DATU VALSTS INSPEKCIJA

Datu valsts inspekcijas rekomendācija „Personas datu definīcija”

Rīgā
2008.gadā

Saturs

Ievads

Datu valsts inspekcijas un Eiropas Savienības dalībvalstu prakse liecina, ka sabiedrībā pastāv zināma nenoteiktība un prakses dažādība attiecībā uz svarīgiem jēdziena „personas dati” aspektiem, kas var ietekmēt datu aizsardzības regulējuma atbilstošu piemērošanu dažādās jomās. Šīs rekomendācijas mērķis ir veicināt vienotu un atbilstošu jēdziena „personas dati” izpratni, vienlaikus veicinot personas datu aizsardzības noteikumu piemērošanu.

Šīs rekomendācijas mērķauditorija ir datu subjekti, pārziņi (datu apstrādātāji), personas datu operatori, datu aizsardzības speciālisti un auditori.

Rekomendācijai ir ieteikuma raksturs, tā nav saistoša trešajām personām un neierobežo pārziņu tiesības brīvi izvēlēties datu apstrādes veikšanai atbilstošās procedūras vai tehnoloģijas. Rekomendācija ir izstrādāta saskaņā ar Eiropas Parlamenta un Padomes 1995.gada 24.oktobra Direktīvas 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti 29.panta datu aizsardzības darba grupas apstiprinātajiem viedokļiem, kā arī ņemot vērā Datu valsts inspekcijas un Eiropas Savienības dalībvalstu personas datu uzraudzības iestāžu pieredzi.

I. Personas datu definīcija saskaņā ar Fizisko personu datu aizsardzības likumu

Fizisko personu datu aizsardzības likumā (turpmāk – FPDAL) ir dota šāda personas datu definīcija:

„Personas dati – jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu.”

Definīcijai ir četri pamatelementi, un katrs no tiem šajā rekomendācijā tiks apskatīts atsevišķi. Tie ir šādi:

1) „jebkāda informācija”;
2) „attiecas uz”;
3) „identificētu vai identificējamu”;
4) „fizisko personu”.

1. Pamatelements „jebkāda informācija”

Attiecībā uz informācijas veidu personas datu definīcija ietver jebkāda veida apgalvojumus par personu. Tas attiecas gan uz „objektīvo” informāciju, piemēram, personas asinīs atrodas konkrēta viela, gan arī uz „subjektīvo” informāciju, viedokļiem vai vērtējumiem, piemēram, banku nozarē (aizņēmēja uzticamības novērtēšanai – „Jānis ir uzticams aizņēmējs”) vai apdrošināšanā („Jānis, visticamāk, nemirs tuvākajā laikā”), vai darba attiecībās („Jānis ir labs darbinieks un ir pelnījis paaugstināšanu amatā”).

Lai informāciju uzskatītu par „personas datiem”, tai nav jābūt patiesai vai pierādītai. Datu aizsardzības noteikumi pieļauj iespēju, ka informācija ir nepareiza, un paredz datu subjektam tiesības piekļūt šai informācijai un to apstrīdēt likumā noteiktajā kārtībā.

Attiecībā uz informācijas saturu personas datu definīcija ietver datus, kas sniedz jebkāda satura informāciju. Līdz ar to personas dati ir ne tikai personas vārds, uzvārds, personas kods, bet arī cita informācija. Tāda noteikti ir personiskā informācija, kas saskaņā ar FPDAL 2.panta 8.punktu tiek uzskatīta par „sensitīviem personas datiem” tās specifiskās darbības dēļ. Taču personas datu definīcija attiecas arī uz citiem vispārīgākas informācijas veidiem. Personas datu definīcija ietver ne tikai informāciju, kas skar personas privāto un ģimenes dzīvi, bet arī informāciju par personas visu veidu citām darbībām, piemēram, saistībā ar darba attiecībām vai personas ekonomisko vai sociālo uzvedību. Tādējādi definīcija attiecas uz informāciju par personām, neņemot vērā šo personu amatu vai stāvokli (patērētājs, pacients, darbinieks, klients utt.).

Pirmkārt, ir jāņem vērā, ka privātās un ģimenes dzīves jēdziens, kā to ir apstiprinājusi Eiropas Cilvēktiesību tiesa, ir ļoti plašs. Otrkārt, personas datu aizsardzības noteikumi ir plašāki par jēdzienu „tiesības uz privātās un ģimenes dzīves aizsardzību”.

Attiecībā uz formu vai informācijas nesēju, kādā informāciju uzglabā, personas datu definīcija attiecas uz jebkādā formā pieejamu informāciju,

piemēram, burtu, ciparu, grafiku, fotogrāfiju vai audio veidā. Definīcija attiecas uz informāciju, kas uzglabāta papīra formā, tieši tāpat kā uz informāciju, kas uzglabāta elektroniski datora atmiņā binārā koda veidā vai, piemēram, ir fiksēta videoierakstā. Šāda pieeja loģiski izriet no automātiskās datu apstrādes iekļaušanas personas datu apstrādes definīcijā. No šī viedokļa skaņas un attēla dati jo īpaši ir uzskatāmi par personas datiem, jo tie sniedz informāciju par personu.

Lai informāciju varētu uzskatīt par personas datiem, tai nav jābūt iekļautai strukturētā datubāzē vai datnē. Tāda informācija, kas atrodas elektroniskā dokumentā brīva teksta formā, arī ir uzskatāma par personas datiem ar noteikumu, ka tā atbilst pārējiem personas datu definīcijas nosacījumiem. Piemēram, elektroniskajā pastā ir atrodami „personas dati”.

Piemērs. Audio saruna

Ja, izmantojot kāda uzņēmuma pakalpojumus, klienta balsi, kad viņš dod mutvārdu rīkojumu vai informācijas pieprasījumu, ieraksta lentē, šīs informācijas audio ieraksts ir jāuzskata par personas datiem.

Piemērs. Videonovērošana

Personu attēli, ko fiksē videonovērošanas sistēma, var būt personas dati tādā situācijā, ja šīs personas ir atpazīstamas. Ja ir slikta iegūtā attēla kvalitāte (slikta datu kvalitāte) un personas datu iegūšanas mērķis bijis identificēt personu, tad arī sliktas kvalitātes attēls ir personas dati.

Piemērs. Bērna zīmējums

Tiesas procesā par kādas meitenes aizbildnību tiek iesniegts viņas neiropsihiatriskā testa rezultātā tapis zīmējums, kurā atspoguļota viņas ģimene. Zīmējums sniedz informāciju par meitenes noskaņojumu un viņas jūtām pret dažādiem ģimenes locekļiem. Šādu zīmējumu var uzskatīt par „personas datiem”. Zīmējums atklās informāciju par pašu meiteni (viņas psiholoģiskās veselības stāvokli) un arī, piemēram, par viņas tēva vai mātes izturēšanos. Tādējādi vecāki šajā gadījumā var izmantot savas tiesības piekļūt šai īpašajai informācijai.

Biometriskie dati var būt dati par cilvēka bioloģiskajām īpašībām, psihisko raksturojumu, ieradumiem vai atkārtotu rīcību, ja šīs īpašības un/vai rīcība ir raksturīga konkrētajam indivīdam un ir izmērāma, neskatoties uz to, ka tehniskai izmērīšanai izmantojamie līdzekļi pieļauj zināmu neprecizitāti. Šādu biometrisko datu tipiski piemēri ir pirkstu nospiedumi, tīklenes raksts, sejas vaibsti, balss, arī rokas ģeometrija, vēnu raksti vai pat atsevišķas dziļi iesakņojušās prasmes vai citi rīcības paradumi (piemēram, paraksts, taustiņsitieni, īpašs gaitas vai runas veids u.tml.).

Biometrisko datu īpatnība ir tāda, ka tos var uzskatīt gan par informācijas saturu attiecībā uz konkrēto personu (šie ir Jāņa pirkstu nospiedumi), gan par elementu, kas veido saikni starp konkrētu informāciju un konkrētu personu (šo objektu ir aizskārusi persona ar šādiem pirkstu nospiedumiem, un šie pirkstu nospiedumi atbilst Jāņa pirkstu nospiedumiem, tādējādi Jānis ir aizskāris šo objektu). Šādā veidā dati var darboties kā „identifikatori”. Unikālās saistības ar konkrētu indivīdu dēļ biometriskos datus var izmantot, lai identificētu personu. Šāda divējāda būtība piemīt arī DNS datiem, kas sniedz informāciju par cilvēka ķermeni un ļauj skaidri un nepārprotami identificēt personu. Cilvēka audu paraugi (piemēram, asins paraugs) ir avoti, no kuriem iegūst biometriskos datus, bet paši par sevi tie nav biometriskie dati (piemēram, pirkstu nospiedumi ir biometriskie dati, bet pirksts pats par sevi nav). Tādējādi informācijas iegūšana no paraugiem ir personas datu vākšana, uz ko attiecas FPDAL noteikumi.

2. Pamatelements „attiecas uz”

Šim personas datu definīcijas elementam ir izšķiroša nozīme, jo tas ir ļoti svarīgs, lai precīzi noteiktu, kāda veida saistība/attiecības ar personu ir nozīmīgas un kā tās atšķirt. Vispārīgi var uzskatīt, ka informācija „attiecas uz” personu, ja tā ir par šo personu. Šāda veida saistību daudzās situācijās var konstatēt ļoti viegli. Piemēram, dati, kas atrodas personas darbavietā darbinieka lietā, attiecas uz personas kā darbinieka statusu. Personas medicīnisko pārbaužu rezultāti, kas atrodas tās medicīniskajā kartē, attiecas uz personas kā pacienta statusu. Tomēr var minēt vairākas citas situācijas, kurās ne vienmēr ir iespējams tik pašsaprotami kā iepriekšējos piemēros noteikt, ka informācija „attiecas uz” personu.

Atsevišķos gadījumos datu sniegtā informācija vispirms skar objektus, nevis personas. Šie objekti parasti kādam pieder, kāds tos ir īpašā veidā ietekmējis vai tie, savukārt, ietekmē kādu, vai tiem ir kāda fiziska vai ģeogrāfiska saistība ar personu vai citiem objektiem. Informācija tādējādi tikai netieši attiecas uz šo personu vai citiem objektiem.

Piemērs. Mājas vērtība

Konkrētas mājas vērtība ir informācija par objektu. Personas datu aizsardzības noteikumi neattieksies uz šo informāciju, ja to izmantos tikai tam, lai raksturotu nekustamā īpašuma cenu līmeni konkrētā teritorijā. Tomēr atsevišķos gadījumos šāda informācija ir jāuzskata par personas datiem, piemēram, ja māja ir personas īpašums un tās vērtību izmantos, lai noteiktu šīs personas pienākumu maksāt noteiktus nodokļus. No šāda viedokļa informācija noteikti ir uzskatāma par personas datiem.

Līdzīga pieeja ir jāizmanto situācijās, kad dati ir par procesiem vai notikumiem, piemēram, informācija par mehāniskas iekārtas darbību, ja tajā ir

nepieciešama cilvēka iejaukšanās. Noteiktos apstākļos šādu informāciju var uzskatīt arī par tādu, kas „attiecas uz” personu.

Piemērs. Automašīnas remonta apraksts

Automašīnas apkopes un remontu uzskaites sistēmā, ko izveido autoserviss, ir informācija par automašīnu, tās nobraukumu, apkopes pārbaužu datumiem, tehniskajām problēmām un faktisko stāvokli. Šī informācija ir saistīta ar automašīnas reģistrācijas numuru vai dzinēja numuru, kas savukārt var norādīt uz īpašnieku. Gadījumos, kad autoserviss, izrakstot rēķinu, konstatēs saistību starp transportlīdzekli un īpašnieku, informācija „attieksies uz” īpašnieku vai šoferi. Ja tiks izveidota saikne ar mehāniķi, kas laboja automašīnu, lai pārliecinātos par viņa darba rezultātiem, šī informācija „attieksies uz” mehāniķi.

Lai datus varētu uzskatīt par tādiem, kas attiecas uz personu, ņemot vērā iepriekš minētos piemērus un vispārinot tajos norādīto, jāsecina, ka ir nepieciešams konstatēt informācijas „satura”, „nolūka” vai „rezultāta” kritērija klātbūtni.

„Satura” kritērijs ir izpildīts gadījumos, kad atbilstoši sabiedrībā valdošajai, nepārprotamākajai vispārējai izpratnei par vārdiem „attiecas uz” informācija ir par konkrētu personu neatkarīgi no pārziņa vai kādas trešās personas mērķiem vai ietekmes, kāda šai informācijai ir uz datu subjektu. Informācija „attiecas uz” personu, kad tā ir „par” šo personu, un tas ir jānovērtē atbilstoši visiem ar šo lietu saistītajiem apstākļiem. Piemēram, medicīniskās izmeklēšanas rezultāti noteikti attiecas uz pacientu vai informācija, kas atrodas uzņēmumā ar konkrēta klienta vārdu, noteikti attiecas uz šo klientu. Informācija, kas atrodas radiofrekvences identifikācijas iekārtā (RFID) vai konkrēta indivīda identitāti apliecinoša dokumenta svītru kodā, attiecas uz šo personu.

Tomēr arī informācijas „nolūks” var norādīt, ka informācija „attiecas uz” konkrētu personu. „Nolūks” pastāv tad, ja, ņemot vērā visus konkrētās lietas apstākļus, datus izmanto vai tos ir iespējams izmantot ar mērķi novērtēt, īpaši attiekties pret personu vai ietekmēt to, tās statusu vai uzvedību.

Piemērs. Tālruņa sarunu izraksts

Tālruņa numuru reģistrs uzņēmumā sniedz informāciju par to, uz kādiem numuriem ir zvanīts no tālruņa, kas pieslēgts konkrētai līnijai. Šo informāciju iespējams saistīt ar dažādiem subjektiem. No vienas puses, līnija ir reģistrēta uz konkrēta uzņēmuma vārda un tam ir pienākums šos zvanus apmaksāt. No otras puses, tālruņa aparāts darba laikā atrodas konkrēta darbinieka rīcībā un zvanīšanu veic šis darbinieks. Numuru reģistrs var sniegt informāciju arī par personu, kam tika zvanīts. Tālruni var izmantot arī jebkura cita persona, kura var iekļūt telpās darbinieka prombūtnē (piemēram,

apkopēji). Informācija par konkrētā tālruņa aparāta izmantošanu atkarībā no tās mērķa var attiekties uz uzņēmumu, darbinieku, apkopēju (piemēram, lai pārbaudītu, cikos apkopēji atstāj darbavietu, jo viņiem pa tālruni ir jāapstiprina sava aiziešana pirms telpu aizslēgšanas). Jānorāda, ka personas datu definīcija aptver gan izejošos, gan ienākošos zvanus tādā veidā, ka tie visi sniedz informāciju par personas privāto dzīvi un sociālajām attiecībām.

Trešā veida saistība ar konkrētu personu rodas, kad konstatējams informācijas „rezultāta” kritērijs. Arī tad, ja informācijas saistību ar personu nenorāda ne tās „saturs”, ne „nolūks”, dati „attiecas uz” personu, jo, izmantojot šos datus, iespējams ietekmēt konkrētas personas tiesības un intereses, ņemot vērā visus ar konkrēto lietu saistītos apstākļus. Jānorāda, ka nav nepieciešams, lai iespējamais rezultāts būtu plaša mēroga ietekme. Pietiek ar to, ja šādu datu apstrādes rezultātā citas personas sāk citādi attiekties pret konkrēto personu.

Piemērs. Taksometru atrašanās vietas novērošana ar mērķi uzlabot pakalpojuma kvalitāti, kas iespaido šoferus

Taksometru pakalpojumu uzņēmums ievieš atrašanās vietas noteikšanas satelītu (GPS) sistēmu, ar kuras palīdzību iespējams noteikt brīvo taksometru atrašanās vietu reālā laikā. Datu apstrādes mērķis ir kvalitatīvāka pakalpojumu sniegšana un degvielas taupība, kas ir iespējama, ikreiz uzdodot pasažiera pārvadāšanu tam taksometram, kas atrodas vistuvāk klienta adresei. Patiesībā dati, kas nepieciešami šai sistēmai, attiecas uz automašīnām, nevis uz šoferiem. Apstrādes mērķis nav novērtēt taksometru šoferu darbu, piemēram, lai uzlabotu maršrutus. Tomēr sistēma ļauj novērot taksometru šoferu darbu un pārbaudīt, vai viņi ievēro ātruma ierobežojumu, izvēlas atbilstošus maršrutus, sēž pie stūres vai atpūšas ārpus automašīnas u.tml. Tādējādi šī informācija var ievērojami ietekmēt šīs personas, un tāpēc šie dati attiecas arī uz fiziskām personām. Uz šādu apstrādi attiecas personas datu aizsardzības noteikumi.

Šie trīs kritēriji (saturs, nolūks, rezultāts) ir alternatīvi, nevis kumulatīvi. Jo īpaši gadījumos, kad saikni ar personu norāda informācijas saturs, pārējo kritēriju klātbūtne nav nepieciešama, lai noteiktu, vai dati attiecas uz personu. No iepriekš minētā izriet secinājums, ka tā pati informācija vienlaikus var attiekties uz dažādām personām atkarībā no tā, kuru no kritērijiem attiecībā uz konkrēto personu var konstatēt. Viena un tā pati informācija var attiekties uz indivīdu Jāni tās „satura” dēļ (dati viennozīmīgi ir par Jāni), uz Pēteri, jo ir konstatējams „nolūks” (to izmantos, lai izturētos pret Pēteri konkrētā veidā), un uz Juri informācijas „rezultāta” dēļ (tā spēj ietekmēt Jura tiesības un intereses). Tādējādi secināms arī tas, ka datiem nav jābūt vērstiem uz personu, lai uzskatītu, ka dati uz to attiecas. Iepriekš apskatītie piemēri rāda, ka uz jautājumu, vai dati

attiecas uz konkrētu personu, var atbildēt, tikai atsevišķi izvērtējot katru kritēriju.

Fakts, ka informācija var attiekties uz dažādām personām, ir jāpatur prātā, arī piemērojot materiālās tiesību normas (piemēram, nosakot piekļuves tiesības).

Piemērs. Sapulces protokolā iekļautā informācija

Tas, kāpēc ir nepieciešams atsevišķi veikt katra iepriekš aprakstītā informācijas kritērija analīzi, ir sapulces protokolā iekļautā informācija, kurā, kā ierasts, konstatēta dalībnieku Jāņa, Pētera un Jura klātbūtne, ierakstīts Jāņa un Pētera teiktais un sniegts sapulces protokola autora Jura apkopotais sapulces norises apraksts. No personas datiem, kas attiecas uz Jāni, var konstatēt tikai to, ka viņš konkrētā laikā un vietā piedalījās sapulcē un izteica konkrētu viedokli. Pētera atrašanās sapulcē, viņa viedoklis un Jura sapulces norises atspoguļojums NAV personas dati, kas attiecas uz Jāni, pat neskatoties uz to, ka šī informācija ir iekļauta vienā un tajā pašā dokumentā, un pat tad, ja Jānis bija tas, kurš sāka jautājuma apspriešanu sapulcē. Tādējādi uz šo informāciju attiecas Jāņa tiesības piekļūt tikai viņa personas datiem. Vai un ciktāl šo informāciju var uzskatīt par Pētera un Jura personas datiem, ir jānosaka atsevišķi, izmantojot iepriekšminēto analīzes metodi.

3. Pamatelements „identificētu vai identificējamu” (fizisko personu)

FPDAL noteikts, ka informācijai ir jāattiecas uz fizisku personu, kura ir „identificēta vai identificējama”. Minētais nosacījums ir pamats turpmāk izklāstītajiem apsvērumiem. Vispārīgi fizisku personu var uzskatīt par „identificētu”, ja personu grupā tā ir atšķirama no visiem pārējiem grupas locekļiem. Tādējādi fiziska persona ir „identificējama”, ja to ir iespējams identificēt, kaut arī tas vēl nav izdarīts. Tādējādi praksē šī otrā alternatīva ir robežkritērijs, kas nosaka, vai informācija satur personas datu jēdziena trešo elementu.

Identifikāciju parasti nodrošina atsevišķi dati, kurus sauc par „identifikatoriem” un kuri ir īpaši priviliģētā un ciešā veidā saistīti ar konkrēto personu. Šādi dati ir, piemēram, personas ārējā izskata pazīmes, kā garums, matu krāsa, drēbes utt., vai arī personas raksturojums, kuru nevar uzreiz saskatīt, kā profesija, amats, vārds utt. Daļa šo „identifikatoru” ir minēti FPDAL 2.panta 8.punktā.

„Tieši” vai „netieši” identificējama

Personu tieši var identificēt ar tās vārda palīdzību, bet netieši ar tālruņa numura, automašīnas numura, sociālās apdrošināšanas numura, pases numura vai citu svarīgu pazīmju palīdzību, kas ļauj personu atpazīt, sašaurinot grupu, pie kuras tā pieder (vecums, nodarbošanās, dzīvesvieta utt.). Tādējādi nepieciešamo identifikatoru skaits, lai nodrošinātu identifikāciju, ir atkarīgs no konkrētās situācijas. Ļoti plaši izplatīts identifikators ir personas vārds vai uzvārds. Šāds

identifikators vienas konkrētas personas nošķiršanai no visiem pārējiem valsts iedzīvotājiem nebūs pietiekams, tomēr tas, iespējams, būs pietiekams, lai klasē identificētu skolēnu vai darbavietā darbinieku. Pat tāda nepilnīga informācija kā „vīrietis melnā uzvalkā” var būt pietiekama, lai identificētu kādu starp gājējiem, kas apstājušies krustojumā pie luksofora. Tātad atbilde uz jautājumu, vai persona, uz kuru attiecas informācija, ir identificēta vai nav, ir atkarīga no konkrētajiem apstākļiem.

Attiecībā uz „tieši” identificētām vai identificējamām personām vārds vai uzvārds patiešām ir viens no visierastākajiem identifikatoriem, un praksē ar „identificētas personas” jēdzienu parasti saprot atsauci uz personas vārdu. Tomēr, lai gūtu pārliecību par identitāti, personas vārds dažkārt ir jāapvieno ar citiem datiem (dzimšanas datums, adrese vai fotogrāfija, vecāku vārdi), lai novērstu iespēju sajaukt šo personu ar citu personu, kurai ir tāds pats vārds. Piemēram, informāciju, ka Jānim pieder konkrēta naudas summa, var uzskatīt par tādu, kas attiecas uz identificētu personu, jo tā ir saistīta ar personas vārdu. Personas vārds ir konkrēta informācijas sastāvdaļa, kas atklāj, ka persona lieto tieši šo burtu un skaņu kombināciju, lai atpazītu sevi un lai to atpazītu citas personas, ar kurām tā nodibina attiecības. Personas vārds var būt arī sākotnējā informācija, pēc kuras var noteikt, kur persona dzīvo vai kur to var atrast, tas var sniegt informāciju par ģimenes locekļiem (ar uzvārda palīdzību) un dažādām tiesiskām vai sociālām attiecībām, kas saistītas ar šo vārdu (izglītības dati, medicīniskie dati, bankas kontu dati). Pastāv iespēja arī uzzināt šīs personas izskatu, ja personas vārdam piesaista fotogrāfiju. Visas šīs ziņas saistībā ar personas vārdu ļauj atpazīt un noteikt konkrētu personu pēc tās izskata un citiem biometriskajiem datiem. Tādējādi ar identifikatoru palīdzību informācija tiek saistīta ar fizisku personu, kuru iespējams atšķirt no citām personām.

Attiecībā uz „netieši” identificētām vai identificējamām personām šī kategorija parasti nozīmē unikālu kombināciju, kas pēc apjoma var būt gan maza, gan liela. Gadījumos, kad pirmajā brīdī pieejamie identifikatori nav pietiekami, lai atpazītu vienu konkrētu personu, šī persona tik un tā var būt „identificējama”, jo, apvienojot esošo informāciju ar citiem datiem (neatkarīgi no tā, vai tie tiek glabāti pie pārziņa vai ne), personu būs iespējams atpazīt (viens vai vairāki šai personai raksturīgi fiziskās, fizioloģiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktori). Dažas pazīmes ir tik unikālas, ka identifikācija neprasa nekādas pūles („Latvijas pašreizējais prezidents”), taču arī plašākas datu kombinācijas (vecuma kategorija, izcelsmes reģions u.tml.) atsevišķos apstākļos var būt pietiekami noteiktas, jo īpaši tad, ja ir pieejama cita veida papildu informācija.

Piemērs. Fragmentāra informācija presē

Publicētā informācija skar senu kriminālllietu, kas agrāk piesaistīja plašu sabiedrības uzmanību. Pašreizējā publikācijā nav neviena no tradicionālajiem

identifikatoriem, nav nosaukts nevienas iesaistītās personas vārds vai dzimšanas datums. Tomēr iegūt papildu informāciju, kas ļautu noskaidrot galvenās iesaistītās personas, nešķiet grūti, piemēram, ielūkojoties attiecīgā laika perioda laikrakstos. Var pieņemt, ka ir visai ticama situācija, ka kāds varētu tā arī izdarīt (ielūkoties vecajās avīzēs) un iegūt piemērā minēto personu vārdus un citus identifikatorus. Ņemot vērā iepriekš minēto, piemērā minēto informāciju, šķiet, var pamatoti uzskatīt par „informāciju par identificējamām personām” un tādējādi par „personas datiem”.

Neskatoties uz to, ka identifikācija ar personas vārdu praksē ir visierastākā, ne visos gadījumos ir nepieciešams personas vārds, lai to identificētu. Tas iespējams, ja atpazīšanai ir izmantoti citi „identifikatori”. Personas datu datorizētas reģistrācijas procesā reģistrētajai personai parasti tiek piešķirts unikāls identifikators, lai novērstu divu datnē iekļauto personu sajaukšanas iespēju. Tāpat arī interneta datu plūsmas uzraudzības līdzekļi atvieglo iespēju identificēt konkrēta datora darbību un arī lietotāja uzvedību. Tādējādi no atsevišķiem fragmentiem tiek salikta indivīda personība, lai tālāk piedēvētu tai konkrētus lēmumus. Pat neinteresējoties par personas vārdu vai adresi, ir iespējams kategorizēt šo personu, pamatojoties uz sociālekonomiskiem, psiholoģiskiem, filozofiskiem vai citiem kritērijiem, un piedēvēt tai konkrētus lēmumus, jo personas kontaktpunkta (datora) dēļ tās identitātes atklāšana šī jēdziena sašaurinātā izpratnē vairs nav nepieciešama. Tātad spēja identificēt personu vairs ne vienmēr nozīmē spēju noskaidrot šīs personas vārdu.

Piemērs. Fragmentāra informācija par personu

Tas, ka mēs nezinām kādas personas vārdu un uzvārdu, nenozīmē, ka šī persona nav identificējama. Parasti lielākā daļa cilvēku pat nezina savu kaimiņu vārdus un uzvārdus, bet vienalga ir spējīgi tos identificēt. Personu var identificēt, piemēram, pēc šādām pazīmēm: garš, pavecs vīrietis, kurš dzīvo 10.dzīvoklī un brauc ar automašīnu *Mercedes*.

Identifikācijas līdzekļi

Lai noteiktu, vai persona ir identificējama, jāņem vērā visi līdzekļi, kurus, iespējams, pamatoti izmantotu vai nu pārzinis, vai jebkura cita persona, lai identificētu konkrētu personu. Tas nozīmē, ka tikai teorētiska iespējamība atpazīt konkrētu personu nav pietiekama, lai personu uzskatītu par „identificējamu”. Ja, ņemot vērā visus līdzekļus, kurus, iespējams, pamatoti izmantotu vai nu pārzinis, vai jebkura cita persona, šī iespējamība nepastāv vai ir niecīga, personu nevajadzētu uzskatīt par „identificējamu” un informācija nebūtu uzskatāma par „personas datiem”. Izmantojot minēto kritēriju – visi līdzekļi, kurus, iespējams, pamatoti izmantotu vai nu pārzinis, vai jebkura cita

persona –, īpaši būtu jāņem vērā visi ietekmējošie faktori. Identifikācijas izmaksas ir viens šāds faktors, bet ne vienīgais.

Nolūks, informācijas sakārtošanas veids, priekšrocības, ko pārzinis no tās sagaida, personu konkrētās intereses, kā arī organizatorisko nepilnību risks (piemēram, konfidencialitātes pienākuma pārkāpšana) un tehniskās kļūdas – visi šie faktori būtu jāņem vērā. Turklāt minētā personas datu apstrāde ir dinamiska, un tajā būtu jāņem vērā tehniskās iespējas ne tikai pašreizējai personas datu apstrādei, bet arī jāparedz iespējamā attīstība visā laika periodā, kurā personas dati tiks apstrādāti. Identifikācija šodien var nebūt iespējama ar līdzekļiem, ko šodien iespējams pamatoti izmantot. Ja datus ir paredzēts uzglabāt vienu mēnesi, nav sagaidāms, ka identifikācija kļūs iespējama informācijas „dzīves” laikā, un to nevajadzētu uzskatīt par personas datiem. Tomēr, ja datus paredzēts uzglabāt 10 gadus, pārzinim vajadzētu apsvērt, vai identifikācija nekļūs iespējama devītajā glabāšanas gadā, konkrētajā brīdī padarot datus par personas datiem. Sistēmai ir jāspēj pielāgoties šādām izmaiņām tad, kad tās notiek, un pienācīgi veikt atbilstošus tehniskos un organizatoriskos pasākumus.

Piemērs. Rentgena uzņēmumu un pacientu vārdu publicēšana

Zinātniskā žurnālā tika publicēts kādas personas rentgena uzņēmums kopā ar šīs personas vārdu, kas bija ļoti neparasts. Personas vārds apvienojumā ar radinieku vai paziņu zināšanām par to, ka šai personai ir bijusi konkrēta slimība, padara to identificējamu konkrētam personu lokam, un rentgena uzņēmums tādējādi ir jāuzskata par personas datiem.

Piemērs. Farmaceitiskās izpētes dati

Slimnīcas vai atsevišķi ārsti nodod savu pacientu medicīniskajās kartēs iekļautās ziņas uzņēmumam medicīnas pētījumu veikšanai. Pacientu vārdi netiek izmantoti, katrai klīniskajai lietai pēc nejaušības principa tiek piešķirts kārtas numurs, kas palīdz nodrošināt skaidrību un izvairīties no informācijas par dažādiem pacientiem sajaukšanas. Pacientu vārdi ir pieejami tikai un vienīgi ārstiem, kurus saista profesionālā noslēpuma glabāšanas pienākums. Datos nav iekļauta nekāda cita papildinformācija, kuru apvienojot būtu iespējama pacientu identifikācija. Turklāt ir veikti visi pārējie tiesiskie, tehniskie un organizatoriskie pasākumi, lai novērstu datu subjektu identifikāciju. Šajos apstākļos var uzskatīt, ka farmaceitiskā uzņēmuma veiktajā apstrādē nav atrodami līdzekļi, kurus būtu iespējams pamatoti izmantot datu subjekta identifikācijai.

Vēl viens nozīmīgs faktors, lai novērtētu „visus līdzekļus, kurus, iespējams, pamatoti izmantotu” personu identificēšanai, kā jau iepriekš minēts, noteikti ir pārziņa nolūks, veicot datu apstrādi. Praksē var saskarties ar lietām, kurās, no vienas puses, pārzinis apgalvo, ka tā rīcībā ir tikai atsevišķi

informācijas fragmenti, kas nav saistīti ar personas vārdu vai jebkādu citu tiešo identifikatoru, tādējādi uzstājot, ka dati nav uzskatāmi par personas datiem un uz tiem neattiecas datu aizsardzības noteikumi, bet, no otras puses, šādas informācijas apstrādei ir jēga tikai tad, ja tā ļauj identificēt atsevišķas personas. Šādos gadījumos, kad apstrādes nolūks netieši norāda uz personu identifikāciju, var pieņemt, ka pārzinim vai jebkurai citai iesaistītajai personai ir vai būs līdzekļi, „kurus iespējams pamatoti izmantot”, lai identificētu datu subjektu. Patiesībā apgalvojums, ka personas nav identificējamas, ja apstrādes nolūks ir tieši to identifikācija, ir klaji pretrunīgs. Šādā gadījumā informācija ir uzskatāma par tādu, kas attiecas uz identificējamām personām, un šādai datu apstrādei ir piemērojami datu aizsardzības noteikumi.

Piemērs. Videonovērošana

Veicot videonovērošanu, pārziņi bieži vien apgalvo, ka identifikācija varētu notikt procentuāli ļoti nelielā savāktā materiāla daļā, un tādējādi, pirms šajos retajos gadījumos identifikācija patiešām nav notikusi, tā nav personas datu apstrāde. Tā kā viens no videonovērošanas mērķiem ir identificēt personas, kas ir redzamas videoierakstā, visos gadījumos, kad pārzinis uzskata šādu identifikāciju par nepieciešamu, viss videonovērošanas process ir uzskatāms par datu apstrādi attiecībā uz identificējamajām personām pat tad, ja dažas nofilmētās personas gandrīz nav identificējamas.

Piemērs. IP (intertīkla protokols) adreses

IP adreses ir jāuzskata par datiem, kas attiecas uz identificējamu personu. Elektronisko sakaru pakalpojumu sniedzēji (interneta nodrošinātāji), izmantojot saprātīgus līdzekļus, identificē interneta lietotājus, kuriem tie ir piešķīruši IP adreses, regulāri „reģistrējot” atsevišķā datnē interneta lietotājam piešķirtās dinamiskās IP adreses piešķiršanas datumu, laiku un termiņu, cik ilgi tā lietota. Tāpat rīkojas elektronisko sakaru pakalpojumu sniedzēji, kas uztur reģistra žurnālu interneta serverī. Nav šaubu, ka šajos gadījumos ir jārunā par personas datiem FPDAL 2.panta 3.punkta nozīmē. Īpaši tajos gadījumos, kad IP adreses apstrāde tiek veikta ar nolūku identificēt datoru lietotājus (piemēram, autortiesību īpašnieki, kuru mērķis ir saukt pie atbildības datoru lietotājus par intelektuālā īpašuma tiesību pārkāpumiem), pārzinis jau laikus parāda, ka „līdzekļi, ko iespējams pamatoti izmantot”, lai identificētu personu, būs pieejami, piemēram, tiesai, kurā tiks iesniegta prasība (citādi informācijas vākšanai nebūtu jēgas), un tādējādi šī informācija ir uzskatāma par personas datiem.

Īpašs gadījums ir atsevišķs IP adrešu veids, kas konkrētos apstākļos patiešām neļauj identificēt lietotāju dažādu tehnisku vai organizatorisku iemeslu dēļ. Viens šāds piemērs ir IP adreses, kas piešķirtas datoriem interneta kafejnīcā, kurā nenotiek klientu identifikācija. Var apgalvot, ka par datora X

lietošanu konkrētā laika periodā ievāktie dati neļauj ar saprātīgiem līdzekļiem identificēt lietotāju, un tādējādi tie nav personas dati. Tomēr ir jānorāda, ka interneta pakalpojumu sniedzēji, visdrīzāk, nezina, vai konkrētā IP adrese ir tāda, kas pieļauj identifikāciju vai ne, un tie apstrādās ar šo IP adresi saistītos datus tieši tāpat kā datus, kas saistīti ar pilnībā reģistrētiem un identificējamiem lietotājiem. Tātad, ja vien interneta pakalpojumu sniedzējs nav spējīgs konkrēti noteikt, ka dati attiecas uz lietotājiem, kas nav identificējami, lai nepārkāptu noteikumus, tam visa IP informācija ir jāapstrādā kā personas dati.

Piemērs. Elektroniskā pasta adrese

Par personas datiem ir uzskatāmas tādas elektroniskā pasta adreses, kurās ietverts personas vārds un uzvārds – *vards.uzvards@domenavards.lv*. Šāda elektroniskā pasta adrese norāda uz vārdu, uzvārdu un šīs personas piederību iestādei vai uzņēmumam u.tml. Savukārt elektroniskā pasta adrese *vards_u@inbox.lv* ir uzskatāma par tādu, kas neietver personas datus, jo pēc tās nevar tieši identificēt personu.

Ja datu subjekta identifikācija nav datu apstrādes mērķis, nozīmīgi ir tehniskie pasākumi identifikācijas novēršanai. Attīstībai atbilstošu tehnisko un organizatorisko pasākumu izmantošana datu aizsardzībai pret identifikāciju ir nozīmīga, kad jānovērtē, vai personas nav identificējamas, ņemot vērā visus līdzekļus, kurus, iespējams, pamatoti izmantotu vai nu pārzinis, vai jebkura cita persona, lai identificētu personas.

Pseidonimizēti dati

Pseidonimizācija ir identitātes maskēšanas process. Šāda procesa mērķis ir iespēja vākt papildu datus, kas attiecas uz to pašu personu, nezinot tās identitāti. Īpaši svarīgi tas ir izpētes un statistikas jomā. Pseidonimizāciju var veikt izsekojamā veidā, lietojot sarakstus ar identitātēm atbilstošajiem pseidonīmiem vai izmantojot pseidonimizācijai divvirzienu kriptogrāfijas algoritmus. Identitātes maskēšanu var veikt arī tādā veidā, ka identitātes noskaidrošana vairs nav iespējama, piemēram, ar vienvirziena kriptogrāfiju, kuras rezultātā iegūst pilnībā anonīmus datus.

Pseidonimizācijas procesa efektivitāte ir atkarīga no vairākiem faktoriem (kurā datu apstrādes procesa stadijā to pielieto, cik tā ir droša pret atpakaļ izsekojamību, cik liela ir datu kopa, kurā personas dati ir pseidonimizēti, kāda ir iespēja sasaistīt individuālus ierakstus ar to pašu personu u.tml.). Pseidonīmiem būtu jābūt nejauši izvēlētiem un iepriekš nenosakāmiem. Iespējamo pseidonīmu skaitam ir jābūt tik lielam, lai to pašu pseidonīmu divas reizes nekad nevarētu izvēlēties. Ja ir nepieciešams augsts drošības līmenis, iespējamo pseidonīmu

skaitam ir jābūt vismaz vienādam ar drošas kriptogrāfiskās jaucējfunkcijas vērtību skaitu.

Izsekojami pseidonimizēti dati ir uzskatāmi par informāciju, kas attiecas uz netieši identificējamām personām. Patiesībā pseidonīma izmantošana nozīmē, ka pastāv iespēja nonākt atpakaļ pie personas un personas identitāti var atklāt, taču tikai jau iepriekš konkretizētos apstākļos. Šādā gadījumā, kaut arī datu aizsardzības noteikumi ir piemērojami, attiecībā uz šādas netieši identificējamas informācijas apstrādi konkrētai personai risks lielākoties būs zems, un tādējādi ir attaisnojama šo noteikumu elastīgāka piemērošana nekā tad, ja tiek apstrādāta informācija par tieši identificējamām personām.

Kodēti dati

Kodēti dati ir klasisks pseidonimizācijas piemērs. Informācija attiecas uz personu, kura ir aizstāta ar kodu, bet koda atslēga, kas ļauj sasaistīt kodu ar parastajiem personas identifikatoriem (piemēram, ar personas vārdu, dzimšanas datumu, adresi u.tml.), tiek glabāta atsevišķi.

Šāda veida datus plaši izmanto medikamentu klīniskajā izpētē. Eiropas Padomes un Parlamenta 2001.gada 4.aprīļa Direktīva 2001/20 par dalībvalstu normatīvo un administratīvo aktu tuvināšanu attiecībā uz labas klīniskās prakses ieviešanu klīniskās izpētes veikšanā ar cilvēkiem paredzētām zālēm nosaka šādu pasākumu tiesisko regulējumu. Medicīnas darbinieks/izpētes veicējs (pētnieks), testējot medikamentus, vāc informāciju par klīniskajiem rezultātiem attiecībā uz katru pacientu, aizstājot pacienta personas datus ar kodu. Izpētes veicējs sniedz informāciju farmācijas uzņēmumam vai citām iesaistītajām personām (sponsoriem) tikai kodētā veidā, jo tos interesē tikai biostatistikas informācija. Tomēr pats pētnieks atsevišķi glabā koda atslēgu, ar kuru iespējams saistīt kodu ar parasto informāciju, kas ļauj atsevišķi identificēt pacientus. Pētniekam ir jāglabā šī koda atslēga pacientu veselības aizsargāšanai, lai gadījumā, ja medikamenti izrādās bīstami un rodas nepieciešamība, individuālus pacientus būtu iespējams identificēt un sniegt tiem atbilstošu medicīnisko aprūpi.

Šeit rodas jautājums, vai klīniskajā izpētē izmantotie dati ir uzskatāmi par tādiem, kas attiecas uz „identificējamu” fizisku personu, un vai uz tiem attiecas datu aizsardzības noteikumi. Ņemot vērā iepriekš aprakstīto analīzi, lai noteiktu, vai persona ir identificējama, būtu jāņem vērā visi līdzekļi, kurus, iespējams, pamatoti izmantotu vai nu pārzinis, vai jebkura cita persona, lai identificētu minēto personu. Šajā gadījumā personu identifikācija (lai nepieciešamības gadījumā sniegtu atbilstošu medicīnisko aprūpi) ir viens no kodēto datu apstrādes mērķiem.

Farmācijas uzņēmums ir izstrādājis apstrādes līdzekļus un noteicis organizatoriskos pasākumus un savas attiecības ar izpētes veicēju, kuram ir pieejamas kodu atslēgas, tādā veidā, ka personu identifikācija dažkārt ne tikai var notikt, bet konkrētos apstākļos tā ir obligāti jāveic. Pacientu identifikācija

tādējādi ir iekļauta apstrādes mērķos un apstrādes līdzekļos. Šajā gadījumā var secināt, ka šādi kodēti dati ir informācija par identificējamu fizisku personu attiecībā uz visiem, kas varētu būt iesaistīti identifikācijā, un uz šiem datiem attiecas personas datu aizsardzības tiesiskā regulējuma noteikumi. Tomēr tas nenozīmē, ka visi pārējie pārziņi, kas apstrādā tādus pašus kodētus datus, arī apstrādā tieši personas datus, jo īpaši, ja konkrētajā shēmā, kuras ietvaros darbojas šie citi pārziņi, atpazīšana ir pilnīgi izslēgta un šajā sakarā ir veikti atbilstoši tehniskie pasākumi.

Citās izpētes jomās vai projektos datu subjekta atpazīšanu iespējams nepieļaut ar speciālu dokumentu un procedūru formulējumu palīdzību, piemēram, neiekļaujot terapeitiskos aspektus. Tehnisku vai citu iemeslu dēļ, iespējams, pastāv līdzekļi, ar kuriem var noskaidrot, uz kuru personu attiecas konkrētie klīniskie dati, tomēr identifikācijai nebūtu jānotiek vai arī tiek paredzēts, ka tā nenotiks nekādos apstākļos, turklāt ir veikti atbilstoši tehniskie pasākumi (piemēram, kriptogrāfija, neatjaunojama skaitļu jaukšana), lai identifikāciju novērstu. Šādā gadījumā, kaut arī tiek veikti attiecīgi drošības pasākumi, atsevišķu datu subjektu identifikācija var notikt iepriekš neparedzamu apstākļu dēļ, piemēram, nejaušas datu subjekta īpašību sakritības dēļ, kas atklāj tā identitāti. Informāciju, ko apstrādā pārzinis, nevar uzskatīt par tādu, kas attiecas uz identificētu vai identificējamu personu, ņemot vērā visus līdzekļus, kurus, iespējams, pamatoti izmantotu vai nu pārzinis, vai jebkura cita persona. Šo datu apstrādei FPDAL noteikumi nav piemērojami. Savukārt pārzinim, kurš apstrādā no cita pārziņa iegūtus personas datus un ir ieguvis pieeju identificējamajai informācijai, tā bez šaubām ir jāuzskata par „personas datiem”.

Anonīmi dati

„Anonīmus datus” FPDAL izpratnē var definēt kā jebkuru informāciju, kas attiecas uz fizisku personu, ja šo personu nevar identificēt ne pārzinis, ne arī kāda cita persona, ņemot vērā visus līdzekļus, kurus, iespējams, pamatoti izmantotu vai nu pārzinis, vai jebkura cita persona, lai identificētu konkrēto personu. „Anonimizēti dati” tādējādi ir anonīmi dati, kas iepriekš attiecās uz identificējamu personu, taču tagad to identifikācija vairs nav iespējama. FPDAL normas nepiemēro anonīmi iesniegtiem datiem, ja datu subjekts vairs nav identificējams. Tomēr novērtējums, vai dati pieļauj indivīda identifikāciju un vai informāciju var uzskatīt par anonīmu, ir atkarīgs no konkrētās lietas apstākļiem. Tādējādi katrs gadījums ir jāanalizē atsevišķi, īpaši ņemot vērā apjomu, kādā, iespējams, pamatoti tiktu izmantoti identifikācijas līdzekļi. Īpaši svarīgi tas ir attiecībā uz statistiku, jo, neskatoties uz faktu, ka informāciju var sniegt kā datu apkopojumu, sākotnējo datu apjoms var būt nepietiekami plašs un savienojumā ar citiem datiem personu identifikācija var kļūt iespējama.

Piemērs. Statistikas aptaujas un atsevišķu datu apvienojumi

Papildus vispārīgajam pienākumam ievērot personas datu aizsardzības noteikumus, lai nodrošinātu statistikas aptauju anonimitāti, statistiķiem ir īpašs profesionālā noslēpuma glabāšanas pienākums, un saskaņā ar šiem abiem pienākumiem datu, kas nav anonīmi, publiskošana ir aizliegta. Tas uzliek pienākumu publicēt apkopotus statistikas datus, kurus nevar sasaistīt ar identificētu personu, kas piedalījusies aptaujā. Šis noteikums ir īpaši svarīgs attiecībā uz tautas skaitīšanas datu publicēšanu. Katrā situācijā ir jānosaka robeža, kad konkrētas personas identifikāciju var uzskatīt par iespējamu. Ja kāds kritērijs šķietami pieļauj identifikāciju konkrētā personu kategorijā neatkarīgi no tās lieluma (piemēram, pilsētā, kurā ir 6000 iedzīvotāju, strādā tikai viens ārsts), šis atšķirīgais kritērijs ir jāizslēdz vai arī ir jāpievieno citi dati, kas mazina iespēju iegūstamo informāciju saistīt ar konkrētu personu un ļauj saglabāt statistikas noslēpumu.

Piemērs. Videonovērošanas datu publicēšana

Televīzijā rāda aizturēto zagļu fotogrāfijas vai videoierakstus, kuros zagļu sejas tiek aizklātas. Tomēr, neskatoties uz šo rīcību, vēl joprojām pastāv iespēja, ka fotogrāfijās redzamo personu draugi, radinieki vai kaimiņi varētu tās atpazīt, piemēram, pēc auguma, matu sakārtojuma un drēbēm.

4. Pamatelements „fiziska persona”

FPDAL paredzētā aizsardzība attiecas uz fiziskām personām, tas nozīmē – uz cilvēkiem. Tiesības uz personas datu aizsardzību tādējādi ir universālas, tās nav ierobežoti attiecināmas tikai uz personām, kas ir kādas konkrētas valsts pilsoņi vai iedzīvotāji.

Saskaņā ar Vispārējās cilvēktiesību deklarācijas 6.pantu „katram cilvēkam, lai kur viņš atrastos, ir tiesības uz viņa tiesībsubjektības atzīšanu”. Fizisku personu raksturo spēja būt par tiesisko attiecību subjektu, kas sākas ar cilvēka piedzimšanu un beidzas ar viņa nāvi. Tādējādi personas dati ir dati, kas attiecas uz identificētu vai identificējamu dzīvu cilvēku.

Mirušu personu dati

Informāciju attiecībā uz mirušām personām principā neuzskata par personas datiem, un FPDAL noteikumi uz to neattiecas, jo saskaņā ar civiltiesībām mirušie nav fiziskas personas. Tomēr atsevišķos gadījumos mirušā dati var būt netieši aizsargājami.

Pārzinis var nebūt spējīgs noteikt, vai persona, uz kuru dati attiecas, vēl joprojām ir dzīva vai, iespējams, jau mirusi. Taču arī tad, ja pārzinis to spēj, informāciju par mirušām personām, iespējams, apstrādā saskaņā ar tiem pašiem noteikumiem kā informāciju par dzīvām personām, to nenodalot. Tā kā pārzinim ir jāievēro FPDAL paredzētie personas datu aizsardzības noteikumi attiecībā uz

dzīvām personām, visticamāk, no prakses viedokļa būs vieglāk arī datus par mirušām personām apstrādāt tādā pašā veidā, nekā tos dalīt divās daļās.

Informācija par mirušām personām var attiekties arī uz dzīvām personām. Piemēram, informācija par to, ka mirusī Anna slimoja ar hemofiliju, norāda, ka viņas dēls Jānis arī slimo ar šo pašu slimību, jo tā ir saistīta ar gēnu, kas atrodas X hromosomā. Tādējādi gadījumos, kad var uzskatīt, ka informācija par mirušām personām vienlaikus attiecas arī uz dzīvām personām, tā ir uzskatāma par personas datiem, uz ko attiecas FPDAL noteikumi, un mirušas personas dati netieši bauda personas datu aizsardzības noteikumos paredzēto aizsardzību. Medicīnas personāla profesionālā noslēpuma glabāšanas pienākums nebeidzas ar pacienta nāvi.

Juridiskas personas

Tā kā personas datu definīcija attiecas uz fiziskām personām, FPDAL paredzētā aizsardzība neattiecas uz informāciju par juridiskām personām. Tomēr atsevišķi datu aizsardzības noteikumi dažādos apstākļos netieši var būt piemērojami arī informācijai, kas attiecas uz biznesa darījumiem vai juridiskām personām.

Informāciju par juridiskām personām pašu par sevi var uzskatīt arī par informāciju, kas „attiecas uz” fiziskām personām, ņemot vērā šajā rekomendācijā iepriekš aprakstītos kritērijus. Tas iespējams, piemēram, gadījumā, kad juridiskas personas nosaukums ir atvasināts no fiziskas personas vārda. Vēl viens piemērs varētu būt korporatīvā elektroniskā pasta adrese, ko parasti lieto konkrēts darbinieks, vai informācija par mazu uzņēmumu (kas vairāk atgādina „objektu” nekā juridisku personu), kas var norādīt uz tā īpašnieku. Visos šajos gadījumos, kad „satura”, „nolūka” vai „rezultāta” kritērijs ļauj informāciju par juridisku personu vai uzņēmumu uzskatīt par tādu informāciju, kas „attiecas uz” fizisku personu, tā ir jāuzskata par personas datiem un uz to jāattiecina datu aizsardzības noteikumi.

Tāpat kā gadījumā ar mirušo personu datiem pārziņu pielietotie praktiskie personas datu apstrādes paņēmieni var būt par iemeslu, kāpēc dati par juridiskām personām *de facto* tiek apstrādāti saskaņā ar personas datu aizsardzības noteikumiem. Ja pārzinis nešķirojot vāc datus par fiziskām un juridiskām personām un iekļauj tos vienā datu bāzē, datu apstrādes mehānismi un personas datu audita sistēma var būt izveidota tā, lai atbilstu datu aizsardzības noteikumiem. Līdz ar to pārzinim varētu būt pat vienkāršāk piemērot personas datu aizsardzības noteikumus visu veidu informācijai, kas tiek glabāta tā datnēs, nekā mēģināt nodalīt, kuri dati attiecas uz fiziskām un kuri uz juridiskām personām.

II. Personas datu aizsardzības vispārējie principi

Ja saskaņā ar šajā rekomendācijā minēto Jūs konstatējat, ka apstrādājat personas datus jeb veicat jebkuras darbības ar personas datiem, tad Jums ir jāievēro FPDAL noteiktie personas datu aizsardzības vispārējie principi. Izņēmumi, kas paredz, ka FPDAL vai atsevišķi tā panti nav jāpiemēro, ir ietverti FPDAL 3., 4. un 5.pantā.

Pārzinim (fiziskā vai juridiskā persona, valsts vai pašvaldību institūcija, kura nosaka personas datu apstrādes mērķus un apstrādes līdzekļus, kā arī atbild par personas datu apstrādi saskaņā ar šo likumu) ir pienākums veikt personas datu apstrādi saskaņā ar FPDAL. Piemēram, saskaņā ar FPDAL personas datu apstrāde ir atļauta, ja pastāv konkrētajā situācijā piemērojamais FPDAL 7., 11., 12., 13. un 13.[1] pantā noteiktais personas datu apstrādes tiesiskais pamats. Tādējādi pirms personas datu apstrādes uzsākšanas pārzinim ir jāizvērtē vai pastāv FPDAL noteiktais personas datu apstrādes tiesiskais pamats personas datu apstrādes uzsākšanai.

Saskaņā ar FPDAL 10.panta pirmo daļu pārzinim ir jānodrošina godprātīga un likumīga personas datu apstrāde (10.panta pirmās daļas 1.punkts), personas datu apstrāde tikai atbilstoši paredzētajam mērķim un tam nepieciešamajā apjomā (10.panta pirmās daļas 2.punkts), kā arī tādu personas datu glabāšanas veidu, kas datu subjektu ļauj identificēt attiecīgā laikposmā, kurš nepārsniedz paredzētajam personas datu apstrādes mērķim noteikto laikposmu (10.panta pirmās daļas 3.punkts) un personas datu pareizību, to savlaicīgu atjaunošanu, labošanu vai dzēšanu, ja personas dati ir nepilnīgi vai neprecīzi, saskaņā ar personas datu apstrādes mērķi (10.panta pirmās daļas 4.punkts).

FPDAL 21.pants nosaka, ka pārzinim ir pienākums reģistrēt personas datu apstrādi Datu valsts inspekcijā FPDAL noteiktā kārtībā, ja vien uz konkrēto personas datu apstrādi neattiecas FPDAL 21.panta otrajā daļā noteiktie izņēmumi. Savukārt FPDAL 15. līdz 20.pants nosaka datu subjekta tiesības uz savu personas datu aizsardzību, paredzot arī attiecīgus pārziņa pienākumus šo tiesību īstenošanā.

Saskaņā ar FPDAL 29.pantu Datu valsts inspekcija uzrauga personas datu apstrādes atbilstību FPDAL, veicot pārbaudes, izskatot sūdzības, kas saistītas ar personas datu aizsardzību, pieņemot lēmumus, ierosinot un veicot darbības, kas vērstas uz efektīvāku personas datu aizsardzību.

Vienlaicīgi Latvijas Administratīvo pārkāpumu kodeksa 204.[7] līdz 204.[11] pantā par nelikumīgām darbībām, kas ir saistītas ar personas datu apstrādi, ir paredzēta administratīvā atbildība - maksimālais sods fiziskajām personām un amatpersonām ir noteikts līdz 500 latiem, bet juridiskajām personām – līdz 10 000 latiem. Savukārt par atsevišķām darbībām, kas saistītas ar personas datu apstrādi, var iestāties krimināltatbildība, piemēram, saskaņā ar Krimināllikuma 241.pantu - patvaļīga piekļūšana automatizētai datu apstrādes sistēmai.