Kad veicams novērtējums par ietekmi uz datu aizsardzību?

Datu valsts inspekcija 2018. gada 18. decembrī apstiprināja sarakstu ar tiem apstrādes darbības veidiem, attiecībā uz kuriem ir jāveic novērtējums par ietekmi uz datu aizsardzību (NIDA). Šāds novērtējams veicams saskaņā ar Eiropas Parlamenta un Padomes regulas (ES) 2016/679 par fizisko personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ direktīvu 95/46 EK (Vispārīgā datu aizsardzības regula, turpmāk VDAR) 35. panta 4. punktu.

Saraksts nosaka tos apstrādes darbības veidus, kas „var radīt augstu risku fizisku personu tiesībām un brīvībām". Šis saraksts papildina un precizē 29. panta darba grupas (DG 29) vadlīnijās par „Novērtējumu par ietekmi uz datu aizsardzību" (NIDA) un regulas 2016/679 vadlīnijās minēto, tai skaitā, ņemot vērā vadlīnijās aprakstītos kritērijus.

Kā minēts 29. panta darba grupas izstrādātajās vadlīnijās par „Novērtējumu par ietekmi uz datu aizsardzību„ (pieņemtas 2017. gada 4. oktobrī), NIDA ir process, kas izveidots tā, lai aprakstītu apstrādi, novērtētu tās nepieciešamību un samērīgumu un palīdzētu pārvaldīt tādus riskus fizisku personu tiesībām un brīvībām, kas izriet no personas datu apstrādes, novērtējot tos un nosakot pasākumus to novēršanai. NIDA novērtējumi ir svarīgi pārskatatbildības rīki, jo tie palīdz pārziņiem ne vien nodrošināt atbilstību VDAR prasībām, bet arī

parādīt, ka ir veikti atbilstošie pasākumi, lai panāktu atbilstību minētajai regulai. Proti, **NIDA ir atbilstības nodrošināšanas un pierādīšanas process.**

Kompetentā uzraudzības iestāde var piemērot sodu par NIDA neveikšanu, ja attiecībā uz apstrādi ir jāveic NIDA (35. panta 1., 3. un 4. punkts), par nepareizu NIDA veikšanu (35. panta 2., 7., 8. un 9. punkts) vai neapspriešanos ar kompetento uzraudzības iestādi, ja tas ir nepieciešams (36. panta 3. punkta e) apakšpunkts). **Administratīvais naudas soda apmērs var būt līdz 10 miljoniem eiro, vai – uzņēmuma gadījumā – līdz 2% no kopējā visā pasaulē iepriekšējā finanšu gadā gūtā apgrozījuma atkarībā no tā, kuras summas apmērs ir lielāks.**

NIDA jēdziens VDAR tekstā formāli nav definēts, taču tās 35. panta 7. punktā ir norādīts tā minimālais saturs, proti, novērtējumā ietver vismaz:

- plānoto apstrādes darbību un apstrādes nolūku, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistemātisku aprakstu;
- novērtējumu par apstrādes darbību nepieciešamību un samērīgumu attiecībā uz nolūkiem;
- novērtējumu par 1. punktā minētajiem riskiem datu subjektu tiesībām un brīvībām;
- pasākumus, kas paredzēti risku novēršanai, tostarp garantijas, drošības pasākumus un mehānismus, ar ko nodrošina personas datu aizsardzību un uzskatāmi parāda, ka ir ievērota šī regula, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses.

Kā norādīts DG29 paziņojumā „Uz risku balstītas pieejas nozīme attiecībā uz datu aizsardzības tiesisko regulējumu", atsauce uz datu subjektu „tiesībām un brīvībām" **galvenokārt attiecas uz tiesībām uz datu aizsardzību un privātumu, taču to var attiecināt arī uz citām pamattiesībām – vārda brīvību, domas brīvību, pārvietošanās brīvību, diskriminācijas aizliegumu, tiesībām uz brīvību, apziņas brīvību un reliģijas brīvību.**

Attiecīgie novērtējuma rezultāti būtu jāņem vērā, nosakot piemērotus pasākumus, kas veicami, lai uzskatāmi parādītu, ka personas datu apstrāde atbilst šai regulai. Tāpat jāņem vērā, ka **NIDA ir jāveic pirms datu apstrādes – jāuzskata, ka NIDA ir rīks, kas palīdz pieņemt lēmumus par apstrādi.** Turklāt NIDA var būt vajadzīgs pēc tam, kad ir mainījušies apstrādes darbību rezultātā radītie riski, piemēram, tāpēc, ka ir ieviesta jauna tehnoloģija vai personas dati tiek izmantoti citā nolūkā. Vēl svarīgi ievērot, ka **NIDA var veikt kāda cita persona organizācijas iekšienē vai ārpus tās, taču galu galā par šā uzdevuma veikšanu joprojām atbild datu pārzinis.**

Zvērinātu advokātu biroja *Sorainen* partnere Ieva Andersone norāda, ka pagaidām nav pilnībā skaidra priekšstata, kā praksē būtu jāizskatās NIDA – vai pāris lappušu garam dokumentam vai arī vairāk nekā simts lapu apjomā, kādu to jau ir izveidojušas lielas starptautiskas korporācijas. Jebkuros neskaidros jautājumos ieteicams konsultēties ar Datu valsts inspekciju.

Pārziņiem ir nepārtraukti jānovērtē savu apstrādes darbību radītie riski, lai identificētu, kad apstrādes veids „varētu radīt augstu risku fizisku personu tiesībām un brīvībām".

Apstrādes darbību veidi, par kuriem ir jāveic NIDA

1. Novērtēšana vai vērtēšana, tostarp profilēšana un prognozēšana, jo īpaši lai analizētu aspektus saistībā ar datu subjekta sniegumu darbā, ekonomisko stāvokli, veselību, personīgajām vēlmēm vai interesēm, uzticamību vai uzvedību, atrašanās vietu vai pārvietošanos" (VDAR 71. un 91. apsvērums).

Piemēri – finanšu iestāde, kas novērtē savu klientu datus, izmantojot kredīta uzziņas datubāzi vai nelikumīgi iegūtu līdzekļu legalizēšanas un terorisma finansēšanas novēršanas (AML/CTF) vai krāpšanas datubāzi; biotehnoloģiju uzņēmums, kas piedāvā ģenētiskus testus tieši patērētājiem, lai novērtētu un prognozētu slimības/veselības riskus; uzņēmums, kas veido uzvedības vai mārketinga profilus, pamatojoties uz pielietojumu vai navigāciju savā tīmekļa vietnē.

2. Automatizēta lēmumu pieņemšana, kuru pamato ar juridisku vai līdzīgu būtisku ietekmi: apstrāde, kuras rezultātā tiek pieņemti lēmumi par datu subjektiem, kas rada „juridiskas sekas attiecībā uz fizisko personu" vai kas „līdzīgi būtiski ietekmē fizisko personu" (VDAR 35. panta 3. punkta a) apakšpunkts).

Piemērs – apstrāde, kuras rezultātā fiziskas personas var tikt izslēgtas vai diskriminētas, izņemot gadījumus, kad apstrāde nerada būtisku kaitējumu fiziskām personām vai tās ietekme vispār netiek konstatēta, līdz ar to šāds apstrādes veids nav attiecināms uz šo īpašo kritēriju.

3. Sistemātiska uzraudzība: piemēro, lai novērotu, uzraudzītu vai kontrolētu datu subjektus, tostarp datus, kas iegūti tīmeklī vai „publiski pieejamas zonas sistemātiskas uzraudzības" rezultātā (VDAR 35. panta 3. punkta c) apakšpunkts).

Piemērs – šāda veida uzraudzība ir datu apstrādes darbība, jo personas datus var ievākt apstākļos, kad datu subjekti, iespējams, nezina, kas vāc viņu datus un kā tie tiks izmantoti. Tāpat personām var nebūt iespējas izvairīties no šādas viņu datu apstrādes publiskajā (–ās) (vai publiski pieejamajā (–ās)) zonā (–ās). Turklāt indivīdiem var būt neiespējami izvairīties no šādas apstrādes publiskās (vai publiski pieejamās) telpās.

4. Sensitīvi dati vai ļoti personiska rakstura dati: attiecas uz īpašas kategorijas personu datiem, kā tas noteikts VDAR 9. pantā (piemēram, informācija par personas politiskajiem uzskatiem), kā arī uz personas datiem saistībā ar sodāmību vai noziedzīgiem nodarījumiem saskaņā ar VDAR 10. pantā noteikto.

Piemērs – medicīnas iestādes datu uzskaite satur pacientu medicīniskos datus; privāta izmeklētāja datu uzskaite, kurā saglabātas ziņas par pārkāpējiem. Papildus VDAR noteikumiem var uzskatīt, ka dažas datu kategorijas paaugstina personu tiesību un brīvību iespējamo apdraudējumu, proti, palielina iespējamo risku personu tiesībām un brīvībām.

5. Datu apstrāde plašā mērogā. VDAR nav norādīta plaša mēroga apstrādes definīcija, taču VDAR 91. apsvērumā ir dotas dažas norādes. Kad apstrāde notiek plašā mērogā, 29. panta darba grupa iesaka ņemt vērā šādus faktorus:

a) datu subjektu skaits tiek identificēts kā konkrēta skaitliska vienība vai proporcionāla daļa no iedzīvotāju kopējā skaita;
b) datu apjoms un/vai dažādu veidu apstrādāto datu vienumu klāsts;
c) datu apstrādes darbības ilgums vai pastāvīgums;
d) apstrādes darbības teritoriālais tvērums.

6. Datu kopu saskaņošana vai apvienošana.

Piemērs – datu apstrāde izriet no divām vai vairākām datu apstrādes darbībām, kas tiek veiktas dažādiem nolūkiem un/vai no dažādiem datu apstrādātājiem, un tādējādi tiek pārsniegtas datu subjekta saprātīgās gaidas.

DATU AIZSARDZĪBA

7. Datu apstrāde attiecībā uz īpaši aizsargājamiem datu subjektiem (VDAR 75. apsvērums).

Piemērs – bērni, uzskatot, ka viņi nespēj apzināti un pārdomāti iebilst datu apstrādei vai piekrišanas sniegšanai, lai veiktu datu apstrādi; darbinieki; mazāk aizsargātas iedzīvotāju grupas, kam nepieciešama īpaša aizsardzība (garīgi slimas personas, patvēruma meklētāji vai vecāka gadagājuma cilvēki, pacienti utt.) un jebkurā citā gadījumā, kad var identificēt neatbilstību attiecībās starp datu subjektu un pārzini.

8. Inovatīva jaunu tehnoloģiju vai risinājumu izmantošana vai to pielietošana, piemēram, apvienojot pirkstu nospiedumu un sejas atpazīšanas lietošanu, lai uzlabotu piekļuves kontroli utt.

Piemērs – dažas lietojumprogrammas „Interneta lietas" var būtiski ietekmēt privātumu ikdienas dzīvē, tādēļ ir nepieciešams NIDA.

9. Ja apstrāde pati par sevi „liedz datu subjektiem īstenot tiesības vai izmantot pakalpojumu vai līgumu" (22. un 91. apsvērums).

Piemērs – banka pēta savus klientus, izmantojot kredīta uzziņas datubāzi, lai lemtu par aizdevuma izsniegšanu.

Datu valsts inspekcija norāda, ka šo sarakstu nevajadzētu uzskatīt par izsmeļošu. Pārzinim pirms datu apstrādes visos gadījumos ir jāņem vērā apstrādes raksturs, apjoms, konteksts un mērķis, kā arī tas, vai pastāv iespējamība, ka apstrāde radīs lielu risku fizisko personu tiesībām un brīvībām un jāveic NIDA, ja pārzinis uzskata, ka datu apstrāde var radīt lielu risku fizisko personu brīvībām un tiesībām.

Ņemot vērā iepriekš minēto, pārzinim, kura galvenā vai vienīgā uzņēmējdarbības vieta ir Latvijas Republikas teritorija, jāveic NIDA vismaz šādos gadījumos:

1) personas datu apstrāde, kas saistīta ar krimināl sodāmību, pārkāpumiem vai citiem drošības pasākumiem;
2) personas datu apstrāde zinātniskiem vai vēsturiskiem nolūkiem, ja tā veikta bez datu subjekta piekrišanas un kopā ar vismaz vienu no kritērijiem;
3) gadījumos, kad saskaņā ar VDAR 19. punktā minētā informācijas sniegšana datu subjektam ir neiespējama;
4) ģenētisko datu apstrāde ar mērķi identificēt fizisku personu, kopā ar vismaz vienu no kritērijiem;
5) datu subjekta uzraudzība, kas tiek veikta šādos gadījumos:
   a) ja to veic plašā apjomā;
   b) ja to veic darbavietā;
   c) ja tā attiecināma uz īpaši aizsargājamiem datu subjektiem (piemēram, veselības aprūpē, sociālajā aprūpē, ieslodzījuma vietā, cietumā, izglītības iestādē, darbavietā);
6) datu apstrāde, izmantojot inovatīvas tehnoloģijas, mehānismus vai metodes, kopā ar vismaz vienu no kritērijiem;
7) **darbinieku novērošana;**
8) plaša mēroga datu subjektu izsekošana, tostarp dzīvesveida lietotnes vai loģistikas uzņēmumi;
9) datu subjekta atrašanās vietas datu izmantošana, kopā ar vismaz vienu no kritērijiem;
10) datu apstrāde attiecināma uz informācijas sabiedrības pakalpojumu piedāvājumu tieši bērnam;
11) automātiska personas datu apstrāde plašā mērogā un datu apstrāde, kā pamatā ir profilēšana;
12) datu apstrāde veids ar mērķi apvienot datus no dažādiem avotiem, lai nodrošinātu saskaņošanas, salīdzināšanas un atkārtotas izmantošanas darbības;
13) biometrisko datu apstrāde ar mērķi identificēt fizisku personu, kopā ar vismaz vienu no kritērijiem.

Fakts, ka apstākļi, kas rada pienākumu veikt NIDA, nav uzņēmumā konstatēti, nemazina pārziņu vispārējo pienākumu īstenot pasākumus, lai atbilstoši pārvaldītu riskus attiecībā uz datu subjektu tiesībām un brīvībām. **Pārziņiem ir nepārtraukti jānovērtē savu apstrādes darbību radītie riski, lai identificētu, kad apstrādes veids „varētu radīt augstu risku fizisku personu tiesībām un brīvībām".**

Katrā ziņā ir jāņem vērā, ka uzņēmumiem jāievieš kārtējā kontroles sistēma, lai neizpelnītos bargus sodus, ja tās trūkuma dēļ būs pārkāptas VDAR prasības. 2019. gadā jāturpina sekot līdzi visam, kas saistās ar VDAR praktisko ieviešanu.

Par pārkāpumiem personas datu aizsardzībā – sods 50 miljoni eiro

Datu valsts inspekcija informē, ka Francijas datu aizsardzības uzraudzības iestāde CNIL (*Commission Nationale de l'Informatique et des Libertés*) 2019. gada 21. janvārī par neatbilstību VDAR prasībām sodīja uzņēmumu *GOOGLE LLC*, piemērojot naudas sodu 50 miljonu eiro apmērā **par personas datu apstrādes pārredzamības principa nenodrošināšanu un neatbilstošu datu subjekta piekrišanu attiecībā uz personalizētu komerciālu paziņojumu saņemšanu.**

CNIL 2018. gada 25. maijā saņēma divu asociāciju sūdzības *None Of Your Business* (NOYB) un *La Quadrature du Net* (LQDN) norādot, ka *GOOGLE LLC* nav juridiska pamata uzņēmuma lietotāju personas datu apstrādei, it īpaši personalizētu komerciālu paziņojumu sūtīšanai. Inspekcija norāda, ka LQDN tika pilnvarots pārstāvēt 10 000 uzņēmuma klientu (sūdzības iesniedzējus). Pēc sūdzību saņemšanas CNIL uzreiz sāka izmeklēšanu par iesniegtajām sūdzībām.

Izskatot lietu, CNIL konstatēja divu veidu pārkāpumus VDAR kontekstā:

- nepietiekama personas datu apstrādes pārredzamības principa nodrošināšana un informācijas trūkums;
- nepastāv tiesiskais pamats personalizētu komerciālo paziņojumu sūtīšanai.

CNIL norāda, ka *GOOGLE* sniegtā informācija nav viegli pieejama klientiem (lietotājiem). Uzņēmuma informācijas izvietošanas struktūra neatbilst VDAR (58. apsvērums – „Pārredzamības principa pamatā ir prasība, ka visa informācija, kas adresēta sabiedrībai vai datu subjektam, ir kodolīga, viegli pieejama un viegli saprotama un ka tiek izmantota skaidra un vienkārša valoda un papildus – vajadzības gadījumā – vizualizācija". Lai iegūtu informāciju par savu personas datu apstrādes mērķi, datu glabāšanas termiņu, komerciālu paziņojumu personalizēšanu, klientiem jāveic 5 līdz 6 darbības.

Ņemot vērā lielo piedāvāto pakalpojumu skaitu (CNIL norāda – aptuveni 20 pakalpojumi), tad attiecībā pret apjomīgo *GOOGLE LLC* veikto personas datu apjomu, tai skaitā kombinēto datu apstrādi, **personām pieejamā informācija par personas datu apstrādes mērķi un apstrādāto personas datu kategorijām ir pārāk vispārīga un neskaidra, lai lietotājs varētu saprast, ka personalizētu komerciālu paziņojumu saņemšanas tiesiskais pamats ir personas (datu subjekta) piekrišana, nevis pārziņa leģitīmo interešu ievērošana.** *GOOGLE LLC* nav sniedzis informāciju par atsevišķu apstrādāto datu glabāšanas termiņiem.

Neskatoties uz *GOOGLE LLC* norādīto, ka uzņēmums saņem klientu (lietotāju) piekrišanu personalizētu komerciālu paziņojumu saņemšanai, CNIL norāda, ka saņemtā piekrišana nav atbilstoša VDAR prasībām, jo lietotājiem izsniegtā piekrišanā nav pietiekami daudz informācijas. Informācija par personalizētu komerciālo paziņojumu (reklāmu) saistītajām darbībām ir sadalīta vairākos informācijas avotos un nedod lietotājam iespēju saņemt visu informāciju par apstrādāto datu apjomu. Piemēram, sadaļā „Reklāmu personalizēšana" klientam nav iespējams saņemt visu informāciju konkrēto datu apstrādes apjomu par visiem *GOOGLE LLC* sniegtajiem pakalpojumiem, tīmekļa vietņu un lietojumprogrammu daudzveidību (*Google search*, *You tube*, *Google home*, *Google maps*, *Playstore*, *Google pictures*).

Piekrišana „nepārprotama" tikai tad, ja klients (lietotājs) ir veicis skaidras, apzinātas un apstiprinošas darbības.

CNIL norāda, ka klientu (lietotāju) sniegtās piekrišanas neatbilst VDAR prasībām, piekrišana nav ne „konkrēta", ne „nepārprotama" (4. panta 1. punkts) – „datu subjekta „piekrišana" ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei". Izveidojot lietotāju kontu, personai ir iespēja mainīt dažādas ar kontu saistītas opcijas, noklikšķinot uz pogas „Citas opcijas", kur iespējams konfigurēt ar iespēju personalizēt komerciālu paziņojumu saņemšanai, savukārt personalizēta komerciālu paziņojumu saņemšana ir jau iepriekš atzīmēta. Komisija norāda, ka konkrētās ieviestās darbības uzreiz nenodrošina atbilstību VDAR prasībām, jo saskaņā ar normatīvo regulējumu piekrišana „nepārprotama" tikai tad, ja klients (lietotājs) ir veicis skaidras, apzinātas un apstiprinošas darbības, piemēram, personīgi ieklikšķinot iepriekš neatzīmētā izvēles lauciņā.

Kā pēdējo argumentu CNIL norāda, ka pirms lietotāja konta izveides personai ir jāatzīmē „Es piekrītu *Google* pakalpojumu sniegšanas noteikumiem" un „Es piekrītu personas datu apstrādei, kas aprakstīta iepriekš un izskaidrota konfidencialitātes politikā". Atzīmējot „Piekrītu" klients (lietotājs) dod savu piekrišanu personas datu apstrādei uz visām apstrādes darbībām, ko veic *GOOGLE LLC*. Tomēr **VDAR paredz, ka piekrišana ir jāsaņem katram personas datu apstrādes nolūkam atsevišķi.**

Naudas sods piemērots, balstoties uz pārkāpuma smagumu attiecībā pret VDAR noteiktajiem principiem – pārredzamība, atbilstošas informācijas sniegšana un datu subjekta piekrišana.

CNIL norāda, ka *GOOGLE LLC* veiktā personas datu apstrāde ir liela apjoma un konstatētie pārkāpumi nedod garantijas klientiem (lietotājiem) attiecībā uz veiktajām apstrādes darbībām, kas varētu atklāt būtiskas privātās dzīves daļas. Turklāt konstatētie pārkāpumi nav viens vienīgs gadījums, bet, ņemot vērā lielo klientu (lietotāju) skaitu, konstatētie pārkāpumi ir uzņēmuma regulāra darbība. DIP

DATU AIZSARDZĪBA

Sagatavots pēc Datu valsts inspekcijas informācijas