifrēšanu;
- rezerves kopijas/žurnāli — uztur rezerves kopijas un žurnālus, ciktāl tas nepieciešams informācijas drošībai, izmanto revīzijas takas un notikumu uzraudzību parastas drošības kontroles veidā. Tos aizsargā pret nesankcionētu un nejaušu piekļuvi un izmaiņām un regulāri pārskata, un incidenti būtu nekavējoties jārisina;
- negadījumu seku novēršana / darbības nepārtrauktība — ievēro informācijas sistēmas negadījumu seku novēršanas un darbības nepārtrauktības prasības, lai atjaunotu persondatu pieejamību pēc būtiskiem incidentiem;
- aizsardzība atbilstoši riskam — visas persondatu kategorijas būtu jāaizsargā ar pasākumiem, kas ir atbilstīgi attiecībā pret drošības pārkāpuma risku. Ja iespējams, dati, kas rada īpašus riskus, būtu jāglabā atsevišķi no pārējiem persondatiem;
- reaģēšanas uz drošības incidentiem pārvaldība — pastāv kārtība, procedūras un resursi datu aizsardzības pārkāpumu atklāšanai, ierobežošanai, ziņošanai par tiem un mācības gūšanai;
- incidentu pārvaldība — pārzinim būtu jāievieš procedūras pārkāpumu un incidentu risināšanai, lai apstrādes sistēmu padarītu stabilāku. Tas ietver paziņošanas procedūras, piemēram, paziņošanas (uzraudzības iestādei) un informācijas (datu subjektiem) pārvaldību.

Piemērs

Pārzinis vēlas izgūt lielus persondatu apjomus no medicīnas datubāzes, kurā ir elektroniskas (pacientu) veselības kartes, un pārnest tos uz īpašu datubāzes serveri uzņēmumā, lai apstrādātu izgūtos datus kvalitātes nodrošināšanas nolūkos. Uzņēmums ir novērtējis, ka izgūto datu pārnešana uz serveri, kas ir pieejams visiem uzņēmuma darbiniekiem, varētu radīt augstu risku datu subjektu tiesībām un brīvībām. Tā kā uzņēmumā ir tikai viens departaments, kam jāapstrādā pacientu datu izraksti, pārzinis nolemj ierobežot piekļuvi šim nolūkam paredzētajam serverim, atļaujot to tikai šā departamenta darbiniekiem. Turklāt, lai vēl vairāk samazinātu risku, dati tiks pseidonimizēti pirms to pārnešanas.

Lai regulētu piekļuvi un mazinātu iespējamo kaitējumu no ļaunprogrammatūras, uzņēmums nolemj nodalīt tīklu un izveidot piekļuves vadību serverim. Turklāt tiek uzstādīta drošības uzraudzības un ielaušanās atklāšanas un novēršanas sistēma, ko nošķir no parastās lietošanas. Lai kontrolētu piekļuvi un izmaiņas, tiek ieviesta automatizēta revīzijas sistēma. Pēc tam, kad ir konfigurēti atsevišķi ar lietošanu saistīti notikumi, tiek ģenerēti pārskati un automatizēti brīdinājumi. Pārzinis nodrošinās, ka lietotājiem būs piekļuve tikai tad, kad tas būs vajadzīgs, un ar attiecīgo piekļuves līmeni. Neatbilstošu izmantošanu ir iespējams ātri un viegli atklāt.

Daži izraksti ir jāsalīdzina ar jauniem izrakstiem, tāpēc tie ir jāuzglabā trīs mēnešus. Pārzinis nolemj tos ievietot atsevišķās datubāzēs tajā pašā serverī un to saglabāšanai izmantot gan caurspīdīgu, gan

kolonnas līmeņa šifrēšanu. Kolonnas datu atšifrēšanas atslēgas glabā īpašos drošības moduļos, ko var izmantot tikai pilnvarots personāls, bet ne izgūt.

Nākotnes incidentu risināšana padara sistēmu stabilāku un uzticamāku. Datu pārzinis saprot, ka visos persondatu apstrādes pienākumos gan šobrīd, gan nākotnē ir jāiekļauj preventīvi un efektīvi pasākumi un garantijas un ka tas var palīdzēt nākotnē novērst šādus datu drošības pārkāpumu incidentus.

Pārzinis nosaka šos drošības pasākumus, gan lai nodrošinātu precizitāti, integritāti un konfidencialitāti, gan arī lai novērstu ļaunprogrammatūru izplatīšanos ar kiberuzbrukumiem un risinājumu padarītu stabilu. Noturīgi drošības pasākumi veicina datu subjektu uzticēšanos.

3.9 Pārskatatbildība[41]

86. Pārskatatbildības princips nosaka, ka pārzinis ir atbildīgs par visu iepriekš minēto principu ievērošanu un spēj to pierādīt.

87. Pārzinim jāspēj pierādīt atbilstību principiem. To darot, pārzinis var uzskatāmi parādīt, kāda ietekme ir pasākumiem, kas veikti, lai aizsargātu datu subjektu tiesības, un kāpēc šie pasākumi tiek uzskatīti par piemērotiem un efektīviem. Piemēram, pierāda, kāpēc pasākums ir piemērots, lai efektīvi nodrošinātu glabāšanas ierobežojuma principu.

88. Lai varētu atbildīgi apstrādāt persondatus, pārzinim vajadzētu būt gan zināšanām par datu aizsardzību, gan spējai to īstenot. Tas nozīmē, ka pārzinim būtu jāizprot savi VDAR noteiktie datu aizsardzības pienākumi un jāspēj tos izpildīt.

4 VDAR 25. PANTA 3. PUNKTS — SERTIFIKĀCIJA

89. Saskaņā ar 25. panta 3. punktu sertifikāciju atbilstoši 42. pantam var izmantot kā elementu, lai pierādītu atbilstību IDADAN. Turpretī dokumenti, kas apliecina atbilstību IDADAN, var būt noderīgi arī sertifikācijas procesā. Tas nozīmē, ka, ja pārziņa vai apstrādātāja veikta apstrādes darbība ir sertificēta saskaņā ar 42. pantu, uzraudzības iestādes to ņem vērā, novērtējot atbilstību VDAR, jo īpaši attiecībā uz IDADAN.

90. Ja pārziņa vai apstrādātāja veikta apstrādes darbība ir sertificēta saskaņā ar 42. pantu, elementi, kas palīdz pierādīt atbilstību 25. panta 1. un 2. punktam, ir izstrādes procesi, t. i., apstrādes līdzekļu noteikšanas process, pārvaldība un tehniskie un organizatoriskie pasākumi, lai īstenotu datu aizsardzības principus. Datu aizsardzības sertifikācijas kritērijus nosaka sertifikācijas struktūras vai sertifikācijas shēmu īpašnieki un pēc tam apstiprina kompetentā uzraudzības iestāde vai EDAK. Sīkāku informāciju par sertifikācijas mehānismiem skatīt EDAK Pamatnostādnēs par sertifikāciju[42] un citos attiecīgos norādījumos, kas publicēti EDAK tīmekļa vietnē.

91. Pat tad, ja apstrādes darbībai ir piešķirts sertifikāts saskaņā ar 42. pantu, pārzinim joprojām ir pienākums pastāvīgi uzraudzīt un uzlabot atbilstību 25. pantā noteiktajiem IDADAN kritērijiem.

[41] Sk. 74. apsvērumu, kurā noteikts, ka pārziņiem ir jāpierāda savu pasākumu efektivitāte.
[42] EDAK, "Pamatnostādnes Nr. 1/2018 par sertifikāciju un sertifikācijas kritēriju noteikšanu saskaņā ar Regulas 42. un 43. pantu", versija 3.0, 2019. gada 4. jūnijs, edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_lv.pdf.

5 25. PANTA IZPILDE UN SEKAS

92. Uzraudzības iestādes var novērtēt atbilstību 25. pantam saskaņā ar 58. pantā uzskaitītajām procedūrām. Korektīvās pilnvaras ir noteiktas 58. panta 2. punktā, un tās ietver brīdinājumus, rājienus, rīkojumus ievērot datu subjektu tiesības, apstrādes ierobežojumus vai aizliegumus, administratīvu naudas sodu piemērošanu u. tml.

93. IDADAN ir papildu faktors, ko ņem vērā, nosakot monetāro sankciju līmeni par VDAR pārkāpumiem; skatīt 83. panta 4. punktu[43] [44].

6 IETEIKUMI

94. Lai gan apstrādātāji un ražotāji nav tieši minēti 25. pantā, arī tie ir atzīti par IDADAN galvenajiem veicinātājiem, un tiem būtu jāapzinās, ka pārziņiem persondati ir jāapstrādā tikai sistēmās un tehnoloģijās, kurās ir integrēta datu aizsardzība.

95. Veicot apstrādi pārziņu vārdā vai nodrošinot risinājumus pārziņiem, apstrādātājiem un ražotājiem būtu jāizmanto savas zināšanas, lai veidotu uzticēšanos un ieteiktu saviem klientiem, tostarp MVU, tādus plānošanas/ieguves risinājumus, kuros datu aizsardzība ir integrēta apstrādē. Tas, savukārt, nozīmē, ka produktu un pakalpojumu izstrādē būtu jāveicina pārziņu vajadzības.

96. Īstenojot 25. pantu, būtu jāpatur prātā, ka galvenais izstrādes mērķis ir principu *efektīva īstenošana* un datu subjektu tiesību *aizsardzība* attiecīgajos apstrādes pasākumos. Lai atvieglotu un veicinātu IDADAN pieņemšanu, mēs sniedzam turpmāk izklāstītos ieteikumus pārziņiem, kā arī ražotājiem un apstrādātājiem.
    - Pārziņiem būtu jāapsver datu aizsardzība jau apstrādes darbību plānošanas *sākotnējos posmos*, pat pirms apstrādes līdzekļu noteikšanas.
    - Ja pārzinim ir datu aizsardzības speciālists (DAS), EDAK mudina DAS aktīvi iesaistīties, lai integrētu IDADAN iepirkuma un izstrādes procedūrās, kā arī visā apstrādes aprites ciklā.
    - Apstrādes darbību var *sertificēt*. Spēja iegūt apstrādes darbības sertificēšanu nodrošina pievienoto vērtību pārzinim, kad tas no ražotājiem vai apstrādātājiem izvēlas dažādu apstrādes programmatūru, aparatūru, pakalpojumus un/vai sistēmas. Tāpēc ražotājiem būtu jātiecas pierādīt IDADAN apstrādes risinājuma izstrādes dzīves ciklā. Sertifikācijas zīmogs var arī palīdzēt datu subjektiem izvēlēties starp dažādām precēm un pakalpojumiem. Spēja panākt, ka apstrāde tiek sertificēta, var radīt konkurences priekšrocības ražotājiem, apstrādātājiem un pārziņiem, un tā pat palielina datu subjektu uzticēšanos viņu persondatu apstrādei. Ja sertifikācija netiek piedāvāta, pārziņiem būtu jācenšas saņemt citas *garantijas,* ka ražotāji vai apstrādātāji ievēro IDADAN prasības.
    - Pārziņiem, apstrādātājiem un ražotājiem būtu jāņem vērā to pienākumi nodrošināt bērniem, kuri jaunāki par 18 gadiem, un citām neaizsargātām grupām īpašu aizsardzību, ievērojot IDADAN.

[43] VDAR 83. panta 2. punkta d) apakšpunktā noteikts, ka, lemjot, vai piemērot naudas sodu par VDAR pārkāpumu, *""pienācīgi" ņem vērā pārziņa vai apstrādātāja atbildības līmeni, ņemot vērā tehniskos un organizatoriskos pasākumus, ko tie īsteno saskaņā ar 25. un 32. pantu".*

[44] Plašākai informācijai par naudas sodiem skatīt 29. panta darba grupas "Pamatnostādnes administratīvo naudas sodu piemērošanai un noteikšanai Regulas 2016/679 nolūkiem", WP 253, 2017. gada 3. oktobris, ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 — apstiprinājusi EDAK.

- Ražotājiem un apstrādātājiem būtu jātiecas veicināt IDADAN īstenošanu, lai atbalstītu pārziņa spēju izpildīt 25. pantā noteiktos pienākumus. Savukārt pārziņiem nebūtu jāizvēlas ražotāji vai apstrādātāji, kuri nepiedāvā sistēmas, kas pārzinim sniedz iespēju vai atbalstu, lai nodrošinātu atbilstību 25. panta prasībām, jo pārziņiem būs jāuzņemas atbildība par to neīstenošanu.
- Ražotājiem un apstrādātājiem būtu aktīvi jāpiedalās, nodrošinot, ka tiek ievēroti "tehnikas līmeņa" kritēriji, un jāinformē pārziņi par jebkādām "tehnikas līmeņa" izmaiņām, kas var ietekmēt viņu ieviesto pasākumu efektivitāti. Pārziņiem šī prasība būtu jāiekļauj līguma nosacījumos, lai nodrošinātu, ka viņiem regulāri tiek sniegta jaunākā informācija.
- EDAK iesaka pārziņiem pieprasīt, lai ražotāji un apstrādātāji pierāda, kā viņu aparatūra, programmatūra, pakalpojumi vai sistēmas ļauj pārzinim izpildīt pārskatatbildības prasības saskaņā ar IDADAN, piemēram, izmantojot galvenos darbības rādītājus, lai pierādītu pasākumu un garantiju efektivitāti principu un tiesību īstenošanā.
- EDAK uzsver vajadzību īstenot saskaņotu pieeju principu un tiesību efektīvai īstenošanai un mudina asociācijas vai struktūras, kas gatavo rīcības kodeksus saskaņā ar 40. pantu, iekļaut arī konkrētās nozares IDADAN.
- Pārziņiem vajadzētu būt godprātīgiem attiecībā pret datu subjektiem un pārredzamiem attiecībā uz efektīvas IDADAN īstenošanas izvērtējumu un pierādīšanu tādā pašā veidā, kā pārziņi pierāda atbilstību VDAR prasībām saskaņā ar pārskatatbildības principu.
- Privātuma aizsardzības tehnoloģijas (*PET*), kas ir sasniegušas attiecīgā brīža maksimālo briedumu, var izmantot kā pasākumu saskaņā ar IDADAN prasībām, ja tas ir atbilstoši uz risku balstītā pieejā. *PET* pašas par sevi ne vienmēr ietver 25. pantā noteiktos pienākumus. Pārziņi novērtē, vai pasākums ir piemērots un efektīvs datu aizsardzības principu un datu subjektu tiesību īstenošanā.
- Uz esošajām mantotajām sistēmām attiecas tādi paši IDADAN pienākumi kā uz jaunām sistēmām. Ja mantotās sistēmas vēl neatbilst IDADAN un nav iespējams veikt izmaiņas, lai izpildītu pienākumus, tad mantotā sistēma vienkārši neatbilst VDAR noteiktajiem pienākumiem un to nevar izmantot persondatu apstrādei.
- 25. pants nepazemina prasību slieksni MVU. MVU atbilstību 25. pantam var veicināt šādi punkti:
    - veic agrīnus riska novērtējumus;
    - sāk ar nelielu apstrādi, pēc tam paplašina tās apmēru un sarežģītības pakāpi;
    - meklē IDADAN ražotāju un apstrādātāju garantijas, piemēram, sertifikāciju un rīcības kodeksu ievērošanu;
    - izmanto partnerus ar labiem līdzšinējiem rādītājiem;
    - runā ar datu aizsardzības iestādēm (DAI);
    - izlasa DAI un EDAK norādījumus;
    - ievēro rīcības kodeksus, ja tādi ir pieejami;
    - prasa profesionālu palīdzību un padomu.

Eiropas Datu aizsardzības kolēģijas vārdā —

priekšsēdētāja

(*Andrea Jelinek*)