17/LV

WP 248 vers. 01

Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē

Pieņemtas 2017. gada 4. aprīlī.

Pēdējoreiz pārskatītas un pieņemtas 2017. gada 4. oktobrī.

DARBA GRUPA PERSONU AIZSARDZĪBAI ATTIECĪBĀ UZ PERSONAS DATU APSTRĀDI,

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

ņemot vērā minētās direktīvas 29. un 30. pantu,

ņemot vērā darba grupas reglamentu,

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

Satura rādītājs

I. Ievads

Regula 2016/679[1] (Vispārīgā datu aizsardzības regula, VDAR) stāsies spēkā 2018. gada 25. maijā. Jēdzienu "novērtējums par ietekmi uz datu aizsardzību" (NIDA[2]) ievieš ar VDAR 35. pantu, tas definēts arī Direktīvā 2016/680[3].

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[4], 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 (sk. arī 24. pantu)[5]. Proti, **NIDA ir atbilstības nodrošināšanas un pierādīšanas process**.

Saskaņā ar VDAR par neatbilstību NIDA prasībām 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), var piemērot administratīvu naudas sodu, kura apmērs var būt līdz EUR 10 miljoniem, vai — uzņēmuma gadījumā — līdz 2 % no kopējā visā pasaulē iepriekšējā finanšu gadā gūtā gada apgrozījuma atkarībā no tā, kuras summas apmērs ir lielāks.

II. Pamatnostādņu darbība joma

Šajās pamatnostādnēs ir ņemti vērā:

---

[1] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (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 (Vispārīgā datu aizsardzības regula).

[2] Citā kontekstā nereti izmanto terminu "ietekmes uz privātumu novērtējums" (IPN), lai atsauktos uz to pašu jēdzienu.

[3] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīvas (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, 27. pantā arī ir noteikts, ka ietekmes uz privātumu novērtējums ir nepieciešams, ja apstrāde "*varētu radīt augstu risku fizisko personu tiesībām un brīvībām*".

[4] NIDA jēdziens kā tāds VDAR formāli nav definēts, taču

- tās 35. panta 7. punktā ir norādīts tā minimālais saturs, proti, ka novērtējumā ietver vismaz:
  - "*a) plānoto apstrādes darbību un apstrādes nolūku, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistemātisku aprakstu*;
  - *b) novērtējumu par apstrādes darbību nepieciešamību un samērīgumu attiecībā uz nolūkiem;*
  - *c) novērtējumu par 1. punktā minētajiem riskiem datu subjektu tiesībām un brīvībām; un*
  - *d) 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";*
- tās 84. apsvērumā minētā novērtējuma nozīme un loma ir precizēta šādi: "*Lai sekmētu šīs regulas noteikumu ievērošanu gadījumos, kad apstrādes darbības varētu izraisīt augstu risku fizisku personu tiesībām un brīvībām, pārzinim vajadzētu būt atbildīgam par novērtējuma par ietekmi uz datu aizsardzību veikšanu, lai jo īpaši izvērtētu minētā riska avotus, raksturu, specifiku un nopietnību.*"

[5] Sk. arī 84. apsvērumu: "*Novērtējuma rezultāti būtu jāņem vērā, nosakot piemērotus pasākumus, kas veicami, lai uzskatāmi parādītu, ka personas datu apstrāde atbilst šai regulai*."

- 29. panta datu aizsardzības darba grupas ("DG29") Paziņojums 14/EN WP 218[6];
- DG29 Pamatnostādnes par datu aizsardzības speciālistu, 16/EN WP 243[7];
- DG29 Atzinums par nolūka ierobežošanu, 13/EN WP 203[8];
- starptautiski standarti[9].

Saskaņā ar VDAR ietverto, uz risku balstīto pieeju NIDA nav obligāti jāveic attiecībā uz visām apstrādes darbībām. NIDA jāveic tikai tad, ja apstrāde "*varētu radīt augstu risku fizisko personu tiesībām un brīvībām*" (35. panta 1. punkts). Lai nodrošinātu konsekventu skaidrojumu par to, kādos apstākļos NIDA ir jāveic obligāti (35. panta 3. punkts), šo pamatnostādņu mērķis, pirmkārt, ir precizēt šo jēdzienu un izvirzīt kritērijus, kas jāievēro datu aizsardzības iestādēm (DAI), pieņemot sarakstus saskaņā ar 35. panta 4. punktu.

Saskaņā ar 70. panta 1. punkta e) apakšpunktu Eiropas Datu aizsardzības kolēģija (EDAK) varēs nākt klajā ar pamatnostādnēm, ieteikumiem un paraugpraksi, lai veicinātu VDAR konsekventu piemērošanu. Šā dokumenta mērķis ir paredzēt tādu EDAK darbību nākotnē un tāpēc precizēt atbilstošos VDAR nosacījumus, lai palīdzētu pārziņiem nodrošināt atbilstību likumam un sniegtu juridisko noteiktību pārziņiem, kuriem ir pienākums veikt NIDA.

Tāpat šo pamatnostādņu mērķis ir pilnveidot:
- vienoto Eiropas Savienības sarakstu, kurā uzskaitītas apstrādes darbības, attiecībā uz kurām ir obligāti jāveic NIDA (35. panta 4. punkts);
- vienoto ES sarakstu, kurā uzskaitītas apstrādes darbības, attiecībā uz kurām nav vajadzīgs NIDA (35. panta 5. punkts);
- kopējos kritērijus attiecībā uz NIDA veikšanas metodoloģiju (35. panta 5. punkts);
- kopējos kritērijus, pēc kuriem nosaka, kad ir jāapspriežas ar uzraudzības iestādi (36. panta 1. punkts);
- ieteikumus, ja iespējams, ņemot vērā ES dalībvalstīs gūto pieredzi.

[6] DG29 Paziņojums 14/EN WP 218 "Uz risku balstītas pieejas nozīme attiecībā uz datu aizsardzības tiesisko regulējumu", pieņemts 2014. gada 30. maijā.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] DG29 Pamatnostādnes par datu aizsardzības speciālistu, 16/EN WP 243; pieņemtas 2016. gada 13. decembrī.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] DG29 Atzinums 03/2013 par nolūka ierobežošanu, 13/EN WP 203; pieņemts 2013. gada 2. aprīlī.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Piem., ISO 31000:2009 "*Riska pārvaldība. Principi un pamatnostādnes*", Starptautiskā Standartizācijas organizācija (*ISO*); ISO/IEC 29134 (projekts) "*Informācijas tehnoloģija. Drošības metodes. Ietekmes uz privātumu novērtējums. Pamatnostādnes*", *ISO*.

III. NIDA — skaidrojums, kas sniegts VDAR

VDAR noteikts, ka pārziņiem ir jāīsteno atbilstoši pasākumi, lai nodrošinātu un spētu parādīt atbilstību VDAR, cita starpā ņemot vērā "dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisko personu tiesībām un brīvībām" (24. panta 1. punkts). Pārziņu pienākums noteiktos apstākļos veikt NIDA ir skaidrojams, ņemot vērā to vispārējo pienākumu atbilstoši pārvaldīt riskus[10], ko rada personas datu apstrāde.

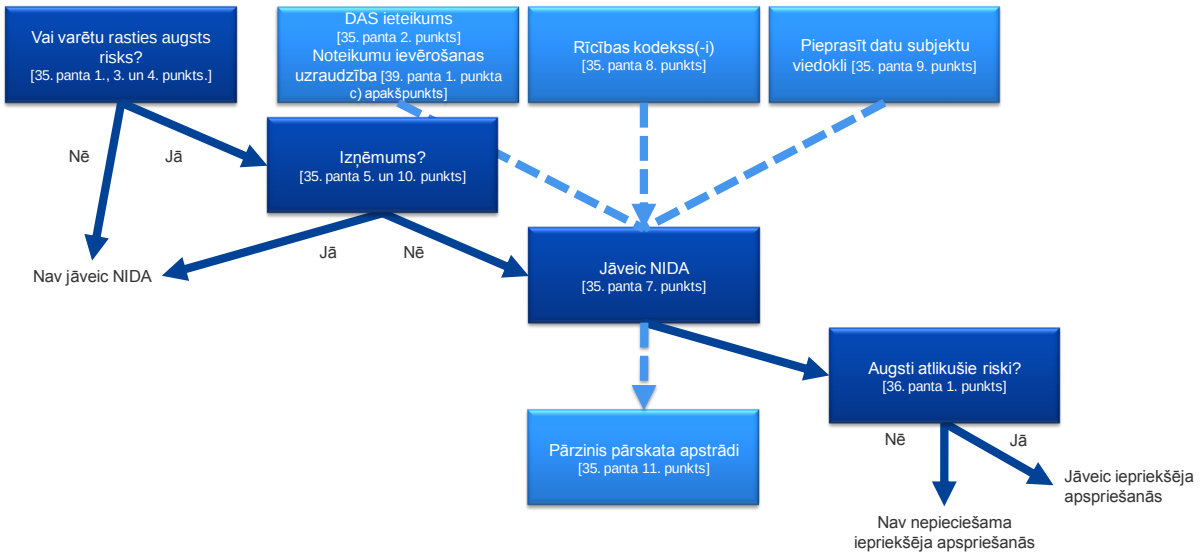
"Risks" ir scenārijs, kas apraksta notikumu un tā sekas, kuras novērtētas pēc smaguma pakāpes un iespējamības. Savukārt "riska pārvaldību" var definēt kā saskaņotas darbības ar mērķi vadīt un kontrolēt organizāciju attiecībā uz risku.

VDAR 35. pantā ir dota atsauce uz iespējamu augstu risku attiecībā uz "fizisku personu tiesībām un brīvībām". 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.

Saskaņā ar VDAR ietverto, uz risku balstīto pieeju NIDA nav obligāti jāveic attiecībā uz visām apstrādes darbībām. Gluži pretēji, NIDA jāveic tikai tad, ja apstrādes veids "varētu radīt augstu risku fizisko personu tiesībām un brīvībām" (35. panta 1. punkts). Taču fakts kā tāds, ka apstākļi, kas rada pienākumu veikt NIDA, nav konstatēti, nemazina pārziņu vispārējo pienākumu īstenot pasākumus, lai atbilstoši pārvaldītu riskus attiecībā uz datu subjektu tiesībām un brīvībām. Praktiski tas nozīmē, ka pārziņiem ir nepārtraukti jānovērtē savu apstrādes darbību radītie riski, lai identificētu, kad apstrādes veids "varētu radīt augstu risku fizisku personu tiesībām un brīvībām".

[10] Jāuzsver, ka, lai pārvaldītu riskus attiecībā uz fizisku personu tiesībām un brīvībām, šie riski ir jāidentificē, jāanalizē, jāaplēš, jānovērtē, jānovērš (piem., jāsamazina) un regulāri jāpārskata. Pārziņi nevar izvairīties no atbildības, nosakot, ka riski tiek segti atbilstoši apdrošināšanas polisēm.

Tālāk dotajā attēlā ir ilustrēti pamatprincipi saistībā ar NIDA veikšanu, kas izklāstīti VDAR.



A. Kam pievērš uzmanību, veicot NIDA? Viena apstrādes darbība vai līdzīgu apstrādes darbību kopums.

NIDA var attiekties uz vienu datu apstrādes darbību. Tomēr 35. panta 1. punktā ir norādīts, ka "*vienā novērtējumā var pievērsties tādu līdzīgu apstrādes darbību kopumam, kurām piemīt līdzīgi augsti riski*". VDAR 92. apsvērumā ir papildināts, ka "*noteiktos apstākļos var būt saprātīgi un ekonomiski veikt plašāku novērtējumu par ietekmi uz datu aizsardzību, kura priekšmets nav tikai viens projekts, piemēram, ja publiskas iestādes vai struktūras vēlas izveidot vienotu lietotņu vai apstrādes platformu vai ja vairāki pārziņi plāno ieviest vienotu lietotņu vai apstrādes vidi kādā rūpniecības nozarē vai segmentā, vai kādai plaši lietotai horizontālai darbībai*".

Vienu un to pašu NIDA var izmantot, lai novērtētu vairākas apstrādes darbības, kas ir līdzīgas pēc rakstura, apmēra, konteksta, nolūka un riskiem. NIDA mērķis ir sistemātiski izskatīt jaunas situācijas, kas varētu radīt augstu risku fizisku personu tiesībām un brīvībām, un nav nekādas vajadzības veikt NIDA gadījumos, kas jau ir izskatīti (t. i., attiecībā uz apstrādes darbībām, kas tiek veiktas konkrētā kontekstā konkrētā nolūkā). Tas varētu attiekties uz gadījumiem, kad tiek izmantota līdzīga tehnoloģija, lai iegūtu tāda paša veida datus tādos pašos nolūkos. Piemēram, tādu pašvaldības iestāžu grupa, kuras katra izveido līdzīgu videonovērošanas sistēmu, var veikt vienu kopīgu NIDA, kas aptver šo atsevišķo pārziņu veikto apstrādi; dzelzceļa operators (viens pārzinis) var aptvert videonovērošanu visās savās dzelzceļa stacijās, veicot vienu kopīgu NIDA. Iespējams, to var attiecināt arī uz līdzīgām apstrādes darbībām, kuras veic dažādi datu pārziņi. Tādos gadījumos atsauces NIDA ir jākopīgo vai jāpadara publiski pieejams, ir jābūt īstenotiem NIDA aprakstītajiem pasākumiem, kā arī ir jāsniedz pamatojums, kāpēc var veikt vienu kopīgu NIDA.

Ja apstrādes darbības veikšanā ir iesaistīti kopīgi pārziņi, tiem ir precīzi jānosaka katra attiecīgie pienākumi. Kopīgu pārziņu NIDA ir jānorāda, kura persona ir atbildīga par dažādajiem pasākumiem, kuru mērķis ir novērst riskus un aizsargāt datu subjektu tiesības un brīvības. Katram datu pārzinim ir jāpauž savas vajadzības un jādalās ar noderīgu informāciju, neietekmējot slepenu informāciju (piem., aizsargājot uzņēmējdarbības noslēpumus, intelektuālo īpašumu, konfidenciālu uzņēmējdarbības informāciju) un neizpaužot ievainojamību.

NIDA var būt noderīgs arī, novērtējot, kā datu aizsardzību ietekmē kāds tehnoloģisks izstrādājums, piemēram, aparatūra vai programmatūra, ja pastāv iespēja, ka to var izmantot dažādi datu pārziņi, lai veiktu dažādas apstrādes darbības. Protams, datu pārzinim, kas izvieto izstrādājumu, saglabājas pienākums veikt pašam savu NIDA attiecībā uz konkrēto īstenošanu, taču to attiecīgā gadījumā var veikt atbilstoši NIDA, kuru veicis izstrādājuma nodrošinātājs. Kā piemēru var minēt attiecības starp viedskaitītāju ražotājiem un komunālo pakalpojumu uzņēmumiem. Katram izstrādājuma nodrošinātājam vai apstrādātājam ir jākopīgo noderīga informācija, neietekmējot noslēpumus un neradot drošības riskus ievainojamības izpaušanas rezultātā.

B. Attiecībā uz kādām apstrādes darbībām ir jāveic NIDA? Papildus izņēmumiem — attiecībā uz darbībām, kas "*varētu radīt augstu risku*".

Šajā sadaļā ir aprakstīts, kad NIDA ir jāveic obligāti un kad tas nav nepieciešams.

Ja vien apstrādes darbība neatbilst izņēmumam (sk. III daļas B. sadaļas a) apakšpunktu), NIDA ir jāveic tad, ja apstrādes darbība "*varētu radīt augstu risku*" (sk. III daļas B. sadaļas b) apakšpunktu).

a) Kad NIDA ir jāveic obligāti? Kad apstrāde "*varētu radīt augstu risku*".

VDAR nav noteikts, ka NIDA ir jāveic attiecībā uz katru apstrādes darbību, kas varētu radīt riskus fizisku personu tiesībām un brīvībām. NIDA ir jāveic obligāti tikai tad, ja apstrāde "*varētu radīt augstu risku fizisku personu tiesībām un brīvībām*" (35. panta 1. punkts, ko ilustrē 35. panta 3. punkts un papildina 35. panta 4. punkts). Tas ir sevišķi būtiski tad, ja tiek ieviesta jauna datu apstrādes tehnoloģija[11].

Gadījumos, kad nav skaidrs, vai NIDA ir jāveic, DG29 iesaka tomēr to veikt, jo tas ir noderīgs rīks, kas palīdz pārziņiem ievērot datu aizsardzības tiesības.

Lai gan NIDA, iespējams, ir jāveic arī citos apstākļos, 35. panta 3. punktā ir doti daži tādu gadījumu piemēri, kad apstrādes darbība "*varētu radīt augstu risku*":

- "*a) ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu;*[12]
- *b) 9. panta 1. punktā minēto īpašo kategoriju datu vai 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā;*[13] *vai*
- *c) publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā*."

Kā uz to norāda vārdi "*jo īpaši*" VDAR 35. panta 3. punkta ievaddaļas teikumā, šis saraksts nav izsmeļošs. Var būt tādas "augsta riska" apstrādes darbības, kas nav iekļautas šajā sarakstā, taču rada līdzīgi augstus riskus. Arī attiecībā uz šādām apstrādes darbībām ir jāveic NIDA. Šā iemesla dēļ

[11] Papildu piemērus skatīt 89. un 91. apsvērumā un 35. panta 1. un 3. punktā.

[12] Sk. 75. apsvērumu: "*jo īpaši analizējot vai prognozējot aspektus attiecībā uz personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm vai interesēm, uzticamību vai uzvedību, atrašanās vietu vai pārvietošanos, lai izveidotu vai izmantotu personiskos profilus*".

[13] Sk. 75. apsvērumu: "*ja tiek apstrādāti personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību, piederību arodbiedrībai, un ja tiek apstrādāti ģenētiskie dati, veselības dati vai dati par dzimumdzīvi, vai sodāmību un pārkāpumiem vai ar tiem saistītiem drošības pasākumiem*".

kritēriji, kas izklāstīti tālāk, reizēm ir interpretējami plašāk nekā ar vienkāršo skaidrojumu, kas izriet no VDAR 35. panta 3. punktā dotajiem trim piemēriem.

Lai konkrētāk definētu tādu apstrādes darbību kopumu, attiecībā uz kurām ir jāveic NIDA tām piemītošā augstā riska dēļ, ņemot vērā 35. panta 1. punktā un 3. punkta a), b) un c) apakšpunktā minētos konkrētos elementus, valsts līmenī apstiprināmo sarakstu saskaņā ar 35. panta 4. punktu un 71., 75. un 91. apsvērumu, kā arī citas VDAR iekļautās atsauces uz apstrādes darbībām, kas "*varētu radīt augstu risku*"[14], ir jāņem vērā tālāk izklāstītie deviņi kritēriji.

1. Vērtēšana vai punktu piešķiršana, tostarp profilēšana un prognozes, īpaši ņemot vērā "*aspektus saistībā ar datu subjekta sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm vai interesēm, uzticamību vai uzvedību, atrašanās vietu vai pārvietošanos*" (71. un 91. apsvērums). Var minēt šādus piemērus: finanšu iestāde, kas pārbauda klientus, izmantojot kredītu uzziņas datubāzi vai datubāzi saistībā ar nelikumīgi iegūtu līdzekļu legalizāciju un teroristu finansēšanas apkarošanu (*AML/CTF*) vai krāpšanas gadījumiem; biotehnoloģiju uzņēmums, kas piedāvā ģenētiskus izmeklējumus tieši klientiem, lai novērtētu un prognozētu slimības / veselības riskus; uzņēmums, kas izstrādā rīcības vai mārketinga profilus, balstoties uz tā tīmekļa vietnes lietošanu.
2. Tādu lēmumu automatizēta pieņemšana, kuriem ir tiesiskas vai līdzīgi būtiskas sekas: apstrāde, kuras mērķis ir pieņemt lēmumus par datu subjektiem, "*kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu*" (35. panta 3. punkta a) apakšpunkts). Piemēram, datu apstrādes rezultātā personas var tikt izslēgtas vai diskriminētas. Apstrāde, kam ir neliela ietekme uz personām vai tādas nav, neatbilst šim īpašajam kritērijam. Sīkāki paskaidrojumi par šiem jēdzieniem būs sniegti DG29 pamatnostādnēs par profilēšanu, kas tiks izdotas drīzumā.
3. Sistemātiska novērošana: apstrāde, ko izmanto, lai novērotu, uzraudzītu vai kontrolētu datu subjektus, tostarp dati, kas iegūti tīmeklī vai "*publiski pieejamas zonas sistemātiskas uzraudzības*" rezultātā (35. panta 3. punkta c) apakšpunkts)[15]. Šāda veida uzraudzība ir kritērijs tāpēc, ka 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).
4. Sensitīvi dati vai ļoti personiska rakstura dati: tie ietver personas datu īpašas kategorijas, kā definēts 9. pantā (piem., informācija par personas politiskajiem uzskatiem), kā arī personas datus, kas attiecas uz sodāmību vai noziedzīgiem nodarījumiem, kā definēts 10. pantā. Var minēt šādus piemērus: slimnīcas uzskaite, kurā glabā pacientu medicīniskos datus; privāta izmeklētāja uzskaite, kurā saglabātas ziņas par pārkāpējiem. Papildus šiem noteikumiem, kas definēti VDAR, var uzskatīt, ka dažas datu kategorijas palielina iespējamo risku personu tiesībām un brīvībām. Šie personas dati ir uzskatāmi par sensitīviem (kā šo terminu ierasti

[14] Sk., piem., 75., 76., 92., 116. apsvērumu.

[15] DG29 jēdzienu "*sistemātisks*" skaidro šādi: tāds, kas atbilst vienam vai vairākiem no tālāk uzskatītajiem kritērijiem (sk. DG29 Pamatnostādnes par datu aizsardzības speciālistu, 16/EN WP 243):

- notiek atbilstoši sistēmai;
- iepriekš noteikts, organizēts vai metodisks;
- notiek datu vākšanas vispārējā plāna ietvaros;
- īstenots stratēģijas ietvaros.

DG29 jēdzienu "*publiski pieejama zona*" skaidro šādi: vieta, kas ir pieejama jebkuram sabiedrības loceklim, piemēram, laukums, iepirkšanās centrs, iela, tirgus, dzelzceļa stacija vai publiska bibliotēka.

izprot) tāpēc, ka tie ir saistīti ar sadzīves un privātām darbībām (piem., elektroniskā saziņa, kuras konfidencialitāte ir jāaizsargā), tie ietekmē pamattiesību īstenošanu (piem., atrašanās vietas datu vākšana, ja tas apdraud pārvietošanās brīvību) vai to aizsardzības pārkāpšana nepārprotami būtiski ietekmē datu subjekta ikdienas dzīvi (piem., finanšu dati, ko var izmantot krāpšanai saistībā ar maksājumiem). Šajā sakarā var būt nozīmīgi, vai datu subjekts vai trešās personas jau ir padarījuši datus publiski pieejamus. Faktu, ka personas dati ir publiski pieejami, var uzskatīt par faktoru, novērtējot, vai datus bija paredzēts tālāk izmantot noteiktiem nolūkiem. Šis kritērijs var aptvert arī šādus datus: privāti dokumenti, e-pasta ziņojumi, dienasgrāmatas, piezīmes e-lasītāju ierīcēs, kas aprīkotas ar piezīmju funkcijām, un ļoti personiska rakstura informācija ikdienas norišu reģistrēšanas lietotnēs.

5. Plašā mērogā apstrādāti dati: VDAR nav definēts, kas ir plaša mēroga apstrāde, taču 91. apsvērumā ir dotas dažas norādes. Jebkurā gadījumā DG29 iesaka, ka, nosakot, vai apstrādi veic plašā mērogā, jo īpaši ir jāņem vērā šādi faktori[16]:
    a) attiecīgo datu subjektu skaits — vai nu kā konkrēts skaitlis, vai kā attiecīgās populācijas daļa;
    b) datu apjoms un/vai dažādo apstrādāto datu vienumu klāsts;
    c) datu apstrādes darbības ilgums vai pastāvīgums;
    d) apstrādes darbības ģeogrāfiskais tvērums.
6. Datu kopu saskaņošana vai apkopošana — piemēram, tādu, kuras iegūst no divām vai vairākām datu apstrādes darbībām, kas veiktas citam nolūkam un/vai ko veica citi datu pārziņi, — tādējādi, ka tas pārsniedz saprātīgas datu subjekta gaidas[17].
7. Dati par neaizsargātiem datu subjektiem (75. apsvērums): šāda veida datu apstrāde ir noteikta kā kritērijs tāpēc, ka pastāv paaugstināta nelīdzsvarotība iespēju ziņā starp datu subjektiem un datu pārzini, un tas nozīmē, ka, iespējams, personas nevar bez grūtībām piekrist savu datu apstrādei vai iebilst pret to, vai īstenot savas tiesības. Neaizsargāti datu subjekti var būt bērni (var uzskatīt, ka viņi nevar apzināti vai pārdomāti iebilst pret savu datu apstrādi vai piekrist tai), darba ņēmēji, tādu neaizsargātāku iedzīvotāju slāņi, kuriem nepieciešama īpaša aizsardzība (garīgi slimas personas, patvēruma meklētāji, vecāka gadagājuma cilvēki, pacienti utt.), un jebkurā gadījumā — datu subjekti gadījumos, kad var konstatēt nelīdzsvarotību attiecībās starp datu subjekta un pārziņa stāvokli.
8. Jaunu tehnoloģisko vai organizatorisko risinājumu izmantošana vai piemērošana, piemēram, pirkstu nospiedumu un sejas atpazīšanas vienlaicīga izmantošana, lai uzlabotu fiziskās piekļuves kontroli, utt. VDAR ir skaidri noteikts (35. panta 1. punkts un 89. un 91. apsvērums), ka jaunas tehnoloģijas lietošana, kā definēts — "*saskaņā ar sasniegto tehnoloģisko zināšanu līmeni*" (91. apsvērums), var noteikt nepieciešamību veikt NIDA. Tas tā ir tāpēc, ka šādas tehnoloģijas lietošana var ietvert jaunus datu vākšanas un lietošanas veidus, kuri, iespējams, rada augstu risku attiecībā uz personu tiesībām un brīvībām. Personiska un sociāla rakstura sekas, ko rada jaunas tehnoloģijas lietošanas uzsākšana, var nebūt zināmas. NIDA palīdzēs datu pārzinim izprast un novērst šādus riskus. Piemēram, dažām "lietiskā interneta" lietotnēm varētu būt būtiska ietekme uz personu ikdienu un privātumu, tāpēc ir jāveic NIDA.
9. Ja apstrāde kā tāda "*kavē datu subjektus īstenot savas tiesības vai izmantot pakalpojumu vai līgumu*" (22. pants un 91. apsvērums). Tas ietver apstrādes darbības, kuru mērķis ir ļaut vai

[16] Sk. DG29 Pamatnostādnes par datu aizsardzības speciālistu, 16/EN WP 243.

[17] Sk. skaidrojumu DG29 Atzinumā par nolūka ierobežošanu (13/EN WP 203, 24. lpp.).

liegt datu subjektiem piekļuvi pakalpojumam vai līguma noslēgšanai, vai grozīt šādas piekļuves nosacījumus. Kā piemēru var minēt gadījumus, kad banka pārbauda savus klientus, izmantojot kredītu uzskaites datubāzi, lai izlemtu, vai piedāvāt tiem aizdevumu.

Vairumā gadījumu datu pārzinis var uzskatīt, ka tad, ja apstrāde atbilst diviem kritērijiem, attiecībā uz to ir jāveic NIDA. Kopumā DG29 uzskata, ka, jo vairāk kritērijiem apstrāde atbilst, jo lielāka ir varbūtība, ka tā radīs augstu risku datu subjektu tiesībām un brīvībām, un tāpēc ir jāveic NIDA neatkarīgi no pasākumiem, kurus pārzinis plāno veikt.

Taču dažos gadījumos **datu pārzinis var uzskatīt, ka NIDA ir jāveic attiecībā uz apstrādi, kas atbilst tikai vienam no šiem kritērijiem.**

Tālāk aprakstītie piemēri ilustrē to, kā jāizmanto minētie kritēriji, lai novērtētu, vai attiecībā uz konkrēto apstrādes darbību ir jāveic NIDA.

Apstrādes piemēri	**Iespējami nozīmīgi kritēriji**	**Vai varētu būt vajadzīgs NIDA?**
Slimnīca apstrādā savu pacientu ģenētiskos un veselības datus (slimnīcas informācijas sistēma).	- sensitīvi dati vai ļoti personiska rakstura dati; - dati par neaizsargātiem datu subjektiem; - plašā mērogā apstrādāti dati	Jā
Ierakstīšanas sistēmas lietošana, lai uzraudzītu braukšanas kultūru uz autoceļiem. Pārzinis plāno izmantot inteliģentas video analīzes sistēmu, lai identificētu automašīnas un automātiski atpazītu numura zīmes.	- sistemātiska novērošana; - tehnoloģisku vai organizatorisku risinājumu inovatīva lietošana vai piemērošana	
Uzņēmums sistemātiski novēro savu darbinieku darbības, tostarp darbinieku darbstaciju, aktivitātes tīmeklī utt.	- sistemātiska novērošana; - dati par neaizsargātiem datu subjektiem	
Publiski pieejamu sociālo plašsaziņas līdzekļu datu vākšana profilu izstrādei.	- vērtēšana vai punktu piešķiršana; - plašā mērogā apstrādāti dati; - datu kopu saskaņošana vai apkopošana; - sensitīvi dati vai ļoti personiska rakstura dati	
Iestāde, kas izstrādā valsts līmeņa kredīta reitingu vai krāpšanas gadījumu datubāzi.	- vērtēšana vai punktu piešķiršana; - tādu lēmumu automatizēta pieņemšana, kuriem ir tiesiskas vai līdzīgi būtiskas sekas; - kavē datu subjektus īstenot savas tiesības vai izmantot pakalpojumu vai līgumu; - sensitīvi dati vai ļoti personiska rakstura dati	
Pseidonimizētu sensitīvu personas datu uzglabāšana arhivēšanas nolūkā attiecībā uz neaizsargātiem datu subjektiem, kas piedalās izpētes projektos vai	- sensitīvi dati; - dati par neaizsargātiem datu subjektiem; - kavē datu subjektus īstenot savas tiesības	

Apstrādes piemēri	Iespējami nozīmīgi kritēriji	Vai varētu būt vajadzīgs NIDA?
klīniskajos pētījumos.	vai izmantot pakalpojumu vai līgumu	
"Pacientu vai klientu personas datu apstrāde, ko veic konkrēts ārsts, veselības aprūpes speciālists vai advokāts" (91. apsvērums).	- sensitīvi dati vai ļoti personiska rakstura dati; - dati par neaizsargātiem datu subjektiem	Nē
Tiešsaistes žurnāls, kas izmanto adresātu sarakstu, lai saviem abonentiem nosūtītu dienas notikumu vispārēju apskatu.	- plašā mērogā apstrādāti dati	
E-komercijas tīmekļa vietne, kurā reklamē antīku automašīnu rezerves daļas, veicot ierobežotu profilēšanu, ņemot vērā tīmekļa vietnē aplūkotās vai nopirktās preces.	- vērtēšana vai punktu piešķiršana	

Un pretēji, apstrādes darbība var atbilst minētajiem gadījumiem, bet pārzinis to tomēr var neatzīt par tādu, kas "varētu radīt augstu risku". Šādos gadījumos pārzinim ir jāpamato un jādokumentē iemesli, kāpēc netiek veikts NIDA, kā arī jāietver/jāreģistrē datu aizsardzības speciālista viedoklis.

Turklāt pārskatatbildības principa ievērošanas kontekstā katrs datu pārzinis "*reģistrē tā pakļautībā veiktās apstrādes darbības*", tostarp apstrādes nolūkus, datu kategoriju aprakstu un datu saņēmējus, un, "*ja iespējams, 32. panta 1. punktā minēto tehnisko un organizatorisko drošības pasākumu vispārēj[u] aprakst[u]*" (30. panta 1. punkts), kā arī viņam ir jānovērtē, vai varētu rasties augsts risks, pat ja viņš galu galā izlemj neveikt NIDA.

Piezīme: uzraudzības iestādēm ir jāizstrādā un jāpublisko to apstrādes darbību saraksts, attiecībā uz kurām ir jāveic NIDA, un tas jāiesniedz Eiropas Datu aizsardzības kolēģijai (EDAK) (35. panta 4. punkts)[18]. Iepriekšminētie kritēriji var palīdzēt uzraudzības iestādēm izveidot šādu sarakstu, pēc nepieciešamības laika gaitā papildinot to ar konkrētāku saturu. Piemēram, jebkāda veida biometrisko datu vai bērnu datu apstrādi arī var uzskatīt par tik būtisku, ka attiecībā uz to ir jāizveido šāds saraksts saskaņā ar 35. panta 4. punktu.

b) Kad NIDA nav jāveic? Kad apstrāde nav tāda, kas "*varētu radīt augstu risku*", vai kad jau ir veikts līdzīgs NIDA, vai kad apstrāde ir apstiprināta pirms 2018. gada maija, vai kad tās veikšanai ir juridisks pamats, vai kad tā ir iekļauta to apstrādes darbību sarakstā, attiecībā uz kurām nav jāveic NIDA.

DG29 uzskata, ka NIDA nav jāveic šādos gadījumos:

- **ja apstrāde nav tāda, kas "*varētu radīt augstu risku fizisku personu tiesībām un brīvībām*"** (35. panta 1. punkts);

[18] Šajā kontekstā, ja "*saraksts ietver apstrādes darbības, kas ir saistītas ar preču vai pakalpojumu sniegšanu datu subjektiem vai ar viņu uzvedības novērošanu vairākās dalībvalstīs, vai kas var būtiski ietekmēt personas datu brīvu apriti Savienībā, kompetentā uzraudzības iestāde .. piemēro 63. pantā paredzēto konsekvences mehānismu*" (35. panta 6. punkts).

- **ja apstrādes raksturs, apmērs, konteksts un nolūki ir ļoti līdzīgi apstrādei, attiecībā uz kuru jau ir veikts NIDA**. Šādos gadījumos var izmantot tā NIDA rezultātus, kas veikts attiecībā uz līdzīgu apstrādi (35. panta 1. punkts[19]);
- ja uzraudzības iestāde pirms 2018. gada maija ir pārbaudījusi apstrādes darbības noteiktos apstākļos, kas nav mainījušies[20] (sk. III daļas C. sadaļu);
- **ja** saskaņā ar 6. panta 1. punkta c) vai e) apakšpunktu **apstrādes darbībai ir juridisks pamats**, kas noteikts ES vai dalībvalsts tiesību aktos, ar kuriem reglamentē konkrēto apstrādes darbību, **un ja NIDA jau ir veikts** saistībā ar juridiskā pamata noteikšanu (35. panta 10. punkts)[21], izņemot, ja dalībvalsts uzskata, ka pirms apstrādes darbībām ir jāveic NIDA;
- **ja apstrādes darbība ir iekļauta izvēles sarakstā (ko izstrādā uzraudzības iestāde), kurā uzskaitītas tās apstrādes darbības**, attiecībā uz kurām nav vajadzīgs NIDA (35. panta 5. punkts). Šāds saraksts var ietvert apstrādes darbības, kas atbilst šīs iestādes nosacījumiem, kuri izvirzīti, pieņemot pamatnostādnes, konkrētus lēmumus vai atļaujas, atbilstības noteikumus utt. (piem., Francijā — atļaujas, izņēmumus, vienkāršotus noteikumus, noteikumu kopumus par atbilstību u. c.). Šādos gadījumos, un ja kompetentā iestāde veic pārskatīšanu, NIDA nav vajadzīgs, taču tikai tad, ja apstrāde precīzi ietilpst attiecīgās sarakstā minētās procedūras darbības jomā un joprojām pilnībā atbilst visām VDAR definētajām attiecīgajām prasībām.

C. <u>Kā rīkoties tādu apstrādes darbību gadījumā, kas jau tiek veiktas? Noteiktos apstākļos NIDA ir vajadzīgs.</u>

Prasība veikt NIDA ir piemērojama apstrādes darbībām, kas jau tiek veiktas, ja tās varētu radīt augstu risku fizisku personu tiesībām un brīvībām un ja ir mainījušies ar tām saistītie riski, ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus.

NIDA nav vajadzīgs attiecībā uz apstrādes darbībām, kuras ir pārbaudījusi uzraudzības iestāde vai datu aizsardzības speciālists saskaņā ar Direktīvas 95/46/EK 20. pantu un kuru īstenošanas veids kopš iepriekšējās pārbaudes veikšanas dienas nav mainījies. VDAR 171. apsvērumā minēts, ka "*saskaņā ar Direktīvu 95/46/EK pieņemtie Komisijas lēmumi un uzraudzības iestāžu izsniegtās atļaujas paliek spēkā līdz brīdim, kad tās tiek grozītas, aizstātas vai atceltas*".

Un pretēji, tas nozīmē, ka NIDA ir jāveic attiecībā uz jebkādu datu apstrādi, kuras īstenošanas apstākļi (apmērs, nolūks, savāktie personas dati, datu pārziņu vai saņēmēju identitāte, datu uzglabāšanas periods, tehniskie un organizatoriskie pasākumi utt.) ir mainījušies kopš iepriekšējās pārbaudes, ko veica uzraudzības iestāde vai datu aizsardzības speciālists, un ja šī apstrāde varētu radīt augstu risku.

[19] "*Vienā novērtējumā var pievērsties tādu līdzīgu apstrādes darbību kopumam, kurām piemīt līdzīgi augsti riski.*"

[20] "*Saskaņā ar Direktīvu 95/46/EK pieņemtie Komisijas lēmumi un uzraudzības iestāžu izsniegtās atļaujas paliek spēkā līdz brīdim, kad tās tiek grozītas, aizstātas vai atceltas*" (171. apsvērums).

[21] Ja NIDA veic tādu tiesību aktu izstrādes posmā, ar kuriem nosaka apstrādes juridisko pamatu, visticamāk, pirms apstrādes uzsākšanas būs nepieciešama tā pārskatīšana, jo pieņemtais tiesību akts var atšķirties no tā priekšlikuma tādējādi, ka tas ietekmē privātuma un datu aizsardzības jautājumus. Turklāt tiesību akta pieņemšanas laikā, iespējams, nav pieejami pietiekami tehniski dati par faktisko apstrādi, pat ja minētajam tiesību aktam ir pievienots NIDA. Šādos gadījumos pirms faktisko apstrādes darbību uzsākšanas, iespējams, joprojām ir nepieciešams veikt konkrēto NIDA.

Turklāt NIDA var būt vajadzīgs pēc tam, kad ir mainījušies apstrādes darbību rezultātā radītie riski[22], piemēram, tāpēc, ka ir ieviesta jauna tehnoloģija vai personas dati tiek izmantoti citā nolūkā. Datu apstrādes darbības var strauji attīstīties, un var parādīties jauni ievainojamības aspekti. Tādēļ jāatzīmē, ka NIDA pārskatīšana ir noderīga ne vien tāpēc, lai īstenotu nepārtrauktus uzlabojumus, bet ir būtiska arī tāpēc, lai saglabātu datu aizsardzības līmeni laika gaitā mainīgajā vidē. Iespējams, var rasties nepieciešamība veikt NIDA arī tāpēc, ka ir mainījies ar konkrēto apstrādes darbību saistītais organizatoriskais vai sociālais konteksts, jo, piemēram, nozīmīgākas ir kļuvušas noteiktu automatizētu lēmumu pieņemšanas sekas vai jaunas datu subjektu kategorijas ir kļuvušas neaizsargātas pret diskrimināciju. Katrs no šiem piemēriem var būt tas elements, kura rezultātā mainās attiecīgās apstrādes darbības radītais risks.

Un pretēji, zināmas pārmaiņas var minēto risku arī samazināt. Piemēram, apstrādes darbība var attīstīties tā, ka lēmumi vairs netiek pieņemti automatizēti vai uzraudzības darbība vairs nav sistemātiska. Tādā gadījumā veiktās riska analīzes pārskatīšanas rezultātā var konstatēt, ka NIDA vairs nav vajadzīgs.

Lai īstenotu labu praksi, **NIDA ir pastāvīgi jāpārskata un regulāri ir jāveic atkārtots novērtējums**. Tāpēc, pat ja NIDA 2018. gada 25. maijā nav jāveic, pārzinim atbilstošajā laikā būs jāveic šāds NIDA tā vispārējo pārskatatbildības pienākumu kontekstā.

D. Kā veikt NIDA?

a) Kad ir jāveic NIDA? Pirms apstrādes uzsākšanas.

NIDA ir jāveic "*pirms apstrādes*" (35. panta 1. punkts un 35. panta 10. punkts, 90. un 93. apsvērums)[23]. Tas atbilst integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma principiem (25. pants un 78. apsvērums). Ir jāuzskata, ka NIDA ir rīks, kas palīdz pieņemt lēmumus par apstrādi.

NIDA veikšana ir jāuzsāk, cik drīz vien tas ir praktiski iespējams, ņemot vērā apstrādes darbības plānu, pat ja dažas apstrādes darbības joprojām nav zināmas. NIDA aktualizēšana projekta dzīves ciklā nodrošinās to, ka ir ņemta vērā datu aizsardzība un privātums, un sekmēs tādu risinājumu izstrādi, kas veicina noteikumu ievērošanu. Tāpat var būt nepieciešams arī atkārtot atsevišķus novērtējuma soļus attīstības process gaitā, jo noteiktu tehnisko vai organizatorisko pasākumu izvēle var ietekmēt apstrādes radīto risku nopietnību vai rašanās varbūtību.

Tas, ka NIDA, iespējams, būs jāaktualizē pēc tam, kad apstrāde faktiski būs sākusies, nav pamatots iemesls, lai atliktu NIDA veikšanu vai to neveiktu vispār. NIDA ir nepārtraukts process, jo īpaši tad, ja apstrādes darbība ir dinamiska un ir pakļauta nepārtrauktām pārmaiņām. **NIDA veikšana ir nepārtraukts process, nevis vienreizējs uzdevums**.

b) Kam ir pienākums veikt NIDA? Pārzinim, sadarbojoties ar datu aizsardzības speciālistu (DAS) un apstrādātājiem.

[22] Šajā kontekstā — savāktie dati, nolūki, funkcionalitāte, apstrādātie personas dati, saņēmēji, datu kombinācijas, riski (atbalsta līdzekļi, riska avoti, potenciālā ietekme, apdraudējumi utt.), drošības pasākumi un starptautiski sūtījumi.

[23] Izņemot gadījumus, kad apstrāde jau notiek un uzraudzības iestāde to iepriekš ir pārbaudījusi, — tad NIDA ir jāveic pirms būtisku izmaiņu ieviešanas.

Par NIDA veikšanu atbild pārzinis (35. panta 2. punkts). NIDA var veikt kāda cita persona organizācijas iekšienē vai ārpus tās, taču galu galā par šā uzdevuma veikšanu joprojām atbild pārzinis.

Pārzinim noteiktos gadījumos **ir arī jālūdz padoms datu aizsardzības speciālistam (DAS)** (35. panta 2. punkts), un šis saņemtais padoms, kā arī pārziņa pieņemtie lēmumi ir jāreģistrē NIDA. DAS ir arī jāpārrauga NIDA īstenošana (39. panta 1. punkta c) apakšpunkts). Papildu norādes ir sniegtas DG29 Pamatnostādnēs par datu aizsardzības speciālistu (16/EN WP 243).

Ja apstrādi pilnībā vai daļēji veic datu apstrādātājs, **apstrādātājam ir jāpalīdz pārzinim veikt NIDA** un ir jāsniedz visa nepieciešamā informācija (saskaņā ar 28. panta 3. punkta f) apakšpunktu).

VDAR ir noteikts, ka **"*attiecīgā gadījumā pārzinis pieprasa datu subjektu vai viņu pārstāvju viedokli*" (35. panta 9. punkts).** DG29 uzskata, ka:

- šāds viedoklis jāpieprasa, izmantojot dažādus līdzekļus, atkarībā no konteksta (piem., vispārēju pētījumu saistībā ar apstrādes darbības nolūku un līdzekļiem; jautājumu personāla pārstāvjiem; parastas aptaujas, ko nosūta datu pārziņa nākamajiem klientiem), nodrošinot, ka pārzinim ir tiesisks pamats apstrādāt jebkādus personas datus saistībā ar šādiem viedokļa pieprasījumiem. Tomēr jāatzīmē, ka piekrišana apstrādei neapšaubāmi nav veids, kā pieprasīt datu subjektu viedokli;
- tad, ja datu pārziņa galīgais lēmums atšķiras no datu subjektu viedokļa, ir jādokumentē iemesli, kāpēc pārzinis uzskata, ka apstrāde ir jāturpina vai jāpārtrauc;
- pārzinim ir jādokumentē arī pamatojums tam, kāpēc netiek pieprasīts datu subjektu viedoklis, ja pārzinis izlemj, ka tas nav lietderīgi, jo, piemēram, viedokļa pieprasīšana apdraudētu uzņēmumu darījumdarbības plānu konfidencialitāti vai tas būtu nesamērīgi vai neiespējami.

Visbeidzot, laba prakse ir definēt un dokumentēt citas specifiskās lomas un pienākumus atkarībā no iekšējās politikas, procesiem un noteikumiem, piemēram:

- ja konkrētas uzņēmuma struktūras var ierosināt veikt NIDA, tad šo struktūru pienākums ir nodrošināt NIDA ievaddatus un tām ir jābūt iesaistītām NIDA validācijas procesā;
- attiecīgā gadījumā ieteicams lūgt padomu neatkarīgiem dažādu profesiju ekspertiem[24] (juristiem, IT speciālistiem, drošības speciālistiem, sociologiem, ētikas speciālistiem utt.).
- apstrādātāju uzdevumi un pienākumi ir jānosaka līgumā; NIDA ir jāveic ar apstrādātāja palīdzību, ņemot vērā apstrādes veidu un apstrādātājam pieejamo informāciju (28. panta 3. punkta f) apakšpunkts);
- informācijas drošības direktors (IDD), ja tāds ir iecelts, kā arī DAS var ierosināt pārzinim veikt NIDA par konkrētu apstrādes darbību, kā arī palīdz ieinteresētajām personām attiecībā uz metodoloģiju, palīdz izvērtēt riska novērtējuma kvalitāti un to, vai atlikušais risks ir pieņemams, kā arī attīstīt zināšanas, kas ir specifiskas datu pārziņa kontekstā;
- informācijas drošības direktors (IDD), ja tāds ir iecelts, un/vai IT nodaļas speciālisti palīdz pārzinim un var ierosināt veikt NIDA par konkrētu apstrādes darbību — atkarībā no drošības vai darbības vajadzībām.

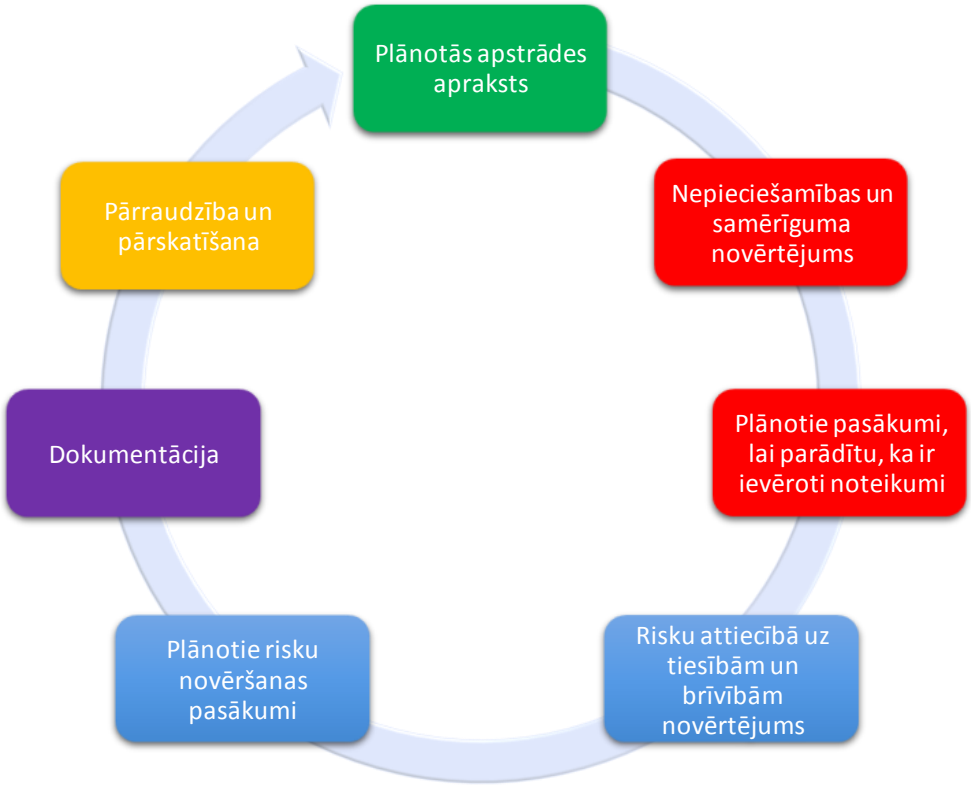
c) Kāda ir NIDA veikšanas metodoloģija? Atšķirīgas metodoloģijas, bet kopīgi kritēriji.

[24] *Ieteikumi ietekmes uz privātumu novērtējuma sistēmai Eiropas Savienībā, Nodevums D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

VDAR ir noteiktas obligātās NIDA iezīmes (35. panta 7. punkts un 84. un 90. apsvērums), proti, novērtējumā ietver vismaz:

- "*plānoto apstrādes darbību un apstrādes nolūku .. aprakstu*";
- "*novērtējumu par apstrādes darbību nepieciešamību un samērīgumu*";
- "*novērtējumu par .. riskiem datu subjektu tiesībām un brīvībām*";
- *pasākumus*,
    - "*kas paredzēti risku novēršanai*";
    - "*ar ko .. uzskatāmi parāda, ka ir ievērota šī regula*".

Tālāk dotajā attēlā ir ilustrēts NIDA veikšanas vispārējais iteratīvais process[25]:



Veicot datu apstrādes darbības ietekmes novērtējumu, ir jāņem vērā (35. panta 8. punkts) atbilstība rīcības kodeksam (40. pants). Tas var būt noderīgi, lai uzskatāmi parādītu, ka ir izvēlēti un ieviesti piemēroti pasākumi, ja rīcības kodekss ir piemērots konkrētajai apstrādes darbībai. Tāpat ir jāņem vērā sertifikāti, zīmogi un marķējumi, lai uzskatāmi parādītu, ka apstrādes darbības, ko veic pārziņi un apstrādātāji, atbilst VDAR (42. pants), kā arī saistošie uzņēmuma noteikumi (SUN).

Visas attiecīgās prasības, kas definētas VDAR, sniedz plašu vispārēju sistēmu attiecībā uz NIDA plānošanu un veikšanu. NIDA praktiskā īstenošana būs atkarīga no VDAR izvirzītajām prasībām, kuras var papildināt ar detalizētākām praktiskām norādēm. Tādējādi NIDA īstenošana ir pielāgojama. Tas nozīmē, ka pat nelielu datu pārzinis var plānot un veikt NIDA, kas atbilst to apstrādes darbībām.

[25] Jāuzsver, ka šeit atspoguļotais process ir iteratīvs, — praksē, iespējams, katru posmu izskata vairākkārt, pirms var pabeigt NIDA.

VDAR 90. apsvērumā ir aprakstīti vairāki NIDA komponenti, kas pārklājas ar labi definētiem risku pārvaldības komponentiem (piem., ISO 31000[26]). Risku pārvaldības izpratnē NIDA mērķis ir "pārvaldīt riskus" attiecībā uz fizisku personu tiesībām un brīvībām, izmantojot šādus procesus:

- konteksta noteikšana: "*ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus un riska avotus*";
- risku izvērtēšana: "*lai izvērtētu augstā riska iespējamību un nopietnību*";
- risku novēršana: "*mazina minēto risku*", "*nodrošina personas datu aizsardzību*" un "*uzskatāmi parāda, ka šīs regulas noteikumi ir ievēroti*".

Piezīme: saskaņā ar VDAR — NIDA ir rīks, ar ko pārvalda riskus attiecībā uz datu subjektu tiesībām, un tādējādi ņem vērā to perspektīvu, kā tas ir noteiktās jomās (piem., sabiedrības drošība). Turpretim citās jomās (piem., informācijas drošības jomā) riska pārvaldībā galvenā uzmanība tiek pievērsta organizācijai.

VDAR nodrošina datu pārziņiem elastīgumu, nosakot konkrēto NIDA struktūru un formu, lai ļautu to iekļaut esošajās darba praksēs. ES un pasaulē ir izveidoti vairāki atšķirīgi procesi, kuros tiek ņemti vērā 90. apsvērumā aprakstītie komponenti. Taču — neatkarīgi no tā formas — NIDA ir jābūt patiesam risku novērtējumam, kas ļauj pārziņiem veikt pasākumus, lai riskus novērstu.

Ir pieejamas dažādas metodoloģijas (sk. 1. pielikumu, kurā doti piemēri — metodoloģijas novērtējuma veikšanai par ietekmi uz datu aizsardzību un privātumu), kuras var izmantot, lai atvieglotu VDAR noteikto pamatprasību ievērošanu. Lai varētu izmantot šādas atšķirīgas pieejas, vienlaikus ļaujot pārziņiem ievērot VDAR noteikumus, ir jānosaka kopīgi kritēriji (sk. 2. pielikumu). Ar tiem ir izskaidrotas regulas pamatprasības, bet tie arī nodrošina pietiekami plašas iespējas izmantot dažādus īstenošanas veidus. Šos kritērijus var izmantot, lai parādītu, ka konkrēta NIDA metodoloģija atbilst VDAR noteiktajiem standartiem. **Datu pārzinis var izvēlēties metodoloģiju, taču tai ir jāatbilst 2. pielikumā noteiktajiem kritērijiem.**

DG29 mudina izveidot nozarei specifiskas NIDA sistēmas, jo šādos NIDA var ietvert nozarei raksturīgas zināšanas, un tas nozīmē, ka NIDA var izskatīt konkrētās apstrādes darbības īpašos aspektus (piem., attiecībā uz noteikta veida datiem, uzņēmuma līdzekļiem, potenciālo ietekmi, apdraudējumiem, pasākumiem). Tas nozīmē, ka NIDA var risināt problēmas, kas rodas konkrētajā tautsaimniecības nozarē, lietojot noteiktas tehnoloģijas vai veicot noteikta veida apstrādes darbības.

Visbeidzot, ja vajadzīgs, "*pārzinis veic pārskatu, lai novērtētu, vai apstrāde notiek saskaņā ar novērtējumu par ietekmi uz datu aizsardzību, vismaz tad, ja ir izmaiņas attiecībā uz apstrādes darbību radīto risku*" (35. panta 11. punkts[27]).

d) Vai NIDA ir jāpublicē? Nē, taču kopsavilkuma publicēšana varētu veicināt uzticēšanos, bet pilnīgs NIDA ir jāiesniedz uzraudzības iestādei iepriekšējas apspriešanās gadījumā vai tad, ja to pieprasa DAI.

[26] Riska pārvaldības procesi: saziņa un konsultācijas, konteksta noteikšana, riska izvērtēšana, novēršana, pārraudzīšana un pārskatīšana (sk. ISO 31000 priekšskatā norādītos jēdzienus un definīcijas, kā arī satura rādītāju: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

[27] VDAR 35. panta 10. punktā ir skaidri izslēgta tikai 35. panta 1.–7. punkta piemērošana.

NIDA publicēšana nav VDAR noteikta juridiska prasība, par publicēšanu izlemj pārzinis. Taču pārziņiem būtu jāapsver iespēja publicēt vismaz atsevišķas sava NIDA daļas, piemēram, kopsavilkumu vai secinājumus.

Šāda procesa nolūks būtu sekmēt uzticēšanos pārziņa apstrādes darbībām un uzskatāmi parādīt pārskatatbildību un caurskatāmību. NIDA publicēšana ir sevišķi laba prakse gadījumos, kad apstrādes darbības ietekmē sabiedrības locekļus. Tā varētu būt īpaši laba prakse tad, ja NIDA veic publiskā sektora iestāde.

Publicētajā NIDA nav jāietver viss novērtējums, jo īpaši tad, ja NIDA varētu būt norādīta specifiska informācija attiecībā uz drošības riskiem datu pārzinim vai izpausti komercnoslēpumi vai sensitīva komercinformācija. Šādos apstākļos publicētajā versijā var ietvert tikai NIDA galveno konstatējumu kopsavilkumu vai pat tikai norādi, ka ir veikts NIDA.

Turklāt tad, ja, veicot NIDA, ir atklāti augsti atlikušie riski, datu pārzinim būs jāpieprasa uzraudzības iestādei iepriekšēja apspriešanās par apstrādi (36. panta 1. punkts). Šā procesa ietvaros ir jāiesniedz NIDA pilns saturs (36. panta 3. punkta e) apakšpunkts). Uzraudzības iestāde var sniegt padomu[28] un neapdraudēs komercnoslēpumus, kā arī neizpaudīs drošības ievainojamību, ievērojot principus, kas piemērojami katrā dalībvalstī attiecībā uz publisku piekļuvi oficiāliem dokumentiem.

E. <u>Kad ir jāapspriežas ar uzraudzības iestādi? Ja ir augsti atlikušie riski.</u>

Kā skaidrots iepriekš:

- NIDA ir jāveic tikai tad, ja apstrādes darbība "*varētu radīt augstu risku fizisku personu tiesībām un brīvībām*" (35. panta 1. punkts, sk. III daļas B. sadaļas a) apakšpunktu). Piemēram, veselības datu apstrāde plašā mērogā ir uzskatāma par tādu, kas varētu radīt augstu risku, un tāpēc attiecībā uz to ir vajadzīgs NIDA;
- datu pārziņa pienākums ir izvērtēt riskus datu subjektu tiesībām un brīvībām un noteikt pasākumus[29], kuru mērķis ir samazināt minētos riskus līdz pieņemamam līmenim un uzskatāmi parādīt, ka ir ievēroti VDAR noteikumi (35. panta 7. punkts, sk. III daļas C. sadaļas c) apakšpunktu). Kā piemēru papildus esošām politikām (paziņošana, piekrišana, piekļuves tiesības, tiesības iebilst utt.) var minēt atbilstošu tehnisko un organizatorisko drošības pasākumu izmantošanu, uzglabājot personas datus klēpjdatoros (efektīva pilnīga diska šifrēšana, spēcīga taustiņu pārvaldība, atbilstoša piekļuves kontrole, nodrošinātas dublējumkopijas utt.).

Iepriekšminētajā piemērā par klēpjdatoru —, ja var uzskatīt, ka datu pārzinis ir pietiekami samazinājis riskus, un ja ir ņemts vērā 84. un 94. apsvērums un 36. panta 1. punkts, apstrādi var turpināt, neapspriežoties ar uzraudzības iestādi. Datu pārzinim ar uzraudzības iestādi jāapspriežas tad, ja tas noteiktos riskus nevar pietiekami samazināt (t. i., ja atlikušie riski vēl aizvien ir augsti).

Nepieņemami augsta atlikušā riska piemērs ir gadījumi, kad datu subjektiem var rasties būtiskas vai pat neatgriezeniskas sekas, kuras tie, iespējams, nevar pārvarēt (piem., pretlikumīga piekļuve datiem, kā rezultātā rodas apdraudējums datu subjektu dzīvei, ir iespējama atlaišana no darba, rodas finanšu

[28] Rakstiskas norādes pārzinim ir nepieciešamas tikai tad, ja uzraudzības iestāde uzskata, ka plānotā apstrāde neatbilst VDAR saskaņā ar tās 36. panta 2. punktu.

[29] Tostarp, ņemot vērā EDAK un uzraudzības iestāžu izdotās norādes, kā arī tehnikas līmeni un īstenošanas izmaksas, kā noteikts 35. panta 1. punktā.

apdraudējums), un/vai kad šķiet pašsaprotami, ka risks radīsies (piem., ja nav iespējams samazināt to cilvēku skaitu, kuri piekļūst datiem to kopīgošanas, lietojuma vai izplatīšanas veida dēļ, vai ja nav novērsta labi zināma ievainojamība).

Ja datu pārzinis nevar piemeklēt atbilstošus pasākumus, lai samazinātu noteiktos riskus līdz pieņemamam līmenim (t. i., ja atlikušie riski vēl aizvien ir augsti), ir jāapspriežas ar uzraudzības iestādi[30].

Turklāt pārzinim būs jāapspriežas ar uzraudzības iestādi, ja dalībvalsts tiesību aktos ir noteikts, ka pārziņiem ir jāapspriežas ar uzraudzības iestādi un jāsaņem no tās iepriekšēja atļauja saistībā ar apstrādi, ko veic pārzinis, lai izpildītu sabiedrības interesēs īstenojamu uzdevumu, tostarp, kad minēto apstrādi veic saistībā ar sociālo aizsardzību un sabiedrības veselību (36. panta 5. punkts).

Taču jānorāda, ka neatkarīgi no tā, vai ir nepieciešama apspriešanās ar uzraudzības iestādi atkarībā no atlikušā riska līmeņa, paliek spēkā pienākums reģistrēt NIDA un noteiktā laikā to aktualizēt.

IV. Secinājumi un ieteikumi

NIDA ir noderīgs veids, kā datu pārziņi var īstenot datu apstrādes sistēmas, kas atbilst VDAR, un attiecībā uz noteiktiem apstrādes darbību veidiem to veikšana var būt obligāta. Tie ir pielāgojami un var būt dažādās formās, taču VDAR nosaka pamatprasības, kas jāievēro, lai NIDA būtu efektīvs. Datu pārziņiem ir jāuztver NIDA veikšana kā noderīga un pozitīva darbība, kas palīdz nodrošināt atbilstību tiesību aktiem.

VDAR 24. panta 1. punktā ir noteikta pārziņa pamata atbildība attiecībā uz VDAR noteikumu ievērošanu: "*Ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai nodrošinātu un spētu uzskatāmi parādīt, ka apstrāde notiek saskaņā ar šo regulu. Ja nepieciešams, minētos pasākumus pārskata un atjaunina*."

NIDA ir būtisks elements, nodrošinot atbilstību minētajai regulai, ja ir plānotas vai notiek augsta riska datu apstrādes darbības. Tas nozīmē, ka datu pārziņiem ir jāizmanto šajā dokumentā izklāstītie kritēriji, lai noskaidrotu, vai ir jāveic NIDA. Īstenojot datu pārziņa iekšējo politiku, šo sarakstu varētu paplašināt, pārsniedzot VDAR noteiktās juridiskās prasības. Tā rezultātā palielinātos datu subjektu un citu datu pārziņu uzticēšanās un paļāvība.

Ja ir plānota iespējama augsta riska datu apstrāde, datu pārziņa pienākums ir:

- izvēlēties NIDA metodoloģiju (1. pielikumā ir doti piemēri), kas apmierina 2. pielikumā norādītos kritērijus, vai precizēt un īstenot sistemātisku NIDA procesu, kas:
  - atbilst 2. pielikumā norādītajiem kritērijiem;
  - ir iekļauts esošajos plānošanas, izstrādes, izmaiņu, riska un darbības pārskatīšanas procesos saskaņā ar iekšējiem procesiem, kontekstu un kultūru;

[30] Piezīme: "*personas datu pseidonimizācija un šifrēšana*" (kā arī datu minimizēšana, uzraudzības mehānismi utt.) ne vienmēr ir piemēroti pasākumi. Tie ir tikai piemēri. Piemēroti pasākumi ir atkarīgi no konteksta un riskiem, kas ir specifiski saistībā ar konkrētajām apstrādes darbībām.

    - ietver attiecīgās ieinteresētās personas un skaidri nosaka to pienākumus (pārzinis, DAS, datu subjekti vai to pārstāvji, uzņēmumi, tehniskie dienesti, apstrādātāji, informācijas drošības direktors utt.);
- kad nepieciešams, iesniegt NIDA ziņojumu kompetentajai uzraudzības iestādei;
- apspriesties ar uzraudzības iestādi, ja nav izdevies noteikt pietiekamus pasākumus, lai mazinātu augstos riskus;
- regulāri pārskatīt NIDA un apstrādes procesu, kas tajā novērtēts, vismaz tad, ja ir notikušas izmaiņas saistībā ar apstrādes darbības radīto risku;
- dokumentēt pieņemtos lēmumus.

1. pielikums. Esošu ES NIDA sistēmu piemēri

VDAR nav precizēts, kāds NIDA process ir jāievēro, bet gan ir ļauts datu pārziņiem ieviest sistēmu, kas papildina to esošās darba prakses, ja tiek ņemti vērā 35. panta 7. punktā aprakstītie komponenti. Šāda sistēma var būt pielāgota datu pārziņa vajadzībām vai var būt kopīga visā konkrētajā nozarē. Tālāk uzskaitītas iepriekš publicētas sistēmas, ko izstrādājušas ES DAI, un ES nozarēm specifiskas sistēmas (saraksts nav izsmeļošs).

Vispārēju sistēmu piemēri ES:

- DE: Standarta datu aizsardzības modelis, 1.0. versija — izmēģinājuma versija, 2016.[31]. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos* (*AGPD*), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Ietekmes uz privātumu novērtējums (IPN), Commission nationale de l'informatique et des libertés* (*CNIL*), 2015. https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice* [Rīcības kodekss ietekmes uz privātumu novērtējumu veikšanai], Informācijas komisāra birojs (*ICO*), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Nozarēm specifisku sistēmu piemēri ES:

- Novērtējumu par ietekmi uz privātumu un datu aizsardzību sistēma *RFID* lietojumiem[32]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Datu aizsardzības ietekmējuma novērtējuma veidlapa viedajiem tīkliem un viedās uzskaites sistēmām[33] http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Starptautisks standarts sniegs norādes arī par metodoloģijām, kuras izmanto, lai veiktu NIDA (ISO/IEC 29134[34]).

---

[31] Vienbalsīgi un pozitīvi atzīts (ar Bavārijas atturēšanos) 92. Federācijas un federālo zemju neatkarīgo datu aizsardzības iestāžu konferencē Kīlungsbornā 2016. gada 9. un 10. novembrī.

[32] Sk. arī:

- Komisijas 2009. gada 12. maija Ieteikumu par privātuma un datu aizsardzības principu īstenošanu saistībā ar radiofrekvenciālās identificēšanas lietojumiem; https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Atzinums 9/2011 attiecībā uz pārskatīto nozares priekšlikumu par privātuma un datu aizsardzības ietekmes novērtējuma sistēmu *RFID* lietojumiem; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_lv.pdf

[33] Sk. arī Atzinumu 07/2013 par Datu aizsardzības ietekmes novērtējuma veidlapu viedajiem tīkliem un viedajām mērierīču sistēmām ("DAIN veidlapu"), ko sagatavojusi Komisijas Viedo tīklu darba grupas 2. ekspertu grupa; http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_lv.pdf

2. pielikums. Kritēriji, kas jāievēro, lai NIDA būtu pieņemams

DG29 piedāvā šādus kritērijus, kurus datu pārziņi var izmantot, lai novērtētu, vai NIDA vai tā veikšanas metodoloģija ir pietiekami visaptveroša, lai nodrošinātu VDAR noteikumu ievērošanu:

- ☐ ir sniegts sistemātisks apstrādes apraksts (35. panta 7. punkta a) apakšpunkts):
  - ☐ ir ņemts vērā apstrādes raksturs, apmērs, konteksts un nolūki (90. apsvērums);
  - ☐ ir norādīti personas dati, saņēmēji un laikposms, cik ilgi tiks uzglabāti personas dati;
  - ☐ ir sniegts apstrādes darbības funkcionāls apraksts;
  - ☐ ir norādīti līdzekļi, uz kuriem balstās personas datu apstrāde (aparatūra, programmatūra, tīkli, personas, papīra formāts vai papīra formāta pārsūtīšanas kanāli);
  - ☐ ir ņemta vērā atbilstība apstiprinātiem rīcības kodeksiem (35. panta 8. punkts);
- ☐ ir novērtēta nepieciešamība un samērīgums (35. panta 7. punkta b) apakšpunkts):
  - ☐ ir noteikti pasākumi, kas paredzēti, lai nodrošinātu atbilstību VDAR regulai (35. panta 7. punkta d) apakšpunkts un 90. apsvērums), ņemot vērā:
    - ☐ pasākumus, kas veicina samērīgumu un apstrādes nepieciešamību, uz šāda pamata:
      - ☐ konkrēti, skaidri un leģitīmi nolūki (5. panta 1. punkta b) apakšpunkts);
      - ☐ apstrādes likumīgums (6. pants);
      - ☐ adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams datu apstrādes nolūkos (5. panta 1. punkta c) apakšpunkts);
      - ☐ ierobežots uzglabāšanas ilgums (5. panta 1. punkta e) apakšpunkts);
    - ☐ pasākumus, kas sekmē datu subjektu tiesību ievērošanu:
      - ☐ datu subjektam sniegtā informācija (12., 13. un 14. pants);
      - ☐ piekļuves tiesības un tiesības uz datu pārnesamību (15. un 20. pants);
      - ☐ tiesības labot un dzēst (16., 17. un 19. pants);
      - ☐ tiesības iebilst un ierobežot apstrādi (18., 19. un 21. pants);
      - ☐ attiecības ar apstrādātājiem (28. pants);
      - ☐ drošības pasākumi attiecībā uz starptautisku nosūtīšanu (V nodaļa);
      - ☐ iepriekšēja apspriešanās (36. pants);
- ☐ ir pārvaldīti riski datu subjektu tiesībām un brīvībām (35. panta 7. punkta c) apakšpunkts):
  - ☐ ir izvērtēti minēto risku avoti, raksturs, specifika un nopietnība (sk. 84. apsvērumu) vai, konkrētāk, attiecībā uz katru risku (pretlikumīga piekļuve, nevēlamas izmaiņas vai datu izzušana) no datu subjektu viedokļa:
    - ☐ ir ņemti vērā risku avoti (90. apsvērums);
    - ☐ ir identificēta potenciāla ietekme uz datu subjektu tiesībām un brīvībām gadījumos, kad ir notikusi pretlikumīga piekļuve, nevēlamas izmaiņas vai datu izzušana;
    - ☐ ir identificēti apdraudējumi, kas varētu izraisīt pretlikumīgu piekļuvi, nevēlamas izmaiņas un datu izzušanu;
    - ☐ ir noteikta iespējamība un nopietnība (90. apsvērums);
  - ☐ ir noteikti pasākumi, kas paredzēti, lai novērstu minētos riskus (35. panta 7. punkta d) apakšpunkts un 90. apsvērums);
- ☐ ir iesaistītas ieinteresētās personas:
  - ☐ ir lūgts DAS padoms (35. panta 2. punkts);
  - ☐ attiecīgā gadījumā ir pieprasīts datu subjektu vai viņu pārstāvju viedoklis (35. panta 9. punkts).

[34] ISO/IEC 29134 (projekts) "Informācijas tehnoloģija. Drošības metodes. Ietekmes uz privātumu novērtējums. Pamatnostādnes", Starptautiskā Standartizācijas organizācija (*ISO*).