Datu valsts inspekcija

NOVĒRTĒJUMS PAR IETEKMI UZ DATU AIZSARDZĪBU

VADLĪNIJAS

2025

Satura rādītājs

Izmantotie termini

1. **Anonimizācija** – process, kurā personas dati tiek pārveidoti tā, ka konkrētā datu subjekta identificēšana nav iespējama, un šo procesu nevar atsaukt.
2. **Apdraudējums** – potenciāls notikums vai faktors, kas var radīt kaitējumu personas datu drošībai.
3. **Datu apstrādes dzīvescikls** – strukturēts process, kas ietver datu vākšanu, apstrādi, analīzi, uzglabāšanu un dzēšanu.
4. **Datu kategorijas** – personas dati, kuri tiek apstrādāti, piemēram, vispārpieejami personas dati, sensitīvi dati, finanšu informācija.
5. **Datu subjekts** – fiziska persona, kuras personas dati tiek apstrādāti.
6. **Datu šifrēšana** – tehniska metode, kas pārveido personas datus tā, lai tie būtu pieejami tikai pilnvarotiem lietotājiem, izmantojot atbilstošas atšifrēšanas atslēgas.
7. **EDAK** – Eiropas datu aizsardzības kolēģija.
8. **Informācijas sistēma/datubāze** – struktūra vai platforma, kas ļauj apkopot, uzglabāt un pārvaldīt datus, nodrošinot piekļuvi un apstrādes iespējas.
9. **Integritāte** – nodrošinājums, ka personas dati ir precīzi un netiek neatļauti mainīti.
10. **Konfidencialitāte** – nodrošinājums, ka piekļuve personas datiem ir tikai pilnvarotām personām.
11. **Metodoloģija** – sistemātiska pieeja, principi un metodes, kas tiek izmantotas, lai plānotu, organizētu un īstenotu kādu uzdevumu, pētījumu vai projektu. Tā nodrošina strukturētu procesu, lai sasniegtu noteiktos mērķus.
12. **Neautorizēta trešā persona** – persona, kurai nav pilnvarojuma piekļūt un/vai rīkoties ar personas datiem.
13. **Novērtējums par ietekmi uz datu aizsardzību** (vadlīniju kontekstā NIDA) – process, kas identificē un novērtē personas datu apstrādes riskus, izstrādājot pasākumus šo risku mazināšanai.
14. **NIDA tvērums** – personas datu apstrādes darbību kopums, ko aptver konkrētais ietekmes novērtējums.
15. **Organizācija** – vadlīniju kontekstā pārzinis Datu regulas 4. panta 7. punkta izpratnē.
16. **Organizācijas datu apstrādes sistēma** – organizācijas iekšējā sistēma, kas pārvalda personas datu apstrādi.
17. **Organizācijas datu aizsardzības sistēma** – pasākumu kopums un procesi, kurus organizācija izveido, lai aizsargātu personas datus un nodrošinātu atbilstību Datu regulai.
18. **Personas datu aizsardzības pārkāpums** – incidents, kura rezultātā tiek pārkāpta personas datu konfidencialitāte, integritāte vai pieejamība.
19. **Personas datu apstrāde** – jebkāda darbība vai darbību kopums, ko veic ar personas datiem, piemēram, vākšana, reģistrēšana, organizēšana, glabāšana, pārveidošana, meklēšana, izpaušana, dzēšana vai iznīcināšana.
20. **Pieejamība** – nodrošinājums, ka personas dati ir pieejami, kad tie nepieciešami apstrādei.
21. **Pirms-NIDA** – vadlīniju kontekstā – posms, kurā tiek izvērtēta nepieciešamība veikt NIDA, pamatojoties uz plānoto datu apstrādes novērtējumu, atbilstoši kritērijiem.
22. **Pseidonimizācija** – personas datu apstrāde, kas veikta tā, ka tos vairs nevar attiecināt uz konkrētu fizisku personu bez papildu informācijas izmantošanas, kurai piekļuve ir tikai īpaši autorizētām personām.
23. **Risks fiziskas personas tiesībām un brīvībām** – iespēja, ka realizēsies potenciāls apdraudējums fiziskas personas tiesībām uz datu aizsardzību vai citu pamattiesību pārkāpšanai, kas izriet no datu apstrādes.
24. **Riska avots** – personu, sistēmu vai notikumu kopums, kas rada potenciālu apdraudējumu personas datiem.
25. **Riska cēlonis** – faktori vai apstākļi, kas rada konkrēto risku.
26. **Riska iestāšanās varbūtība** (riska iespējamība) – cik ticams ir, ka risks varētu materializēties (piem., ļoti augsta, augsta, vidēja, zema).
27. **Riska faktors** – apstākļi vai situācijas, kas var pastiprināt riska sekas.
28. **Riska ietekmes līmenis** – riska potenciālās sekas uz fiziskas personas tiesībām un brīvībām (piem., ļoti augsts, augsts, vidējs, zems).
29. **Riska mijiedarbība** – savstarpēja ietekme starp dažādiem riskiem, kas var pastiprināt vai mainīt to ietekmi.
30. **Riska sekas** – rezultāti vai ietekme, kas rodas riska materializēšanās gadījumā.
31. **Trešā valsts** – valsts, kas nav Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalsts.

32. **Uzraudzības iestāde** (vadlīniju kontekstā Datu valsts inspekcija; tekstā – Inspekcija) – neatkarīga publiska iestāde, kas atbild par Datu regulas īstenošanas uzraudzību un atbilstības nodrošināšanu.

Apzīmējumi

Ņem vērā! – Pievērsiet uzmanību norādītajai informācijai

Piemēram, – Ilustratīvs piemērs, lai skaidrotu vadlīnijās ietverto informāciju

Ievads

Personas datu aizsardzības ietekmes novērtējums (NIDA) ir process, kas palīdz identificēt un pārvaldīt riskus, kas var rasties fiziskas personas tiesībām un brīvībām, apstrādājot personas datus. Tas apvieno risku identificēšanu, to ietekmes novērtēšanu un piemērotu pasākumu plānošanu risku mazināšanai. Lai gan NIDA veikšana noteiktos gadījumos ir obligāta saskaņā ar Datu regulas prasībām[1], tas ir arī efektīvs instruments, kuru organizācijas var izmantot, lai uzlabotu savu riska pārvaldības praksi.

Nepieciešamība veikt riska izvērtējumu, apstrādājot personas datus, nav jauna prasība datu aizsardzībā. Jau 2014. gadā 29. panta darba grupa izdeva paziņojumu "Paziņojums par uz risku balstītas pieejas nozīmi datu aizsardzības tiesiskajā regulējumā". Minētajā paziņojumā risks tiesībām un brīvībām galvenokārt attiecas uz tiesībām uz datu aizsardzību un privātumu, tomēr ir skaidri minētas arī citas pamattiesības kā vārda un domas brīvība, pārvietošanās brīvība, diskriminācijas aizliegums, apziņas un reliģijas brīvība u. c. Paziņojumā bija norādīts, ka veicot novērtējumu bija jāņem vērā ietekme un tās iespējamība gan uz attiecīgo personu, gan uz sabiedrību kopumā[2].

Šīs vadlīnijas ir izstrādātas, lai palīdzētu organizācijām veiksmīgi izprast un īstenot NIDA, nodrošinot praktiskus ieteikumus un strukturētu pieeju. Vadlīnijas sniedz skaidrojumu par gadījumiem, kuros NIDA ir jāveic, un piedāvā instrumentus, kas palīdz izvērtēt, vai organizācijai ir pietiekama kapacitāte un zināšanas veikt NIDA patstāvīgi vai arī nepieciešams ārējais atbalsts.

Vadlīniju struktūra:

- Sagatavošanās posms jeb datu apstrādes likumīguma izvērtējums: šajā posmā tiek noteikts, vai plānotā datu apstrāde ir likumīga. Ja apstrāde neatbilst Datu regulas prasībām, turpmākās darbības nav jāveic.
- Pirms-NIDA posms: šajā posmā tiek novērtēta nepieciešamība veikt NIDA. Ja konstatēts, ka apstrāde nerada augstu risku fiziskas personas tiesībām un brīvībām, tālāka NIDA veikšana nav nepieciešama.
- NIDA veikšanas process: šī nodaļa ietver skaidrojumu par NIDA izstrādi, sniedzot ieteikumus metodoloģijas izvēlei un riska novērtēšanai.
- Praktiskie ieteikumi NIDA izstrādei: šī nodaļa piedāvā konkrētus risinājumus, lai efektīvi veiktu NIDA un integrētu to organizācijas darbības procesos.

Vadlīnijas strukturētas tā, lai tās būtu viegli pielāgojamas konkrētām situācijām. Organizācija var izvēlēties koncentrēties uz atsevišķām nodaļām, atkarībā no nepieciešamības un esošā apstrādes posma. Pilnvērtīga NIDA veikšana tomēr ietver visus posmus, kas aprakstīti vadlīnijās un veidlapu pielikumos.

Svarīgākie apsvērumi:

- NIDA ir ne tikai vienreizējs pasākums, bet gan, ņemot vērā apstrādes darbību vai organizācijas darbības jomas izmaiņas, nepārtraukts process, kas jāuztur visa datu apstrādes cikla laikā;
- Vadlīnijas piedāvā gan teorētisku skaidrojumu, gan praktiskus soļus, taču organizācijai jāpielāgo ieteikumi konkrētās apstrādes loģikai un specifikai;
- NIDA metodoloģija, lai gan ieteikta, nav juridiski saistoša. Organizācijām ir tiesības izvēlēties alternatīvas pieejas, ja tās nodrošina Datu regulā noteikto rezultātu sasniegšanu.

Šīs vadlīnijas palīdzēs organizācijām saprast, kā izmantot NIDA kā efektīvu instrumentu risku pārvaldībā, vienlaikus ievērojot datu aizsardzības pamatprincipus un veicinot atbilstību normatīvajām prasībām.

[1] Datu regulas 35. pants.
[2] 29. panta darba grupas viedoklis. Pieejams angļu valodā: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

I nodaļa "Sagatavošanās"
Plānotās datu apstrādes nolūks un likumība

[1] Organizācijai, izvērtējot nepieciešamību veikt fizisku personu datu apstrādi, lai nodrošinātu produkta vai pakalpojuma pieejamību klientiem, ir jāpārliecinās, ka plānotā datu apstrāde ir likumīga un atbilst Datu regulas prasībām. Likumības un citu datu aizsardzības principu izvērtēšana ir jāveic visos gadījumos, pat, ja plānotās datu apstrādes raksturs, apjoms, konteksts un nolūks nerada augstu risku fizisku personu tiesībām un brīvībām. Tas, vai plānotajai apstrādei veicams NIDA un kā risku fiziskām personām novērtēšana un mazināšana ietekmēs kopējo atbilstību Datu regulai, ir vērtējams tikai pēc tam, kad organizācija ir secinājusi, ka plānotā personas datu apstrāde ir likumīga.

Ņem vērā! Vadlīnijās ietverts tikai tādu datu apstrādes likumības aspektu novērtēšana, kuriem, Inspekcijas ieskatā, ir tieša saikne ar NIDA. Zemāk sniegtais plānotās datu apstrādes nolūka un likumības izvērtējums ir ilustratīvs un nav uzskatāms par izsmeļošu. Tas arī neizslēdz, ka ar NIDA veikšanu var saistīt arī citus likumības novērtēšanas aspektus, kuri šajās vadlīnijās nav apskatīti.

[2] Plānotās datu apstrādes likumības analīze sākas ar datu apstrādes nolūka noteikšanu un izvērtējumu, kādi tieši personas dati būs nepieciešami konkrētā nolūka sasniegšanai. Datu apstrādes atbilstības un likumības novērtējums ir veicams visām datu apstrādes dzīvescikla[3] apraksta laikā noteiktajām darbībām, kā arī par visām personas datu kategorijām[4], ko organizācija plāno apstrādāt konkrētās datu apstrādes kontekstā.

Ņem vērā! Datu regula noteic, ka plānotā personas datu apstrāde būs likumīga tikai tajos gadījumos, ja tai pastāv vismaz viens Datu regulas 6., 9. vai 10. pantā norādītais tiesiskais pamats un/vai izņēmums. Papildus jāņem vērā, ja datu apstrāde balstās uz personas piekrišanu – jāievēro Datu regulas 7. pants, bērnu piekrišanai attiecībā uz informācijas sabiedrības pakalpojumiem – Datu regulas 8. pants un Fizisko personu datu apstrādes likuma 33. pants, kā arī, ja personas datus plānots nosūtīt uz trešo valsti vai starptautisku organizāciju – jāievēro Datu regulas V nodaļā noteiktais.

1. Datu apstrādes principi

[3] Datu apstrādes principu ievērošana ir neatņemami saistīta ar plānoto datu apstrādes nolūku un datu kategorijām. Jāņem vērā, ka paaugstinātus riskus un ietekmi uz fiziskas personas tiesībām un brīvībām var radīt tieši tas, ka organizācija nespēj nodrošināt atbilstību kādam personas datu apstrādes principam.

[4] Paaugstinātu risku un ietekmi uz fiziskas personas tiesībām un brīvībām lielākoties radīs "integritātes un konfidencialitātes" principa neievērošana. Vēl augstāks risks radīsies, ja organizācija neievēros vairākus principus vienlaikus, piemēram, "precizitāti", "datu minimizēšanu" un "glabāšanas ierobežojumu".

Piemēram, veselības aprūpes klīnika izmanto tiešsaistes pacientu pārvaldības sistēmu, lai uzglabātu un pārvaldītu ziņas par pacientu (tai skaitā, par pacientu ģimenes stāvokli, nodarbošanos un ar veselības aprūpes klīnikas pakalpojumiem nesaistītu veselības vēsturi), vizītes laikus un norēķinu informāciju. Veselības aprūpes klīnikas ieviestā datu apstrādes sistēma (datu kategorijas, apjoms un tehniskie rīki) ir izveidota 2013. gadā un tā pēdējo 10 gadu laikā nav izvērtēta un/vai atjaunota. Ikviens veselības aprūpes klīnikas darbinieks var piekļūt klientu medicīnas datiem. Klientu dati netiek regulāri atjaunināti vai pārbaudīti. Veselības aprūpes klīnika nav noteikusi, cik ilgi klientu dati tiek glabāti, kā arī tie nav dzēsti kopš 2013. gada.

[3] Skatīt IV nodaļas "NIDA AIZPILDĪŠANA" sadaļu "Datu apstrādes dzīves cikls".
[4] Skatīt IV nodaļas "NIDA AIZPILDĪŠANA" sadaļu "Datu kategorijas".

Šajā situācijā, nenodrošinot [4] punktā norādītos personas datu aizsardzības principus, veselības aprūpes iestāde rada vairākus riskus to klientu tiesībām un brīvībām, piemēram:

- Nesankcionēta piekļuve veselības datiem var izraisīt identitātes zādzību, diskrimināciju vai emocionālu kaitējumu;
- Neprecīzi dati var izraisīt, ka klienta medicīnas dati var tikt nosūtīti citai personai vai arī savlaicīgi netiek sniegta ar veselības aizsardzību saistīta informācija, tādējādi liedzot klientam saņemt nepieciešamo medicīnisko palīdzību;
- Pārmērīgais datu apjoms palielina iespējamo kaitējumu, ko nesankcionētas piekļuves gadījumā klientam vai tam piesaistītam radiniekam var nodarīt neautorizēta trešā persona;
- Ilgstoša datu saglabāšana palielina risku, ka datus kādā datu dzīvescikla posmā neautorizēti apstrādās iekšēji vai ārēji spēlētāji;
- Datu aizsardzības principu neievērošana kopumā pārkāpj klienta tiesības uz datu aizsardzību, kas ir Datu regulas "kodols". Līdz ar to principu neievērošana pārkāpj ietvaru, kādā pārzinis var rīkoties.

[5] Formāla pieeja principu izvērtējumam (aprakstam par atbilstību principiem), piemēram, tikai konstatējums, ka tiek izpildītas prasības, neveicot analīzi, kā tieši prasības tiek izpildītas, nav uzskatāma par atbilstošu Datu regulai, jo īpaši, ja plānotajai datu apstrādei ir nepieciešams veikt NIDA. Personas datu apstrādes darbību un nolūku analīze ir NIDA elements[5].

[6] Atbilstība datu apstrādes principiem jānovērtē un jāanalizē visa datu apstrādes dzīvescikla laikā, lai nodrošinātu, ka nav kāds apstrādes starpposms, kurā datu apstrāde kādam no principiem tomēr neatbilst. Ja tiek identificēts, ka apstrādes ietvaros var rasties situācijas, kad ir apšaubāmas iespējas nodrošināt pilnīgu atbilstību kādam no datu aizsardzības principiem, tas ir uzskatāms par risku paaugstinošu faktoru fiziskai personai, un šādās situācijās ir ļoti ticama nepieciešamība veikt NIDA.

1.1. "Likumīgums, godprātība un pārredzamība"

[7] Sākotnēji organizācijai ir nepieciešams noteikt, kāds būs plānotās datu apstrādes likumīgais jeb tiesiskais pamats atbilstoši Datu regulai[6]. Tiesiskā pamata analīze nevar būt formāla, bet tā jāveic izvērsti un rūpīgi novērtējot piemērojamo tiesisko pamatu. Tas ļaus efektīvāk pārvaldīt izmaiņas, ja gadījumā datu apstrādes tiesiskais pamats mainās. Skaidra un izvērsta tiesiskā pamata piemērošanas aprakstīšana arī ļaus identificēt ieviešamos papildu pasākumus, ja tiks konstatēts, ka pastāv ierobežojumi, kas saistīti ar tiesiskā pamata nodrošināšanu[7].

Piemēram, ja datu apstrādes nolūks nav skaidri definēts vai nav pietiekami pamatots, pastāv risks, ka tiesiskais pamats, piemēram, leģitīmās intereses vai piekrišana, netiks uzskatīts par atbilstošu. Vai arī, ja izvēlētais tiesiskais pamats ir piekrišana, tas var pēc būtības būt nepiemērots plānotajai apstrādes darbībai, līdz ar to tas būs neatbilstošs Datu regulas prasībām. Organizācijai ir nepieciešams skaidri un detalizēti formulēt apstrādes nolūkus un izvēlēties atbilstošāko tiesisko pamatu.

[8] Šī principa piemērošana saistīta arī ar pārredzamības[8] nodrošināšanu. Tas nozīmē, ka organizācijai ir nepieciešams izvērsti analizēt, kā tiks nodrošināta datu subjektu informēšana par visām plānotajām datu apstrādes darbībām datu apstrādes dzīvesciklā.

[9] Godprātības elements paredz, ka plānotās apstrādes darbības netiks veiktas nelikumīga nolūka sasniegšanai, kā arī fiziska persona netiks maldināta attiecībā uz plānoto tās personas datu apstrādi.

[5] Datu regulas 35. panta 7. punkta a) apakšpunkts Novērtējumā ietver vismaz plānoto apstrādes darbību un apstrādes nolūku, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistemātisku aprakstu.
[6] Datu regulas 6., 7., 9., 10. pants un V nodaļa "Personas datu nosūtīšana uz trešām valstīm vai starptautiskām organizācijām"
[7] Ierobežojumi, kas saistīti ar tiesiskā pamata nodrošināšanu, attiecas uz apstākļiem, kas varētu traucēt efektīvi piemērot tiesisko pamatu personas datu apstrādei saskaņā ar Datu regulu. Šie ierobežojumi var rasties, ja tiesiskais pamats neatbilst noteiktiem kritērijiem vai nav pietiekami skaidri definēts, lai garantētu atbilstību tiesību aktiem un datu subjekta tiesību aizsardzību.
[8] Datu regulas 12., 13. un 14. pants

Tas nozīmē, ka organizācijai ir jāņem vērā arī fiziskās personas saprātīgās gaidas[9] un principa pārkāpums būs datu apstrāde veidā, kas, vadoties no veselā saprāta viedokļa, ir bijusi fiziskai personai negaidīta.

[10] Ja, analizējot principa "Likumīgums, godprātība un pārredzamība" piemērošanu, secināms, ka apstrādei nav iespējams nodrošināt atbilstošu tiesisko pamatu un tā ir nelikumīga, tad tālākas darbības, tai skaitā, NIDA veikšana nav lietderīga. Tas pats attiecas uz "godprātīgu" datu apstrādi – ja datu apstrāde pēc būtības kvalificējas kā negodprātīga, tad plānotā datu apstrāde nav atļauta, neatkarīgi no NIDA rezultātiem. Vienlaikus, ja kādā datu apstrādes posmiem netiek nodrošināta pārredzamības principa ievērošana (piemēram, noteiktu informāciju fiziskai personai nedrīkst sniegt ievērojot normatīvo aktu prasības), tad organizācija var šo apstākli uzskatīt par risku fiziskas personas tiesībām un brīvībām paaugstinošu apstākli, vienlaikus pati apstrāde nav uzskatāma par nelikumīgu pēc noklusējuma.

[11] Organizācija nodrošina plānotās datu apstrādes tiesiskā pamata analīzi, iekļaujot informāciju, tai skaitā, par datu apstrādes atbilstību tiesību aktiem. Tiesiskā pamata analīzi jāveic attiecībā uz katru noteikto datu apstrādes nolūku un datu apstrādes dzīves cikla posmu.

[12] Tiesiskā pamata analīze jāveic saskaņā ar Datu regulas 6. Pantu, un gadījumos, kad tiek veikta īpašu kategoriju personas datu apstrāde – Datu regulas 9. pantu, savukārt, ja tiek apstrādāta informācija par sodāmību – Datu regulas 10. pantu.

[13] Ja plānotā datu apstrāde tiek balstīta uz Datu regulas 6. panta 1. punkta f) apakšpunktu jeb organizācijas leģitīmām interesēm, tad ir jāveic leģitīmo interešu izvērtēšana, savukārt, ja publiskās iestādes plānoto datu apstrādi balstīs uz Datu regulas 6. panta 1. punkta e) apakšpunktu – nepieciešams veikt proporcionalitātes testu. Atgādinām, ka pārziņa leģitīmo interešu apraksts ir neatņemama NIDA sastāvdaļa atbilstoši Datu regulas 35. panta 7. punkta a) apakšpunktam.

[14] Ja plānotā datu apstrāde tiek balstīta uz datu subjekta piekrišanu, šajā sadaļā ir jāanalizē arī piekrišanas nosacījumi, lai tā atbilstu Datu regulas 7. pantam. Ja plānots iegūt bērna piekrišanu attiecībā uz informācijas sabiedrības pakalpojumiem, jāskata Datu regulas 8. pants. Savukārt, ja plānots datus nosūtīt uz trešo valsti vai starptautisku organizāciju – Datu regulas V nodaļa.

1.2. "Nolūka ierobežojumi"

[15] Nākamais solis ir novērtēt, vai tiek nodrošināts, ka personas dati tiks izmantoti tikai plānotā datu apstrādes nolūka vai ar to savietojamiem nolūkiem sasniegšanai. Nepieciešams novērtēt, vai ir mazināta/novērsta personas datu starpizmantošana neparedzētu un fiziskai personai nezināmu nolūku sasniegšanai[10]. Lai šo novērtējumu veiktu, jāanalizē ar kādiem paņēmieniem plānotā personas datu apstrāde tiks nodalīta no citām organizācijas veiktām datu apstrādēm. Sistēmiskas personas datu apstrādes gadījumā datu nodalīšanu labi demonstrē shematisks informācijas aprites attēlojums[11].

[16] Organizācija, veicot nolūka ierobežojuma analīzi, ir jāņem vērā vismaz:
- iekšējo noteikumu attiecībā uz informācijas apstrādi analīze;
- piešķirto sistēmas lietotāju lomu un datu izmantošanas monitoringa novērtējums;
- ieviesto tehnisko risinājumu analīze, kas izstrādāta un ieviesta, lai nodalītu plānoto datu apstrādes plūsmu no jau esošas (vai jebkuras citas) datu apstrādes plūsmas, kas tiek veikta,

[9] Skatīt III nodaļas "NIDA veikšana un tās posmi" sadaļu "Apspriešanās un komunikācija ar datu subjektu".
[10] Personas datu starpizmantošanas novēršana attiecas gan uz organizācijas iekšējiem procesiem, gan iespējamo ārējo piekļuvi datiem. Tas nozīmē, ka personas dati nedrīkst tikt izmantoti nolūkiem, kas nav skaidri definēti un atrunāti iekšējos dokumentos vai noslēgtajā līgumā ar kopīgu pārzini vai apstrādātāju. Tas attiecas gan uz organizācijas iekšējām datu apstrādēm, gan uz datu nodošanu.
[11] Skatīt IV nodaļas "NIDA AIZPILDĪŠANA", sadaļu "Datu apstrādes dzīves cikls".

lai sasniegtu citu nolūku (respektīvi, kā tiek nodrošināts, ka datu kategorijas, kuras plānots apstrādāt konkrēta nolūka sasniegšanai, netiek izmantotas citiem, nesaistītiem nolūkiem).

Ņem vērā! Ja personas dati tiek iegūti viena nolūka sasniegšanai, tad to izmantošana citam nolūkam ir uzskatāma par jaunu personas datu apstrādi, kurai arī jāatbilst visiem personas datu apstrādes principiem, tai skaitā šādai apstrādei jābūt tiesiskajam pamatam jeb likumiskai.

[17] Ja šajā posmā tiek secināts, ka pastāv iespēja datu izmantošanai nesaistītos nolūkos, tad tas ir ņemams vērā kā risku paaugstinošs apstāklis.

Piemēram, šajā posmā organizācija var nonākt pie secinājuma, ka, lai īstenotu principu, nepieciešams izveidot pilnīgi jaunas datu plūsmas, kas paredzētas tikai šiem datu masīviem. Tai skaitā, glabājot tos datu centros, kas no pārējām organizācijas datu bāzēm nodalītas ne tikai tehniski, bet arī fiziski[12]. Tas nodrošinātu, ka organizācijā nenotiek informācijas sistēmu izmantošana sākotnēji neparedzētiem nolūkiem, un piekļuve personas datiem notiek tikai lietotājiem piešķirto piekļuvju apjomā[13].

Ņem vērā! Organizācijai arī jāvērtē, vai un kā papildināsies darbinieku lomu apraksti saistībā ar jauno datu apstrādi, kā arī kas veiks uzraudzību nepieciešamo izmaiņu veikšanai[14].

1.3. "Datu minimizēšana"

[18] Atbilstība šim principam periodiski un/vai mainoties būtiskiem ārējiem apstākļiem jāpārskata pārliecinoties, ka joprojām tiek apstrādāts tikai tas datu apjoms, kas minimāli nepieciešams nolūka sasniegšanai. Datu minimizēšanas principa ievērošana jāvērtē visā datu dzīvescikla posmā, analizējot, vai katrs posma elements apstrādā tikai nolūka sasniegšanai nepieciešamo datu apjomu.

[19] Organizācijai, veicot datu minimizēšanas principa analīzi, vismaz ir:

- katrā konkrētā gadījumā jāizvērtē, ko konkrētie personas dati dos, lai sasniegtu datu apstrādes nolūku (piemēram, vai tiešām ir nepieciešams personas kods, lai nodrošinātu preču piegādi);
- pēc kāda laika perioda jāpārskata personas datu kategorijas, kuras tiek apstrādātas;
- jāsaprot, kā tiks izvērtēts, vai netiek apstrādāts vairāk personas datu kā nepieciešams un kādas būs turpmākās darbības (piemēram, kā tiks nodrošināta datu, kuri nav nepieciešami nolūka sasniegšanai, dzēšana, un kā par to tiks informēti datu subjekti);
- gadījumos, ja personas dati tiek apstrādāti dažādos nolūkos, jāizvērtē – kā tiks nodrošināts, ka dati tiek nošķirti un tiek apstrādāts tikai tāds datu apjoms, kas nepieciešams.

[20] Arī, ja šajā posmā tiek secināts, ka pastāv iespēja, ka tiek apstrādāti vairāk personas dati kā nepieciešams nolūka sasniegšanai, tad tas nākamajā solī ir ņemams vērā kā risku paaugstinošs apstāklis (*skatīt zemāk esošo piemēru*). Datu minimizēšanas principa ievērošana, jo īpaši svarīga, ja kā datu apstrādes tiesiskais pamats tiek piemērota "piekrišana", kur fiziska persona izvēlas un piekrīt kādus datus par sevi vēlas nodot organizācijas rīcībā, jo šādos gadījumos neveicot pietiekamu analīzi, organizācija var pieprasīt un saskaņot ar datu subjektu praktiski neierobežota daudzuma datu kategoriju izmantošanu, kas pēc būtības būs nelikumīga. Vienlaikus vēlāk veikt iekšējas kontroles pasākumus par pārmērīgo datu apjomu, var būt sarežģīti.

[12] Piemēram, ja tiek veikts pilns NIDA, organizācija šādu risinājumu var ieviest, lai mazinātu riskus fiziskas personas tiesībām un brīvībām.
[13] Piemēram, ja tiek veikts pilns NIDA, organizācija šādu risinājumu var ieviest, lai mazinātu riskus fiziskas personas tiesībām un brīvībām.
[14] Piemēram, ja tiek veikts pilns NIDA, organizācija izvērtē iesaistīto personu lomas un nosaka papildu drošības prasības darbiniekiem, lai mazinātu riskus fiziskas personas tiesībām un brīvībām.

Piemēram, ja šajā posmā tiek secināts, ka var tikt apstrādāti vairāk personas dati kā nepieciešams, organizācija var izvērtēt, kā samazināt apstrādājamo datu apjomu, lai sasniegtu nolūku. Tai skaitā, savienojot ar nolūka ierobežojuma principu, veicot sistemātisku datu apstrādes aprakstu, izvērtēt apstrādājamo datu apjomu katrā dzīves cikla posmā un nolūkā. Viens no risinājumiem var būt, izmantojot tehniskus līdzekļus, ierobežot personas iespējas dalīties ar saviem datiem, piemēram, izvērtēt un neizmantot jau esošas tīmekļa vietnes funkcionalitātes, bet gan pielāgot tās savām vajadzībām, jo īpaši, ja tiek izmantotas sīkdatnes.[15]

1.4. "Precizitāte"

[21] Lai ievēroto precizitātes principu, organizācijai ir jāveic gan analīze, kā neprecīzi dati iespaidos nolūka sasniegšanu, tā arī neprecīzu datu apstrādes iespējamā ietekme uz fizisku personu. Nepieciešams novērtēt, kādi tehniski un organizatoriski pasākumi jāievieš, lai nodrošinātu iespējami precīzu datu apstrādi. Arī šajā gadījumā princips jāpiemēro visam datu dzīvesciklam, vērtējot ietekmi uz katra atsevišķā dzīvescikla posma uzdevumu izpildi.

Ņem vērā! Ja pakalpojums datu subjektam datu neprecizitātes dēļ tiek pilnībā vai daļēji atteikts, pakalpojums vai tā saņemšana apgrūtināta – tas ir risku fiziskas personas tiesībām un brīvībām paaugstinošs/veidojošs faktors.

[22] Šajā gadījumā ietekmes aspekts var izrietēt no datu veida, apstrādes nolūka vai arī fiziskas personas gaidām, bet varbūtības faktors veidotos gan no iespējamības, ka dati, kam tiks noteikts sākotnējais risks, ir neprecīzi, gan no varbūtības, ka neprecīzo datu rezultātā veidosies ietekme uz pakalpojuma kvalitāti, kur noteiktais sākotnējais risks veidos sākotnējo ietekmi.

[23] Šis ir viens no principiem, kuram ir lielākā ietekme uz datu subjekta citu (ne personas datu aizsardzības) pamattiesību un brīvību nodrošināšanu. Pakalpojuma nesaņemšana vai saņemšana negaidītā veidā ietekmē ne tikai datu aizsardzības aspektus, bet arī tās datu subjekta tiesības, kas saistītas ar pakalpojuma būtību.

1.5. "Glabāšanas ierobežojums"

[24] Organizācijai jāpārliecinās, ka dati tiks glabāti tikai tādu laika posmu, kas nepieciešams datu apstrādes mērķa sasniegšanai. Jānovērtē ieviestie tehniskie un organizatoriskie pasākumi, ar kuriem tiks nodrošināts, ka dati netiek glabāti ilgāk kā nepieciešams nolūka sasniegšanai.

[25] Organizācijai, veicot glabāšanas ierobežojuma principa analīzi, ir jāņem vērā vismaz:

- izvēlētais pamatojums, kāpēc organizācija izvēlējusies attiecīgo glabāšanas termiņu konkrētajiem datiem;
- kā par principa izpildi iespējams pārliecināties pēc datu subjekta iesnieguma saņemšanas;
- kādi tehniski un organizatoriski pasākumi ieviesti, lai nodrošinātu datu dzēšanu vai to iznīcināšanu;
- kādi mehānismi ieviesti, lai pārbaudītu, ka automatizētu risinājumu izmantošanas gadījumā tiek veiktas pēcpārbaudes par prasību izpildi.

[26] Arī, ja šajā posmā tiek secināts, ka pastāv iespēja, ka organizācija nespēj nodrošināt personas datu glabāšanu atbilstoši noteiktajam periodam, tad tas ir ņemams vērā kā riska paaugstinošs apstāklis, jo īpaši, ja ir ieviesti tehniskie risinājumi, kas ir novecojuši un pastāv bažas, ka dati netiek dzēsti no sistēmas.

[15] Piemēram, ja tiek veikts pilns NIDA, organizācija šādu risinājumu var ieviest, lai mazinātu riskus fiziskas personas tiesībām un brīvībām.

Ņem vērā! Tehniskie un organizatoriskie pasākumi, ja tiek veikta NIDA, var būt, tai skaitā – kā tiek noteikts glabāšanas ilgums, kā tiek uzraudzīts, ka tiek nodrošināta personas datu dzēšana/iznīcināšana. Katrs no minētajiem elementiem var radīt risku fiziskas personas tiesībām un brīvībām. Tāpēc organizācija var ieviest papildus kontroles, lai pārliecinātos, ka pēc datu dzēšanas tie neglabājas citos serveros[16].

1.6. "Integritāte un konfidencialitāte"

[27] Integritātes un konfidencialitātes principa efektīva piemērošana palīdzēs aizsargāt ne tikai organizācijas apstrādātos personas datus, bet arī citus organizācijas biznesa procesu datus. Objektīva situācijas novērtēšana ir izšķirošs posms veiksmīgas sistēmas aizsardzības un atbilstošas funkcionēšanas pārraudzības izveidei.

[28] Organizācijai, veicot integritātes un konfidencialitātes principa analīzi, ir jāņem vērā vismaz:
- datu apstrādē izmantoto sistēmu tehniskos raksturlielumi un ieviestie ilgtspējas un aizsardzības pasākumi;
- iekšējie organizatoriskie pasākumi datu aizsardzībai;
- augstāk minēto punktu mijiedarbība.

[29] Integritātes un konfidencialitātes princips radīs lielāko ietekmi uz tādām fizisko personu tiesībām un brīvībām, kas nav tieši saistītas ar personas datu aizsardzību. Līdz ar to konfidencialitātes un integritātes nodrošināšanai var būt NIDA ietvaros horizontāli plašāka nozīme risku fizisku personu tiesībām un brīvībām noteikšanā un novērtēšanā.

Ņem vērā! Jo īpaši, ja vēlākā posmā tiks veikta NIDA, šī principa izvērtēšanas laikā ir būtiski neuzdot vēlamo par esošo, bet savu sistēmu novērtēt pēc iespējas objektīvāk.

[30] Organizācijai jāpievērš uzmanība sistēmas darbības ilgtspējas ietekmei uz fiziskas personas tiesībām un brīvībām, respektīvi, kas notiek, ja sistēmā personas datu apstrāde kādu laiku nenotiek:
- Kā tas ietekmē plānotā personas datu apstrādes nolūka sasniegšanu?
- Kā tas ietekmē fizisku personu un tās gaidas?

Piemēram, organizācija izstrādā lietotni lietotāja pārvietošanās maršruta fiksācijai, lai balstoties uz saņemtajām ziņām piedāvātu lietotājam atlīdzību par veikto attālumu, bet saņemto informāciju izmanto lietotāja paradumos balstītu reklāmu izplatīšanā – ja lietotne pārstāj saņemt ziņas par maršrutu, vai tās tiek saglabātas ar lietotāju nesaistāmā veidā, vai lietotne kļūst nepieejama drošības incidenta dēļ – lietotne nespēs sasniegt plānoto datu apstrādes nolūku. Tāpat lietotājs nesaņems gaidīto pakalpojumu – mērķētas reklāmas un atlīdzību par veikto attālumu.

1.7. "Pārskatatbildība"

[31] Visas darbības un pasākumi, ko organizācija ir veikusi, lai nodrošinātu atbilstību Datu regulai, ir jādokumentē un jāsaglabā izsekojamā veidā organizācijas lietvedībā. Šis ne tikai palīdzēs efektīvi atsekot izmaiņu nepieciešamībai un pārvaldīt datu apstrādes procesu kopumā, bet arī nodrošinās, ka Inspekcijas pieprasījuma gadījumā viss nepieciešamais materiāls, kas saistīts ar attiecīgās personas datu apstrādes novērtējumu un analīzi, ir vienkopus. Organizācijas pamatojumiem un lēmumam par plānoto personas datu apstrādi ir jābūt balstītiem faktos un loģiski argumentētiem[17].

Ņem vērā! Jāvērtē atbilstība visiem datu apstrādes principiem, kuri noteikti Datu regulas 5. pantā.

[16] Piemēram, ja tiek veikts pilns NIDA, organizācija šādu risinājumu var ieviest, lai mazinātu riskus fiziskas personas tiesībām un brīvībām.
[17] Skatīt III nodaļas "NIDA veikšana un tās posmi" sadaļu "Lēmumu pieņemšanas dokumentācija".

Ņem vērā! Sagatavošanās posmā un plānotās datu apstrādes nolūka un likumības izvērtējuma laikā organizācija var konsultēties ar un iesaistīt datu aizsardzības speciālistu, ja tāds ir norīkots.

Ilustratīvs piemērs, kuru papildināt un pielāgot atbilstoši vadlīnijās augstāk minētajam[18]:

Mazumtirdzniecības uzņēmums plāno ieviest lojalitātes programmu, kurā klienti saņem atlaides un personalizētus piedāvājumus, pamatojoties uz klienta vēlmēm, kuras norādītas reģistrācijas laikā ((a) tiek izsniegta fiziska klienta karte; (b) lai mainītu vēlmes, klientam atkārtoti jāaizpilda veidlapa, norādot klienta numuru, kas redzams uz lojalitātes kartes).

1. Plānotās **datu apstrādes nolūks** varētu būt: veicināt klientu iesaistīšanos un nodrošināt tādas priekšrocības kā atlaides un personalizētu piedāvājumus lojalitātes programmas dalībniekiem. Plānotās **datu kategorijas**, kuras tiks apstrādātas lojalitātes programmas ietvaros – vārds, e-pasts vai tālruņa numurs (pēc izvēles), izvēlētas pakalpojumu vai produktu preferences.
2. **Datu apstrādes dzīves cikla apraksts:** IEGŪŠANA: personu datu kategorijas, kas savākti lojalitātes programmas reģistrācijas laikā; IZPLATĪŠANA: darbinieks ievada informāciju lokālā klientu datu bāzē; IZMANTOŠANA: iegūtie personas dati tiek izmantoti, lai personalizētu piedāvājumu un ģenerētu atlaides; UZTURĒŠANA: dati tiek saglabāti tikai tik ilgi, kamēr klients vēlas piedalīties lojalitātes programmā vai kamēr ir cits tiesisks pamats turpmākai datu apstrādei. DZĒŠANA: personas dati tiek dzēsti pēc klienta pieprasījuma vai lojalitātes programmas darbības noslēgšanas.
3. **Datu apstrādes likumība:** Piekrišana (Datu regulas 6.panta 1.punkta a)apakšpunkts) - klients piekrīt, ka viņa dati reģistrācijas brīdī tiek apstrādāti lojalitātes programmas ietvaros.

Datu apstrādes atbilstības un nepieciešamības novērtēšana

4. **Atbilstība:** Vai visi savāktie dati ir nepieciešami mērķa sasniegšanai? Piemēram, vārds, e-pasts vai tālruņa numurs ir būtisks piedāvājumu personalizēšanai un komunikācijai ar klientu (nosūtīt informāciju par piedāvājumiem); izvēlētās pakalpojumu vai produkta preferences nav obligātas, un dati jāiegūst tikai tad, ja klients vēlas saņemt personalizētus piedāvājumus un/vai atlaides. Mazumtirdzniecības uzņēmums neievāc pārmērīgus datus (Piemēram, sensitīvi dati/veselības informācija, nav būtiski nolūka sasniegšanai un nav jāievāc).
5. **Nepieciešamība:** Vai uzņēmums varētu sasniegt nolūku citādā veidā? Piemēram, ja klients izvēlas nenorādīt savas preferences attiecībā uz personīgajiem iestatījumiem, tad iepirkšanos varētu analizēt, izmantojot vispārējās tendences, nevis saistīt tās ar atsevišķiem klientiem, taču tas neatbalstītu personalizētus piedāvājumus. Tāpēc personas datu vākšana ir pamatota.

Datu regulas principu izvērtējums

6. **Likumīgums, godprātība un pārredzamība**: dati tiks apstrādāti tikai pēc klienta iniciatīvas un sniegtās piekrišanas, bez slēptiem nolūkiem. Klienti tiks informēti par plānoto datu apstrādi un to tiesībām, izmantojot *Privātuma politiku* tīmekļa vietnē un uz vietas, kad tiks iesniegts pieteikums lojalitātes programmai.
7. **Nolūka ierobežojums:** dati tiks izmantoti tikai lojalitātes programmas darbībām, nevis nesaistītām mārketinga kampaņām.
8. **Datu minimizēšana:** tiek apkopoti tikai mērķa sasniegšanai nepieciešami dati. Izvēles datu lauki ir skaidri atzīmēti.
9. **Precizitāte:** klienti var atjaunināt savu informāciju, lai nodrošinātu precizitāti un aktualitāti.
10. **Datu glabāšana:** personas dati tiek glabāti noteiktu laiku, pēc tam tie tiek dzēsti, un tiek veiktas pārbaudes, lai dati neglabājas citos serveros. Datu dzēšana skaidrota *Privātuma politikā* un iekšējos dokumentos.

[18] Nepieciešams veikt detalizētāku izvērtējumu atbilstoši vadlīnijās minētajam.

11. **Integritāte un konfidencialitāte:** dati ir šifrēti un piekļuve ir atļauta tikai pilnvarotam personālam.
12. **Pārskatatbildība:** izstrādāti iekšējie kārtības dokumenti, kuri nosaka datu apstrādes un aizsardzības prasības uzņēmumā, un publicēta *Privātuma politika*.

1.8. Papildus nosacījumi, ja plānotās datu apstrādes ietvaros paredzēta datu nosūtīšana uz trešo valsti vai starptautisku organizāciju[19]

[32] Vērtējot kopējo plānotās personas datu apstrādes likumību, organizācijai būtu jāņem vērā arī tas, vai plānotās datu apstrādes ietvaros kādā no datu apstrādes dzīvescikla posmiem tiek plānota šo datu nodošana uz trešo valsti.

Ņem vērā! Datu apstrāde nav uzskatāma par likumīgu, ja datu nodošanas uz trešo valsti ietvaros organizācija nespēj nodrošināt atbilstību Datu regulas V nodaļai.

[33] Informācija par datu nodošanu var organizācijai palīdzēt noteikt risku apmēru fizisku personu tiesībām un brīvībām gan no risku avotu perspektīvas, gan no risku iespējamās ietekmes. Tāpat atsevišķu apdraudējumu iespējamība būs lielāka, ja personas datu apstrāde notiks trešajā valstī.

[34] Lai nodrošinātu atbilstību Datu regulas V nodaļai, organizācijai var būt nepieciešams ieviest noteiktu risku mazinošo apstākļu kopumu. Šis risku mazinošo apstākļu kopums ir jāņem vērā, ja organizācija veic NIDA. Pats datu nodošanas uz trešo valsti fakts, ja tas tiek darīts atbilstoši Datu regulas V nodaļai, atsevišķu risku datu subjekta tiesībām un brīvībām nerada, arī, ja tiks konstatēts, ka NIDA ir nepieciešama (analizējot datu apstrādi pirms-NIDA ietvaros).

[19] Skatīt Datu valsts inspekcijas 2021. gada rekomendāciju "Par personas datu nodošanu uz valstīm, kas nav ES vai EEZ dalībvalstis, atbilstoši Vispārīgajai datu aizsardzības regulai (VDAR)". Pieejams: https://www.dvi.gov.lv/lv/dvi#par-personas-datu-nodosanu-uz-valstim-kas-nav-es-vai-eez-dalibvalstis-atbilstosi-visparigajai-datu-aizsardzibas-regulai

II NODAĻA "NIDA veikšanas nepieciešamības izvērtējums"

2. Pirms-NIDA

[35] NIDA ir veicams tikai personas datu apstrādēm, kas rada paaugstinātu risku fiziskas personas tiesībām un brīvībām. Pastāv dažādi risinājumi kā nodrošināt, ka NIDA tiek veikts Datu regulā noteiktajos gadījumos. Viens no risinājumiem, lai noteiktu – ir vai nav jāveic NIDA, ir veikts pirms-NIDA.

[36] Pirms-NIDA ir process, kas norāda uz to, vai plānotā datu apstrāde varētu radīt augstus riskus datu subjektiem. Vadlīniju [40] punktā ir norādītas apstrādes darbības, kuras varētu izraisīt augstu risku fizisku personu tiesībām un brīvībām, kā arī vadlīniju 2.3. sadaļā iekļauti norādījumi, par to, kad NIDA nav jāveic. Veicot pirms-NIDA, atbildīgajai personai ir jāņem vērā kritēriji, kuri norādīti minētajā nodaļā.

[37] Līdzīgi kā ar NIDA procesu, normatīvais regulējums neparedz nedz nepieciešamību, nedz konkrētu ietvaru kā veikt pirms-NIDA. Inspekcijas ieskatā, pirms-NIDA procesu ir jāsāk ar īsu datu apstrādes raksturojumu un izvērtējumu, kas ļaus fiksēt galvenos plānotās personas datu apstrādes elementus, kuriem piemērojot [40] punktā norādītos kritērijus, varēs noteikt, vai apstrāde ir uzskatāma par potenciāli augstu risku fiziskām personām radošu.

[38] Ja organizācijai joprojām ir bažas par nepieciešamību veikt NIDA, tā, balstoties uz īsu datu apstrādes izvērtējumu, var veikt arī padziļinātāku izpēti, kas sevī ietvertu dzīves cikla analīzi [20].

Ņem vērā! Pirms-NIDA izvērtējuma laikā organizācija var konsultēties ar un iesaistīt datu aizsardzības speciālistu, ja tāds ir norīkots.

2.1. Īss plānotās datu apstrādes izvērtējums

[39] Atbildīgajai personai, kura plāno veikt NIDA, īss datu apstrādes kopsavilkums ļaus noteikt, vai plānotā datu apstrāde varētu radīt iespējamu risku datu subjektu tiesībām un brīvībām.

[40] Šajā posmā jāapraksta un jāizvērtē galvenie datu apstrādes elementi. Aprakstā iekļaujams izvērtējums, kurā apskatīts:

- Datu veidi (piemēram, vai ir plānots apstrādāt "parastos datus", īpašo kategoriju datus vai datus par sodāmību);
- Datu apstrādes veids (piemēram, plānots veikt darbinieku kontroli, veidot klientu datu bāzi, lai izsūtītu mārketinga paziņojumus, plānots apstrādāt datus veicot profilēšanu, plānota automatizēta lēmumu pieņemšana);
- Datu avots (piemēram, personas dati iegūti no publiski pieejamas informācijas, ģenerēti, izmantojot jaunas tehnoloģijas, plānota datu kopu saskaņošana un apvienošana);
- Datu apstrādes apjoms (piemēram, vai uzskatāms, ka personas datu apstrāde veikta plašā mērogā[21])
- Datu subjektu kategoriju raksturojums (piemēram, vai ir plānots apstrādāt nepilngadīgu personu, personu, kuras atrodas pārziņa ietekmē vai personu ar īpašām vajadzībām, datus);
- Datu apstrādē izmantotās tehnoloģijas (piemēram, vai plānotā datu apstrāde tiks veikta izmantojot inovatīvas, iepriekš attiecīgā veidā neizmantotas tehnoloģijas, vai arī personas dati tiks apstrādāti izmantojot tīmekļa vietnes anketu);
- Datu subjekta tiesību īstenošana (Piemēram, pārzinis pieņem automatizētu lēmumu un nepiedāvā iespēju klientam lūgt to izskatīt cilvēkam).

[20] Skatīt IV nodaļas "NIDA AIZPILDĪŠANA" sadaļu "Datu apstrādes dzīves cikls".
[21] Skatīt Inspekcijas 2024. gada "Vadlīnijas datu apstrādei plašā mērogā". Vadlīnijas pieejamas: https://www.dvi.gov.lv/lv/media/3408/download?attachment

[41] Ja veicot plānotās datu apstrādes īsu raksturojumu un salīdzinot to ar šo vadlīniju [40] punktā minētajiem kritērijiem organizācija secina, ka plānotā personas datu apstrāde var radīt augstu vai ļoti augstu risku fizisku personu tiesībām un brīvībām – ir jāveic NIDA.

[42] Savukārt, ja veicot plānotās datu apstrādes izvērtējumu organizācija secina, ka plānotā datu apstrāde rada vidēju vai mazu risku datu subjektiem – NIDA nav jāveic un process ir pārtraucams. Vienlaikus, arī neveicot NIDA, uz minēto apstrādi ir attiecināmi ierastie datu apstrādes atbilstības nodrošināšanas pasākumi.

Ņem vērā! Augstāk minētie datu apstrādes elementi, kā arī Inspekcijas apstiprināto kritēriju un datu apstrādes veidi, kuriem ir obligāts pienākums veikt NIDA nav izsmeļoši un organizācijai ir jāpieņem lēmums par nepieciešamību veikt vai neveikt NIDA vērtējot katru apstrādes gadījumu atsevišķi.

2.2. Kad veikt NIDA?

[43] Datu regulā ir noteikts, ka **NIDA veikšana ir pienākums, kad apstrāde varētu radīt augstu risku fizisku personu tiesībām un brīvībām,** it īpaši gadījumos, kad:

- tiek veikta sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde;
- tiek veikta publiski pieejamas zonas uzraudzība plašā mērogā;
- pārzinis veic īpašu kategoriju personas datu vai Datu regulas 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā;
- apstrāde ir iekļauta Inspekcijas izstrādātajā sarakstā[22] ar datu apstrādēm, kurām obligāti jāveic NIDA.

Ņem vērā! Inspekcijas saraksts izstrādāts pamatojoties uz EDAK kritērijiem[4]. Kritēriju mērķis ir veidot vienotu pieeju organizācijas plānoto apstrāžu analīzei, lai novērtētu, kuros gadījumos iespējamā ietekme uz datu subjektu ir paaugstināta.
Ja organizācijas veiktā vai potenciālā apstrāde atbilst vismaz diviem kritērijiem, tad uzskatāms, ka ir pamats NIDA veikšanai.
Tomēr dažos gadījumos NIDA var būt veicams arī apstrādei, kas atbilst tikai vienam no šiem kritērijiem, līdz ar to organizācija no katras apstrādes radīto risku izvērtējuma, no gadījuma uz gadījumu, nevarēs izvairīties.

[44] Galvenais nosacījums pēc kā organizācijai vērtēt NIDA veikšanas nepieciešamību, ir pastāvošs augsts risks, ko plānotā vai jau esošā apstrāde rada fizisku personu tiesībām un brīvībām.

Ņem vērā! Šaubu gadījumā Inspekcija rekomendē veikt NIDA. Iegūto informāciju var izmantot, lai noteiktu atbilstības nodrošināšanai nepieciešamos pasākumus, gan attiecībā uz fizisku personu tiesību nodrošināšanu, gan arī uz nepieciešamo tehnisko un organizatorisko datu aizsardzības pasākumu ieviešanu

2.3. Kad NIDA var neveikt?

2.3.1.Nav augsta riska datu subjektu tiesībām un brīvībām

[45] NIDA var neveikt, ja pirms-NIDA laikā secināts, ka plānotā datu apstrāde neatbilst kritērijiem, kas noteikti Datu regulā vai Inspekcijas publicētajā sarakstā, kā arī, ja sākotnēji apstrādes veids, jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, neliecina par iespējamu augstu risku fiziskas personas tiesībām un brīvībām.

[22] Datu valsts inspekcijas 2018. gada 18. decembra saraksts "Apstrādes darbību veidi, attiecībā uz kuriem ir jāveic datu aizsardzības ietekmes novērtējums saskaņā ar VDAR 35. panta 4. punktu" . Pieejams: https://www.dvi.gov.lv/lv/media/92/download?attachment

Piemēram, augsts risks datu subjekta tiesībām un brīvībām nebūs, ja automašīnu rezerves daļu tirdzniecības uzņēmums ar 2000 klientiem izlēmis izveidot elektronisku klientu vadības sistēmu. Sistēmā tiktu iekļauta tikai klienta kontaktinformācija un transportlīdzekļa ražotājs un modelis, ar kādu klients ikdienā pārvietojas. Sistēmas izveides mērķis ir pielāgot produkcijas sortimentu, lai piedāvātu klientiem atbilstošākas preces.

[46] Šajā gadījumā vērtējot riskus tiek ņemts vērā, ka datu veidi ir kontaktinformācija un transportlīdzekļa modelis, kas nav klasificējami kā īpašu kategoriju dati. Datu apstrādes veids ir iekšējas datu bāzes izveide, nav paredzēta profilēšana vai jebkādu lēmumu pieņemšana attiecībā uz klientu. Datu avots ir pats klients, un tie iegūti fiziskai personai caurspīdīgā un saprotamā veidā, saprotamu un izskaidrotu iemeslu dēļ. Datu apstrādes apjoms, gan kopējā datu masīvu dēļ, gan arī datu potenciālās ietekmes uz fizisku personu dēļ, nav uzskatāms par plašu. Fizisku personu kategorijas ir klienti – tie neatrodas īpašā statusā attiecībā pret organizāciju un nav no organizācijas īpašā veidā ietekmējami. Datu apstrādē netiek izmantotas inovatīvas tehnoloģijas vai tradicionālas tehnoloģijas inovatīvā veidā. Automašīnas rezerves daļu tirdzniecības uzņēmums nedarbojas jomā, kas var potenciāli skart un izpaust fiziskas personas īpašu kategoriju datus vai datus par fiziskās personas sodāmību. Datu apstrādes ietvaros netiek plānots veikt nosūtīšanu uz trešo valsti. Dati arī neizpauž cita veida informāciju par klientu, ko varētu uzskatīt par īpaši jutīgu (piemēram, ziņas par klienta finansēm).

Ņem vērā! Organizācijai jāspēj uzskatāmi demonstrēt (atspoguļot pirms-NIDA) un pamatot savu pārliecību, ka apstrāde neradīs paaugstinātu risku fiziskas personas tiesībām un brīvībām.

2.3.2.NIDA jau ir veikts par līdzīgu datu apstrādi

[47] NIDA var neveikt, ja NIDA par analogām apstrādes darbībām pati organizācija (vai cita līdzīga organizācija) jau ir veikusi. Svarīgākais ir apzināties, ka datu apstrādes apstākļi, par kuriem NIDA jau ir veikts, ir analogi no jauna vērtējamajam procesam, kā arī organizācijai, kura ir atbildīga par NIDA veikšanu, ir jābūt pieejai pie pilna veiktā NIDA.

Piemēram, organizācija atver jaunu filiāli, kura darbojas uz identiskiem principiem, kā jau esošās darbības vietas. Organizācija arī jaunajā filiālē plāno ieviest identisku videonovērošanas sistēmu, kā jau aktīvajās organizācijas darbības vietās. Ja organizācija jau ir veikusi NIDA par videonovērošanas sistēmas darbību vienā organizācijas darbības vietā, citās darbības vietās, kas darbojas uz identiskiem principiem, NIDA nav jāveic. Vienlaikus jau veiktajā NIDA ir jāpapildina plānotās datu apstrādes veikšanas vietas ar jauno objektu.

[48] Piemērā norādītajā gadījumā nav atšķirības datu apstrādes nolūkā/-os, apstrādājamo datu veidos, apjomā (tai skaitā, ka, veicot apstrādi, dati netiek nodoti trešajām valstīm) un veidā kā dati tiek apstrādāti, nav parādījies jauns datu ieguves avots, nemainīgas ir arī fizisku personu kategorijas un apstrādē izmantotās tehnoloģijas, kā arī organizācijas darbības joma. Līdz ar to veicot novērtējumu par riskiem, tas pēc būtības nemainīsies esošai datu apstrādei un jaunajai datu apstrādei.

[49] Ja mainās būtiski apstrādes aspekti, piemēram, apjoms mainās tādēļ, ka videonovērošana jaunajā objektā vērsta ne tikai uz pakalpojuma sniegšanas vietu, bet arī noliktavas zonu, tad uzskatāms, ka mainījies apstrādājamo datu apjoms un šī apstrāde vairs nav līdzīga tai, par kuru veikts NIDA.

[50] Vēršam uzmanību, ka jebkurā gadījumā, lai apstrāde būtu atbilstīga, tai būs jāpiemēro iepriekšējā NIDA identificētie risku mazināšanas pasākumi, tai skaitā, piemēram, videonovērošanas

kameru objektīva leņķa samazināšana līdz minimāli nepieciešamajam, apstrādes nolūka sasniegšanai.

Ņem vērā! Šādos gadījumos organizācijas rīcībā ir jābūt sākotnēji veiktajam NIDA, jo tikai šādi būs iespējams pilnīgi novērtēt visus apsvērumus un to līdzību ar jaunās plānotās datu apstrādes apstākļiem. Ja trūkst informācijas par soļiem, ko vērtējis sākotnējais NIDA veicējs, tad nav pamata apgalvojumam, ka veiktais NIDA ir par to pašu apstrādi, kuru plāno veikt pārzinis.

2.3.3. Ja novērtējums veikts ārēju normatīvo aktu izstrādes laikā

[51] Normatīvā akta izstrādātājs veic analīzi, vai un kādā veidā paredzētā norma varētu ietekmēt fiziskas personas tiesības un brīvības. Tas nozīmē, ka atsevišķos gadījumos NIDA var tikt veikta vēl ārējā normatīvā akta pieņemšanas procesā vai pirms tā.

Piemēram, normatīvā akta izstrādātājam ir pienākums veikt analīzi, lai noskaidrotu, vai un kādā veidā plānotā norma varētu ietekmēt fizisku personu tiesības un brīvības. Tas paredz tai skaitā, identificēt potenciālās datu apstrādes riskus, kas var rasties, ja norma tiek pieņemta un īstenota.

Normatīvā akta pieņemšanas laikā var tikt veikta, piemēram, pieņemtās normas:

- mērķa un konteksta analīze;
- atbilstības novērtēšana Datu regulas vai cita speciālā normatīvā akta prasībām;
- samērīgums un nepieciešamība, lai sasniegtu nolūku;
- potenciālais risks fiziskas personas tiesībām (piemēram, vai un kā noteiktie ierobežojumi tiesībām uz piekļuvi datiem, datu labošanu, dzēšanu var ietekmēt fizisku personu) un to ietekmes novērtējums.

Ja likumdevējs nosaka sistēmas izveidi un par to atbildīgo organizāciju, var tikt noteikts pienākums novērtējumu veikt attiecīgajai institūcijai sistēmas izstrādes laikā.

[52] Vienlaikus organizācija nedrīkst pieņemt, ka NIDA veikšanas pienākums jau ir izpildīts normatīvā akta pieņemšanas procesā tikai tāpēc, ka konkrētā datu apstrāde ir paredzēta likumā. Lai uzskatītu NIDA veikšanas pienākumu par izpildītu, organizācijai jāpārliecinās, ka normatīvā akta pieņemšanas procesā patiesi veikts pilns iespējamās ietekmes uz personu tiesībām un brīvībām novērtējums, ko radītu plānotā personas datu apstrāde.

[53] Ja organizācija, veidojot jaunu personas datu apstrādes sistēmu, aizpildījusi attīstības aktivitātes aprakstu atbilstoši Ministru kabineta 2023. gada 31. oktobra noteikumu Nr. 619 pielikumam un Ministru kabineta 2023. gada 4. jūlija noteikumu Nr. 368 2. pielikumam, tad šis attīstības aktivitātes apraksts var tikt uzskatīts par NIDA, ja tas ir papildināts ar ietekmes uz datu subjekta datu aizsardzību novērtējumu. Aspekti, kas attīstības aktivitātes aprakstā nav atspoguļoti rakstu zīmju ierobežojuma dēļ, pārzinim jāglabā ar šo aprakstu saistāmā veidā pārskatabildības nodrošināšanai.

Ņem vērā! Informāciju par veiktām darbībām novērtējuma veikšanā varētu meklēt anotācijā un citos dokumentos, kas pamato normatīvā akta nepieciešamību, kā arī institūciju un citu personu sniegtos atzinumos par normatīvā akta projektu[23].

[54] Organizācijas veiktais mājasdarbs – secinājumi par to, vai normatīvā akta pieņemšanas procesā NIDA ir vai nav veikts, ir jādokumentē un jāsaglabā nepieciešamībai:

- ja apstrādē notiek būtiskas izmaiņas un jāsaprot, vai jauno apstākļu ietekme ir vai nav novērtēta;
- ja Inspekcija pieprasa skaidrot, kāpēc veiktās apstrādes ietekme nav vērtēta pirms apstrādes darbību uzsākšanas.

[23] Ja ir veikts novērtējums normatīvā akta pieņemšanas laikā, bet tas nav publiski pieejams, organizācija var vērsties pie normatīvā akta izstrādātāja Informācijas atklātības likuma kārtībā.

[55] Organizācijai nevajadzētu uztvert NIDA par formalitāti – šī instrumenta pirmais un galvenais uzdevums ir palīdzēt novērtēt plānotās personas datu apstrādes ietekmi uz datu subjektu (klientu/iedzīvotāju, nodarbināto) datu aizsardzību. Tāpēc gadījumos, kad normatīvais akts vai tā anotācija satur tikai vispārīgu aprakstu par datu apstrādi un ietekmes novērtējumu, organizācijai ir jāveic atsevišķs NIDA, vismaz par apstrādes tehniskajiem aspektiem, lai noteiktu no apstrādei izvēlētajiem risinājumiem izrietošos potenciālus riskus un to novēršanas pasākumus.

Piemēram, Ministru kabineta 2005. gada 30. augusta noteikumos Nr. 662 "Akcīzes preču aprites kārtība" ir noteikts pienākums noliktavas turētājiem noteiktās vietās uzstādīt videonovērošanas sistēmas noteiktu apstrādes darbību veikšanai (lai novērstu nelikumīgas darbības akcīzes preču apritē). Likumdevējs šo precīzo pienākumu ir uzlicis ar normatīvo aktu, pārzinim nav izvēles kā tieši īstenot plānoto personas datu apstrādi, jo tās nianses jau ir noteiktas normatīvajā aktā. Komersants var prezumēt, ka šādos gadījumos NIDA ir veikts jau juridiskā regulējuma izveides laikā. Nepieciešams vērtēt tikai to aspektu ietekmi, kas nav saistīti ar normatīvo prasību izpildi (piemēram, apstrādei izvēlētās videonovērošanas sistēmas modelis, datu glabāšanas veids u. tml.).

2.3.4. NIDA "baltais saraksts"

[56] Inspekcijas izstrādātais "baltais saraksts"[24] ir izsmeļošs datu apstrāžu uzskaitījums, kurās pastāv paaugstināti riski datu subjekta tiesībām un brīvībām, bet nav jāveic NIDA. **Ja apstrādes darbības ir risku datu subjektu tiesībām un brīvībām radošas un nav nepārprotami minētas "baltajā sarakstā", bet ir tikai līdzīgas apstrādes darbībām, kas šajā sarakstā norādītas, tad NIDA šādam apstrādes procesam tomēr ir veicams.**

[24] Saraksts pieejams: https://www.dvi.gov.lv/lv/novertejums-par-ietekmi-uz-datu-aizsardzibu-nida

III nodaļa "NIDA veikšana un tās posmi"

3.1. Nosaki NIDA veikšanā iesaistītos un to pienākumus

[57] Brīdī, kad organizācija pieņem lēmumu, ka ir nepieciešams veikt NIDA, organizācijas vadībai ir jānosaka ne tikai datu apstrādes procesā iesaistītās personas, bet arī atbildīgās personas par NIDA izstrādi un uzraudzību.

[58] Datu regula atbildību par NIDA veikšanu uzliek pārzinim. Vienlaikus gadījumos, ja tiek iesaistīts apstrādātājs, tam ir pārzinim jāsniedz visa nepieciešamā informācija un atbalsts NIDA izstrādes procesā. Tāpēc ir svarīgi jau sākotnēji noteikt datu apstrādes procesā iesaistīto personu lomas – pārzinis, kopīgi pārziņi (saukts arī kā "koppārzinis") vai apstrādātājs. Ja pārzinis ir iecēlis datu aizsardzības speciālistu (DAS), pārzinim ir pienākums uzklausīt DAS padomu NIDA izstrādes gaitā.

3.1.1. Lomu "pārzinis, kopīgie pārziņi un apstrādātājs", nozīme NIDA procesā

[59] Pārzinis ir tā persona, kura noteiks un pieņems lēmumu – kāpēc un kā personu dati ir apstrādājami. Ja šo lēmumu pieņem vairākas personas kopā (piemēram, divas organizācijas), tie tiks uzskatīti par kopīgiem pārziņiem. Kopīgiem pārziņiem savā starpā ir jāvienojas un jānosaka katra konkrētā pārziņa pienākumi.

[60] Atbilstoši Datu regulas 35. panta 1. punktam, pārzinis (vai kopīgi pārziņi) ir atbildīgs par NIDA un tas uzņemas atbildību par NIDA izstrādi un risku mazinošo pasākumu īstenošanu. Tas nozīmē, ja gadījumā pārzinis uzdod NIDA izstrādāt kādam savas organizācijas darbiniekam vai darbinieku grupai, vai arī pilnībā vai daļēji NIDA veikšanai piesaista ārpakalpojumu sniedzēju (sk. NIDA veicējs), pārzinis jebkurā gadījumā būs atbildīgs par NIDA atbilstību Datu regulas prasībām.

[61] Apstrādātājs ir tā persona, kura veic datu apstrādi pārziņa (vai kopīgu pārziņu) vārdā. Apstrādātājs nenosaka un nepieņem lēmumu – kāpēc un kā tiks apstrādāti personas dati. Pārzinim un apstrādātājam ir jānoslēdz vienošanās, kurā nosaka vismaz Datu regulas 28. pantā noteiktās sastāvdaļas, tai skaitā, bet ne tikai vienošanās priekšmetu un apstrādes ilgumu, apstrādes raksturu un nolūku, apstrādājamo personas datu veidus un datu subjektu kategorijas, kā arī abu pušu pienākumus un tiesības.

[62] Ja datu apstrādi pilnībā vai daļēji veic apstrādātājs, tam ir pienākums palīdzēt pārzinim NIDA izstrādes procesā, sniedzot tam visu nepieciešamo informāciju.[2] Tas nozīmē, ka, pamatojoties uz starp pārzini un apstrādātāju noslēgto vienošanos, apstrādātājam ir jāsniedz visa tam pieejamā informācija, kas attiecas uz darbībām, ko apstrādātājs nodrošina pārziņa vārdā, piemēram, bet ne tikai, par ieviestajiem tehniskajiem un organizatoriskajiem pasākumiem datu apstrādes drošībai.

[63] Gadījumā, ja apstrādātājs pārzinim piedāvā jau izstrādātu tehnisko risinājumu, lai sniegtu pakalpojumu pārzinim, apstrādājot personas datus tā vārdā, pārzinim ir jābūt pārliecinātam, ka tam joprojām ir kontrole pār datu apstrādes rakstura, apjoma, nolūka, līdzekļu u.c. noteikšanu. Pārzinim jāapzinās, ka, izmatojot produktu, par kura atbilstību tam ir šaubas, tas uzņemas atbildību par iespējamām neatbilstībām.

[64] Detalizētu informāciju par pārziņa, kopīga pārziņa un apstrādātāja jēdzieniem, kā arī to pienākumu un tiesību noteikšanu skatīt EDAK 2021. gada 7. jūlijā pieņemtajās pamatnostādnēs[25].

[25] EDAK 2021. gada "Pamatnostādnes par pārziņa un apstrādātāja jēdzieniem VDAR Versija 2.0". Pieejams: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

3.1.2. Datu aizsardzības speciālists

[65] DAS ir tā persona, kura ar savām speciālajām zināšanām datu aizsardzībā konsultē pārzini. DAS galvenā funkcija ir sniegt neatkarīgu viedokli par plānotas vai jau ieviestas datu apstrādes atbilstību Datu regulai un citiem datu aizsardzības jomai saistošiem normatīvajiem aktiem.[3] DAS nevarēs sniegt neatkarīgu viedokli par plānoto vai ieviesto datu apstrādes atbilstību Datu regulai, ja DAS pats veiks NIDA. Ja DAS tiek nostādīts pozīcijā, kur tas faktiski veic NIDA, DAS nonāks interešu konfliktā[26].

[66] Saskaņā ar Datu regulas 35. panta 2. punktu, pārzinis veicot NIDA lūdz padomu DAS (ja tāds ir norīkots). Jāņem vērā, ka DAS konkrētajā gadījumā var tikai ieteikt, kuros gadījumos NIDA veicams, kādu metodoloģiju izmantot, var izskaidrot iespējamo datu apstrādes tiesisko pamatu, kā arī sniegt citus padomus NIDA izstrādes laikā, neradot interešu konfliktu.

[67] Pēc pārziņa lūguma[27] DAS novērtē, vai NIDA ir veikts atbilstoši un vai novērtējumā ietvertie secinājumi ir atbilstoši Datu regulai. Noslēgumā DAS var ieteikt pasākumus, kuri pārzinim jāievieš, lai mazinātu, vai novērstu identificētos riskus fiziskas personas tiesībām un brīvībām.

[68] DAS, saskaņā ar Datu regulas 39. panta 1. punkta c) apakšpunktu, pārrauga NIDA īstenošanu organizācijā, tai skaitā, konsultējot un pārraugot atbilstību NIDA veikšanas procesā. Pārzinim ir pienākums nodrošināt, ka DAS NIDA īstenošanas atbilstību Datu regulai vērtē gan attiecībā uz organizācijas iekšēji veikto, gan attiecībā uz citu piesaistīto ekspertu izstrādāto NIDA. Neatkarīgi no DAS sniegtajiem ieteikumiem, atbildīgs par datu apstrādi un ar to saistītiem jautājumiem ir pārzinis. Gadījumā, ja DAS sniedz viedokli, ka nepiekrīt NIDA secinājumiem, pārzinim ir rakstiski jāpamato, kāpēc šis viedoklis nav ņemts vērā[28].

Ņem vērā! Būtisks priekšnoteikums atbilstoša NIDA izstrādes procesā ir dokumentēt visu iesaistīto personu sniegtos viedokļus, padomus vai pieņemtos lēmumus.

3.1.3. NIDA veicējs

[69] Organizācija ieceļ NIDA veicēju. Organizācija, pēc savas izvēles, var apspriesties ar DAS (ja tāds ir norīkots), kura persona/-as vai struktūrvienības būs atbildīgas par NIDA veikšanu. Jebkurā gadījumā NIDA veicējam ir nepieciešamas padziļinātas zināšanas par personas datu apstrādi un aizsardzību. NIDA veicējam nepieciešamas arī zināšanas par to organizācijas darbības aspektu, uz kuru ir attiecināma plānotā personas datu apstrāde. Ja NIDA veicējam šādu zināšanu nav, tad organizācijai jānorīko atbildīgās personas, kuras sniegs atbalstu attiecībā uz jomas specifiskajiem apstrādes aspektiem.

[70] Lai arī vadlīniju kontekstā par NIDA veicēju runā vienskaitlī un lielākoties tā būs viena persona, kas apliecinās veiktās NIDA atbilstību Datu regulai, lielākoties NIDA ir komandas darbs, un NIDA būs vairāku personu un lielāku organizāciju gadījumā – vairāku struktūrvienību mijiedarbības produkts.

[71] Tā būs arī gadījumā, ja NIDA veikšanai tiks piesaistīts ārpakalpojuma sniedzējs. Bez sadarbības nodrošināšanas starp uzņēmuma attiecīgajām struktūrām un NIDA veicēju nebūs iespējams nodrošināt efektīvu plānotās apstrādes ietekmes novērtējumu.

[26] Datu regulas 39. panta 1. punkta c) apakšpunkts.
[27] 29. panta darba grupas 2016. gada 13. decembra (redakcija 05.04.2017.) pamatnostādnes par datu aizsardzības speciālistiem ("DAS"). https://ec.europa.eu/newsroom/article29/items/612048
[28] Turpat, 17. lpp.

3.2. Apraksti plānoto personas datu apstrādi un tās vietu organizācijas procesos

[72] Nākamais posms, kad organizācija ir pieņēmusi lēmumu, ka ir nepieciešams un ir noteiktas atbildīgās personas, kuras veiks NIDA, tā process ir jāsāk ar plānotās personas datu apstrādes aprakstu un tās vietu organizācijas procesos, jo īpaši sasaistot to kopā ar kiberdrošības un biznesa vadības procesiem.

[73] Personas datu apstrāde nav atrauta no organizācijā esošajiem drošības un biznesa vadības procesiem. Jebkurā gadījumā, veidojot jaunu personas datu apstrādi, tā būs saistīta ar kādu organizācijas darbības aspektu un tādejādi saistīsies ar citiem jau pastāvošiem procesiem. Līdz ar to NIDA nesākas no "tukšas" lapas, bet drīzāk tajā saplūst informācija no dažādiem citiem, ar plānoto apstrādi saistītiem, avotiem. Efektīva darba plānošana ļaus no saistītajiem avotiem paņemt nepieciešamo informāciju, aiztaupot darba veikšanā ieguldāmo kopējo resursu.

[74] Šajā posmā organizācijai ir nepieciešams veikt plašāku plānotās datu apstrādes analīzi, kas sevī ietver kodolīgu plānotās datu apstrādes aprakstu, datu apstrādes funkcionālā apraksta izstrādi (pamatojoties uz datu apstrādes dzīves ciklu). Datu apstrādes analīze var ietvert arī personas datu apstrādes vizualizāciju, kas izriet no datu apstrādes dzīves cikla.

[75] Datu apstrādes analīze palīdzēs organizācijai identificēt gan galvenos personas datu apstrādes elementus, gan arī dažādas darbības datu aizsardzībai (tai skaitā, to nepieciešamību) un datu apstrādes procesu savstarpējo mijiedarbību.

Ņem vērā! Šajā sadaļā organizācija var veikt arī plānotās datu apstrādes identifikāciju (tai skaitā, piešķirt tai nosaukumu, kuru vēlāk varēs iekļaut "datu apstrādes reģistrā"). Šis process atvieglos vēlākas darbības, ja pēc NIDA veikšanas tiks secināts, ka apstrāde var tikt veikta. Ieteicams arī norādīt izmaiņas datu apstrādē, ja tādas ir bijušas un ja datu apstrādes raksturojums un analīze tiek veikta par jau esošu datu apstrādi.

3.2.1. Datu kategorijas

[76] Plānotās personas datu apstrādes kontekstu un tās vietu organizācijas procesos, kas saistīti ar kiberdrošības un biznesa vadību, ir grūti definēt, ja nav izvērtēts, kādas personas datu kategorijas un kādā apjomā tiks apstrādātas. Plānojot, kā apstrādājamās personas datu kategorijas mijiedarbosies ar datu apstrādes kontekstu, ir nepieciešams klasificēt personas datus, kurus organizācija plāno apstrādāt.

[77] Visus personas datus nosacīti var iedalīt trīs lielās grupās – personas dati, īpašu kategoriju personas dati un dati par personu sodāmību. Vērtējot ierobežojumus īpašu kategoriju personas datu apstrādei vai ziņu par sodāmību apstrādei, secināms, ka Datu regulā noteikts, ka šādu datu apstrāde pati par sevi ir ar potenciāli lielāku ietekmi uz fizisku personu.

Ņem vērā! Vispārējā likumības novērtējuma ietvaros organizācijai nav nepieciešams veikt tālāku analīzi par plānotās apstrādes datu veidu iespējamo ietekmi uz fizisku personu, kā vien noteikt, vai tie ietilpst kādā no trīs lielajām iepriekš pieminētajām datu grupām, un secināt, vai to apstrāde būs tiesiska. Taču NIDA kontekstā organizācijai datu klasifikācijā, atbilstoši to potenciālajai ietekmei uz fizisku personu, var būt nepieciešams pielikt lielākas pūles.

3.2.2. Datu kategoriju izvērtējums

[78] NIDA veikšanas kontekstā organizācija, nosakot plānotās datu apstrādes ietekmi, var ņemt vērā vismaz šādus kritērijus:

- Dati, kuru neatbilstoša apstrāde var radīt tiešu ietekmi uz fizisku personu. Jo lielāks ir tiešas ietekmes risks uz datu apstrādi, jo lielāks tiešas potenciālas ietekmes risks fiziskai personai.
- Datu apjoma, ko apstrādā organizācija, atbilstība fiziskas personas gaidām.
- Kāda ir fiziskas personas attieksme pret datu apstrādi? Vai tā uzskata, ka konkrētā datu apstrāde tai var radīt īpašu risku?
- Novērtējums par datu turpmākas izmantošanas iespējām citu personu nolūku sasniegšanai. Vai konkrētie dati ir nepieciešami un lietderīgi citām personām (tirgus dalībniekiem, ļaunprātīgiem uzbrucējiem, konkurentiem, jebkurai personai, kas teorētiski var datus iegūt)? Vai šo datu izmantošana ļauj gūt lielāku peļņu vai konkurences priekšrocības, vai arī dati var tikt izmantoti krāpniecības shēmās? Jo iekārojamāki šie dati ir trešajām personām, jo lielāki riski šo datu apstrādei rodas no mērķtiecīga trešās puses uzbrukuma.

[79] Šo un, iespējams, arī citu kritēriju kopums ļaus noteikt kopējo risku, kas fizisku personu tiesībām un brīvībām veidojas tieši izrietoši datu kategorijām, kuras plānots apstrādāt.

[80] Jāņem vērā, ka, visticamāk, plānotā personas datu apstrādes nolūka sasniegšanai tiks apstrādāti dažādi personas datu veidi. Apstrādājamo datu veidu kategorizēšana un sistematizēšana atvieglos plānoto apstrādes darbību apraksta izstrādi.

[81] Kārtot datus grupās ir iespējams atbilstoši dažādām metodēm:
- atbilstoši plānotajam datu izmantošanas nolūkam (lai organizācija nodrošinātu normatīvajos aktos noteiktos pienākumus attiecībā uz grāmatvedības kārtošanu, tai jāglabā informācija par personas veiktajiem maksājumiem);
- atbilstoši datu raksturojumam (piemēram, viens no datu veidiem var būt fiziskas personas kontaktinformācija).

Ņem vērā! Konkrētais sistematizācijas un kategorizēšanas veids ir atkarīgs tieši no organizācijas, un ir iespējami visdažādākie risinājumi.

[82] NIDA ietvaros kategorizēti dati ir izmantojami risku novērtējumā par potenciālās datu apstrādes ietekmi uz fizisku personu tiesībām un brīvībām. Katrai atsevišķai datu kategorijai veicams atsevišķs tās radīto – gan ārējo, gan iekšējo risku un apdraudējumu novērtējums. Līdz ar to pilnvērtīga datu veidu analīze sniegs pirmo riska faktora vērtību, kas tiks izmantota kopējās riska vērtības noteikšanā.[29]

3.3. NIDA veikšanas metodoloģija

[83] Pirms atbilstošas metodoloģijas izvēles un risku novērtējuma veikšanas, organizācijai ir jādefinē skaidrs un saprotams novērtējuma tvērums. Nav viena universāla veida, kā veikt NIDA. Atbilstošās metodes izvēle būs atkarīga no plānotās datu apstrādes situācijas sarežģītības, tai skaitā datu apstrādē izmantotajiem tehnoloģiskajiem risinājumiem. Ja organizācijai nav pieredzes plānotai datu apstrādei līdzīgu darbību veikšanā vai ir maz pieejamās informācijas par izvēlēto tehnoloģisko procesu, un/vai datu apstrādes darbības pēc būtības ir komplicētas – organizācijai vai tās pilnvarotajai personai ir attiecīgi jāpaplašina NIDA ietvars, lai NIDA attiektos ne tikai uz tiešajām riskantajām datu apstrādes darbībām, bet arī uz ar tām saistītajām datu apstrādes darbībām.

Ņem vērā! Organizācija ir atbildīga un tai ir jāveic visi nepieciešamie pasākumi, izvērtējot un izvēloties plānotajai datu apstrādei atbilstošāko NIDA veikšanas metodoloģiju.

[84] NIDA tiek veidots tā, lai analizētu kā incidentu (tai skaitā, personas datu aizsardzības pārkāpumu) un dažādu notikumu iespējamība varētu ietekmēt fiziskas personas tiesības un brīvības,

[29] Riska novērtēšanas vienādojumu skatīt III nodaļas "NIDA veikšana un tās posmi" sadaļu "Riska novērtējums".

identificēt un noteikt konkrētus procesus, kas ir jāievieš, lai tos novērstu vai pēc iespējas veiksmīgāk pārvaldītu. Veicot NIDA, viens no priekšnosacījumiem ir kvalitatīvi veikt priekšdarbus, apzinot esošo situāciju vai pagātnes notikumus, ja ir notikušas līdzīgas datu apstrādes (arī ārpus konkrētās organizācijas).

[85] NIDA palīdz organizācijām identificēt, novērtēt un novērst riskus, kas saistīti ar datu apstrādes darbībām. Tie ir īpaši svarīgi, kad tiek ieviests jauns datu apstrādes process, sistēma vai tehnoloģija. NIDA nodrošinās, ka organizācijā notiek:

- analīze par riska iespējamajām sekām uz personu;
- analīze tam, vai datu kategorijas, apstrādes veids, datu subjektu kategorijas, datu apstrādē izmantotas tehnoloģijas rada augstu risku, ka incidents var notikt.

[86] Šajā nodaļā Inspekcija, pamatojoties uz iepriekšējo pieredzi izskatot NIDA, kurus iesnieguši pārziņi saskaņā ar Datu regulas 36. pantu, ir izstrādājusi metodoloģiju un ieteikumus NIDA veikšanai[30].

Ņem vērā! Inspekcijas piedāvātā metodoloģija nav universāla, un katra organizācija to var pielāgot savām vajadzībām.

[87] Neatņemama NIDA sastāvdaļa ir atbilstoši apstākļiem veikts riska faktoru novērtējums. Vēršam uzmanību, ka praksē būs nepieciešams katrai riska faktoru grupai pievērsties detalizētāk, sadalot to no apstrādes faktiskajiem apstākļiem atkarīgos apakšelementos.

Ņem vērā! Ietekmes faktoru piemēri un ietekmes līmeņi ir ilustratīvi, un katra organizācija, pamatojot ietekmes novērtēšanu var noteikt, izmantojot piedāvātos kritērijus.

3.3.1. Datu kategorijas

[88] Ietekmes faktora noteikšana un ietekmes līmeņa klasifikācija, kas izriet no datu apstrādē iesaistītajām datu kategorijām. Lai noteiktu ietekmes līmeni attiecībā uz personas datu kategorijām, kuras plānots apstrādāt, organizācijai ir jāņem vērā:

- datu jutīgums: vai personas dati ietilpst "parasto" vai "īpašo" datu kategorijās;
- datu apjoms: vai dati ietver lielas datu kopas vai ļoti detalizētu privātu informāciju;
- iespējamais kaitējums: kādas varētu būt ļaunprātīgas datu izmantošanas vai nesankcionētas izpaušanas sekas (piemēram, identitātes zādzība, diskriminācija).

Piemēram:

Ietekmes faktors	Ietekmes līmenis (kvalitatīvi)	Ietekmes līmenis (kvantitatīvi)
Īpašu kategoriju dati, dati par sodāmību	Ļoti augsts	4
Finanšu dati, kas tiek iegūti un apstrādāti, lai novērtētu, tostarp profilētu vai prognozētu datu subjekta ekonomisko stāvokli	Augsts	3
Personas apliecinošo dokumentu kopijas, dati, kuri izmantoti profilēšanai (nesatur īpašo kategoriju datus)	Vidējs	2
Personas vārds, uzvārds, dzīvesvietas adrese, kontaktinformācija	Zems	1

[30] NIDA metodoloģijas izstrādei izmantots ISO IEC 31010:2019 "Risk management -- Risk assessment techniques". Standarta izmantošanai nepieciešama licence. Iegādei pieejams: https://www.lvs.lv/lv/products/148861. Izmantotas arī Spānijas datu aizsardzības iestādes (AEPD) 2021. gadā izstrādātās vadlīnijas "Risk Management and Impact Assessment in the Processing of Personal Data". Pieejamas angļu valodā: https://www.aepd.es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf

3.3.2. Datu apstrāde

[89] Ietekmes faktora noteikšana un ietekmes līmeņa klasifikācija, kas izriet no plānotās datu apstrādes. Lai noteiktu ietekmes līmeni attiecībā uz personas datu apstrādes veidu, kuru plānots veikt, organizācijai ir jāņem vērā:

- Automatizēta datu apstrāde un profilēšana: vai apstrāde ietver automatizētu lēmumu pieņemšanu vai profilēšanu ar juridiskām vai citām būtiskām sekām;
- Datu avotu kombinācija: vai dati tiek sapludināti no vairākiem datu avotiem, palielinot datu apstrādes sarežģītību un tādējādi radot lielākus riskus, ka varētu notikt kļūda datu apstrādes procesā;
- Apstrāde reāllaikā: apstrādes tiešums (piemēram, izsekošana reāllaikā) un tās potenciāls radīt tūlītēju kaitējumu.

Piemēram:

Ietekmes faktors	**Ietekmes līmenis (kvalitatīvi)**	**Ietekmes līmenis (kvantitatīvi)**
Apstrāde kuras mērķis ir radīt jaunus īpašu kategoriju datus. Piemēram: • Ģenētiski novērtētas un/vai prognozētas slimības/veselības.	Ļoti augsts	4
Profilēšana. Piemēram: • Profila izmantošana • Uzvedības analīze	Augsta	3
Darbinieku kontrole. Piemēram: • Videonovērošana darbavietā • Audioieraksts darba vietā • E-pasta uzraudzība un kontrole • Interneta pārlūkošanas uzraudzība un kontrole darba vietā • Lietojumprogrammu/pakalpojumu izmantošanas darba vietā uzraudzība • Tālruņa lietošanas, telefonsarunu ieraksts un analīze	Vidējs	2
Fiziskās piekļuves kontrole, neizmantojot biometrijas datus. Piemēram: • Darba vietas piekļuves kontrole • Piekļuves kontrole ēkām (publisks/privāts)	Zems	1

3.3.3. Datu avots

[90] Ietekmes faktora noteikšana un ietekmes līmeņa klasifikācija, kas izriet no datu avota. Lai noteiktu ietekmes līmeni attiecībā uz personas datu apstrādes avotu, kuru plānots izmantot, organizācijai ir jāņem vērā:

- Tieša vai netieša vākšana: vai dati tiek vākti tieši no fiziskas personas vai arī izsecināti no apstrādes, vai netieši no trešām personām;
- Datu ieguves avotu ticamība: vai datu avoti ir ticami un nodrošina atbilstību Datu regulai;
- Datu subjekta informētība: vai datu subjekti ir informēti par to datu vākšanu un izmantošanu.

Piemēram:

Ietekmes faktors	Ietekmes līmenis (kvalitatīvi)	Ietekmes līmenis (kvantitatīvi)
Personas dati ģenerēti, izmantojot jaunas tehnoloģijas un/vai ir veikta datu subjekta profilēšana. Piemēram, dati izgūti no tādas trešās personas, kuras pamatdarbība saistīta ar personas datu apstrādi.	Ļoti augsts	4
Personas dati iegūti no iepriekš veiktas datu apstrādes vai cita pārziņa, un ir šaubas par šī pārziņa rīcības likumību.	Augsta	3
Personas dati iegūti no iepriekš veiktas datu apstrādes vai cita pārziņa jauna datu apstrādes nolūka sasniegšanai.	Vidējs	2
Personas dati iegūti no publiski pieejamas informācijas.	Zems	1

3.3.4. Datu apstrādes apjoms

[91] Ietekmes faktora noteikšana un ietekmes līmeņa klasifikācija, kas izriet no datu apstrādes apjoma. Lai noteiktu ietekmes līmeni attiecībā uz personas datu apstrādes apjomu, organizācijai ir jāņem vērā:

- Ģeogrāfiskā darbības joma: vai datu apstrāde attiecas tikai uz konkrētu reģionu vai ir saistīta ar starptautisku darbības jomu;
- Apstrādes nolūks: vai nolūks ir šauri definēts vai plašā mērogā, potenciāli izraisot datu apstrādi nenoteiktā apjomā;
- Apstrādes ilgums: cik ilgi dati tiks apstrādāti un glabāti.

Piemēram:

Ietekmes faktors	Ietekmes līmenis (kvalitatīvi)	Ietekmes līmenis (kvantitatīvi)
Sistemātiska plaša mēroga datu apstrāde	Ļoti augsts	4
Organizācijai nav iespējams skaidri noteikt apstrādājamo datu apjomu vai organizācijai ir ierobežota ietekme kontrolēt datu glabāšanas ilgumu	Augsts	3
Normatīvajā aktā noteiktas datu apstrādes veikšana, ja tiek izmantoti jauni tehnoloģiski risinājumi	Vidējs	2
Datu apstrāde ne plašā mērogā, neizmantojot inovatīvus tehniskus risinājumus	Zems	1

3.3.5. Datu subjekta kategorijas

[92]Ietekmes faktora noteikšana un ietekmes līmeņa klasifikācija, kas izriet no datu apstrādē iesaistītajām datu subjektu kategorijām. Lai noteiktu ietekmes līmeni attiecībā uz fizisku personu kategorijām, kuras pakļautas datu apstrādei, organizācijai ir jāņem vērā:

- Neaizsargātas grupas: vai datu subjektu vidū ir bērni, gados vecāki indivīdi vai citas neaizsargātas iedzīvotāju grupas;
- Datu subjektu skaits: ietekmēto datu subjektu mērogu;
- Datu subjektu attiecības: datu subjektu un pārziņa (piemēram, klientu, darbinieku) attiecības.

Piemēram:

Ietekmes faktors	Ietekmes līmenis (kvalitatīvi)	Ietekmes līmenis (kvantitatīvi)
Bērni, kas jaunāki par 13 gadiem; Cilvēki ar garīga rakstura traucējumiem; Noziegumu upuri.	Ļoti augsts	4
Gados vecāki cilvēki; Pacienti; Citi riska grupā esoši cilvēki (piemēram, ar redzes, dzirdes, kustību traucējumiem; sociālo minoritāšu grupas (arī, ja plānotā datu apstrāde varētu radīt šādu risku)).	Augsts	3
Darbinieki; Organizācijas klienti.	Vidējs	2
Datu subjekts (iedzīvotājs), kuram nav īpaša statusa attiecībās ar organizāciju	Zems	1

3.3.6. Datu apstrādē izmantotās tehnoloģijas

[93]Ietekmes faktora noteikšana un ietekmes līmeņa klasifikācija, kas izriet no datu apstrādē izmantotajām tehnoloģijām. Lai noteiktu ietekmes līmeni attiecībā uz datu apstrādē izmantotajām tehnoloģijām, organizācijai ir jāņem vērā:

- vai apstrādē tiek izmantotas jaunas (inovatīvas) vai nepārbaudītas tehnoloģijas, kas var radīt nezināmus riskus;
- kāds ir ieviesto drošības pasākumu šifrēšanas, piekļuves kontroles un citu tehnisko garantiju atbilstības novērtējums;
- kāds ir tehnoloģijas nepareizas izmantošanas vai ļaunprātīgas izmantošanas iespējas (piemēram, sejas atpazīšana novērošanai) izvērtējums/iespējamība.

Piemēram:

Ietekmes faktors	Ietekmes līmenis (kvalitatīvi)	Ietekmes līmenis (kvantitatīvi)
Jaunu un/vai nepārbaudītu tehnoloģiju izmantošana, kurām nav veiks novērtējums par ietekmi uz privātumu.	Ļoti augsts	4
Plaša mēroga informācijas sistēmas; Izsekošanas (GPS) tehnoloģijas; Tehnoloģijas, kas domātas personas unikālai identifikācijai (biometrisko datu izmantošana);	Augsta	3
Risinājumi, kuru nolūks ir iegūt datus no klienta, tai skaitā mobilās lietotnes; Videonovērošanas sistēmas; Informācijas sistēmas	Vidējs	2
Risinājumi, ar kuru starpniecību netiek iegūti dati, ar kuru palīdzību iespējama tieša klienta identifikācija, piemēram, tīmekļa vietne.	Zems	1

3.3.7. Pārziņa/apstrādātāja darbības jomas

[94] Ietekmes faktora noteikšana un ietekmes līmeņa klasifikācija, kas izriet no organizācijas/apstrādātāja darbības jomas. Lai noteiktu ietekmes līmeni attiecībā uz pārziņa vai apstrādātāja darbības jomu, organizācijai ir jāņem vērā, vismaz:

- Lielums un mērogs: organizācijas lielums un tās apstrādes iespējas;
- Atbilstības vēsture: ņemta vērā pārziņa vai apstrādātāja līdzšinējā atbilstības Datu regulai nodrošināšana (vai ir piemēroti sodi, notikuši personas datu aizsardzības pārkāpumi);
- Darbības sfēra: nozare, kurā organizācija darbojas un iespējamās sekas, ja trešās personas nesankcionēti piekļūst personas datiem.

Piemēram:

Ietekmes faktors	**Ietekmes līmenis (kvalitatīvi)**	**Ietekmes līmenis (kvantitatīvi)**
Veselības aprūpes/ biotehnoloģiju uzņēmums	Ļoti augsts	4
AML likuma subjekti	Augsts	3
Mārketinga uzņēmums	Vidējs	2
Kurjerserviss	Zems	1

3.3.8. Datu nosūtīšana uz trešajām valstīm vai starptautiskām organizācijām

[95] Ietekmes faktora noteikšana un ietekmes līmeņa klasifikācija, kas izriet no datu nosūtīšanas uz trešo valsti. Lai noteiktu ietekmes līmeni attiecībā uz datu nosūtīšanu uz trešajām valstīm vai starptautiskām organizācijām, organizācijai ir jāņem vērā:

- Lēmumi par atbilstību: pārbaudīt, vai galamērķa valsts vai organizācija nodrošina atbilstošu datu aizsardzības līmeni saskaņā ar Datu regulu;
- Nodošanas mehānismi: izvērtēt drošības pasākumu, piemēram, standarta līguma klauzulu vai saistošo korporatīvo noteikumu izmantošanu;
- Jurisdikcijas riski: ņem vērā riskus, ko rada konfliktējoši tiesību akti galamērķa valstī, piemēram, valdības uzraudzība.

Piemēram:

Ietekmes faktors	**Ietekmes līmenis (kvalitatīvi)**	**Ietekmes līmenis (kvantitatīvi)**
Datu nosūtīšana uz trešajām valstīm vai starptautiskām organizācijām, kur organizācijai ir šaubas par iespēju nodrošināt pietiekamus aizsardzības pasākumus, piemēram, kompetento iestāžu attiecīgajā valstī plašo pilnvaru dēļ.	Ļoti augsts	4
Datu, kas savas būtības dēļ attiecīgajā trešajā valstī var radīt paaugstinātu risku personas tiesībām un brīvībām.	Augsts	3
Nepārskatāma pārredzamības nodrošināšana attiecībā uz personas datu apstrādi (piemēram, publikācijas sociālajos tīklos).	Vidējs	2
Personas datu nodošana uz trešajām valstīm, vai starptautiskām organizācijām, bez papildu identifikatoriem (pseidonimizētu datu nodošana) vai tādā apjomā, kas tikai netieši identificē personu, vai ko pats datu subjekts ir padarījis publisku (publiski pieejams lietotājvārds/segvārds).	Zems	1

3.4. Riska novērtējums

[96] Kad organizācija ir izvēlējusies, kādā veidā tiks veikta risku izvērtēšana par personas datu apstrādes ietekmi uz fiziskas personas tiesībām un brīvībām, tai ir jāuzsāk risku noteikšanas process un izvērtēšana. Riska pārvaldība ir organizācijas jebkuru procesu būtisks elements, lai apzinātu iespējamās problēmas un risinājumus un lai tās vadītājs spētu pieņemt pamatotu lēmumu turpmākai rīcībai.

[97] Datu regulā organizācijām ir noteikta prasība identificēt, novērtēt un mazināt iespējamos riskus attiecībā uz fizisku personu tiesībām un brīvībām, kurus var radīt to datu apstrāde. Identificēto risku mazināšana ir jāveic, pieņemot un ieviešot samērīgus, bet atbilstošus tehniskos un organizatoriskos pasākumus, kas nodrošina un demonstrē šo tiesību aizsardzību.

Ņem vērā! Datu regulas 76. apsvērumā noteikts, ka risks jāizvērtē pamatojoties uz objektīvu novērtējumu, ar ko nosaka, vai datu apstrādes darbības ietver risku vai augstu risku.

3.4.1. Kas ir risks?

[98] Risks fizisku personu tiesībām un brīvībām ir saistāms ar potenciālu iespēju fiziskam, materiālam vai nemateriālam kaitējumam. Īpaši, ja datu apstrāde izraisa, vai var izraisīt diskrimināciju, identitātes zādzību vai viltošanu, finansiālu zaudējumu, kaitējumu reputācijai, ar dienesta noslēpumu aizsargātu personas datu konfidencialitātes zaudēšanu, neatļautu pseidonimizācijas atcelšanu vai jebkādu citu īpaši nelabvēlīgu ekonomisko vai sociālo situāciju. Tāpat paaugstinātu risku var radīt datu subjektiem atņemtas viņu tiesības un brīvības, vai liegta iespēja kontrolēt savus personas datus, kā arī, ja tiek apstrādāti īpašas kategorijas dati vai dati par sodāmību[31].

[99] Vienlaikus Datu regulā jēdziens "risks" nav definēts, tomēr, ievērojot minētās regulas tvērumu un piemērojamību, Inspekcija vadlīniju ietvaros šo jēdzienu skaidro pamatojoties uz Starptautiskās standartizācijas organizācijas (turpmāk – ISO) 31000:2018 "Riska pārvaldība" definīciju, kas pasaka, ka **"risks" ir "kaitējuma rašanās varbūtības un tā ietekmes kombinācija[32]"**. Nosakot risku ir jāņem vērā tā raksturojošās pazīmes.

Ņem vērā! Risku raksturojošās pazīmes ir:
- iespējamība (angļu valodā: likelihood) – iespēja, ka kaut kas notiks;
- iespēja (angļu valodā: opportunity) – apstākļu kopums, kas varētu būt labvēlīgs mērķiem;
- varbūtība (angļu valodā: probability) – iespējamības mērvienība *(ISO 31010:2019[33] skala ir 0 (neiespējami) un 1 (pilnīgi noteikti)*;
- riska virzītājs (angļu valodā: driver of risk) – faktors, kas būtiski ietekmē risku;
- apdraudējums (angļu valodā: threat) – potenciālais apdraudējuma, kaitējuma vai cita nevēlama iznākuma avots

[100] Atbilstoši ISO 31010:2019 "Riska pārvaldība. Riska novērtēšanas metodes", risku var raksturot arī balstoties uz riska avotiem, iespējamiem notikumiem, to sekām un seku iestāšanās iespējamību.

Ņem vērā!
- riska avoti var būt mainīgi. Tie var būt saistīti ar dažādiem faktoriem, tostarp cilvēka uzvedību, organizatoriskām struktūrām vai sabiedrības ietekmēm. Līdz ar to var būt grūti paredzēt kāda konkrēta notikuma iestāšanos;

[31] ISO 31000:2018 "Risk management Guidelines". Standarta izmantošanai nepieciešama licence. Iegādei pieejams: https://www.lvs.lv/lv/products/137874
[32] ISO 31000:2018 "Risk management Guidelines". Standarta izmantošanai nepieciešama licence. Iegādei pieejams: https://www.lvs.lv/lv/products/137874
[33] ISO IEC 31010:2019 "Risk management -- Risk assessment techniques". Standarta izmantošanai nepieciešama licence. Iegādei pieejams: https://www.lvs.lv/lv/products/148861

- notikumam var būt vairāki cēloņi, un tam var būt vairākas sekas;
- sekām var būt vairākas atsevišķas vērtības, tās var būt nepārtrauktas vai nezināmas. Sekas var nebūt saskatāmas vai izmērāmas sākumā, bet tās var uzkrāties laika gaitā.

[101] Tas nozīmē, ka organizācijai, uzsākot jaunu darbības veidu, kas sevī ietver datu apstrādi, ir jāizvērtē iespējamie riski cilvēka tiesībām un brīvībām. Izvērtējumā ir jāņem vērā dažādi potenciālie notikumi, apdraudējumi un faktori, kurus savieno kopā ar iespējamību un varbūtību, ka minētais apdraudējums varētu iestāties.

Piemēram, uzņēmums plāno nodrošināt pilsētas "X" iedzīvotājiem elektroskūteru nomu. Lai saņemtu pakalpojumu, iedzīvotājiem nepieciešams lejupielādēt lietotni, reģistrēt profilu, autentificēties, lai apliecinātu savu vecumu un pievienot bankas datus. Šajā gadījumā, lai sāktu savu uzņēmējdarbību, komersantam papildus potenciālo finanšu risku (piemēram, izmaksas, peļņu); nepieciešamo cilvēkresursu, lai īstenotu plānoto uzņēmējdarbību izvērtējumam, vērtē arī kādus riskus plānotā datu apstrāde, izmantojot jaunus paņēmienus un tehnoloģiskos risinājumus, varētu radīt uzņēmuma klientiem. Tie ietver, tai skaitā, drošības riskus personai (kas var rezultēties gan materiālos, gan nemateriālos zaudējumos), kā arī potenciālo ietekmi uz citām fiziskas personas tiesībām un brīvībām. Ja organizācija risku novērtējumā secina, ka tie ir augsti, tad nepieciešams veikt NIDA.

3.4.2. Kāds ir riska apjoms, ko organizācija ir gatava uzņemties?

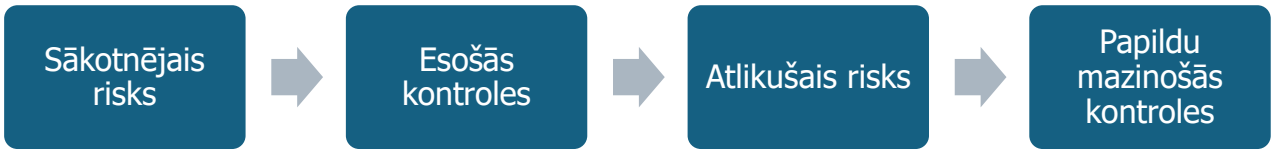
[102] Riska apetīte jeb riska apjoms, ko organizācija ir gatava uzņemties, ir atlikušais risks, kas ir palicis pēc aizsardzības pasākumu ieviešanas. Nolūks ir samazināt atlikušo risku līdz pieņemamam riska līmenim, kuru organizācija ir gatava uzņemties.

Ņem vērā! Organizācija var būt gatava uzņemties arī riska apjomu, kas ir uzskatāms par augstu. Tomēr šādā gadījumā pēc NIDA veikšanas ir nepieciešams konsultēties ar Inspekciju, ievērojot Datu regulas 36. pantā noteikto procedūru.

[103] Riska apjoms, ko organizācija ir gatava uzņemties, ietver visu iespējamo riska faktoru ietekmi, visos iespējamajos scenārijos, kuros tie varētu materializēties.

Riska tolerances līmenis:

Pieņemams	Risks ir pieņemams un nav nepieciešamas vai iespējamas papildu kontroles vai uzlabojumi organizācijas darbībā (pārsvarā ārējiem riskiem, kurus grūti ietekmēt)
Nebūtiski uzlabojumi	Risks kopumā ir pieņemams, taču nepieciešami nelieli uzlabojumi organizācijas darbībā un kontroļu ieviešana ilgākā termiņā (no 6 mēnešiem līdz gadam)
Vidēji uzlabojumi	Risks nav pilnībā pieņemams, ir nepieciešami zināmi uzlabojumi un risinājumi vidējā termiņā (no 3 –6 mēnešiem)
Būtiski uzlabojumi	Risks ir nepieņemams, ir nepieciešami būtiski uzlabojumi organizācijas darbībā un tūlītēji risinājumi, lai to mazinātu (laika posmā līdz 3 mēnešiem)
Atcelts	Risks vairs nav aktuāls
Tiek izvērtēts	Iekšējie vai ārējie faktori ir mainījušies, tādēļ riska novērtēšanai jāveic papildu analīze vai risks ir jāpārvērtē



[104] Tādējādi ir jādefinē sākotnējais risks, tad jānosaka kontroles un pasākumi, lai riska iestāšanās gadījumā sekas būtu mazinātas. Pēc tam ir jānovērtē atlikušais risks, vai tas joprojām ir augsts vai vidējs. Ja tas joprojām ir augsts vai vidējs, tad jānosaka papildu mazinošās kontroles.

[105] Ja atlikušais risks ir virs riska apetītes:
- ja risku var mazināt – definēt risku mazinošās darbības (mazina varbūtību, ietekmi vai abus);
- ja risku nevar ietekmēt vai izmaksas pārsniedz ieguvumus, risku jāpieņem un jāturpina uzraudzība.

Ņem vērā! Organizācijai ir jāizvērtē riska iestāšanās varbūtība, kas rada ietekmi uz personas tiesībām un brīvībām.

3.4.3. Riska izvērtēšana

[106] Riska kritēriji, kas jāņem vērā, pieņemot lēmumu par riska kopējo apmēru, ir jānosaka NIDA veikšanas laikā. Kritēriji var būt kvalitatīvi vai kvantitatīvi. Kritēriji ir jānosaka un jādefinē, lai pārzinis var pieņemt lēmumu, vai risks ir pieņemams, mazināms vai uzskatāms par augstu.

[107] Attiecībā uz katru identificēto riska faktoru pārzinim ir jānosaka tam raksturīgā ietekme, t. i., iespējamie rezultāti. Ietekme būs atkarīga no kaitējuma, kas īstermiņā, vidējā termiņā un ilgtermiņā var rasties, jo īpaši, datu subjektiem un sabiedrībai kopumā.

[108] Piemēram,
- Ja pieņem, ka risks ir datu centra darbības apdraudējums plūdu rezultātā, tad riska faktors šajā gadījumā varētu būt tā atrašanās vieta potenciāli applūstošā teritorijā. Šajā gadījumā īstermiņa, vidēja termiņa un ilgtermiņa ietekme ir tieši saistāma ar regularitāti (šajā gadījumā – varbūtību), cik bieži un cik pamatīgi attiecīgā teritorija un, līdz ar to, datu centrs applūst. Kaitējums datu centra applūšanas gadījumā būs atkarīgs no plūdu smaguma – sākot ar pilnīgu apstrādē esošo datu iznīcināšanu katastrofālu plūdu gadījumā un beidzot ar īslaicīgiem kavējumiem datu centra darbībā, ja plūdu dēļ kavēta elektroapgāde vai komunikācija.
- Ja pieņem, ka risks ir lietotnes darbības pārrāvumi palielinātas serveru noslodzes dēļ, tad riska faktori (neizsmeļoši) ir gan serveru skaits, gan to atrašanās vieta, gan serveru nodrošinātāju piedāvātie darbības nepārtrauktības plāni. Šajā gadījumā, vērtējot īstermiņa, vidēja termiņa un ilgtermiņa ietekmi, ir jāvērtē arī plānotās datu apstrādes radītas noslodzes palielināšanās laika gaitā un tehnoloģiju darbības ietekme uz plānotās personas datu apstrādes nolūka sasniegšanu.

[108] Riska faktoru analīzē arī jānosaka varbūtība, ka identificētais risks materializēsies. Jānosaka arī identificētā riska materializēšanās iespējamība.

Ņem vērā! Pirms riska novērtēšanas, organizācijai ir jāiegūst un jāapkopo tai pieejamā informācija par riska ietekmi un iestāšanās varbūtību. Dažos gadījumos lēmumu pieņēmēji šo informāciju var izmantot bez turpmākas (padziļinātas) analīzes.

3.4.4. Riska noteikšana

[109] Fizisko personu tiesību un brīvību riska faktoru noteikšana un analīze ir plānotās datu apstrādes pamatā esošo risku līmeņa novērtēšanas sākumposms.

[110] Riska faktoru noteikšanu un analīzi vienmēr dokumentē un pamato tā, lai pārzinis varētu pierādīt, ka lēmumi, kas pieņemti jebkurā konkrētā brīdī saistībā ar riska pārvaldību, ir bijuši vispiemērotākie pasākumi, pamatojoties uz pieejamo informāciju ("pārskatāmība").

[111] Jāņem vērā, ka NIDA ietvaros veiktajam risku novērtējumam ir jāatspoguļo visu iespējamo riska faktoru kopums, tāpēc organizācijai ir jānosaka visi iespējamie, zināmie riska faktori, kas varētu ticami ietekmēt plānoto datu apstrādi.

Risku noteikšana un analīze var būt kvalitatīva, kvantitatīva vai puskvantitatīva.

- Kvalitatīva risku novērtējuma metode ir pieeja riska novērtēšanā, kas fokusējas uz kvalitatīvu informācijas apkopošanu un analīzi par iespējamiem riskiem, to cēloņiem un sekām. Šī metode izmanto detalizētus aprakstus, lai izprastu riskus, balstoties uz pieejamo informāciju un ekspertu viedokļiem.
- Kvantitatīvā risku novērtējuma metode ir pieeja riska novērtēšanai, kurā izmanto matemātiskus un statistiskus līdzekļus, lai mērītu un novērtētu riskus skaitliskā formā. Šī metode balstās uz datiem un skaitliskiem aprēķiniem, lai noteiktu iespējamību un potenciālās sekas dažādiem riskiem.
- Puskvantitatīvā metode apkopo abas iepriekšējās, izmantojot gan statistiskus un matemātiskus elementus, gan aprakstošus elementus.

  Veidam, kādā tiek novērtēts risks, ir jābūt saderīgam ar visiem definētajiem kritērijiem.

Piemēram, kvantitatīvie kritēriji prasa kvantitatīvās analīzes metodi, kas nodrošina rezultātu ar atbilstošām vienībām. Kvantitatīvos kritērijus var izmantot tikai tad, ja to atļauj izvēlētie rādītāji.

[112] Līdz ar to, nosakot riskus, organizācijai izmantojot kādu no iepriekš minētajām metodēm, ir jāņem vērā, kādi apstākļi (materiāli vai nemateriāli) veido potenciālo risku, kā arī nepieciešams izvērtēt esošos riskus un to potenciālo ietekmi uz plānoto datu apstrādi.

[113] Tāpat organizācijai jāvērtē:

- kādi ir riska avoti, to cēloņi un virzītājspēki;
- kādas kontroles ir ieviestas un vai tās ir efektīvas;
- riska iestāšanās iespējamība un sekas;
- kas ir noticis pagātnē un tas, cik ticami tas varētu attiekties uz nākotni;
- cilvēcisko un organizatorisko faktoru loma.

Ņem vērā! Rezultātus no riska identificēšanas var reģistrēt kā sarakstu ar riskiem, kas saistīti ar notikumiem, cēloņiem un sekām, vai izmantojot citus piemērotus formātus.

3.4.5. Riska avotu un to cēloņu noteikšana

[114] Riska avoti var būt gan labvēlīgi, gan nelabvēlīgi notikumi, lēmumi, darbības un procesi, kā arī situācijas, par kurām zināms, ka tās pastāv, bet kurās rezultāti ir neskaidri. Jebkāda veida nenoteiktība var būt riska avots.

[115] Riska cēloņu, avotu un virzītājspēku noteikšana:

- palīdz novērtēt notikuma vai to seku iespējamību;
- palīdzēt identificēt darbības, kas jāveic, lai novērstu risku;
- palīdz noteikt agrīnās brīdināšanas rādītājus un to atklāšanas robežvērtības;
- noteikt kopīgus cēloņus, kas var palīdzēt izstrādāt prioritātes riska mazināšanai.

Notikumiem un sekām var būt vairāki cēloņi vai cēloņsakarību ķēdes.

Ņem vērā! Katrā brīdī nepieciešamā informācija ir atkarīga no iepriekšējās informācijas vākšanas rezultātiem, novērtējuma nolūka un apjoma, kā arī analīzes metodes vai metodēm. Būtu jāizlemj, kā informācija jāvāc, jāglabā un jādara pieejama.

3.4.6. Risku mijiedarbības analīze

[116] Starp identificētajiem riskiem var pastāvēt mijiedarbība. Tas nozīmē, ka viens risks var ietekmēt cita riska iestāšanos vai to iestāšanās sekas uz plānoto datu apstrādi. Piemēram, vairākas sekas var rasties no viena cēloņa vai arī konkrētām sekām var būt vairāki cēloņi. Dažu risku rašanās var padarīt citu parādīšanos vairāk vai mazāk iespējamu.

[117] Mijiedarbībai starp riskiem var būt dažāda ietekme uz lēmumu pieņemšanu par plānoto datu apstrādi. Tāpat jāņem vērā, kā ieviestie kontroles pasākumi vienam riskam ietekmē citus identificētos riskus, piemēram, viena riska mazināšanas kontroles pasākumi atstāj pozitīvu ietekmi uz vienu noteiktu risku, vienlaikus, iespējams, radot negatīvas sekas citam riskam.

Ņem vērā! Lai vienkāršotu riska novērtējumu gadījumos, kad starp riskiem pastāv cēloņsakarības, ir lietderīgi šīs cēloņsakarības modelēt, piemēram, uzskaitot saistītos riska cēloņus vai saistītās sekas. Piemēram, integritātes un ilgtspējas nodrošināšanai uzturētas rezerves kopijas rada risku, ka atjaunošanas gadījumā no tām dzīvesciklā var atgriezties neaktuāli dati. Līdz ar to ir jāvērtē vairāku risku mijiedarbība un to ietekme uz apstrādes darbībām.

[118] Dažādu riska faktoru savstarpējā mijiedarbība var palielināt apstrādes riska līmeni, pārsniedzot katra riska faktora gadījumu atsevišķi. Ja ir dažādi riska faktori, ir nepieciešams interpretēt, kā šie neatkarīgi aplūkotie faktori varētu mijiedarboties viens ar otru:

- lai palielinātu apstrādes riska līmeni;
- analizējot to kopējo atkarību un ietekmi.

[119] Risku mazināšanas plānā ir jāņem vērā faktoru kopums, nevis jāpieņem, ka katrs risks ir jārisina neatkarīgi.

3.4.7. Datu aizsardzības risku reģistrs

[120] Organizācijai, lai izvērtētu saistītos riskus un novērtētu to iespējamību un ietekmi, var palīdzēt datu aizsardzības risku reģistrs. Risku reģistra izveide atvieglotu organizācijas pienākumu regulāri pārskatīt riskus, lai nepieciešamības gadījumā tos mazinātu vai novērstu.

[121] Datu aizsardzības risku reģistrs tiek izmantots, lai reģistrētu informāciju par datu aizsardzības riskiem, kas konstatēti saistībā ar konkrētu NIDA, kā arī riska ietekmes analīzi un iespējamo piemērojamo risinājumu izvērtējumu. Ja organizācija veic divus vai vairāk NIDA, tad informāciju par datu aizsardzības riskiem var iekļaut jau iepriekš izveidotā datu aizsardzības risku reģistrā.

Ņem vērā! Datu aizsardzības risku reģistrs ir jāatjaunina personas datu apstrādes dzīvescikla laikā, lai atspoguļotu visus konstatētos risinājumus vai jaunus riskus, ja tādi rodas.

[122] Datu aizsardzības risku reģistrā vajadzētu atzīmēt visus pasākumus, kas veikti riska mazināšanai, kā arī tas papildināms ar jebkādiem papildu riskiem, kas radušies, veicot riska mazināšanas pasākumus.

[123] Datu aizsardzības risku reģistrs var būt daļa no kopējās organizācijas risku pārvaldības sistēmas, un proti, būt daļa no kopējā organizācijas risku reģistra. Tas, ka noteiktie riski primāri saistāmi ar NIDA nenozīmē, ka tos nevar izmantot citu organizācijas procesu laikā, veidojot riskos balstītu pieeju visā organizācijas darbu pārvaldībā.

[124] Datu aizsardzības risku reģistrācija un uzkrāšana vienuviet palīdzētu pārvaldīt NIDA veikšanas laikā konstatētos riskus, to ietekmi un ietekmes mazināšanas pasākumus. Vienlaikus datu aizsardzības risku reģistra uzturēšana nav uzskatāma par obligātu prasību.

3.4.8. Risku pārvaldības plāns

[125] No NIDA ziņojumā konstatētā var veidoties cits risku pārvaldības elements – risku pārvaldības plāns. Plāns var tikt noformēts kā atsevišķs dokuments, vai arī tikt iekļauts NIDA ziņojumā. Tas varētu palīdzēt organizācijai, lai īstenotu visus identificētos riska mazināšanas pasākumus, un to varētu izmantot, pārbaudot katra pasākuma īstenošanas gaitu.

[126] Šajā apkopojošajā plānā būtu pārskatāmi jānorāda identificētie riski, to novēršanai plānotie pasākumi, kā arī šādu pasākumu plānotā ietekme uz risku. Veicamajiem pasākumiem norādāmi skaidri un atsekojami izpildes termiņi un kritēriji. Ar pasākumu plānu ir saistāmi dokumenti, kas apliecina organizācijas kontroli pār novēršanas pasākumu īstenošanu un to izpildes gaitu. Arī šis rīks, lai arī ir uzskatāms par labās prakses risku vadībā elementu, tomēr nav obligāta NIDA sastāvdaļa.

Ņem vērā! Ja identificētais risks tiek noteikts kā neatbilstošas informācijas sniegšana organizācijas privātuma politikā, rosinot veikt attiecīgus grozījumus tajā, tad precizētā privātuma politika ir jāsaista ar risku novēršanas plānu. Sasaisti var veikt, norādot datumu, kurā veikti grozījumi, kā arī kādi grozījumi izdarīti.

3.5. NIDA ziņojums

[127] Noslēdzot risku izvērtēšanu, atbildīgā persona sagatavo NIDA ziņojumu, kuru iesniedz organizācijas vadībai lēmuma pieņemšanai. NIDA ziņojums ir NIDA procesa starprezultāts, kurā tiek apkopoti veiktā risku novērtējuma un plānotās personas datu apstrādes analīzes rezultāti. Tāpat kā pašu NIDA, NIDA ziņojumu izstrādā/apstiprina NIDA veicējs. Šajā ziņojumā būtu jāapkopo katra NIDA procesa posma apraksts un jāatzīmē secinājumi. Tajā jāiekļauj arī pārskats par NIDA, paskaidrojot kāpēc tas tika uzsākts un kā tas ietekmēs datu aizsardzību. Tajā jāapraksta process, kādā veikts NIDA, un jānorāda datu aizsardzības riski un novēršanas pasākumi, kas tika identificēti NIDA veikšanas procesā.

Ņem vērā! Ja organizācija uzskata, ka konsultācijas nav nepieciešamas, Inspekcija NIDA ziņojumu var izskatīt vēlāk, piemēram, audita vai pārbaudes procesa ietvaros, kas veikts par personas datu apstrādi, par kuru veikts NIDA. NIDA ir viens no elementiem, ko Inspekcija ņems vērā, vērtējot datu subjekta sūdzību, notikušu drošības incidentu vai arī pārbaudot datu apstrādi pēc iestādes iniciatīvas.

3.6. Apspriešanās un komunikācija ar datu subjektu

[128] Uzsākot NIDA, organizācijai būtu jāapsver iespēja veikt datu subjektu, kuru datus plānots apstrādāt, viedokļu noskaidrošanu. Tas palīdzēs noteikt sākotnējo ietekmi personas datiem, kas tiks apstrādāti, tāpat datu subjektu sniegtajai informācijai var būt tieša nepastarpināta ietekme uz "likumības, godprātības un pārredzamības" principa nodrošināšanu, tai skaitā palīdzot noteikt datu subjektu saprātīgās gaidas, kā īstenot datu subjektu informēšanas pasākumus un arī vai ir piemērots visatbilstošākais tiesiskais pamats.

[129] Šāds viedoklis ir pieprasāms, organizācijai izmantojot dažādus sev pieejamos līdzekļus (piemēram, jautājumu formā organizācijas darbiniekiem vai izmantojot vienkāršas aptaujas, kuras dara pieejamas pārziņa klientiem).

3.6.1.Fokusa grupas diskusija

[130] Fokusa grupas diskusija ir kvalitatīvs pētniecības paņēmiens, ko izmanto, lai apkopotu indivīdu grupas ieskatus un viedokļus par konkrētu tēmu vai jautājumu. Saistībā ar plānoto datu apstrādi fokusa grupu diskusijas var būt noderīgas organizācijām, lai novērtētu cilvēku domas un bažas par to, kā viņu dati tiks/tiek apstrādāti. Formāts:

- Fokusa grupā parasti ir 6 – 10 dalībnieki, kas atlasīti pamatojoties uz konkrētiem kritērijiem, kas attiecas uz konkrēto tematu. Dalībniekiem jāatspoguļo to viedokļu daudzveidība, kas attiecas uz apspriežamo jautājumu;
- Kvalificēts moderators atvieglo diskusiju, virzot dalībniekus strukturētā sarunā, vienlaikus nodrošinot ikvienam iespēju paust savu viedokli. Diskusijas vadīšanai moderators izmanto iepriekš noteiktu jautājumu vai tematu kopumu;
- Dalībnieki tiek aicināti atklāti dalīties ar savām domām, pieredzi un bažām grupas ietvaros. Diskusijas var aptvert virkni tematu, kas saistīti ar datu apstrādi, piemēram, plānotās datu apstrādes nolūku, nepieciešamo datu apjomu problēmām, kuras tie saredz, datu drošību un uzticēšanos organizācijai utt.;
- Pēc diskusijas organizācija kopā ar moderatoru analizē fokusa grupas gūtās atziņas. Dalībnieku atbilžu tēmas, modeļi un kopīgas iezīmes tiek identificētas, lai gūtu dziļāku izpratni par viņu perspektīvām.

[131] Ieguvumi organizācijai:

- Fokusa grupas diskusijas sniedz organizācijai vērtīgu ieskatu par to, kā datu subjekti uztver un saprot plānoto datu apstrādi, gūstot labāku izpratni par klientu vēlmēm, bažām un gaidām attiecībā uz datu privātumu un aizsardzību;
- Organizācija var identificēt iespējamās bažas un problēmas saistībā ar datu apstrādi, kuras, iespējams, nav konstatētas iekšējos novērtējumos. Fokusa grupas diskusijās var izcelt jomas, kurās datu subjekti jūtas neērti vai tiem nav skaidrības attiecībā uz savu personas datu apstrādi;
- Iesaistīšanās fokusa grupas diskusijās apliecina organizācijas apņemšanos nodrošināt datu apstrādes pārredzamību un atbilstību tiesību aktiem. Organizācijas var izmantot fokusa grupu viedokļus, lai uzlabotu komunikācijas stratēģijas, nodrošinot, ka datu subjekti ir labi informēti par to, kā viņu dati tiks izmantoti un aizsargāti;
- Fokusa grupu diskusijās gūtās atziņas sniegs papildu informāciju lēmumu pieņemšanas procesos, kas saistīti ar konkrēto datu apstrādi, privātuma politikas attiecīgo sadaļu izstrādi. Organizācija var izmantot šo informāciju, lai pieņemtu uz datiem balstītus lēmumus, kas atbilst datu subjektu vēlmēm un vajadzībām.

3.6.2. Strukturētas vai daļēji strukturētas intervijas

[132] Līdzīgi kā fokuss grupas diskusijas, arī strukturētas un daļēji strukturētas intervijas ar datu subjektiem ir kvalitatīvas pētniecības metodes, ko organizācija var izmantot, lai apkopotu ieskatus, viedokļus un perspektīvas tieši no personām, kuru dati tiks apstrādāti. Atšķirībā no fokusa grupas intervijām, šīs intervijas sniedz padziļinātu izpratni par konkrēta datu subjektu domām, bažām un preferencēm attiecībā uz datu apstrādes praksi, kuru var salīdzināt, ja tiek veiktas vairākas šādas intervijas ar citiem datu subjektiem par to pašu datu apstrādi. Formāts:

- strukturētas intervijas seko iepriekš noteiktam jautājumu kopumam. Jautājumi ir paredzēti, lai iegūtu konkrētas atbildes, un tie tiek uzdoti noteiktā secībā;
- daļēji strukturētas intervijas nodrošina elastīgu sarunas ietvaru, ļaujot intervētājiem iedziļināties sev interesējošā jautājumā (piemēram, uzdot papildu jautājumus), vienlaikus saglabājot noteiktu struktūru;
- Strukturētas intervijas nodrošina konsekvenci datu vākšanā starp dažādiem dalībniekiem un var sistemātiski salīdzināt atbildes, veicot vienkāršāku analīzi. Savukārt daļēji strukturētas intervijas ļauj niansētāk izpētīt dalībnieku perspektīvas un pieredzi, padziļināti izpētot konkrētas tēmas, atklājot esošo datu subjektu attieksmi, kas saistīta ar datu apstrādi;

- Dalībnieki bieži jūtas vairāk ieinteresēti un spējīgāki piedalīties individuālās intervijās, jo tiem ir iespēja brīvi izteikties, nekautrējoties no apkārtējo domām un uzskatiem. Vienlaikus, intervētājs var mudināt datu subjektu izteikties atklātāk, veidojot savstarpējo uzticēšanos un drošu vidi.

[133] Ieguvumi organizācijai:
- Intervijas ar datu subjektiem sniedz organizācijai tiešu ieskatu par to, kā konkrētā persona vērtē plānoto datu apstrādi, iegūstot dziļāku izpratni par tās bažām, vēlmēm un gaidām attiecībā uz datu privātumu un drošību;
- Intervijas palīdz organizācijai noteikt konkrētas jomas, kurās datu subjektiem var būt bažas vai jautājumi par plānoto datu apstrādi. Iegūto informāciju var izmantot, piemēram, lai novērstu saziņas, pārredzamības vai datu aizsardzības pasākumu nepilnības;
- organizējot šādas intervijas, organizācijas apliecina apņemšanos nodrošināt datu apstrādes pārredzamību un atbilstību tiesību aktiem. Organizācijas interviju laikā iegūtās atziņas var izmantot, lai uzlabotu saziņas stratēģijas un veidotu datu subjekta uzticēšanos;
- Intervijās gūtās atziņas var kalpot par pamatu lēmumu pieņemšanas procesiem, kas saistīti ar plānoto datu apstrādi, iekšējām procedūrām utt. Organizācijas var izmantot iegūtās atziņas, lai pieņemtu uz datiem balstītus lēmumus, kas atbilst datu subjektu interesēm un gaidām.

3.6.3. Aptaujas

[134] Aptaujas ir kvantitatīva pētniecības metode, kas atspoguļojas kā strukturētu atsauksmju vākšanu no personām, kuru dati tiks apstrādāti. Aptaujas parasti sastāv no jautājumu kopuma, kas veidots, lai apkopotu plašas sabiedrības daļas ieskatus, viedokļus un gaidas par organizācijas datu apstrādes praksi, problēmām utt. Formāts:
- organizācija var izstrādāt anketu, kas ietver virkni jautājumu saistībā ar plānoto datu apstrādi un citiem būtiskiem tematiem. Jautājumi var tikt veidoti ar vienu vai vairākiem atbilžu variantiem, izmantojot reitinga skalu, atvērtā veidā vai izmantojot šo formātu kombināciju;
- Organizācija iegūst plašākas sabiedrības daļas ieskatus par plānoto datu apstrādi.

[135] Ieguvumi organizācijai:
- Izmantojot dažādus saziņas kanālus, aptaujas dod iespēju organizācijai iegūt un apkopot atsauksmes no daudziem datu subjektiem dažādās demogrāfiskajās grupās un ģeogrāfiskajās vietās. Izmantojot šo metodi, organizācija var gūt plašu izpratni par datu subjektu domām, bažām un attieksmi pret plānoto datu apstrādi;
- Aptaujas nodrošina datu subjektiem platformu, kurā paust savu viedokli anonīmi, un tas var veicināt atklātākas atbildes. Dalībnieki var justies ērtāk daloties savās domās, nebaidoties no sekām;
- Šī metode rada skaitļos izsakāmus datus, kurus var statistiski analizēt, lai noteiktu tendences un korelācijas. Organizācijas var izmantot kvantitatīvus datus, lai novērtētu vispārējo apmierinātības līmeni un izsekotu izmaiņas laika gaitā (ja identiska aptauja tiek veikta pēc konkrēta laika perioda);
- Aptaujas ir rentabla metode, lai apkopotu atsauksmes no liela datu subjektu skaita. Salīdzinājumā ar kvalitatīvām pētniecības metodēm, piemēram, fokusa grupām vai intervijām, aptaujas prasa mazāk resursu un var sasniegt plašāku auditoriju;
- Organizējot šādas aptaujas, organizācija apliecina apņemšanos nodrošināt datu apstrādes pārredzamību un atbilstību tiesību aktiem. Organizācijas iegūtās atziņas var izmantot, lai uzlabotu saziņas stratēģijas un veidotu datu subjektu uzticēšanos;
- No aptaujas atbildēm gūtās atziņas var izmantot uz datiem balstītu lēmumu pieņemšanā, kas saistīti ar plānoto datu apstrādi, iekšējām procedūrām, sistēmu izstrādi utt. Organizācijas var izmantot izdarītos secinājumus, lai noteiktu prioritātes jomām, kurās jāveic uzlabojumi, efektīvi sadalītu resursus un pielāgotu datu apstrādes praksi, lai tā labāk atbilstu datu subjektu vajadzībām un gaidām.

[136] Organizācija, iesaistot datu subjektus NIDA veikšanas procesā, lai uzzinātu to viedokli par plānoto datu apstrādi, varēs arī uzskatāmāk pieradīt datu apstrādes prakses pārredzamību, kā arī proaktīvi reaģēt uz datu subjektu paustajām bažām.

3.6.4. Ziņošana citām iesaistītajām personām un NIDA publicēšana

[137] Organizācijai nav pienākums publicēt NIDA. Tomēr, ja organizācija vēlas demonstrēt organizācijas atbildību par tās veikto datu apstrādi, tā var publicēt īsu kopsavilkumu, ka NIDA ir veikta par konkrēto datu apstrādi. Publicētajā NIDA nav jāietver viss novērtējums. Īpaši uzmanīgi vērtējama to NIDA elementu publicēšana, kas varētu sniegt informāciju par iespējamām drošības ievainojamībām vai komerciāli sensitīvu informāciju.

[138] Līdz ar to publicētajā informācijā varētu būt tikai NIDA galveno konstatējumu kopsavilkums, kas demonstrē lasītājam, ka attiecīgajā personas datu apstrādē ir sasniegts pieņemams ietekmes līmenis uz datu subjektu tiesībām un brīvībām.

3.7. Rezultātu pēcpārbaude un apstiprināšana

[139] Organizācijas norīkotajai personai, kura pārskata veikto NIDA, ir jānovērtē rezultātu ticamība. Atbilstoši Datu regulai viens no DAS uzdevumiem ir sniegt organizācijai viedokli par sagatavotu NIDA un tā konstatēto risku mazināšanas pasākumu lietderību.

[140] Rezultātu pārbaudei un NIDA apstiprināšanai nepieciešams:
- pārbaudīt, vai risku analīze atbilst izvirzītajam mērķim;
- pārbaudīt risku aprēķinu (gan kvalitatīvi, gan kvantitatīvi) derīgumu;
- ja dati ir pieejami, salīdzināt rezultātus ar iepriekšējo pieredzi. Var izmantot citu NIDA veikšanas metodi (ja izmantota kvalitatīvā, tad piemērot kvantitatīvo un otrādi), lai pārbaudītu un apstiprinātu secinājumus;
- pārskatīt pieņēmumus, lai nodrošinātu, ka tie ir ticami, ņemot vērā pieejamo informāciju;
- pārbaudīt, vai ir izmantotas piemērotas metodes un dati.

Ņem vērā! Ja organizācijai nav izveidota DAS štata vieta, ir pieļaujams, ka DAS kā ārpakalpojums tiek piesaistīts tieši attiecībā uz konkrēto NIDA.

[141] Izvērtējot izstrādāto NIDA, jāņem vērā:
- vai dati ir no uzticama avota, konsekventi un pietiekami, tāpat, piemēram, iespējams ir mainījušās datu iegūšanas metodes vai datu veidi;
- vai izvēlētā risku analīzes metode ļauj pienācīgi novērtēt plānotās datu apstrādes sarežģītību;
- jāapsver, kāda ir piesaistīto ekspertu kvalifikācija. Jānovērtē, vai iegūtais ekspertu viedoklis aptver visus plānotās personas datu apstrādes aspektus. Jāņem vērā, vai pastāv liela paļaušanās uz tādu ekspertu atzinumu vai spriedumu, kas nav saistīti ar nozari un kuru kvalifikācija rada šaubas. Ja iegūts datu subjektu viedoklis, nepieciešams novērtēt iegūtās informācijas un datu subjektu viedokļa atbilstību datu apstrādes problemātikai, piemēram, tiek iegūts viedoklis no datu subjektiem, kuri nav galvenā plānotās personas datu apstrādes mērķauditorija, un/vai tiek iegūts viedoklis, kas nav reprezentatīvs, salīdzinot ar plānotās personas datu apstrādes mērogu. Apsvērumi attiecībā uz NIDA veicēja un tā komandas kvalifikācijas piemērotību ir iekļaujami NIDA veidlapā.
- vai NIDA veicējs ieguvis un apkopojis vajadzīgos datus/informāciju? Vai priekšizpētes laikā iegūtā informācija joprojām ir aktuāla un tās bāzes vērtības nav mainījušās? Piemēram, informācijas aktualitāte mainījusies un, balstoties uz to, izdarītie secinājumi neļauj izdarīt objektīvu pastāvošās situācijas novērtējumu, kā arī izteikt prognozes par nākotni;
- NIDA ietvaros modelēto scenāriju potenciālā ietekme uz datu subjekta tiesībām un brīvībām. Jāvērtē, vai izdarītajos pieņēmumos ir neskaidrības, vai kāda no scenārijiem novērtējums veikts apšaubāmā kvalitātē.

Ņem vērā! Ja secinājumu daļā tiek konstatētas pastāvošas neskaidrības vai šaubas par veiktās NIDA kvalitāti un atbilstību plānotai datu apstrādei, ir nepieciešams informēt lēmumu pieņēmējus organizācijā.

3.7.1. Lēmumu par riska nozīmīgumu pieņemšana

[142] Atbilstoši vadlīnijās norādītājam nepastāv tāda datu apstrāde, kurai būtu nulle risks. Tas nozīmē, ka organizācijai ir jāatrod kompromiss starp sasniegto atlikušā riska līmeni un apstrādes iespējamību, kas nozīmē lēmuma pieņemšanu par to, kad riska līmenis ir pieņemams.

[143] Sākotnēji jānovērtē, kāds ir atlikušā (pēc riska mazināšanas pasākumu ieviešanas) riska līmenis. Atlikušā riska līmenis ir jāsalīdzina ar riska apjomu, kuru organizācija bija gatava uzņemties pirms-NIDA laikā.

[144] Ja konstatēts zemāka un/vai vidēja atlikušā riska līmenis, kas prasa samērīgus pārvaldības centienus visā apstrādes dzīves ciklā, to var uzskatīt par pieņemamu atlikušā riska līmeni. Ja analīzes laikā konstatēts, ka apstrādes atlikušais riska līmenis ir augstāks par vidējo vērtību, ir jāveic turpmāki pasākumi, lai pārvaldītu identificētos riskus. Pēc risku mazinošo pasākumu ieviešanas, organizācijai atkārtoti jānovērtē riska līmenis, līdz atlikušais riska līmenis ir pieņemams.

3.7.2. Lēmumu pieņemšanas dokumentācija

[145] Izpildot pārskatatbildības principa prasības, lai organizācija varētu arī tālākos personas datu apstrādes atbilstības novērtēšanas posmos veiksmīgi izmantot NIDA iegūtas atziņas, organizācijai svarīgi ir dokumentēt veiktos pasākumus, darbības, kā arī pieņemtos lēmumus.

[146] Organizācijai ir jādokumentē pieņemtie lēmumi, kas saistīti ar plānoto datu apstrādi. NIDA dokumentācijā var izmantot jebkurus līdzekļus, kas ir vispiemērotākie organizācijai un attiecīgajai apstrādei.

[147] To var darīt arī izmantojot vizuālos palīglīdzekļus, piemēram, shēmas, lai demonstrētu, kā personas datus plānots izmantot projektā. Šādas vizualizācijas var uzskatāmi demonstrēt iespējamos riskus personas datiem. Rūpīga procesa dokumentācija veicinās iekšējo komunikāciju, ļaujot projekta komandai un citiem organizācijas darbiniekiem labāk izprast apstrādes procesus, kas savukārt veicinās konsekventumu attiecībā uz projekta komandas veikto risku analīzi.

[148] Dokumentējot iepriekš minētos procesa posmus, svarīgi ir pamatot izdarītās izvēles, veiktos pasākumus, kā arī paskaidrot, kādi pasākumi tiks veikti, lai samazinātu katru risku, sniedzot novērtējumu par to, vai ierosinātie pasākumi novērš, samazina vai kontrolē risku. Atceramies, ne visi riski ir pilnībā jānovērš, kā arī ne visus riskus var pilnībā novērst.

3.8. Apspriešanās ar uzraudzības iestādi

[149] Ja NIDA ietvaros secināts, ka vienu vai vairākus identificētos riskus nevar novērst vai samazināt līdz pieņemam līmenim un atlikušie riski ir joprojām augsti, tad pirms apstrādes uzsākšanas organizācijai ir jāpieprasa iepriekšēja apspriešanās ar Inspekciju par plānoto apstrādi. Šā procesa ietvaros organizācijai ir jāiesniedz NIDA pilns saturs.

[150] Inspekcija, izvērtējot visu saņemto informāciju, sniegs savu vērtējumu konkrētā situācijā. Pēc būtības pastāv iespēja, ka Inspekcija:

- atzīst riskus par pieņemamiem un ļauj apstrādi veikt bez tālāku pasākumu veikšanas;
- izsaka ierosinājumus papildu pasākumu ieviešanai, kas riskus varētu mazināt līdz pieņemamam līmenim;

- novērtē, ka plānotās apstrādes darbības rada neproporcionālu apdraudējumu datu subjekta tiesībām un brīvībām, un pie faktiskajiem apstākļiem nav informācijas par pasākumu kopumu, kas varētu pastāvošos riskus mazināt līdz pieņemamam līmenim.

Ņem vērā! Ja NIDA veikšanas procesā identificētie riski pēc to mazināšanai veiktajiem pasākumiem vairs nav uzskatāmi par augstiem, organizācijai ar Inspekciju nav jākonsultējas.

3.9. Uzraudzība un pārskatīšana

3.9.1. Integrācijas datu aizsardzības sistēmā

[151] Kad NIDA ir pabeigts, nepieciešams ieviest NIDA procesā iegūtos secinājumus un risinājumus, iekļaujot visas nepieciešamās izmaiņas apstrādē. Kavēšanās NIDA rezultātu integrēšanā var apgrūtināt vēlāku riska mazināšanas pasākumu veikšanu. Pastāv iespēja, ka novēlotas rīcības rezultātā NIDA identificētie riski un to ietekme jau būs mainījusies un īstenotie pasākumi nebūs atbilstoši, līdz ar to NIDA būs jāpārskata pilnībā un tiks aizkavēta personas datu apstrādes uzsākšana.

[152] Būtiski ir pēc NIDA veikšanas atrast tā vietu kopējā organizācijas datu aizsardzības sistēmā. Būtu vērā ņemama saikne ar līdzsvarošanas testu un datu apstrāžu reģistru, kuros izmantojamā informācija ir savstarpēji izmantojama arī NIDA. Vienlaikus NIDA var ietekmēt pilnīgi visus organizācijas datu apstrādes procesus, ne tikai tos, kas saistīti ar konkrēto personas datu apstrādi, kuras ietekme tiek novērtēta.

Piemēram, NIDA veikšanas brīdī organizācijai bija noteikta veida tehniskā infrastruktūra un datu bāzes veidošanas sistēma, bet, kādam nominēto elementiem mainoties, var mainīties arī NIDA. Nesavietojot datu aizsardzības jomā veiktos pasākumus vienotā sistēmā, pastāv iespēja, ka kādas izmaiņas ietekme netiek atbilstoši ņemta vērā, tādējādi palielinot risku iestāšanos, vienlaikus neveicot atbilstošus drošības pasākumus.

[153] NIDA ieviešanas ietvaros organizācijai ir jāpārskata iekšējie datu aizsardzības risinājumi. Jo īpaši jānovērtē, vai īstenotie riska mazināšanas pasākumi ir pārzinim pieņemami un samērīgi ar plānoto personas datu apstrādes nolūku. Turklāt, ja apstrādes, par ko veikta NIDA, nolūks ir mainīts vai paplašināts NIDA darbības laikā, var būt nepieciešams pārskatīt NIDA, lai novērtētu izmaiņu ietekmi uz identificētajiem datu aizsardzības riskiem. Nepieciešamību šādu pārskatu veikt, kā arī tā veikšanas periodiskumu, būtu jāietver organizācijas esošajās darbības procedūrās.

3.9.2. Apstrādes darbību pastāvīga uzraudzība

[154] Atbilstoša integrācija ar citiem datu aizsardzības pasākumiem ļaus veikt apstrādes darbību, par kurām veikts NIDA, pastāvīgu uzraudzību – šim nebūs jādeleģē atsevišķs organizācijas resurss, jo visa datu aizsardzība notiks vienotā shēmā.

[155] Vienlaikus ir nepieciešams skaidri iezīmēt procesus, kas mijiedarbojas ar personas datu apstrādi, par kuru veikts NIDA. Ja saistībā ar šiem procesiem organizācijā notikušas izmaiņas, būtu nepieciešams pārvērtēt potenciālo ietekmi uz datu apstrādi.

[156] Ir rekomendējams noteikt kritērijus, atbilstoši kuriem organizācija noteiks, kuras izmaiņas ir uzskatāmas par būtiskām un tādām, kas izraisa nepieciešamību pārskatīt NIDA, un kuras ir nenozīmīgas un NIDA būtību neietekmējošas.

3.10. NIDA periodiska pārskatīšana

[157] Papildus NIDA veiktās datu apstrādes pastāvīgai uzraudzībai, kas tiek īstenota, ja notiek kādas ārējas vai iekšējas izmaiņas, kas attiecas uz datu apstrādi, ir veicama arī regulāra NIDA pārskatīšana.

[158] NIDA periodiska pārskatīšanas biežums katrai organizācijai būs individuāls. Termiņš iekļaujams NIDA ziņojumā. NIDA ietverams arī apsvērumu kopums, atbilstoši kuram izvēlēts NIDA pārskatīšanas periods (ja nolemts, ka NIDA pārskatāms tikai gadījumos, kad apstrādē notikušas būtiskas izmaiņas, tad jāatspoguļo, kāds mehānisms ieviests, lai konstatētu notikušas būtiskas izmaiņas apstrādē, un kāpēc organizācija uzskata, ka šāds mehānisms ir pietiekošs).

Ņem vērā! NIDA periodiskās pārskatīšanas laikā ir jāpievērš uzmanība, vai identificētie riski un ietekmes novērtētas pareizi un vai praksē personas datu apstrādes radītā ietekme nav lielāka par NIDA laikā identificēto. NIDA, kurā viens no kritērijiem ietekmes novērtējuma veikšanai bija tehnoloģisko inovāciju izmantošana, šim termiņam katrā ziņā vajadzētu būt īsākam. Mainīgie ārējie un/vai iekšējie faktori ietekmēs to, cik aktuāli ir NIDA veikšanas laikā identificētie riski un novērtētās ietekmes. Mainoties risku avotiem, ļoti ticami mainīsies arī pārējie ar riskiem saistītie aspekti un būs nepieciešams no jauna vērtēt ieviesto pasākumu rezultativitāti.

[159] **Nepārtraukta pilnveidošana.** NIDA nav uzskatāms par statisku "paveicu un aizmirsu" dokumentu. Organizācijai ir jāņem vērā, ka, iestājoties ārējām vai iekšējām izmaiņām, kas saistītas ar datu apstrādi, ir jāpilnveido arī NIDA, ņemot vērā jaunos apstākļus, kas saistīti ar personas datu apstrādi. Arī, ja analīzes rezultātā pārzinis secina, ka ietekmes mazināšanas pasākumi nav jāmaina, jebkurā gadījumā ir jāpapildina ar NIDA saistīto dokumentu kopums, lai demonstrētu, ka organizācija šos mainīgos apstākļus ir novērtējusi un ņēmusi vērā.

IV nodaļa "NIDA AIZPILDĪŠANA"

[160] Atbilstoši Datu regulas 35. panta 7. punktam, NIDA jāiekļauj vismaz četri būtiski elementi. Pirmkārt, ir jāsniedz sistemātisks apraksts par plānotajām datu apstrādes darbībām un to nolūkiem, tostarp jānorāda pārziņa leģitīmās intereses, ja tādas pastāv. Otrkārt, jāveic novērtējums par to, vai apstrādes darbības ir nepieciešamas un samērīgas, lai sasniegtu izvirzītos nolūkus. Treškārt, jāizvērtē riski, ko datu apstrāde rada fizisku personu tiesībām un brīvībām, piemēram, risks privātumam vai datu drošībai. Visbeidzot, jānosaka un jāapraksta pasākumi šo risku novēršanai, tostarp garantijas, drošības pasākumi un mehānismi, kas nodrošina atbilstību Datu regulas prasībām, ņemot vērā fizisku personu un citu iesaistīto personu tiesības un likumīgās intereses.

[161] Šī nodaļa ir paredzēta, lai skaidrotu, kā veikt šo vadlīniju pielikumā pievienotās anketas aizpildīšanu kā to paredz Datu regula.

I. NIDA procesā iesaistītās personas un to apraksts	
Pārzinis	
Kontaktinformācija	
Kopīgi pārziņi	
Apstrādātājs	
Citas iesaistītas personas	
Reģistrētā struktūra Latvijā	
Atbildīgā struktūrvienība	
Datu aizsardzības speciālists	
Datu aizsardzības speciālista iesaistes NIDA veikšanas procesā nepieciešamības izvērtēšana	
Atbildīgais par NIDA veikšanu (vārds, uzvārds, kontaktinformācija)	
Novērtējuma veikšanas periods	

Personas datu apstrādē iesaistīto personu un to lomu uzskaitījums

[162] Šajā sadaļā NIDA veicējs apraksta un identificē pārzini, iekļauj arī informāciju par kopīgajiem pārziņiem, kā arī citām datu apstrādē iesaistītajām personām, nepārprotami nosakot katras puses pienākumus un uzdevumus (pušu pienākumus un uzdevumus var pievienot kā pielikumu NIDA veidlapai).

[163] Jānorāda NIDA veicējs, tā kvalifikācija un loma organizācijā, ja tam tāda ir. Jāsniedz informācija par organizācijas DAS un tā lomu NIDA veikšanā, ja DAS ir iecelts. Ja apstrādē iesaistītas citas puses (piemēram, apstrādātājs vai sadarbības partneris), tad jāsniedz gan tā uzdevumu apraksts attiecībā uz personas datu apstrādi, gan arī darbības sfēras apraksts. Ja darbības sfēra ir novērtēta pirms NIDA veikšanas, tad NIDA veidlapā var ietvert sasaisti ar iekšēju dokumentu, kurā apraksts atrodams.

Ņem vērā! NIDA arī jāiekļauj informācija par pārstāvja reģistrēto struktūru Latvijā (filiāli, pārstāvniecību u. tml.), ja pārziņa uzņēmējdarbības vieta atrodas ārpus Eiropas Ekonomikas zonas.

II. Informācija par plānoto apstrādi un datu apstrādes sistēmu	
Datu apstrādes dzīves cikla vizualizācija	
Datu apstrādes funkcionāls apraksts	

Datu apstrādes dzīves cikls

[164] Plānojot uzsākt jaunu personas datu apstrādi vai ieviešot izmaiņas jau esošā procesā, ir nepieciešams ne tikai noteikt atbilstošas personas datu apstrādes pamatelementus (šajā gadījumā atbilstību personas datu aizsardzības principiem), bet arī apzināt, kurā elementā un tieši kādi riski apstrādē iesaistīto fizisko personu tiesībām var izveidoties. Sadaļā aprakstāma pārziņa darbības joma un jāraksturo, kādi datu veidi vai kategorijas un kādā apjomā tiek apstrādāti vai plānots apstrādāt (jāapraksta esošā situācija), kādas datu apstrādes darbības plānotas vai tiek veiktas. Kopēju pārziņu gadījumā apraksts jāsniedz par katra pārziņa plānotajām personas datu apstrādes darbībām.

[165] Personas datu aizsardzībai ir jābūt daļai no organizācijas biznesa vadības procesiem. Tāpat personas datu aizsardzības pasākumi lielākajā daļā gadījumu būs cieši saistīti ar uzņēmuma biznesa datu aizsardzības pasākumiem. Līdz ar to, izvēloties metodes, kuras tiks izmantotas personas datu apstrādes pamatelementu novērtēšanā, būtu vēlams izmantot tādas metodes un paņēmienus, kuri organizācijā jau tiek izmantoti datu aizsardzībā un organizācijas biznesa procesu vadībā.

[166] Pārskatu par plānotās personas datu apstrādes posmiem var iegūt izmantojot dažādas metodes. Šajā vadlīnijās tiks izmantota sertificētu informācijas sistēmu drošības profesionāļu (CISSP) pieeja, kurā datu apstrādes darbību kopums sadalīts nosacītās fāzēs[34]. Šīs fāzes kopā sauc par datu apstrādes dzīvesciklu. Kopumā tiek izdalītas piecas datu dzīvescikla fāzes. Datu dzīvescikla analīzes izmantošana vienkāršo katrā apstrādes etapā iespējamo datu aizsardzības risku identifikāciju, kā arī piemērojamo drošības pasākumu noteikšanu datu aizsardzībai.

Datu apstrādes dzīvescikla posmu raksturojums

Iegūšana

[167] Šajā fāzē personas dati nonāk organizācijas (pārziņa) rīcībā. Visbiežāk datu avots ir pats datu subjekts, valsts iestāžu vai privātas datu bāzes, no kurām par datu subjektu tiek iegūta informācija (piemēram, kredītinformācijas biroja datu bāze vai Uzturlīdzekļu garantiju fonda uzturētā uzturlīdzekļu parādnieku datu bāze), kā arī – organizācijas veikto darbību rezultātā iegūtā informācija par klientu (piemēram, datu subjekta paradumu analīzes rezultātā radītie dati).

[168] Šī fāze iezīmē sākuma punktu datu apstrādes darbībās organizācijā. Iegūšanas fāze uzskatāma par noslēgtu, kad dati ir ievietoti lokācijā, no kuras tos var pārvirzīt uz to paredzēto atrašanās vietu, sākot nākamo dzīvescikla fāzi – izplatīšanu.

Piemēram, ja informācija par jaunu klientu, klienta kartes izsniegšanai, tiek iegūta ar papīra veidlapu palīdzību, tad "radi vai saņem" fāze tiek noslēgta ar veidlapā esošās informācijas ievadi uzņēmuma datu bāzē. Šai fāzei ir izšķirīga nozīme, lai personas dati, ko uzņēmums uzsāk apstrādāt, būtu iegūti likumīgi, droši un apstrādāti novēršot iespējamos riskus integritātei un konfidencialitātei.

[34] Robin Abernathy un Darren R. Hayes (2023) "Asset Security". Pieejams: https://www.pearsonitcertification.com/articles/article.aspx?p=3167978&seqNum=5

Izplatīšana

[169] Šīs nosacītās starpfāzes laikā iegūtie dati tiek pārvirzīti uz tām organizācijas sistēmām, kurās tiek plānots veikt datu izmantošanu atbilstoši to iegūšanas nolūkam. Iespējams fāzes elements ir piekļuves informācijai konfigurācija, nosakot tiesības, ko ar datiem drīkst darīt konkrētas organizācijas deleģētas personas. Lielākajā daļā gadījumu šī starpfāze ir automatizēta, jo lietotāju piekļuves tiesības ir noteiktas sistēmiski, savukārt iekļaušana atbilstošajās informācijas sistēmās arī tiek paveikta automatizēti. Vienlaikus arī šajā fāzē iespējami specifiski drošības riski, kas var būt saistīti, tai skaitā, ar dažādu sistēmu savstarpējo sadarbspēju un datu bāžu rindu atbilstošu konfigurāciju. Fāze uzskatāma par noslēgtu ar brīdi, kad organizācija ir pārliecinājusies, ka dati nonākuši tiem paredzētajā atrašanās vietā. Savukārt nākamā dzīvescikla fāze ir datu izmantošana atbilstoši to ieguves nolūkam.

Ņem vērā! Fāze "izplatīšana" ir noslēgusies ar brīdi, kad organizācijas darbinieks saņemtos datus ir nogādājis konkrētiem datiem paredzētajā vietā, organizācijas datu bāzē (piemēram, piešķirot identifikācijas numuru klientam).

Izmantošana

[170] Pēc izplatīšanas fāzes, kad dati ir nonākuši tiem paredzētajā izmantošanas vietā, tiek uzsākta datu izmantošana atbilstoši to iegūšanas nepastarpinātajam nolūkam.

Piemēram, saņemto datu novērtēšana, lai piedāvātu atlaides un personalizētus piedāvājumus klientiem.

Ņem vērā! Organizācijai ir jābūvē sistēma un jākonfigurē piekļuves tiesības tā, lai katram lietotājam būtu tiesības datiem piekļūt tikai veidā, kas nodrošinātu datu izmantošanu plānoto nolūku sasniegšanai. Jāpatur prātā, ka lietotājiem nav nepieciešams piešķirt tiesības rediģēt datus, ja to funkciju sasniegšanai pietiek ar tiesībām datus tikai apskatīt.

[171] Tāpat datu izmantošanas fāze var būt nepastarpināti saistīta ar datu arhivēšanas jeb datu dzīvescikla noslēdzošo fāzi. Šādi tas būs gadījumos, kad datu izmantošanas vienīgais nolūks ir tos uzglabāt likumā noteiktu pienākumu vai potenciālas pastāvošas leģitīmās intereses aizsardzības nolūkā.

Uzturēšana

[172] Datu uzturēšanas starpfāze ir brīdis, kad organizācija joprojām esot "izmantošanas" fāzē, veic konkrētas darbības ar klientu datiem, iepriekš noteikta nolūka sasniegšanai. Tas nozīmē, ka organizācija uzturēšanas starpfāzē novērtē ne tikai to, vai nolūks ar tā rīcībā esošiem datiem ir sasniedzams, bet arī to, vai tā rīcībā esošie dati joprojām tiek apstrādāti likumīgi, godprātīgi u. tml.

Piemēram, organizācijas darbinieks konstatē, ka klientam ir mainījusies dzīvesvietas adrese, un veic labojumus klientu datu bāzē.

Ņem vērā! Šī starpfāze noslēgsies ar brīdi, kad personas datu apstrādei zudīs tiesiskais pamats – līdz ar to ir nepieciešams veidot rūpīgu monitoringa sistēmu, lai organizācija savlaicīgi spētu noteikt datu apstrādes tiesiskā pamata maiņu (tā cēloņi var būt visdažādākie, – līguma nosacījumu izpilde, datu subjekta piekrišanas atsaukšana, termiņa beigšanās informācijas glabāšanai u. c.).

[173] Šī starpfāze ļauj noteikt, kad dati ir novecojuši, kļuvuši neprecīzi un vairāk nav izmantojami neviena godprātīga un likumīga datu apstrādes nolūka sasniegšanai. Konstatējot kādu no apsvērumiem, kas traucē ar datu palīdzību sasniegt plānoto nolūku, dati vai nu atgriežas

iegūšanas/radīšanas fāzē (ja nolūks joprojām ir sasniedzams un tam pastāv likumīgs pamats) vai nonāk dzīvescikla noslēdzošajā fāzē.

Dzēšana

[174] Noslēdzošais posms datu apstrādes dzīvesciklā ir organizācijas rīcībā esošo datu anonimizācija un/vai dzēšana. Tas nozīmē, ka organizācija tās rīcībā esošos datus padara par nelasāmiem trešajām personām (datu neatgriezeniska iznīcināšana vai anonimizācija[35]).

Piemēram, klients izlemj pārtraukt līgumattiecības ar organizāciju par klientu kartes izmantošanu. Organizācija, ievērojot Grāmatvedības likumā noteikto termiņu, arhivē ziņas par klienta pirkumiem. Beidzoties dokumentu glabāšanas termiņam, organizācija tās rīcībā esošos datus iznīcina.

Ņem vērā! Arhivēta informācija, noslēdzoties tās uzglabāšanas termiņam, ir iznīcināma. Ņemot vērā, ka, ja vien neiestājas īpaša vajadzība, arhivētiem personas datiem vairāk nevajadzētu nonākt aktīvās izmantošanas fāzē. Tie jau ir uzskatāmi par nonākušiem dzīvescikla noslēdzošajā posmā. Lai atsekotu dažādo datu kopu glabāšanas termiņus un nodrošinātu, ka dati tiek izdzēsti paredzētajā termiņā, pārzinim ir jāizveido sistēma datu glabāšanas termiņa ievērošanai un jāievieš procedūras, kas nosaka datu dzēšanas un arhivēšanas kārtību organizācijā.

[175] Datu dzīvescikla apraksts/analīze, tieši NIDA veikšanas nepieciešamībai, ir jāveic vizualizācijas veidā. Respektīvi, ieteicams veids, kā īstenot datu dzīvescikla aprakstu, ir to aprakstīt un uzzīmēt soli pa solim, atbilstoši organizācijas izveidotajai datu apstrādes sistēmai – grafiski attēlojot konkrētās personas datu apstrādes algoritmu.

Organizācijas datu apstrādes sistēma

[176] Organizācijas datu apstrādes sistēma ietver tehnisko vidi un operatīvās darbplūsmas, kas saistītas ar personas datu pārvaldību visā tās dzīves ciklā. Tā attiecas gan uz infrastruktūru, gan lietojumprogrammām un procesiem, ko organizācija izmanto personas datu vākšanai, glabāšanai, pārsūtīšanai un apstrādei. Piemēram:

- Datu apstrādes darbības: ietver visas darbības, kas saistītas ar personas datu vākšanu, reģistrēšanu, organizēšanu, strukturēšanu, glabāšanu, pielāgošanu, pārveidošanu, atgūšanu, aplūkošanu, izmantošanu, izpaušanu, pārsūtīšanu, izplatīšanu, saskaņošanu, kombinēšanu, ierobežošanu, dzēšanu vai iznīcināšanu.
- Informācijas sistēmas un datubāzes: organizācijā izveidotā tehnoloģiju infrastruktūra un datubāzu sistēmas, ko izmanto personas datu glabāšanai un pārvaldībai, piemēram, klientu attiecību pārvaldības sistēmas, cilvēkresursu informācijas sistēmas un organizācijas resursu plānošanas sistēmas.
- Datu plūsmas un integrācija: organizācijā izveidotā sistēma, kā personas dati plūst organizācijas sistēmās un tiek nosūtīti citām, trešām personām, piemēram, pakalpojumu sniedzējiem vai partneriem.
- Datu glabāšanas un iznīcināšanas procesi: organizācijā ieviestās procedūras personas datu glabāšanai noteikto laika posmu un drošai iznīcināšanai, kad tie vairs nav vajadzīgi.

Plānotās datu apstrādes analīze

[177] Šajā sadaļā NIDA izstrādātājs veic vispārēju datu aprites dzīves cikla analīzi. Datu aprites dzīves cikla analīzi ir jāveic par konkrētajām, personas datu apstrādē iesaistītajām datu kopām, kas

[35] Atbilstoši Datu regulas 26. apsvērumam datu aizsardzības principi nebūtu jāpiemēro anonīmai informācijai, proti, informācijai, kura neattiecas uz identificētu vai identificējamu fizisku personu, vai personas datiem, ko sniedz anonīmi tādā veidā, ka datu subjekts nav vai vairs nav identificējams. Tādēļ Datu regula neattiecas uz šādas anonīmas informācijas apstrādi, tostarp statistikas vai pētniecības nolūkos.

ietver dažādu posmu izpēti no to vākšanas vai ģenerēšanas līdz datu iznīcināšanai. Labākas uztveramības dēļ vēlams šādu analīzi veikt ar vizualizācijas palīdzību.

[178] Analizējot (vizualizējot) plānoto datu apstrādes modeli, jāataino datu apstrādes objektīvā realitāte. Vizualizācijas mērķis ir grafiski/shematiski atveidot personas datu apstrādes procesu, padarot to vienkāršāk uztveramu un, līdz ar to, arī vienkāršāk analizējamu. Tas jāizmanto, lai izprastu datu nozīmi un modelētu to, kas praksē varētu notikt ar personas datu apstrādi dažādos apstākļos. Modelēšana parasti ietver šādus posmus:

- apraksta modeļa izveides mērķi un vēlamie rezultāti;
- datu apstrādes dzīvescikla vizualizācijas izstrāde;
- dažādu scenāriju testēšana, lai pārskatītu, kā modelis varētu potenciāli darboties praksē.

[179] Katrs no šiem soļiem var ietvert arī organizācijas pieņēmumus par datu apstrādes sistēmas funkcionēšanu, ekspertu slēdzienus un (ja iespējams) datu subjektu viedokli. Organizācijas pieņēmumi būtu jāpārskata ņemot vērā pieejamo informāciju, lai novērtētu to ticamību.

[180] Izstrādājot datu apstrādes dzīves cikla analīzes aprakstu, būs iespējams iegūt informāciju par visiem nepieciešamajiem līdzekļiem vai darbībām, kas dos iespēju NIDA izstrādātājam risināt neskaidros jautājumus par plānotās datu apstrādes uzsākšanu un veikt pienācīgu risku pārvaldību, kas var būt nepieciešams, lai īstenotu un uzturētu apstrādes darbību jebkurā tās dzīves cikla posmā – sākot no datu iegūšanas līdz datu apstrādes pārtraukšanai un datu glabāšanai/iznīcināšanai. Jebkuras pieejas apstrādes apraksts būtu jāvērš uz to, lai tas palīdzētu organizācijai efektīvi demonstrēt, kā plānotā datu apstrāde varētu ietekmēt personu tiesības un brīvības.

[181] Neatņemama datu apstrādes dzīvescikla daļa ir datu apstrādes funkcionāls apraksts. Šo vadlīniju kontekstā par datu apstrādes funkcionālu aprakstu tiek uzskatīts katra datu apstrādes soļa īstenošanas apraksts. Datu apstrādes īstenošanas soļa aprakstā ietver datu apstrādes darbību uzskaitījumu, attiecināmo drošības pasākumu kopumu un citu detalizētu praktiskās informācijas aprites elementu analīzi. Funkcionālais apraksts tiek izstrādāts kopā ar datu apstrādes vizualizāciju. Tas nozīmē, ka abi procesi viens otru papildina, un funkcionālais apraksts vārdiski izskaidro vizuāli attēlotās datu apstrādes shēmu.

Piemēram, funkcionālajā aprakstā norādāma datu nosūtīšana trešajām personām attiecībā uz katru saņēmēju; un veicams trešo personu pārsūtīšanas, saņēmēju un/vai saņēmēju kategoriju apraksts saistībā ar apstrādes nolūkiem, lomu dzīves ciklā un citām ar datu nosūtīšanu saistītām apstrādes darbībām.

Ņem vērā! Informācijai, kas tiek iekļauta plānotās datu apstrādes funkcionālajā aprakstā, ir jābūt pietiekamai, lai izprastu, kā tiks pārvaldīta datu apstrāde, izmantojot kādus tehniskos un organizatoriskos līdzekļus.

Ņem vērā! Katrs datu nosūtīšanas gadījums ir jauns elements datu apstrādes dzīvesciklā. Nododot informāciju citai personai – apstrādātājam, citai organizācijai – organizācija zaudē daļu kontroles pār datu apstrādi. Līdzīgi tas ietekmē arī datu subjektu. Veicot NIDA, pievēršama īpaša uzmanība šādiem dzīvescikla posmiem, kur mainās persona, kurai ir piekļuve datiem. Šajos gadījumos ir jāņem vērā ne tikai saistošo noteikumu kopums, kas attiecināms uz organizāciju, bet arī tās normas, kas būs saistošas datu saņēmējam. Piemēram, datu nodošanas gadījumos ir pienākums vērtēt likumus, kas būs saistoši personai trešajā valstī, neatkarīgi no starp organizāciju un saņēmēju noslēgtā līguma satura.

Lai arī nodošana uz trešajām valstīm nav atsevišķs NIDA elements, tomēr datu apstrāde trešajā valstī ir nozīmīgs aspekts, kas atstāj vērā ņemamu ietekmi uz vairāku risku iestāšanās iespējamību un pēc būtības var radīt arī virkni jaunu potenciālu risku avotu.

[182] Ja NIDA tiek veikta par jaunu, vēl tikai plānotu datu apstrādi, šajā sadaļā tiek aprakstīta arī plānotās datu apstrādes uzsākšana. Ja datu apstrāde ir sākta pirms NIDA vai gadījumos, kad NIDA ir veikts, bet ir konstatēta nepieciešamība konsultēties ar Inspekciju, organizācija veic objektīvu izvērtējumu un pieņem pamatotu lēmumu, kurā tiek paskaidrots, kāpēc datu apstrāde ir uzsākta pirms NIDA veikšanas vai bez iepriekšējas apspriešanās ar uzraudzības iestādi.

III. Organizācijas datu aizsardzības sistēma	
Pārziņa datu aizsardzības sistēmas apraksts	
Citi pasākumi, kurus pārzinis veicis pārskatatbildības principa vai citu Datu regulā izvirzīto prasību nodrošināšanai.	

Organizācijas datu aizsardzības sistēma

[183] Organizācijas datu aizsardzības sistēma aptver visu to darbību spektru, kuru mērķis ir aizsargāt to personu privātumu un tiesības, kuru dati tiek apstrādāti. Tā ietver iekšējos normatīvos aktus, datu apstrādes politiku, procedūras un tehniskos pasākumus, ko organizācija īsteno, lai nodrošinātu atbilstību datu aizsardzības normatīvajiem aktiem. Sadaļā "Organizācijas datu aizsardzības sistēma" jānorāda, piemēram:

- esošās iekšējās kārtības noteikumi un procedūras: norāda, vai organizācija ir izstrādājusi datu apstrādes un aizsardzības politiku, procedūras un iekšējās kārtības noteikumus, kurās izklāstīts, kā organizācijā jārīkojas ar personas datiem un nodrošina šīs kārtības īstenošanu;
- vai nodrošināta atbilstība tiesību aktiem: norāda, vai organizācija zina un spēj apliecināt, ka tiek ievēroti piemērojamie datu aizsardzības tiesību akti, piemēram, Datu regula, Fizisko personu datu apstrādes likums un citi nozares, kurā strādā organizācija, tiesību akti;
- Ieviestie drošības pasākumi: norāda, vai organizācija ir izveidojusi un īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai aizsargātu personas datus pret nesankcionētu piekļuvi, izpaušanu, pārveidošanu un iznīcināšanu;
- Esošā piekļuves kontrole un autentificēšanas mehānismi: norāda organizācijas īstenotās kontroles, lai ierobežotu piekļuvi personas datiem, pamatojoties uz lietotāju lomām, atļaujām un autentifikācijas mehānismiem;
- Informācija, ja ir iepriekš veikts novērtējums par ietekmi uz datu aizsardzību: norāda, vai organizācija jau iepriekš (par citu datu apstrādi) veikusi novērtējumu, lai identificētu un mazinātu privātuma riskus, kas saistīti ar datu apstrādes darbībām;
- Vai ir veiktas apmācības darbiniekiem: norāda, vai organizācija nodrošina darbiniekiem apmācības un izpratnes veidošanas programmas par datu aizsardzības principiem, privātuma praksi un viņu pienākumiem.

IV. Risku datu subjekta tiesībām un brīvībām analīze

Riska iespējamības un ietekmes analīze

[184] Datu regulas 75. apsvērumā skaidrots "tiesību un brīvību apdraudējuma" jēdziens, kā jebkāda neparedzēta ietekme vai sekas attiecībā uz datu subjektiem, kas var radīt kaitējumu fiziskai personai.

[185] Riska faktori var izrietēt no pašas apstrādes, piemēram, apstrādes nolūka, apstrādes darbības, izmantotajām tehnoloģijām u. c. Katram riska faktoram ir potenciāla ietekme uz datu subjektiem, un tā iespējamība būs atkarīga gan no apstrādes iekšējiem, gan ārējiem faktoriem.

Daži, ar datu apstrādi saistītie, ietekmes faktori:

Darbības, kas saistītas ar apstrādes nolūkiem	izriet no apstrādes nolūka
Izmantoto datu veidi	izriet no personas datiem, kuri tiek iegūti, apstrādāti vai nodoti "datu dzīvescikla" laikā;
Apstrādāto datu apjoms	saistīts ar attiecīgo datu subjektu skaitu, apstrādāto datu vai aspektu daudzveidību, laika ilgumu, vākšanas biežumu utt.;
Datu subjektu kategorijas	ar datu subjektu kategoriju, piemēram, darbinieki, nepilngadīgie, vecāka gadagājuma cilvēki, mazākaizsargātas personas, u. c.;
Apstrādes tehniskie aspekti	rodas no apstrādes veida, ja tos īsteno ar noteiktiem tehniskiem līdzekļiem;
Datu iegūšana	rodas no apstrādes veida, kad dati tiek vākti vai ģenerēti;
Pārziņa/apstrādātāja darbības joma	izriet no nozares, kurā darbojas organizācija, piemēram, veselības nozare, finanšu nozare, mazumtirdzniecība u. c.
Datu izpaušana	izriet no konteksta, kādā personas dati tiek izpausti trešajām personām datu apstrādes ietvaros;
Datu aizsardzības pārkāpums	izriet no personas datu aizsardzības pārkāpumu iespējamības, piemēram, tas, ka darbiniekiem darba uzdevumu veikšanai ir regulāri jāsūta elektroniskais pasts trešajām personām, vairo iespēju, ka tie kļūdīsies adresātā un nosūtīs vēstuli nepareizam adresātam;
Sekas, kas nav savietojamas ar sākotnējo datu apstrādes nolūku	Izriet no datu apstrādes konteksta, ja rodas iepriekš neparedzētas sekas un tās nav savietojamas ar datu apstrādes nolūku.

Ņem vērā! Jaunu tehnoloģiju izmantošana vai pastāvošu tehnoloģiju izmantošana inovatīvā veidā ir elementi, kas paši par sevi izraisa nepieciešamību veikt NIDA. Tas darīts ar nolūku, lai, plānojot personas datu apstrādi, tiktu apsvērta tās ietekme uz datu subjekta tiesībām un brīvībām veidos, kas iepriekš nav notikuši. Darot ko jaunu, arī rīcības sekas ne visos gadījumos ir skaidras – līdz ar to nepieciešams pirms inovāciju ieviešanas veikt rūpīgu novērtējumu, vai ir veikts novērtējums par visām iespējamajām ietekmēm atbilstoši labākajam organizācijas zināšanu līmenim.

Piemēram, organizācijas var ņemt vērā Mākslīgā intelekta akta[36] 7. panta 2. punktā noteiktos kritērijus, un tos pielāgot, lai tie attiektos uz datu apstrādes kontekstu:

- datu apstrādes paredzētais nolūks;
- datu apstrādes apjoms un biežums;
- apstrādāto datu raksturs un apjoms;
- fiziskas personas kontroles iespējas pār apstrādes rezultātiem;
- iepriekšējā ietekme vai riski, kas saistīti ar datu apstrādi;
- potenciālā negatīvā ietekme;
- datu subjekta atkarība no apstrādes rezultātiem;
- ietekmes samērošana starp datu subjektu un pārziņa vai apstrādātāja pozīciju;
- iespēja labot vai novērst nelabvēlīgu ietekmi;
- ieguvumi no datu apstrādes;
- esošo normatīvo aktu efektivitāte (vai spēkā esošie normatīvie akti nodrošina efektīvus aizsardzības mehānismus pret riskiem, kas saistīti ar datu apstrādi, un paredzētie pasākumi šo risku būtiskai samazināšanai vai novēršanai.

[36] EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2024/1689 (2024. gada 13. jūnijs), ar ko nosaka saskaņotas normas mākslīgā intelekta jomā un groza Regulas (EK) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 un (ES) 2019/2144 un Direktīvas 2014/90/ES, (ES) 2016/797 un (ES) 2020/1828 (Mākslīgā intelekta akts) (Dokuments attiecas uz EEZ) https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=OJ:L_202401689

Riska novērtējums

[186] Saskaņā ar Datu regulas 35. pantu, organizācijai ir jāveic apstrādes radītā kopējā raksturīgā riska analīze/novērtējums, ņemot vērā visus elementus, kas noteikti attiecībā uz katru no apstrādes laikā konstatētajiem riska faktoriem. Praksē riska līmeņa novērtēšanas procesu nevar veikt, neņemot vērā riska iespējamās sekas uz datu subjektiem.

[187] Jānosaka kritēriji riska novērtējuma konsekvencei, tādejādi novēršot to, ka sākotnējais riska novērtējums atšķiras attiecībā uz sekām, ko datu subjektiem rada konfidencialitātes, integritātes, datu pieejamības zudums, anonimizācijas/pseidonimizācijas atcelšana, datu izmantošana nesaderīgiem nolūkiem, garantiju pārkāpumi utt.

[188] Apzinot un analizējot riska faktorus, ir jānosaka kaitējums, ko riska iestāšanās var radīt datu subjektiem.

Riska iespējamības analīze[37]

[189] Iespējamība var attiekties gan uz konkrēta notikuma iestāšanās iespējamību, gan arī konkrētu seku iespējamību. Organizācijai ir skaidri jānorāda riska iespējamība, uz kuru attiecas varbūtības vērtība, skaidri un precīzi jādefinē notikums vai sekas. Lai pilnībā noteiktu riska iestāšanās iespējamību, novērtējumā ir nepieciešams iekļaut informāciju par tā iestāšanās varbūtību un laika periodu, piemēram, varbūtība, ka tas notiks vienu reizi gadā.

[190] Iespējamību var raksturot dažādos veidos, tostarp kā skaitlisku sagaidāmās varbūtības biežumu, vai aprakstošā veidā (piemēram, "ļoti ticams"). Ja izmanto aprakstošu apzīmējumu, tam būtu jādefinē nozīme.

[191] Lai pēc iespējas samazinātu nepareizu interpretāciju, izsakot varbūtību kvalitatīvi vai kvantitatīvi, laikposmam un attiecīgajai datu kopai vajadzētu būt skaidrai un saskanīgai ar konkrētā novērtējuma tvērumu.

Piemēram, veicot riska iespējamības analīzi izveidotam datu centram, kā arī nosakot notikuma iestāšanās periodu – 1 gads; "maz ticams" risks – plūdi Rīgas centrā izveidotajam datu centram (iespējamība, ka nākamā gada laikā datu centrs applūdīs, ir niecīga/teorētiska). Savukārt "ļoti ticams" risks ir, ka datu centra elementi pārstāj darboties tehniska nolietojuma dēļ (iespējamība, ka nākamā gada laikā datu centrs saskaras ar tehniskām kļūdām, ir ticama). Ir jāņem vērā, ka risku iespējamība ir neatņemami saistīta ar personas datu apstrādes apstākļiem (personas datu apstrādes vieta, raksturs, u. tml.).

[192] Dažādās situācijās ir lietderīgi izveidot riska skalu. Tā var ietvert kvalitatīvus, puskvantitatīvus vai kvantitatīvus pasākumus:

- Kvalitatīvās pieejas parasti balstās uz aprakstošām (nominālām) vai intervāla (parastām) skalām, attiecībā uz sekām un iespējamību.
- Puskvantitatīvas pieejas ietver to, ka vienu parametru (parasti varbūtību) izsaka kvantitatīvi, otru raksturo vai izsaka reitingu skalā.
- Kvantitatīvās pieejās izmanto seku un varbūtību mērījumus, kas izteikti skaitliskajās (attiecības) skalās. Ja risku analizē kvantitatīvi, būtu jānodrošina, ka, izmantojot novērtējumu, tiek izmantotas un pārnestas atbilstošas vienības un izmēri.

[37] NIDA metodoloģijas izstrādei izmantots ISO IEC 31010:2019 "Risk management -- Risk assessment techniques". Standarta izmantošanai nepieciešama licence. Iegādei pieejams: https://www.lvs.lv/lv/products/148861. Izmantotas arī Spānijas datu aizsardzības iestādes (AEPD) 2021. gadā izstrādātās vadlīnijas "Risk Management and Impact Assessment in the Processing of Personal Data". Pieejamas angļu valodā: https://www.aepd.es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf

Ņem vērā! Kvalitatīvos un puskvantitatīvos paņēmienus var izmantot tikai, lai salīdzinātu riskus ar citiem riskiem, kas novērtēti tajā pašā veidā vai ar tiem pašiem nosacījumiem. Tos nevar izmantot, lai tieši apvienotu vai apkopotu riskus, un tos ir ļoti grūti izmantot situācijās, kad ir gan pozitīvas, gan negatīvas sekas vai kad ir jāpanāk kompromisi starp riskiem. Jo īpaši starp riskiem, kuriem ir lielas sekas un maza iespējamība, un riskiem, kuriem ir mazas sekas un kuri bieži rodas.

[193] Izmantojot iepriekš aprakstītos riska iespējamības novērtēšanas pasākumus, organizācijai nepieciešams novērtēt identificēto risku iespējamās sekas. Sekas rodas no pastāvīgas pakļaušanas riska avotam, un tās ne vienmēr var pienācīgi aprakstīt vai aplēst kā vienu vērtību. Piemēram:

- sekas var izteikt kā seku varbūtības sadalījumu;
- notikumam ir dažādi cēloņi, un tas noved pie vairākiem iznākumiem un iespējamām sekām.

Ņem vērā! Kad riska avoti (piemēram, sistemātiskas problēmas) ir identificējami, bet ir ļoti grūti paredzēt iespējamo seku veidu un/vai iespējamību – ticama riska apmēra noteikšana, iespējamības un seku ziņā, kļūst neiespējama.

[194] Ja riskam ir iespējamas vairākas sekas, riska iespējamības novērtējumu var veikt kā seku vidējās varbūtības (t. i., sagaidāmo vērtību) aprēķinu. Tomēr šādā gadījumā organizācijai jābūt piesardzīgai, jo šāda pieeja ne vienmēr var būt labs riska rādītājs, jo tas atspoguļo sadalījuma vidējās sekas. Tā rezultātā tiek zaudēta informācija par mazāk iespējamām sekām, kas var būt smagas un līdz ar to svarīgas riska izpratnei. Iespējamo seku iestāšanās ticamība un ietekme veido riska apmēru.

[195] Atgādinām, ka organizācijai uzsākot risku novērtējumu, bija jānosaka pieņemamais riska apmērs[38]. Riska iespējamības novērtējuma rezultāts ir reālais datu apstrādes risku apmērs. Organizācijai pēc iespējamības novērtējuma veikšanas jāpārliecinās, ka noteiktais riska apmērs nepārsniedz pieņemamo līmeni.

[196] Kā vispārēju pieeju, lai panāktu līdzsvaru starp riska pārvaldības procesu, var izmantot četrus riska ietekmes līmeņus (ļoti nozīmīgs, nozīmīgs, maznozīmīgs un ļoti maznozīmīgs (vai arī neietekmē neko)), kā arī četrus varbūtības līmeņus (ļoti augsts, augsts, zems un maz ticams), lai to kopējās vērtības ļautu noteikt šādus riska līmeņus: ļoti augsts, augsts, vidējas un zems.

Piemēram:

Varbūtība	**Ļoti augsta**	Vidējs	Augsts	Ļoti augsts	Ļoti augsts
	Augsta	Zems	Vidējs	Augsts	Ļoti augsts
	Zema	Zems	Vidējs	Vidējs	Augsts
	Maz ticama	Zems	Zems	Zems	Vidējs
		Nenozīmīga	**Maznozīmīga**	**Nozīmīga**	**Ļoti nozīmīga**
		Ietekme			

[197] Rezultātu kvantitatīvā izteiksmē var interpretēt šādi:

- Zems risks: ja tas ir mazāks par 3;
- Vidējs risks: no 4 līdz 7;
- Augsts risks: no 8 līdz 11;
- Ļoti augsts risks: vienāds vai lielāks par 12.

[38] Šo vadlīniju 3.4. apakšnodaļa Riska novērtējums

Rezultātu kvantitatīvo izteiksmi iegūst, sareizinot varbūtību ar iespējamību.

Piemēram:

Varbūtība	**4**	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	**2**	**3**	**4**
		Ietekme			

[198] Ietekmes līmeņa izvērtējuma piemērs:

Apraksts	**Ietekmes līmenis (kvalitatīvi)**	**Ietekmes līmenis (kvantitatīvi)**
Tas ietekmē tiesību un brīvību īstenošanu, un radītās sekas ir neatgriezeniskas: • vai sekas ir saistītas ar īpašu kategoriju datiem (datu kategorijām) vai noziedzīgiem nodarījumiem, un ir neatgriezeniskas; • un/vai tās rada būtisku sociālu kaitējumu, piemēram, diskrimināciju, un ir neatgriezeniskas; • un/vai neatgriezeniski ietekmē īpaši neaizsargātus datu subjektus, jo īpaši bērnus; • un/vai rada būtiskus un neatgriezeniskus morālos vai materiālos zaudējumus.	Ļoti nozīmīgs	4
Iepriekš minētie gadījumi, kad ietekme ir atgriezeniska: • un/vai datu subjekta kontroles zaudēšana pār saviem personas datiem, ja datu apjoms ir liels attiecībā pret datu kategorijām vai datu subjektu skaitu; • un/vai datu subjektu identitātes zādzība notiek vai var notikt; • un/vai datu subjektiem var rasties ievērojami finansiāli zaudējumi; • un/vai konfidencialitātes zaudēšana attiecībā uz datiem, uz kuriem attiecas pienākums glabāt dienesta noslēpumu, vai konfidencialitātes pienākuma pārkāpums; • un/vai pastāv sociāls kaitējums datu subjektiem vai noteiktām datu subjektu grupām;	Nozīmīgs	3
Ļoti ierobežota kontroles zaudēšana pār dažiem personas datiem un konkrētiem datu subjektiem, izņemot īpašu kategoriju datu apstrādi.	Maznozīmīgs	2
Sadaļā "maznozīmīgs" minētajos gadījumos, kad visas sekas ir novēršamas	Neietekmē	1

[199] Varbūtības izvērtējuma piemērs:

Apraksts	Varbūtības līmenis (kvalitatīvi)	Varbūtības līmenis (kvantitatīvi)
Riska faktors jau iepriekš ir materializējies vai ir pierādījumi par vairākiem šā riska materializēšanās gadījumiem pēdējā gada laikā: • vai ir pierādījumi, ka šāds risks pēdējā gadā ir materializējies; • un/vai ir revīzijas/pētījumi, kuros konstatētas būtiskas nepilnības organizatoriskajās procedūrās vai tehniskajos līdzekļos, kas saistīti ar šo risku.	Ļoti augsts	4
Vai ir pierādījumi, ka šāds risks pēdējā gadā kādā organizācijā ir materializējies: • vai pētījumi liecina, ka iespējamība varētu būt augsta; • un/vai ir revīzijas/pētījumi, kuros tiek konstatētas iespējamās nepilnības organizatoriskajās procedūrās vai tehniskajos līdzekļos, kas saistīti ar šo risku; • un/vai elementi, kas saistīti ar riska faktoriem, ir īstenoti ar jaunām tehnoloģijām vai organizatoriskām procedūrām, neievērojot kvalitātes standartus.	Augsts	3
Ja ir pierādījumi par šāda riska materializēšanos noteiktā laika periodā, piemēram, kas ir ilgāks par 5 gadiem (termiņš ir saistāms ar personas datu apstrādes nolūku).	Zems	2
Ja ir pierādījumi, ka šāds risks nematerializēsies vai tas nebija konstatēts pēdējos 5 gados.	Maz ticams	1

Personas datu aizsardzības pārkāpuma iestāšanās riska novērtēšana[39]

[200]Organizācijai, veicot NIDA, ir jānosaka datu aizsardzības pārkāpuma iestāšanās kritērijus un jāņem vērā personas datu aizsardzības pārkāpumu iespējamās sekas uz datu subjektiem. Veicot NIDA, organizācijai jāvērtē sekas, ko datu subjektiem varētu radīt konfidencialitātes, integritātes, datu pieejamības zudums, anonimizācijas/pseidonimizācijas atcelšana, datu izmantošana neatbilstīgiem nolūkiem, garantiju pārkāpumi utt.

[201] Identificējot un analizējot riska faktorus, organizācijai ir jānosaka personas datu aizsardzības pārkāpumu iespējamais kaitējums, piemēram, problēmas, kas var rasties saistībā gan ar pašiem riska mazināšanas pasākumiem (piemēram, datu pieejamība trešajām personām neveiksmīgas pseidonimizācijas gadījumā), gan arī tehniskas problēmas datu apstrādes sistēmās (piemēram, nespēja sasniegt personas datu apstrādes nolūku, ja pārtrauc darboties klientu vadības sistēma).

[202] Organizācijai jāidentificē riski, kas var rasties personas datu apstrādes procesā, un jānosaka to iespējamība un ietekme. Tas var ietvert, tai skaitā, piemēram, šādus apdraudējumus:

[39] NIDA metodoloģijas izstrādei izmantots ISO IEC 31010:2019 "Risk management -- Risk assessment techniques". Standarta izmantošanai nepieciešama licence. Iegādei pieejams: https://www.lvs.lv/lv/products/148861. Izmantotas arī Spānijas datu aizsardzības iestādes (AEPD) 2021.gadā izstrādātās vadlīnijas "Risk Management and Impact Assessment in the Processing of Personal Data". Pieejamas angļu valodā: https://www.aepd.es/documento/risk-management-and-impact-assessment-in-processing-personal-data.pdf

- Konfidencialitātes pārkāpums: personas dati tiek nosūtīti nepareizam adresātam;
- Integritātes pārkāpums: datu izmainīšana ļaunprātīga uzbrukuma rezultātā;
- Pieejamības pārkāpums: datu nepieejamība elektrības vai servera atteices dēļ;
- Anonimizācijas vai pseidonimizācijas "atcelšana": nepareiza tehnisko vai organizatorisko pasākumu pielietošana, lai pseidonimizētu vai anonimizētu personas datus.

[203] Augstāk minētajos apdraudējumos kaitējuma ietekme var būt dažāda, piemēram:
- Konfidencialitāte: Personas sensitīvo datu izpaušana var radīt reputācijas zaudējumus vai finansiālas sekas datu subjektam;
- Integritāte: Izmainīti dati var izraisīt kļūdainu lēmumu pieņemšanu, piemēram, nepareizi aprēķinot kredītspēju;
- Pieejamība: Datu nepieejamība, piemēram, medicīniskās informācijas trūkums, var radīt dzīvībai bīstamas situācijas;
- Anonimizācijas vai pseidonimizācijas "atcelšana": piemēram, personas dati, kas satur sensitīvu informāciju, nav atbilstoši pseidonimizēti, tos nodod izpētes institūtam – var radīt būtiskas sekas datu subjektam.

[204] Lai veiktu personas datu aizsardzības pārkāpuma riska līmeņa novērtēšanu, organizācija var modelēt dažādas personas datu aizsardzības pārkāpuma situācijas. Situācijas aprakstam organizācijai jāizmanto vismaz šādi elementi:
- Pārkāpuma veida apraksts (piemēram, cilvēciskas kļūdas rezultātā nepareizam adresātam nosūtīts elektroniskais pasts; pakalpojums nav pieejams elektrības pārrāvuma dēļ; ļaunprātīga uzbrukuma rezultātā organizācijas rīcībā esošā informācija nonākusi neautorizētu personu rīcībā).
- Personas datu kategoriju uzskaitījums un datu subjektu raksturojums, kuriem pārkāpuma rezultātā ir nodarīts kaitējums.
- Kāds kaitējums var tikt nodarīts datu subjekta tiesībām un brīvībām.

[205] Katrai situācijai ir nepieciešams aizpildīt gan pārkāpuma ietekmes, gan pārkāpuma iestāšanās iespējamības novērtējumu.

Piemērs riska līmeņa noteikšanai:

Pārkāpuma ietekme

Pārkāpuma raksturs	**Ietekme uz tiesībām un brīvībām (kvalitatīvi)**	**Ietekme uz tiesībām un brīvībām (kvantitatīvi)**
Konfidencialitāte	Ļoti augsta, augsta, vidēja, zema	4/3/2/1
Integritāte	Ļoti augsta, augsta, vidēja, zema	4/3/2/1
Pieejamība	Ļoti augsta, augsta, vidēja, zema	4/3/2/1
Utt.	Ļoti augsta, augsta, vidēja, zema	4/3/2/1

Pārkāpuma iestāšanās iespējamība

Pārkāpuma raksturs	**Iestāšanās iespējamība (kvalitatīvi)**	**Iestāšanās iespējamība (kvantitatīvi)**
Konfidencialitāte	Ļoti augsta, augsta, zema, maz ticama	4/3/2/1
Integritāte	Ļoti augsts, augsta, zema, maz ticama	4/3/2/1
Pieejamība	Ļoti augsta, augsta, zema, maz ticama	4/3/2/1
Utt.	Ļoti augsta, augsta, zema, maz ticama	4/3/2/1

Piemēram, ja darba devējam tiktu nosūtīts elektroniskais pasts ar darbinieka sensitīvajiem medicīnas datiem par tā slimības vēsturi, saistībā ar psiholoģiskām bērnības traumām.

- Pārkāpuma raksturs: Konfidencialitātes pārkāpums;
- Iestājušās sekas: finansiāli zaudējumi, jo darba devējs diskriminē darbinieku un uzsaka darba tiesiskas attiecības; emocionālas ciešanas, jo kolēģi darbā uzzina par darbinieka slimības vēsturi un pārtrauc komunicēt vai izmaina komunikāciju;

Ietekme uz tiesībām un brīvībām: iestājušās sekas fiziskai personai;
Kvalitatīvi: augsta
Kvantitatīvi: 3
Iestāšanās iespējamība: iestādē jau iepriekš ir bijušas kļūdas ar elektroniskā pasta adresātiem.
Kvalitatīvi: Ļoti augsta
Kvantitatīvi: 4
Riska līmenis (Ietekme*iestāšanās iespējamība – 3*4):
Kvalitatīvi: augsts risks
Kvantitatīvi: 12

Ņem vērā! Iespējamības analīzē ir jāapsver, kad tiks uzsākta plānotā datu apstrāde, jo no tā izrietēs arī iespējamā pārkāpuma varbūtība (piemēram, vai tas varētu notikt mēneša laikā no izvērtējuma veikšanas, īstermiņā, vidējā termiņā vai ilgtermiņā).

Riska rādītāju apkopošana

[206] Apstrādes kopējā riska līmeņa novērtējumu iegūst no riska līmeņa novērtējuma attiecībā uz katru no apstrādē konstatētajiem riska faktoriem. Dažādu riska faktoru savstarpējā atkarība varētu paaugstināt apstrādes riska līmeni.

[207] Ja ir dažādi riska faktori, ir nepieciešams izvērtēt, kā šie neatkarīgie faktori var mijiedarboties viens ar otru, analizējot to kopējo ietekmi vai savstarpējo mijiedarbību, kas starp tiem pastāv.

Ņem vērā! Lai novērtētu identificētu apstrādes riska faktoru kopumu un kopējo riska līmeni, kas izriet no apstrādes, var izmantot dažādas metodes .

[208] Pirms pasākumu īstenošanas jānovērtē apstrādes riska līmenis, lai noteiktu raksturīgā riska līmeni. Tomēr tas ir jāpārrēķina arī pēc tam, kad ir ieviesti visi riska mazināšanas pasākumi. Tas ir veids, kā novērtēt pasākumu efektivitāti un aprēķināt atlikušo risku, līdz tas sasniedz pieņemamu līmeni.

[209] Efektivitātes vērtību (kopējo efektivitāti) nosaka katram identificētajam riska faktoram, ko iedala šādos līmeņos:

- **Pieņemams:** Kontroles pasākumu īstenošana neietekmē apdraudējuma iespējamību un ietekmi. Tie lielā mērā paliek nemainīgi vai nedaudz atšķiras. Riska faktora līmenis ir pieņemts.
- **Kontrolēts:** Apdraudējuma iespējamība un ietekme ir ievērojami samazināta. Šādā gadījumā aplēš jauno riska līmeni.
- **Novērsts:** Apdraudējuma iespējamība un/vai ietekme ir krasi samazināta līdz nenozīmīgām vai tuvu niecīgām vērtībām. Riska faktora riska līmeni samazina līdz zemam.

[210] Atbilstoši ieviesto kontroļu efektivitātei tiks novērtēts atlikušā riska līmenis. Ja pirmajā posmā apstrādes riska līmenis ir aprēķināts no katra riska faktora raksturīgā riska līmeņa, šajā riska pārvaldības posmā to aprēķina no atlikušā riska līmeņiem.

V. "Ietekmes uz datu subjektu raksturojums"	
Tiesības uz datu aizsardzību	
Informācijas pārredzamība, saziņa un datu subjekta tiesību īstenošanas kārtība	
Informēšana	
Piekļuve datiem	
Datu labošana	
Datu dzēšana, iebilšana datu apstrādei un pārnesamība	
Datu ierobežošana	
Automatizēta individuālu lēmumu pieņemšana	
Citas pamattiesības	
Vienlīdzība un nediskriminācija	
Dzīvības drošības tiesības	
Brīvības tiesības	
Taisnīga tiesa	
Privātās un ģimenes dzīves ievērošana	
Tiesības uz darbu, īpašumu un taisnīgu atalgojumu	
Tiesības uz izglītību	
Tiesības uz veselību	
Piederība politiskai sabiedrībai	

[211] Analizējot, kā veidojas ietekme uz datu subjekta tiesībām un brīvībām, ir nepieciešams aprakstīt esošo situāciju, kā attiecīgās tiesības īstenošana notiek pirms datu apstrādes, par kuru tiek veikta NIDA, uzsākšanas. Tai blakus jānostāda plānotā apstrāde ar tās tehniskajiem elementiem un niansēm, un jāvērtē, vai šie abi raksturlielumi mijiedarbosies savstarpēji un, ja mijiedarbosies, tad kā.

[212] Tas, cik liela varbūtība ir, ka ietekme iestāsies, nosakāms risku analīzes nodaļā. Šeit ir nepieciešams identificēt visas iespējamās, arī hipotētiskās ietekmes uz datu subjektu. Tāpat jāatceras, ka iespējamas ietekmes pastāvēšana šajā brīdī nenozīmē, ka apstrāde būs neiespējama – drīzāk ietekmes pastāvēšana ļaus noteikt riskus, kas ir vērtējami nākamajā NIDA veikšanas posmā.

[213] Analizējot iespējamo ietekmi, ir jāņem vērā arī personas datu aizsardzības pārkāpuma iespējamība, un organizācijai vērtējot iespējamo ietekmi, ir jāņem vērā ne tikai tās datu apstrādes sistēmās plānotā apstrāde, bet iespējamības līmenī jāpieļauj, ka dati, kas tiek apstrādāti, var nonākt jebkuras citas – trešās personas rīcībā.

[214] Vērtējamā ietekme var būt gan tieša, – piemēram, datu apstrādes rezultātā izveidojusies tieša ietekme, gan netieša – datu apstrādes rezultātā ietekmes nav, bet radītais galaprodukts ļauj izdarīt secinājumus un ietekmē personu kādā no norādītajām pamattiesību kategorijām.

[215] Šis novērtējums jādala divās daļās – personas datu aizsardzības tiesības (jo novērtējums vērsts uz datu aizsardzības novērtējumu, un līdz ar to šīs tiesības un ietekme uz tām vērtējama primāri) un citas tiesības un brīvības.

Ņem vērā! Ja organizācija nespēj atrast atbilstošus tehniskus rīkus tiesību aizsardzībai, tad šāda situācija rada paaugstinātu risku datu subjekta tiesībām un brīvībām.

Datu aizsardzības tiesības

- **Informācijas pārredzamība, saziņa un datu subjekta tiesību īstenošanas kārtība.**

[216] Jāizvērtē, vai plānotā datu apstrāde savā būtībā neierobežo datu subjektiem sniedzamās informācijas uztveramību un pieejamību. Tāpat jāvērtē, kā datu apstrādē izmantotie rīki ietekmēs organizācijas ierastos komunikācijas kanālus ar datu subjektu – kā apstrāde ietekmēs organizācijas pieejamību saziņai ar datu subjektu.
[217] Jāsāk ir ar esošās situācijas izvērtējumu – kāda ir organizācijas iekšējā procedūra saziņai ar datu subjektu, kā tiek nodrošināts, ka nepieciešamā informācija tiek sniegta datu subjektam saprotamā, uztveramā un pieejamā veidā, un vai to var piemērot jaunajai apstrādei.

Piemērs – Organizācija plāno veikt videonovērošanu āra kafejnīcā. Videonovērošanas kameras nav iespējams uzstādīt veidā, kas neļautu filmēt garāmgājējus – personas, kas nav kafejnīcas klienti. Garāmgājējiem, neesot kafejnīcas klientiem, arī nav iespējams uzzināt, ka viņu datu apstrāde notikusi. Atbildīgais par videonovērošanas sistēmu uz jautājumiem ir gatavs sniegt atbildes tikai klātienē – nav paredzēta iespēja organizācijai datu subjekta iesniegumu iesniegt attālināti. Šādā gadījumā tiek radīts apdraudējums datu subjekta tiesībām no pārredzamības, saziņas un datu subjekta tiesību īstenošanas perspektīvas.

- **Informēšana**

[218] Jāizvērtē plānotās datu apstrādes ietekme uz organizācijas pienākumu sniegt datu subjektam informāciju par datu apstrādi pirms datu apstrādes uzsākšanas. Jāņem vērā, ka citu apstrāžu gadījumā var rasties no lietošanas un apstrādes loģikas izrietošas problēmas nodrošināt datu subjektu ar visu Datu regulas 13. un 14. pantā norādīto obligāti sniedzamo informāciju.

[219] Gadījumā, ja, veicot datu subjektu tiesību aprakstu, tiek secināts, ka ar līdzšinējām metodēm datu subjekta informēšanas pienākumu organizācija jaunajā datu apstrādes procesā nespēs nodrošināt (piemēram, datu subjektam sniedzamā Datu regulas 13. pantā noteiktā informācija netiktu sniegta pirms datu apstrādes uzsākšanas, bet Datu regulas 14. pantā sniedzamā informācija netiktu sniegta uzsākot datu subjekta datu apstrādi), tad jādomā par piemērotiem ietekmes mazināšanas pasākumiem – kā nodrošināt, ka datu subjekts informāciju par apstrādi tomēr saņems laicīgi.

Piemēram, organizācija izvērš savu darbību, sākot piedāvāt pakalpojumu vēl kādā Eiropas Savienības dalībvalstī. Organizācija savu privātuma politiku papildus latviešu valodai izstrādā angļu valodā, tomēr šī nav dominējošā valoda Eiropas Savienības dalībvalstī, kuras iedzīvotāji ir organizācijas paplašināto pakalpojumu mērķauditorija. Šādā gadījumā rodas apdraudējums datu subjekta tiesībām uz informāciju, jo ziņām par savu datu apstrādi klients var piekļūt tikai valodā, kas nav tā dzimtā, vai arī veicot atsevišķu pieejamās informācijas tulkojumu.

- **Piekļuve datiem**

[220] Jāizvērtē, vai organizācijai jaunajā personas datu apstrādes sistēmā tehniski būs iespējams atlasīt, izgūt un apstrādāt visus datus, uz kuriem attiecināmas datu subjekta piekļuves tiesības. Nepieciešama analīze, kā jau pastāvošie organizācijas procesi savietosies ar jaunizveidotās personas datu apstrādes sistēmas praktisko pusi. Atkarībā no plānotās datu apstrādes, mainīsies arī datu subjekta tiesību īstenošanas procesi.

Piemēram, Organizācijas veikta klientu datu apstrāde tiek īstenota tās interneta vietnē ar klienta reģistrēta profila starpniecību. Visa informācija, ko organizācija iegūst - gan klienta sniegtā, gan Organizācijas par klientu radītā, ir piesaistīta šim klienta profilam. Vienlaikus organizācija plāno saglabāt kārtību, ka klientam, lai vērstos pie organizācijas, ir jāiesniedz pašrocīgi parakstīts papīra dokuments. Šādā gadījumā organizācijas plānotā informācijas aprites kārtība radītu vērā ņemamus ierobežojumus datu subjekta piekļuves tiesībām.

- **Datu labošana**

[221] Datiem, atkarībā no to nozīmes datu apstrādē, var būt atšķirīga loma apstrādes darbības nodrošināšanā. Dati var būt gan apstrādes veiksmīgas darbības priekšnoteikums (piemēram, apstrādēs, kas vērstas uz datu analīzi), gan nepieciešami kādas citas darbības veikšanai (piemēram, kad dati vajadzīgi personas identifikācijai sistēmā), gan arī citos gadījumos.

[222] Šīs tiesības novērtējums būtu jāsāk ar:
- veida, kā dati tiek iegūti, noteikšanu;
- datu ieguves avota vietas datu dzīvesciklā un apstrādes loģikā noteikšanu;
- analīzi par to, kāda ir ietekme uz datu subjektu, ja plānotajā datu apstrādē tiek apstrādāti neprecīzi datu subjekta dati.

[223] Organizācijai ir jāorganizē darbs ar sistēmu veidā, kas ļautu iezīmēt atsevišķas datu kopas, kuras var būt nepieciešams mainīt, lai nodrošinātu iespēju, ka dati tiek grozīti, neapdraudot visas sistēmas darbības integritāti.

Ņem vērā! Nedrīkst aizmirst arī par datu labošanas organizatorisko aspektu. Skaidra procesa izklāstīšana iekšējā kārtībā ļaus izstrādāt arī veidojamo informācijas aprites sistēmu loģisku un efektīvu.

Piemēram, Organizācija veido iepazīšanās lietotni/portālu. Viena no pirmajām izvēlēm, kas datu subjektam ir jāveic, ir tā seksuālās orientācijas norādīšana. Vēlāk datu subjektam jāsniedz arī tā identificējoša informācija un citas ziņas. Pēc datu ievadīšanas, ko veic datu subjekts, informāciju aplikācijā viņš pats vairs nevar labot. To izlabot var tikai ar Organizācijas saskaņojumu. Šādā situācijā rodas riski datu subjekta tiesību uz informācijas labošanu īstenošanai. Būtu jāievēro princips, ka informāciju, ko datu subjekts ir pats iesniedzis, pats arī var izlabot.

- **Datu dzēšana, iebilšana pret datu apstrādi un pārnesamība**

[224] Jāatceras, ka šīs nav universālas tiesības un datu subjekts tās var īstenot Datu regulā noteiktos gadījumos un apmērā. Ja šie gadījumi iestājas, tad organizācijai ir pienākums minētās tiesības nodrošināt.

[225] Šo tiesību novērtējumā jāņem vērā:
- vai plānotajā datu apstrādē ir īstenojamas minētās tiesības;
- analīze par to, kādi tehniskie līdzekļi tiks izmantoti datu subjekta tiesību nodrošināšanai.

[226] Pēc datu apstrādes procesu identifikācijas datu dzīvesciklā, kurā šīs tiesības var būt attiecināmas, ir jāizstrādā organizatoriska kārtība tiesību īstenošanai un jāveido datu apstrāde tādā veidā, lai tiesību īstenošana neietekmētu sistēmas drošību un integritāti.

Ņem vērā! Attiecībā par tiesībām iebilst pret datu apstrādi, ir jāparedz strīdu izskatīšanas procedūra, kurā pārzinis ņem vērā datu subjekta īpašo situāciju, salīdzinot ar jau veikto līdzsvarošanas testu.
Attiecībā uz datu pārnesamību, var veikt novērtējumu, vai tiek plānots izmantot datu kopas, kuras klients pārnestu no citiem pārziņiem. Būtu jāizstrādā rīcības plāns arī šādiem gadījumiem.

- **Datu subjekta tiesību ierobežošana**

[227] Datu regulā noteiktos gadījumos organizācijai var izveidoties pienākums veikt datu apstrādes ierobežošanu. Pamatā šīs tiesības īstenojamas gadījumā, kad organizācijai ir strīds ar datu subjektu par datu precizitāti vai organizācijas tiesībām datus apstrādāt, kā arī gadījumā, kad datu subjekts to ir palūdzis savas īpašās tiesiskās situācijas dēļ (piemēram, šie dati datu subjektam var būt nepieciešami tiesvedībai pret organizāciju vai kādu trešo personu).

[228] Ierobežošanas tiesības nozīmē, ka pārzinim konkrētie dati ir jāspēj iezīmēt un pārvietot uz vietu sistēmā, kur tie uz ierobežojuma pastāvēšanas laiku glabātos bez kādas tālākas apstrādes no organizācijas puses.

[229] Organizācijai jāpievērš uzmanība tiesības īstenošanas organizatoriskajiem aspektiem.

Ņem vērā! Tiesības ierobežot datu apstrādi datu subjektam ir Datu regulas 18. pantā noteiktajos gadījumos. Organizācijai ir jāizstrādā iekšējās procedūras, kādos gadījumos un attiecībā uz kādām datu kopām datu subjektiem būs iespējams īstenot tiesības uz ierobežošanu.

[230] Sistēmas uzbūves specifikācijā jāparedz iespēja uz nepieciešamo laiku apturēt datu apstrādi, norobežojot to no pārējās apstrādē esošo datu kopas. Kā arī iespēja vēlāk – pēc tam kad ierobežojums datu apstrādei atcelts, atjaunot datus atbilstošajā vietā, sākotnējā datu kopā.

Piemēram, organizācija plāno uzsākt aizdevumu izsniegšanu, izmantojot aplikācijas starpniecību. Aplikācijā tiek integrētas nepieciešamās "Zini savu klientu" darbības, tiek saglabāti darījuma pamatdati, kā arī informācija, kuru aplikācijai klients sniedz brīvprātīgi – gatavību saņemt komerciālus paziņojumus no organizācijas un ziņas par to, kādi organizācijas un tās partneru produkti ir klientam īpaši interesanti. Informācijas aizsardzībai organizācija izvēlas izmantot blokķēžu tehnoloģiju.
Tiesības tikt dzēstam nav attiecināmas uz darījuma pamatdatiem un uz "Zini savu klientu" pasākumu ietvaros paveikto, savukārt uz klienta brīvprātīgi sniegto informāciju gadījumos, kad klients atsauc tālākas šīs informācijas apstrādei sniegto piekrišanu, gan šīs tiesības ir piemērojamas.
Organizācijai ir jāveic novērtējums, uz kurām datu kopām datu dzēšanas tiesības būs attiecināmas, vai informācijas sistēmā šos datus būs iespējams iezīmēt un dzēst, neietekmējot pārējo datu integritāti. Gadījumā, ja izmantotā tehnoloģija rada riskus, ka konkrētā datu subjekta tiesība nebūs īstenojama (blokķēžu tehnoloģiju būtība ir informācijas atsekojamība un negrozāmība, līdz ar to datu dzēšanu lielākajā daļu blokķēžu risinājumu ir sarežģīti integrēt), uzskatāms, ka apstrādē saglabājas augsti riski, kuru mazināšanai organizācijai jāatrod risinājumi.

- **Automatizēta individuālu lēmumu pieņemšana**

[231] Jāizvērtē, vai plānotā personas datu apstrāde ir uzskatāma par automatizētu lēmumu pieņemšanu Datu regulas izpratnē vai var tikt izmantota automatizētu lēmumu pieņemšanai. Organizācijai jāņem vērā:

- automatizēto lēmumu pieņemšanas lomas plānotajā datu apstrādē atbilstība Datu regulas 22. panta 2. punkta nosacījumiem;
- ieviesto pasākumu, lai vismaz nodrošinātu cilvēka līdzdalību no organizācijas puses, un lai datu subjekts varētu paust savu viedokli un apstrīdēt lēmumu, novērtējums;
- ka īpašu kategoriju datu apstrāde tiek veikta ievērojot Datu regulas 22. panta 4. punktā noteikto.

[232] Aprakstā jānovērtē gan datu subjekta saprātīgās gaidas un izpratne par datu apstrādi, gan arī automatizētu lēmumu pieņemšanas nozīme plānotās personas datu apstrādes nolūku sasniegšanai.

Ņem vērā! Automatizētas lēmumu pieņemšanas elements var būt arī profilēšana. *"Profilēšana" ir jebkura veida automatizēta personas datu apstrāde, kas izpaužas kā personas datu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos*[40]*.* Profilēšana cieši saistīta ar noteikta veida tiesiskajiem pamatiem, un šeit var būt izmantojama informācija, kas jau tika gatavota iepriekšējā sadaļā, kad notika vērtējums par plānotās datu apstrādes atbilstību datu aizsardzības principiem.

Ņem vērā! Organizācijai NIDA ir jāvērtē arī iespējamība, kā datus varētu izmantot trešās personas gadījumā, ja organizācija zaudētu kontroli pār datiem. Viens no elementiem, kas jāņem vērā ir, piemēram, vai trešās personas datus varētu izmantot profilēšanai.

Citas tiesības un brīvības

[233] Pamattiesību ierobežošana var būt attaisnota tikai tajos gadījumos, kad nepieciešams līdzsvarot dažādas pamattiesības un intereses, ņemot vērā Latvijas Republikas Satversmes 116. pantā noteikto. Likumīgas un godprātīgas personas datu apstrādes princips var tikt ievērots tajos gadījumos, kad personas pamattiesības netiek aizskartas vai arī kad to ierobežošana ir pamatota un nepieciešama demokrātiskajā sabiedrībā.

[234] Līdz ar to, šajā gadījumā, vērtējot ietekmi uz personas pamattiesībām, ieteikumi tiks izteikti attiecībā uz izpausmēm, kur šī ietekme izpaužas netieši, vai pastāv tikai ietekmes risks. To cik liela varbūtība ir, ka ietekme iestāsies, noteiks risku analīze.

[235] Šeit ir nepieciešams identificēt visas iespējamās, arī hipotētiskās ietekmes uz datu subjektu. Tāpat atceramies, ka iespējamas ietekmes pastāvēšana šajā brīdī nenozīmē, ka apstrāde būs neiespējama – drīzāk ietekmes pastāvēšana ļaus noteikt riskus, kas ir vērtējami nākamajā NIDA veikšanas posmā.

[236] Analizējot iespējamo ietekmi, ir jāņem vērā drošības incidenta iespējamība. Organizācijai, vērtējot iespējamo ietekmi, ir jāņem vērā ne tikai tās datu apstrādes sistēmās plānotā apstrāde, bet iespējamības līmenī jāpieļauj, ka dati, kas tiek apstrādāti, var nonākt jebkuras citas – trešās personas rīcībā.

[40] Datu regulas 4. panta 4) punkts.

[237] Vērtējamā ietekme var būt gan tieša, – piemēram, datu apstrādes rezultātā izveidojusies tieša ietekme, gan netieša – datu apstrādes rezultātā ietekmes nav, bet vērtējuma rezultāti ļauj izdarīt secinājumus un ietekmē personu kādā no norādītajām pamattiesību kategorijām.

[238] Jāpatur prātā, ka vienai plānotai apstrādei var būt ietekme uz vairākām pamattiesībām, kas savstarpēji savijušās kopā. Pastāv iespēja, ka viena plānota darbība var ietekmēt vairākas pamattiesību kategorijas. Piemēram, neatbilstošs darba produktivitātes mērījums, kurā ņemti vērā dzimuma faktori, varētu ietekmēt gan tiesības nebūt diskriminācijas subjektam, gan arī tiesības uz īpašumu un taisnīga atalgojuma saņemšanu.

- **Vienlīdzība un nediskriminācija:** *Visiem cilvēkiem ir jābūt vienlīdzīgiem un tiem ir jābūt aizsargātiem pret diskrimināciju.*

[239] Jānovērtē, vai plānotā datu apstrāde pēc savas būtības nebūs diskriminējoša vai neradīs apstākļus, kas veidos negodīgu vidi attiecībā uz kādu identificētu vai identificējamu personu. Kā piemērs negatīvai ietekmei uz šo pamattiesību varētu būt situācija, kur ietekmes novērtējums tiek veikts mašīnapmācībai, kas analizē kādu vienu datu subjekta raksturojošo parametru, piemēram, sejas izteiksmi, bet kuras apmācības datu bāze ir ierobežota un reprezentē tikai nelielu populācijas daļu. Šādi apmācīts mašīnas prāts nebūs savos spriedumos godīgs pret visiem vienādi, un pastāvēs būtisks risks plānotās datu apstrādes ietekmei uz vienlīdzības un nediskriminācijas tiesību pārkāpumu.

- **Dzīvības drošības tiesības:** *Katram cilvēkam ir tiesības uz dzīvību, personīgo brīvību un fizisko neaizskaramību.*

[240] Ietekmes piemērs šajā gadījumā būtu tādas informācijas izpaušana par personu, kas radītu tiešu personas apdraudējumu. Kā arī gadījumi, kad tiek izpausta informācija par personu, kas var izsaukt citu personu reakciju pret šo cilvēku – sākot ar ziņu izpaušanu par personas mantisko stāvokli (tādejādi pakļaujot personu iespējamiem uzbrukumiem no laupītāju un krāpnieku puses) un beidzot ar ziņām, ka persona tiek turēta aizdomās par kāda vardarbīga nozieguma pastrādāšanu (kas var pakļaut personu "pūļa tiesas" riskam).

- **Brīvības tiesības:** *Cilvēkiem ir tiesības uz domas brīvību, pašizpausmi, pārvietošanās un sapulcēšanās brīvību.*

[241] Netiešas ietekmes piemērs ir atrašanās vietas datu, kas liecina par datu subjektu pārvietošanās paradumiem, izgūšana un apstrāde dažādos nolūkos. Pie noteiktiem apstākļiem šāda informācija var gan izpaust informāciju, kas ir uzskatāma par privātu, gan ierobežot personas tiesības brīvi pārvietoties. Attīstoties personības analīzes modeļiem un mašīnmācīšanās algoritmiem, noteikta veida apstrādes spēs noteikt cilvēka uzvedības modeli un domāšanas virzienu pietiekami precīzi, lai ietekmētu un manipulētu personas brīvu spēju pieņemt lēmumus.

- **Taisnīga tiesa:** *Katram cilvēkam ir tiesības uz godīgu tiesu.*

[242] Izmantojot datu analīzes rīkus, piemēram, lai vērtētu, vai persona kvalificējas priekšlaicīgas atbrīvošanas kritērijiem, un kāda ir tās noziedzīga nodarījuma izdarīšanas recidīva iespējamība, pastāv risks, ka neprecīzu datu izvērtēšana vai arī algoritmu, kas sevī iekļauj diskriminācijas pazīmes, izmantošana ietekmēs personas tiesības uz godīgu tiesu.

- **Privātās un ģimenes dzīves ievērošana:** *Tiesības uz privātumu un ģimenes dzīvi ir jāievēro un jāaizsargā.*

[243] Papildus tiesībām uz personas datu aizsardzību, kas tika apskatītas atsevišķā nodaļā un kas ir cieši savijušās ar privātās dzīves aizsardzības tiesībām, ir nepieciešams vērtēt arī iespējamo ietekmi

uz personas privātuma aizskārumu. Vērtējams, vai datu apstrādes rezultātā nenotiks plašāka datu subjekta datu apstrāde, kā tas varēja saprātīgi pieņemt. Pārzinis var ņemt vērā aptaujāto datu subjektu vērtējumu, ko un cik lielā mērā par privātu un attiecināmu uz ģimenes dzīvi no apstrādātajiem datiem uzskata paši datu subjekti.

- **Tiesības uz darbu, īpašumu un taisnīgu atalgojumu:** *Visiem cilvēkiem ir tiesības uz darbu un taisnīgu atalgojumu par savu darbu.*

[244] Šo pamattiesību ietvaros ir jāvērtē ietekme, tai skaitā uz jebko, kas saistāms ar datu subjekta mantisko stāvokli. Piemēram, ja apstrāde paredz pēc noklusējuma piedāvāt atšķirīga veida (un cenas) pakalpojumus klientiem ar atšķirīgu pirktspēju – šādai rīcībai ir tiešas ietekmes iespējamība uz personas īpašumu, jo vienai personu grupai pastāvētu lielāka iespēja notērēt vairāk kā citai. Tāpat šeit būtu vērtējama ietekme, ko var izraisīt neatbilstoša darba produktivitātes novērtēšana.

- **Tiesības uz izglītību***: Katram cilvēkam ir tiesības uz izglītību, kas jānodrošina vispārēji un līdzvērtīgi.*

[245] Veidojot speciālu programmu, kas, balstoties uz līdzšinējo sekmju līmeni, prezumē skolēnu prāta spējas un piešķir atšķirīgas nākotnes iespējas tiem, kas saņēmuši labākas atzīmes pagātnē, var rasties risks, ka noteiktām skolēnu grupām tiek liegtas iespējas saņemt līdzvērtīgu izglītību. Ir jāvērtē iespējamība, vai izveidotā sistēma neierobežos kādas grupas tiesības, balstoties uz kādiem kritērijiem.

- **Tiesības uz veselību:** *Cilvēkiem ir tiesības būt veseliem.*

[246] Iespējama gan tieša, gan netieša ietekme. Tiešā veidā nosakot diagnozi personai vai diagnozes iestāšanās iespējamību, tā tiek ielikta grupās, kurās noteiktiem simptomiem tiek piešķirta paaugstināta vērība un tādejādi tiek nodrošināts precīzāks un kvalitatīvāks ārstēšanas pakalpojums. Nepareizi noteikta diagnoze vai diagnozes iespējamība, vai saslimšanas risks var radīt personai maldīgu priekšstatu par tās veselības stāvokli, un tādejādi vai nu liedzot laicīgi meklēt profesionālu palīdzību vai arī gluži pretēji – liekot koncentrēt uzmanību uz veselības apdraudējumiem, kuri īstenībā nepastāv. Cits piemērs varētu būt, ka, vērtējot personas apdrošināšanas prēmijas apmēru, personas saslimšanas varbūtības novērtējums paaugstina apdrošināšanas izmaksas līdz līmenim, kas personai apgrūtinātu iespēju iegādāties sev piemērotu veselības apdrošināšanas polisi.

Abos gadījumos ir secināms, ka iespējama ietekme uz personas veselību pastāv – ietekmes riska apmērs ir nosakāms iepriekšējā nodaļā, kurā aprakstīta iespējamo risku novērtējuma veikšana.

- **Piederība politiskai sabiedrībai:** *Visiem cilvēkiem ir tiesības piedalīties valsts lietu pārvaldē, tieši vai netieši, un pieprasīt tiesību aizsardzību.*

[247] Vērtējama gan tieša ietekme, – piemēram iespējamība, ka apstrādes rezultātā personas attieksme pret politiskajām norisēm vai sociālajiem procesiem valstī mainīsies. Tai skaitā, iespējams, personu, balstoties uz datu apstrādē izdarītiem secinājumiem, izolējot no pilnvērtīgas informācijas par politisko situāciju valstī iegūšanas (piemēram, pielāgojot saturu, kas personai tiek rādīts kā interesējošais sociālajos tīklos). Gan arī netiešā ietekme, kad personai, balstoties uz vērtējumu par tās politisko pārliecību, var tikt piedāvāts atšķirīgs pakalpojumu un preču pieejamības apjoms.

Ņem vērā! Veicot NIDA, organizācija tajā iekļauj skarto tiesību uzskaitījumu un raksturojumu, lai nodrošinātu visaptverošu novērtējumu par datu apstrādes darbību iespējamo ietekmi uz personu privātumu, datu aizsardzības tiesībām un pārējām pamattiesībām.

VI. "Risku pārvaldība un risku mazinošie pasākumi"	
Līgumiskie paņēmieni	
Tehniskie paņēmieni	
Organizatoriskie paņēmieni	

Risku pārvaldība

[248] Efektīvs pārvaldīšanas mehānisms ir viens no risku mazināšanas rīkiem. Risku pārvaldība nozīmē, ka ir nepieciešams izstrādāt iekšējos kārtības noteikumus to uzraudzībai, norīkot atbildīgo personu, kura uzrauga, kā tiek ieviesta un īstenota risku pārvaldība. Organizācijai arī jāparedz līdzekļus šo darbu veikšanai budžetā, kā arī visbeidzot sekot, lai šie pasākumi arī patiesi un pēc būtības tiktu veikti. Risku mazināšanas pārvaldību var iedalīt trīs lielās grupās – līgumiskā, tehniskā un organizatoriskā.

[249] Risku mazināšanas paņēmiens īstenojams, ja organizācija, veicot NIDA, konstatē riska attiecināmību uz plānoto datu apstrādi. Ietekmes uz apstrādi novērtējums un veicamo riska mazināšanas pasākumu apzināšana nepalīdzēs organizācijai mazināt risku ietekmi, ja noteiktie riski netiks pārvaldīti sekojot izmaiņām tajos un ieviesto pasākumu efektivitātei. Līdz ar to bez risku pārvaldības procesu ieviešanas, veiktais NIDA būs atbilstošs tikai NIDA ziņojuma apstiprināšanas brīdī.

Ņem vērā! Katrā grupā norādītie risku mazināšanas pasākumi nav izsmeļoši un iespējami arī vēl citi risinājumi, ar kuru palīdzību varētu mazināt potenciālos riskus un ietekmi uz datu subjekta tiesībām un brīvībām.

Līgumiskie paņēmieni

[250] Līgumiskie paņēmieni ir svarīgs instruments risku mazināšanā un to pārvaldē. Līgumu pamatuzdevums ir noslēgt abpusēji saistošu vienošanos par tiesībām, pienākumiem un atbildību starp pusēm. Lai arī līgumiskie risku mazināšanas paņēmieni tieši ietekmi nemaina, tie tomēr ļauj precīzi noteikt atbildības par noteiktu risku iestāšanos un pārvaldīt riskus.

[251] Līgumiskajos paņēmienos ietilptu visdažādākie līgumi, gan starp organizāciju un darbiniekiem (piemēram, darba līgumā iekļauts pienākums ievērot konfidencialitāti ir līgumisks risku pārvaldības paņēmiens), gan organizāciju un sadarbības partneriem (precīzu pienākumu noteikšana datu apstrādē starp pusēm mazina riskus, ka kādas neizdarības dēļ var izcelties drošības incidents). Zemāk uzskaitīti līgumiskie paņēmieni, kas var tikt izmantoti risku mazināšanā:

- *Atbildības, termiņa un nosacījumu:*

[252] Līgumā un tā pielikumos tiek precīzi noteikts, kura puse uzņemas atbildību par konkrētiem veicamiem pasākumiem, lai novērstu potenciālos riskus vai kaitējumus. Var tikt iekļauti nosacījumi, kas noteic, kuri riski tiek nodoti vienai vai otrai pusei un kuri ir kopīgi. Šāda pieeja gan tiešā veidā pārnes, nevis mazina riskus, bet vienlaikus līgumiskās atbildības noteikšana skaidri nosaka rīcību noteiktu ietekmju un risku mazināšanai. Šis ir atbilstošs risku mazināšanas rīks gadījumos, kad apstrādē iesaistīta kāda cita personu. Ar rīka starpniecību mazināma iespējamā kopējā ietekme un riski, jo novēršami tie apdraudējumi, kas varētu izcelties, ja viena persona nav informēta par pasākumiem, kas jādara datu aizsardzībā.

- *Kontroles un auditu tiesības:*

[253] Līgumā iekļautās tiesības vienai pusei veikt kontroles un auditus, lai pārliecinātos par otras puses ievēroto noteikumu un prasību izpildi. Kad apstrādē tiek iesaistīta vairāk nekā viena persona, riskus, ka partneris nerīkosies atbilstoši noteikumiem, var mazināt, iekļaujot līgumā savstarpējo

pārbaužu mehānismu, un šo mehānismu arī iedzīvinot praksē. Šāda mehānisma ieviešana un īstenošana, ne tikai palīdz novērst identificētos potenciālos riskus, bet palīdz arī mazināt kopējos riskus, kas noteikti NIDA attiecībā uz otras puses veiktas darbības neatbilstību.

- *Konfidencialitātes nosacījumi:*

[254] Jāietver konfidencialitātes noteikumi, kas noteic, kā tiks apstrādāta un aizsargāta jebkura informācija, ko viena puse nodod otrai. Līgumiski konfidencialitātes nosacījumi mazinās iespēju, ka persona, kas apstrādā datus, tos neizpaudīs citām trešajām personām. Konfidencialitātes atruna līgumā neattiecas uz gadījumiem, kad tiesībsargājošās iestādes īsteno savas pilnvaras. Jo striktāki un īstenojamāki konfidencialitātes nosacījumi, jo mazāki ir riski, kas veidojas no informācijas neatbilstošas izpaušanas.

- *Strīdu risināšanas mehānismi:*

[255] Jāiekļauj līgumā mehānismi strīdu risināšanai vai alternatīvas strīdu risināšanas metodes. Šādu mehānismu skaidra noteikšana mazina riskus, kas var veidoties gadījumā, ja augstus riskus datu subjektam rada tiesiska nenoteiktība dažādu strīdus jautājumu izskatīšanas kārtībā starp apstrādē iesaistītajām vairākām personām.

Ņem vērā! Kopumā izmantotie līgumiskie paņēmieni var būt ļoti dažādi, un to izvēle būs atkarīga no konkrētajiem apstākļiem, industrijas un risku rakstura. Līgumiskie pasākumi ir būtisks instruments, lai nodrošinātu godīgu un skaidru sadarbību starp pusēm, tādejādi samazinot iespējamos riskus.

Tehniski paņēmieni

[256] Tehniskie riski ietver iespējamību, ka tehniskās sistēmas vai procesi var ciest no neparedzētiem traucējumiem, kļūdām vai drošības apdraudējumiem. Risku pārvaldība, izmantojot tehniskos paņēmienus, nodrošina tehnisko sistēmu stabilitāti un efektivitāti. Zemāk uzskaitīti paņēmieni, kas var tikt izmantoti tehnisko risku mazināšanā:

- *Drošības pārbaudes un audits:*

[257] Apsveriet iespēju veikt regulāras drošības pārbaudes, lai identificētu potenciālos iekšējos un ārējos drošības apdraudējumus (pārbaužu veikšanu atbilstoši vajadzībai var organizēt gan iekšējiem resursiem, gan arī piesaistot ārpakalpojumu; katras konkrētās drošības pārbaudes un audita veicēja noteikšana būs saistīta ar pārbaudes un audita tvērumu un var notikt visaptveroši, kā arī būt ierobežota tikai vienas organizācijas struktūras iekšienē). Izpētiet un pārbaudiet savas tehniskās sistēmas, lai atrastu un novērstu iespējamās kļūmes. Vēlams izstrādāt iekšēju kārtību drošības pārbaužu un auditu veikšanai. Tikai gadījumā, ja organizācija paveikusi iepriekš minētos mājasdarbus, var uzskatīt, ka noteiktie riski un ietekmes ar šo stratēģiju tiek mazinātas.

- *Rezerves kopijas un atjaunināšanas plāni:*

[258] Laba prakse ir regulāru rezerves kopiju veidošana kritiskajiem datiem un informācijai. Vēlama ir plāna izveide, kā ātri atjaunot darbību pēc datu zaudēšanas vai sistēmas traucējumiem. Šādi risku mazināšanas paņēmieni ļaus mazināt sistēmas darbības pārtraukumu radīto ietekmi un riskus, kas datu subjektam var rasties no sistēmas nepieejamības vai datu nozaudēšanas.

[259] Sistēmas ilgtspējas plāna izstrādes un kārtības sagatavošana, kā tieši atjauninājumi un rezerves kopijas ir veidojamas, veicinātu risku novēršanu. Riskus mazināt palīdzēs arī plāns, kā ātri atjaunot darbību pēc katastrofas vai liela sistēmas traucējuma, un rezerves infrastruktūru un resursu, kas var tikt aktivizēti nepieciešamības gadījumā, nodrošināšana.

- *Programmatūras pārbaudes*

[262] Lai novērstu drošības ievainojamības, organizācijai būtu jāpārliecinās, ka visi programmatūras produkti un operētājsistēmas tiek regulāri pārbaudītas un atjaunotas. Automatizētas

programmatūras atjaunināšanas procesi nodrošina cilvēciskas kļūdas iespējamības mazināšanu. Izmantojiet licencētu un aktuālu programmatūru, kurai joprojām tiek nodrošināts tehniskais atbalsts. Ja programmatūru izstrādā pati organizācija, tad jānodrošina labas programmatūras inženierijas prakses un standartu ievērošana, lai novērstu programmatūras kļūmes.

- *Datu šifrēšana:*

[263] Ja riskus rada trešo personu neautorizēta piekļuve datiem, tad organizācija šos riskus var mazināt ar apstrādē esošo datu kopu šifrēšanu vai to pseidonimizāciju. Tas pats attiecas uz datu glabāšanu.

[264] Pareizi glabājot pseidonimizācijas atslēgas, organizācija nodrošina, ka arī gadījumos, kad datus iegūst neautorizēta trešā persona, tā nespēs bez nozīmīgu pūļu ieguldījuma attiecināt iegūto datu masīvu uz datu subjektu.

Ņem vērā! Tāpat drošības pasākums, ka organizācijas izmantotie datu nesēji ir aizsargāti ar paroli un neautorizētas piekļuves gadījumā tiek sašifrēti, būs viens no risku mazināšanas paņēmienu elementiem.

Ņem vērā! Ja tiek ieviests drošības pasākums "anonimizācija", tad Datu regula uz informācijas apstrādi pēc anonimizācijas neattiecas. Informācija uzskatāma par anonimizētu, ja trešajai personai nav iespējams datus saistīt ar datu subjektu un netiek ietekmēts veids, kā cita persona izturas pret datu subjektu.

- *Ieguldījums drošības tehnoloģijās:*

[265] Lai sekotu potenciālai jaunu tehnoloģiju ietekmei uz plānoto datu apstrādi, nepieciešams sekot līdzi tehnoloģisko risinājumu attīstībai. Tehnoloģiskās attīstības procesa uzraudzības plānveidīga veikšana arī ļautu mazināt riskus, ka kāda jauna risinājuma atklāšana radītu neprognozētus apdraudējumus datu subjekta tiesībām un brīvībām.

[266] Elements no šīs drošības paņēmiena ir arī jaunāko drošības tehnoloģiju, lai novērstu un atklātu iespējamus draudus, izmantošana organizācijas ikdienas darbā. Jaudīgāku drošības sistēmu izmantošana ļaus organizācijai saprātīgi pieņemt, ka potenciālie draudi drošības sistēmas kompromitēšanai ir mazāki.

Organizatoriskie paņēmieni

[267] Organizatoriskie paņēmieni ir saistīti ar pasākumiem un stratēģijām, kas, ja ir jau ieviesti – novērš, vai tiks veikti, lai novērstu vai samazinātu iespējamos riskus, kas saistīti ar organizācijas darbību un vadību. Zemāk uzskaitīti pasākumi un stratēģijas, kas var tikt izmantoti organizatorisko risku mazināšanā:

- *Rūpīga risku izvērtēšana un stratēģiskā plānošana:*

[268] Rūpīga un sistemātiska risku identificēšana, analizējot gan iekšējos gan ārējos faktorus, dod iespēju organizācijai raksturot potenciālos riskus un to ietekmi uz organizāciju.

[269] Risku izvērtēšana, to analīzes un uzraudzības iekšēja kārtība un konstatēto risku mazināšanas pasākumu īstenošanas plāns palīdzēs mazināt potenciālo ietekmi praktiski visos aspektos. Skaidri un mērķtiecīgi plāni nodrošina, ka organizācija ir orientēta uz ilgtermiņa mērķiem un spēj identificēt un novērst riskus.

Ņem vērā! Organizācijai ir jāizstrādā savi pašuzraudzības paņēmieni (iekšējā audita sistēma, ieviesto pasākumu kvalitātes un lietderības kontrole utt.), kas nav formāli, bet gan praksē funkcionējoši.

- *Darbinieku līdzdalība:*

[270] Plānotajā datu apstrādē iesaistīto darbinieku iesaiste risku identifikācijā ir nozīmīgs pilnvērtīgi veiktas NIDA elements. Tomēr tikai ar NIDA paveikšanu darbinieku iesaistei nevajadzētu beigties. Darbinieks ir būtisks elements arī apstrādes darbību pārraudzības procesā.

[271] Galalietotāju iesaiste risku identifikācijā un vadīšanā nodrošina to, ka faktiski risku iestāšanās iespējamība samazinās, jo proaktīvi tiek meklētas sistēmas ievainojamības, tās novērstas, līdz ar to mazinot risku iestāšanās iespējamību.

Ņem vērā! Organizācijai būtu jāizstrādā pašuzraudzības paņēmieni (iekšējās kārtības noteikumi, procesu shēmas utt.), kas nodrošinās darbinieku iesaisti risku vadības procesos. Šis arī ir aspekts, ko organizācija var ņemt vērā, kad vērtē apstākļus, kas mazina risku vadības sistēmas ilgtspēju.

- *Proaktīva komunikācija ar datu subjektu:*

[271] Izstrādāta procedūra proaktīvai un pārredzamai komunikācijai nodrošina, ka datu subjekti saņem tiem nozīmīgu informāciju, kas saistīta ar to personas datu apstrādi. Tādējādi tiek ievērojami mazināti riski, kas var rasties saistībā ar neatbilstošu datu subjekta informēšanas pienākuma izpildi.

- *Personāla apmācība:*

[272] Apmācīts un informēts personāls par datu apstrādes un aizsardzības procedūrām nodrošina risku mazināšanu visas tajās risku grupās, kurās ietekmi uz datu subjekta tiesībām un brīvībām izraisa personāla nezināšana, cilvēciska kļūda vai ļaunprātība. Tas arī nodrošina, ka darbinieki daudz drošāk spēs izvairīties no kļūšanas par veiksmīgu sociālās inženierijas uzbrukumu upuriem, tādejādi mazinot ne tikai iekšējos, bet arī daļu no iespējamajiem ārējiem apdraudējumiem.

Ņem vērā! Personālu vēlams izglītot gan attiecībā uz pārziņa iekšējiem organizatoriskajiem procesiem, gan normatīvo aktu prasībām, gan arī attiecībā uz pārziņa izmantotajiem tehniskajiem risinājumiem un to piemērošanu praksē.

- *Iekšējie kārtības noteikumi un procedūras:*

[273] Iekšējie kārtības noteikumi jāizstrādā par organizatoriskajiem procesiem, izmantotajiem tehniskajiem rīkiem, iekšējo un ārējo komunikāciju, utt. Veiciet regulāras pārbaudes un pārvaldību, lai nodrošinātu to efektivitāti un to ievērošanu. Katrs no šiem pasākumiem palīdz mazināt tehniskos riskus, uzlabot sistēmas drošību un darbību, kā arī citus riskus, kas saistīti ar plānoto datu apstrādi.

Ņem vērā! Vairumā gadījumu situācijās, kad ir konstatēti vairāki datu aizsardzības riski, kas rada/var radīt augstu ietekmi uz datu subjekta tiesībām un brīvībām, kurus nevar novērst vai samazināt, apstrāde nebūs iespējama.

Esošo kontroļu efektivitātes izvērtējums

[274] Šajā sadaļā organizācijai jānovērtē risku mazinošie pasākumi, kas sevī ietver jau ieviesto kontroļu efektivitātes salīdzināšanu attiecībā uz plānoto datu apstrādi. Ņemot vērā, ka NIDA ir process un tas nebeidzas ar to, ka tiek sagatavots gala ziņojums – var nebūt pietiekoši tikai noteikt un novērtēt riskus, vēlams arī izstrādāt pasākumus, lai riskus un to ietekmi kontrolētu. Konstatēto risku vadība un uzraudzība var kalpot ne tikai kā būtisks aspekts noteikto risku ietekmes mazināšanai, bet arī NIDA ilgtspējas nodrošināšanai.

Ņem vērā! NIDA ietvaros konstatēto jauno risku kontroles elementu ieviešana ir solis, kas veicams, kad NIDA ir apstiprināts, bet vēl nav uzsāktas personas datu apstrādes darbības.

[275] Kad riski un kontroles mehānismi ir apzināti, nepieciešams izvērtēt arī apzināto un plānoto kontroles mehānismu efektivitāti. Kontroles mehānismu efektivitātes vērtējums ļaus izprast, ka ieviestie mehānismi nav formāli, bet tādi, kuri praksē mazina vai novērš riskus.

[276] Risku ietekme visu ieviesto kontroļu vispārējā efektivitāte. Efektivitātes novērtējumā jāņem vērā šādi aspekti:

- kontroļu ieviešanas mehānisma vispārējais raksturojums;
- vai kontroles pasākumu izstrādē un ieviešanā ir konstatēti trūkumi;
- vai kontroles jau ir ieviestas, vai tās darbojas kā paredzēt un vai tās sasniedz gaidītos rezultātus;
- vai kontroles darbojas neatkarīgi vai arī tām jādarbojas kolektīvi, lai tās būtu efektīvas;
- vai pastāv apstākļi kas var samazināt vai novērst kontroles efektivitāti, tostarp bieži sastopamas kļūmes;
- vai kontrole pati par sevi rada/nerada papildu riskus (piemēram, lai dati neglabātos ilgāk par noteikto datu glabāšanas termiņu, tiek ieviests automatizēts datu dzēšanas risinājums).

[277] Ja risinājums nedarbojas, var rasties situācija, ka tas izdzēš pārāk daudz vai neizdzēš pietiekami. Tāpat nepareizi konfigurēts rīks var radīt drošības ievainojamību. Šajos gadījumos no ieviestās drošības kontroles izriet jaunas ievainojamības, kurām riska novērtējums var būt veicams.

[278] Riskam var būt vairāk par vienu kontroli, tāpat viena kontrole var ietekmēt vairāk par vienu risku. Būtu jānošķir kontroles, kas maina iespējamību, sekas vai abus. Tāpat ir jānodala ieviestās kontroles, kas ir sadalītas starp dažādām iesaistītajām personām – pārzini, koppārzini un apstrādātāju. Izdarītie pieņēmumi par kontroļu faktisko ietekmi un uzticamību ir jādokumentē un jāapstiprina, īpašu uzmanību pievēršot atsevišķām kontrolēm vai to kombinācijām, par kurām pieņem, ka tām ir būtiska ietekme uz identificēto risku.

[279] Risku kontroles elementu ieviešana ir solis, ko var veikt brīdī, kad NIDA ir apstiprināts un tiek uzsāktas personas datu apstrādes darbības.

[280] Riska mazināšanas darbības dažkārt var konsolidēt, lai samazinātu darba apjomu un efektīvāk līdzsvarotu pieejamos resursus. Koordinētā riska mazināšanas plānā būtu jāņem vērā šie faktori, nevis jāpieņem, ka katrs risks būtu jārisina neatkarīgi.

Ņem vērā! Mijiedarbībai starp riskiem var būt dažāda ietekme uz lēmumu pieņemšanu, piemēram, palielinot to darbību nozīmi, kas aptver vairākus saistītus riskus, vai palielinot vienas iespējas pievilcību salīdzinājumā ar citām. Riski var būt jutīgi pret to kopīgu mazināšanu, vai arī var būt tādas situācijas, ka viena riska mazināšanai ir pozitīvas vai negatīvas sekas cita riska mazināšanai. Piemēram, ja tiek izlemts novērst riskus no trešās puses piekļuves datu centram atslēdzot to no iekšējiem un ārējiem tīkliem, tas ievērojami samazinātu kiberuzbrukuma iespēju. Vienlaikus tas radītu jaunu risku – nespēju sasniegt datu apstrādes nolūku, ja datu apstrādes nolūks ir saistīts ar datu apstrādes centrā ievietotās informācijas aktīvu izmantošanu organizācijas ikdienas darbā.

VII. "Cita papildu informācija"	
Vai NIDA veikšanas procesā ir pieprasīts datu subjektu vai viņu pārstāvju viedoklis?	
Lēmumu pieņemšanas dokumentācija	
Risku pārvaldības plāns	
Ziņošana citām iesaistītajām personām un NIDA publicēšana	
NIDA uzraudzība un pārskatīšana	

[281] Ņemot vērā, ka NIDA veikšanas laikā tiks izmantoti daudzi un dažāda satura gan tehniski (piemēram, sistēmas darbības parametru apraksti), gan juridiski dokumenti, ir nepieciešams veikt pasākumus, lai nodrošinātu, ka tie veido loģisku un sakārtotu lietvedības lietu, kuru nepieciešamības gadījumā var iesniegt Inspekcijai izvērtēšanai. Tā pat NIDA veikšanas procesā var būt nepieciešams jaunu dokumentu izstrādi (piemēram, risku pārvaldības plānu, NIDA uzraudzības un pārskatīšanas plānu).

[282] Šajā sadaļā nepieciešams arī iekļaut informāciju, vai organizācija ir ieguvusi datu subjektu viedokli par plānoto datu apstrādi un komunikāciju ari citām iesaistītājām personām, tai skaitā NIDA publicēšanu.

Ņem vērā! Par labo praksi būtu uzskatāms ar NIDA veikšanu saistīto informāciju turēt vienkopus. Lēmumu pieņemšanu atbalstoša dokumentācija būtu saistāma ar NIDA būtiskākajām sastāvdaļām.

IIX. "Secinājumi"	
Datu aizsardzības speciālista komentāri	
Nepieciešamība veikt iepriekšēju apspriešanos ar uzraudzības iestādi atbilstoši Datu regulas 36. pantam.	

[283] Noslēguma daļā, pirms organizācijas vadītājs pieņemtu lēmumu par plānoto datu apstrādi, ja ir norīkots DAS, jāiegūst tā viedoklis un to jāpievieno NIDA dokumentācijai. Tā pat ir nepieciešams izvērtēt, vai ir jāveic iepriekšējā apspriešanās ar Inspekciju, ja ir secināts, ka pēc risku mazinošo pasākumu ieviešanas joprojām ir augsts risks fizisku personu tiesībām un brīvībām.

Pielikums Nr. 1 "Datu apstrādes atbilstības un likumības novērtējums"

Plānotās datu apstrādes likumības analīze

Šo veidlapu organizācija var izmantot, lai veiktu esošas un/vai plānotas datu apstrādes tiesiskā pamata analīzi, iekļaujot informāciju, tai skaitā, par datu apstrādes atbilstību tiesību aktiem. Tiesiskā pamata analīze jāveic attiecībā uz katru noteikto datu apstrādes nolūku un datu apstrādes dzīves cikla posmu. "Plānotās datu apstrādes likumības analīze" veidlapa, lai gan ieteikta, nav juridiski saistoša. Organizācijām ir tiesības izvēlēties alternatīvas pieejas, ja tās nodrošina Datu regulā noteikto rezultātu sasniegšanu.

I. Datu apstrādes procesā iesaistītās personas un to apraksts	
Pārzinis	*Šajā sadaļā norāda informāciju par organizāciju, piemēram, juridiskās personas nosaukumu.*
Kontaktinformācija	*Šajā sadaļā norāda informāciju kā sazināties ar organizāciju, piemēram, organizācijas oficiālo elektronisko adresi, elektroniskā pasta adresi vai juridisko adresi.*
Kopīgi pārziņi	*Aizpilda, ja lēmumu par personas datu apstrādes veidu un tās nepieciešamību kopīgi pieņem vairākas personas. Šajā sadaļā norāda informāciju arī par kopīgiem pārziņiem.*
Apstrādātājs	*Ja personas datu apstrādei pārzinis piesaista citu organizāciju, kā apstrādātāju, tad šajā sadaļā norāda informāciju par apstrādātāju.*
Citas iesaistītas personas	*Šo sadaļu aizpilda, ja datu apstrādes procesā ir iesaistītas trešās personas un personas datu saņēmēji, kuri veic datu apstrādi (piekļūst datiem, iegūst datus, redz datus, glabā datus u. tml.), piemēram, sadarbības partneri, kuriem ir pieeja organizācijas datiem, bet nav klasificēti kā "kopīgs pārzinis" vai "apstrādātājs".*
Reģistrētā struktūra Latvijā	*Ja pārzinis nav dibināts Latvijas Republikā, iekļauj informāciju par pārstāvja reģistrēto struktūru Latvijā.*
Atbildīgā struktūrvienība	*Ja ir, tad šajā sadaļā norāda informāciju par atbildīgo departamentu (nodaļa, struktūrvienība), kura atbildēs par plānoto datu apstrādi organizācijā.*
Datu apstrādes atbilstība un likumība	
Datu veidi	*Šajā nodaļā organizācija klasificē personas datus, kurus organizācija plāno apstrādāt. Kārtot datus grupās ir iespējams atbilstoši dažādām metodēm:* • *atbilstoši datu plānotajam izmantošanas nolūkam (lai saņemtu maksu par produktu, organizācijai jāapstrādā personas maksājuma informācija);* • *atbilstoši datu pielietojumam (piemēram, viens no datu veidiem var būt datu subjekta kontaktinformācijas apstrāde).*
Datu aizsardzības principi	*Šajā nodaļā organizācija vērtē atbilstību visiem datu apstrādes principiem, kuri noteikti Datu regulas 5. pantā.*
"likumīgums, godprātība un pārredzamība"	
Kāds ir plānotās personas datu apstrādes tiesiskais pamats?	*Šajā sadaļā organizācija nodrošina esošas un/vai plānotas datu apstrādes tiesiskā pamata analīzi, iekļaujot informāciju, tai skaitā, par datu apstrādes atbilstību tiesību aktiem. Tiesiskā pamata analīze jāveic attiecībā uz katru noteikto datu apstrādes nolūku un datu apstrādes dzīves cikla posmu.* *Tiesiskā pamata analīze jāveic saskaņā ar Datu regulas 6. Pantu, un gadījumos, kad tiek veikta īpašu kategoriju datu apstrāde – Datu regulas 9. pantu, savukārt, ja tiek apstrādāta informācija par personas sodāmību – Datu regulas 10. pantu.* *Ja plānotā datu apstrāde tiek pamatota ar datu subjekta "piekrišanu", šajā sadaļā ir jāanalizē arī piekrišanas nosacījumi, lai tā atbilstu Datu regulas 7. pantam.*
"datu minimizēšana"	
Vai ir izvērtēts apstrādājamo personas datu apjoms un to	JĀ NĒ

<table>
<tr><td>atbilstība personas datu apstrādes nolūka sasniegšanai?</td><td colspan="3"></td></tr>
<tr><td colspan="4">Ja atbilde ir "JĀ", uzskaitiet šos datus, norādot, kādēļ tie nepieciešami personas datu apstrādes nolūka sasniegšanai.
Ja atbilde ir "NĒ", norādiet iemeslus, kāpēc nav veikts šāds izvērtējums.</td></tr>
<tr><td colspan="4">"nolūka ierobežojums"</td></tr>
<tr><td>Kāds ir personas datu apstrādes nolūks</td><td colspan="3">Šeit tiek norādīts precīzi definēts personas datu apstrādes nolūks. Nolūks, kura sasniegšanai tiks veikta personas datu apstrāde.</td></tr>
<tr><td>Kā tiek nodrošināts, ka dati tiek apstrādāti tikai iepriekš noteiktā nolūka sasniegšanai norobežojot tos no citām organizācijas datu plūsmām?</td><td colspan="3">Šajā sadaļā organizācija veic analīzi, lai novērtētu, vai un kā tiks nodrošināts, ka iegūtie personas dati tiks apstrādāti tikai konkrētam nolūkam.</td></tr>
<tr><td colspan="4">"precizitāte"</td></tr>
<tr><td>Vai un kā tiek aktualizēti (precizēti) personas dati?</td><td colspan="3">Šajā sadaļā organizācija veic analīzi, lai novērtētu, vai un kā tiks aktualizēti tās rīcībā esošie personas dati, tai skaitā, vai un kā neprecīzi personas datu var ietekmēt datu subjektu.</td></tr>
<tr><td colspan="4">"glabāšanas ierobežojums"</td></tr>
<tr><td rowspan="2">Kāds ir personas datu glabāšanas termiņš?</td><td colspan="3">Šajā sadaļā organizācija veic analīzi un raksturo personas datu glabāšanas termiņu atbilstoši datu apstrādes nolūkam. Analīze jāveic attiecībā uz izvelētajiem datu glabāšanas risinājumiem gan datu dzīvescikla apstrādes, gan dzīvescikla glabāšanas fāzēs.</td></tr>
<tr><td>Personas datu veidi:</td><td>Glabāšanas ilgums:</td><td>Apstrādes tiesiskais pamats:</td></tr>
<tr><td colspan="4">"integritāte un konfidencialitāte"</td></tr>
<tr><td rowspan="2">Kādi ir datu apstrādes sistēmas tehniskie raksturlielumi?
Kā datu apstrādes procesā tiek nodrošināta konfidencialitāte?</td><td colspan="3">Šajā sadaļā organizācija veic analīzi attiecībā uz sistēmas darbības ilgtspēju un tās ietekmi uz datu subjekta tiesībām un brīvībām. Ja apstrādē tiek plānots piesaistīt apstrādātājus, uzskaite ir veicama sadarbībā ar operatoriem.</td></tr>
<tr><td>Apstrādes process, kurā resurss tiks izmantots:</td><td colspan="2">Resurss: *Piemēram, aparatūra, programmatūra, tīkli, cilvēki, informācijas apmaiņas kanāli, papīra formāta informācijas apmaiņa u. c.</td></tr>
<tr><td colspan="4">"pārskatatbildība"</td></tr>
<tr><td>Vai organizācija spēj demonstrēt, ka plānotā datu apstrāde atbilst visām Datu regulas prasībām?</td><td colspan="3">Šajā sadaļā organizācija veic analīzi attiecībā uz tās veiktajām darbībām, lai apliecinātu plānotās datu apstrādes atbilstību Datu regulai. Organizācijas pamatojumiem un lēmumam par plānoto personas datu apstrādi ir jābūt balstītiem faktos un loģiski argumentētiem</td></tr>
<tr><td colspan="4">Cita papildu informācija</td></tr>
<tr><td>Lēmumu pieņemšanas dokumentācija</td><td colspan="3">Šajā sadaļā organizācija norāda, vai un kā dokumentēti pieņemtie lēmumi saistībā ar plānoto datu apstrādi.</td></tr>
<tr><td>Datu aizsardzības speciālista komentāri</td><td colspan="3">Šajā sadaļā organizācija, ja ir, iekļauj datu aizsardzības speciālista sniegto viedokli vai ieteikumus par veikto plānoto datu apstrādi.</td></tr>
</table>

Pielikums Nr. 2 "NIDA veikšanas nepieciešamības novērtēšanas veidlapa"

NIDA veikšanas nepieciešamības novērtējums

Šo veidlapu organizācija var izmantot, lai veiktu NIDA veikšanas nepieciešamības novērtējumu atbilstoši vadlīniju II nodaļai "NIDA veikšanas nepieciešamības novērtējums". Ja NIDA nepieciešamības novērtējuma laikā tiek secināts, ka NIDA nav jāveic, tad tālāku NIDA izstrādi var pārtraukt, paveikto darbu sākotnējā izpētē saglabājot pārskatatbildības nodrošināšanas nolūkos. "NIDA veikšanas nepieciešamības novērtējums" veidlapa, lai gan ieteikta, nav juridiski saistoša. Organizācijām ir tiesības izvēlēties alternatīvas pieejas, ja tās nodrošina Datu regulā noteikto rezultātu sasniegšanu.

I. Datu apstrādes procesā iesaistītās personas un to apraksts	
Pārzinis	*Šajā sadaļā norāda informāciju par organizāciju, piemēram, juridiskās personas nosaukumu.*
Kontaktinformācija	*Šajā sadaļā norāda informāciju kā sazināties ar organizāciju, piemēram, organizācijas oficiālo elektronisko adresi, elektroniskā pasta adresi vai juridisko adresi.*
Kopīgi pārziņi	*Aizpilda, ja lēmumu par personas datu apstrādes veidu un tās nepieciešamību kopīgi pieņem vairākas personas. Šajā sadaļā norāda informāciju arī par kopīgiem pārziņiem.*
Apstrādātājs	*Ja personas datu apstrādei pārzinis piesaista citu organizāciju, kā apstrādātāju, tad šajā sadaļā norāda informāciju par apstrādātāju.*
Citas iesaistītas personas	*Šo sadaļu aizpilda, ja datu apstrādes procesā ir iesaistītas trešās personas un personas datu saņēmēji, kuri veic datu apstrādi (piekļūst datiem, iegūst datus, redz datus, glabā datus u. tml.), piemēram, sadarbības partneri, kuriem ir pieeja organizācijas datiem, bet nav klasificēti kā "kopīgs pārzinis" vai "apstrādātājs".*
Reģistrētā struktūra Latvijā	*Ja pārzinis nav dibināts Latvijas Republikā, iekļauj informāciju par pārstāvja reģistrēto struktūru Latvijā.*
Atbildīgā struktūrvienība	*Ja ir, tad šajā sadaļā norāda informāciju par atbildīgo departamentu (nodaļa, struktūrvienība), kura atbildēs par plānoto datu apstrādi organizācijā, par kuru tiek veikts NIDA veikšanas nepieciešamības novērtējums.*
Datu aizsardzības speciālists	*Šajā sadaļā norāda informāciju par DAS, ja tāds ir norīkots.*
Atbildīgais par NIDA veikšanas nepieciešamības izvērtēšana	*Šajā sadaļā norāda informāciju (vārds, uzvārds, kontaktinformācija) par personu, kura veic NIDA nepieciešamības novērtējumu.*
NIDA VEIKŠANAS NEPIECIEŠAMĪBAS NOVĒRTĒJUMS	
NIDA veikšanas nepieciešamības novērtējums	*Šajā sadaļā organizācija norāda objektīvu informāciju, uz kuras pamata tiek pieņemts lēmums par nepieciešamību veikt vai neveikt. Vai plānotā datu apstrāde ietilpst Datu regulas 35. panta tvērumā? Vai plānotā datu apstrāde ir iekļauta Inspekcijas izstrādātajā sarakstā ar datu apstrādēm, kurām obligāti jāveic NIDA? Vai pastāv citi apstākļi, kādēļ pārzinis uzskata par nepieciešamību veikt NIDA? Vai apstrāde ir iekļauta sarakstā ("baltais saraksts") , kas izveidots saskaņā ar Datu regulas 35. pantu un nav jāveic NIDA .*
Vai NIDA ir jāveic?	JĀ NĒ
Cita papildu informācija	
Lēmumu pieņemšanas dokumentācija	*Šajā sadaļā organizācija norāda, vai un kā dokumentēti pieņemtie lēmumi saistībā ar plānoto datu apstrādi NIDA veikšanas nepieciešamības novērtējuma laikā (ja tādi ir).*
Datu aizsardzības speciālista komentāri	*Šajā sadaļā organizācija, ja ir, iekļauj datu aizsardzības speciālista sniegto viedokli vai ieteikumus par nepieciešamību veikt NIDA.*

Pielikums Nr. 3 "NIDA veikšanas veidlapa"

Novērtējums par ietekmi uz datu aizsardzību

Šī veidlapa paredzēta kā strukturēts un pārskatāms NIDA ietvaros veicamo pasākumu apraksts. Veidlapas nodaļas ir sasaistītas ar attiecīgo vadlīniju nodaļu, kurā var atrast sīkāku informāciju par loģiku, kāpēc veidlapā iekļauta tieši šāda nodaļa un apskatāmie personas datu apstrādes aspekti. Tabulas kreisajā pusē norādīts, ko konkrētajā veidlapas vietā apskatīt, savukārt labajā pusē slīprakstā tiek skaidrots kā apskatāmais jautājums risināms. *Aizpildot veidlapu, slīprakstā esošais teksts ir dzēšams.* "Novērtējums par ietekmi uz datu aizsardzību" veidlapa, lai gan ieteikta, nav juridiski saistoša. Organizācijām ir tiesības izvēlēties alternatīvas pieejas, ja tās nodrošina Datu regulā noteikto rezultātu sasniegšanu.

I. NIDA procesā iesaistītās personas un to apraksts	
Pārzinis	*Šajā sadaļā norāda informāciju par organizāciju, kura plāno veikt personas datu apstrādi un veic NIDA, piemēram, juridiskās personas nosaukumu.*
Kontaktinformācija	*Šajā sadaļā norāda informāciju kā sazināties ar organizāciju, piemēram, organizācijas oficiālo elektronisko adresi, elektroniskā pasta adresi vai juridisko adresi.*
Kopīgi pārziņi	*Aizpilda, ja lēmumu par personas datu apstrādes veidu un tās nepieciešamību kopīgi pieņem vairākas personas. Šajā sadaļā norāda informāciju arī par kopīgiem pārziņiem.*
Apstrādātājs	*Ja personas datu apstrādei pārzinis piesaista citu organizāciju, kā apstrādātāju, tad šajā sadaļā norāda informāciju par apstrādātāju.*
Citas iesaistītas personas	*Šo sadaļu aizpilda, ja datu apstrādes procesā ir iesaistītas trešās personas un personas datu saņēmēji, kuri veic datu apstrādi (piekļūst datiem, iegūst datus, redz datus, glabā datus u. tml.), piemēram, sadarbības partneri, kuriem ir pieeja organizācijas datiem, bet nav klasificēti kā "kopīgs pārzinis" vai "apstrādātājs".*
Reģistrētā struktūra Latvijā	*Ja pārzinis nav dibināts Latvijas Republikā, iekļauj informāciju par pārstāvja reģistrēto struktūru Latvijā.*
Atbildīgā struktūrvienība	*Ja ir, tad šajā sadaļā norāda informāciju par atbildīgo departamentu (nodaļa, struktūrvienība), kura atbildēs par plānoto datu apstrādi organizācijā, par kuru tiek veikts NIDA.*
Datu aizsardzības speciālists	*Šajā sadaļā norāda informāciju par DAS, ja tāds ir norīkots.*
Datu aizsardzības speciālista iesaistes NIDA veikšanas procesā nepieciešamības izvērtēšana	*Ja organizācijai ir norīkots datu aizsardzības speciālists, bet tas nav ticis iesaistīts NIDA veikšanas procesā, tad NIDA veicējs šajā sadaļā norāda informāciju par iemesliem, kāpēc datu aizsardzības speciālists nav iesaistīts NIDA veikšanas procesā.*
Atbildīgais par NIDA veikšanu (vārds, uzvārds, kontaktinformācija)	*Šajā sadaļā norāda informāciju par personu, kura veic NIDA.*
Novērtējuma veikšanas periods	*Šajā sadaļā norāda informāciju par laika periodu, kurā veikts NIDA, piemēram, no 2023. gada 14. decembra līdz 2024. gada 23. februārim.*
II. Informācija par plānoto apstrādi	
Datu apstrādes dzīves cikla vizualizācija	*Ja ir izstrādāts, tad šajā sadaļā iekļauj plānotās datu apstrādes dzīves cikla vizualizāciju. Datu apstrādes dzīves cikla vizualizāciju var pievienot arī novērtējuma pielikumā.*
Datu apstrādes funkcionāls apraksts	*Šajā sadaļā organizācija veic datu apstrādes funkcionālo aprakstu, kurā jāietver datu apstrādes darbību uzskaitījums; detalizēta faktisko informācijas aprites elementu analīze.*
III. Organizācijas datu aizsardzības sistēma	
Pārziņa datu aizsardzības sistēmas apraksts	
Citi pasākumi, kurus pārzinis veicis pārskatatbildības principa	

vai citu Datu regulas izvirzīto prasību nodrošināšanai.	
IV. Risku datu subjekta tiesībām un brīvībām analīze *Šo sadaļu aizpilda ievērojot organizācijas izvēlēto riska novērtējuma metodoloģiju konkrētajā gadījumā.*	
V. "Ietekmes uz datu subjektu raksturojums"	
Datu aizsardzības tiesības	*Šajā sadaļā organizācija iekļauj skarto tiesību uzskaitījumu un raksturojumu, lai nodrošinātu visaptverošu novērtējumu par datu apstrādes darbību iespējamo ietekmi uz personu privātumu un datu aizsardzības tiesībām:* • *katrā konkrētā gadījumā aprakstiet, kā tiek nodrošināta konkrētās tiesības īstenošana;* • *ja konkrētā tiesības īstenošana netiek nodrošināta, aprakstiet iemeslus.*
Informācijas pārredzamība, saziņa un datu subjekta tiesību īstenošanas kārtība	
Informēšana	
Piekļuve datiem	
Datu labošana	
Datu dzēšana, iebilšana pret datu apstrādi un pārnesamība	
Datu ierobežošana	
Automatizēta individuālu lēmumu pieņemšana	
Citas pamattiesības	*Šajā sadaļā organizācija apraksta, kā plānotā datu apstrāde varētu ietekmēt vai ietekmē vispārējās pamattiesības.*
Vienlīdzība un nediskriminācija	
Dzīvības drošības tiesības	
Brīvības tiesības	
Taisnīga tiesa	
Privātās un ģimenes dzīves ievērošana	
Tiesības uz darbu, īpašumu un taisnīgu atalgojumu	
Tiesības uz izglītību	
Tiesības uz veselību	
Piederība politiskai sabiedrībai	
VI. "Risku pārvaldība un risku mazinošie pasākumi"	
Līgumiskie paņēmieni	*Šajā sadaļā organizācija veic analīzi attiecībā ieviesto kontroļu efektivitāti, lai mazinātu identificētos riskus.*
Tehniskie paņēmieni	
Organizatoriskie paņēmieni	
VII. "Cita papildu informācija"	
Vai NIDA veikšanas procesā ir pieprasīts datu subjektu vai viņu pārstāvju viedoklis?	*Šajā sadaļā organizācija norāda iegūto vai apsvērumus/apstākļus viedokļa neiegūšanai.*
Lēmumu pieņemšanas dokumentācija	*Šajā sadaļā organizācija norāda, vai un kā dokumentēti pieņemtie lēmumi saistībā ar plānoto datu apstrādi.*
Risku pārvaldības plāns	*Šajā sadaļā organizācija apraksta identificēto risku pārvaldības plānu, ja tāds ir izstrādāts.*
Ziņošana citām iesaistītajām personām un NIDA publicēšana	*Šajā sadaļā organizācija norāda, vai un kādā apjomā ir paredzēts publicēt veikto NIDA vai par to informēt citas personas.*
NIDA uzraudzība un pārskatīšana	*Šajā sadaļā organizācija norāda, kāda ir NIDA uzraudzības un pārskatīšanas sistēma.*
IIX. "Secinājumi"	
Datu aizsardzības speciālista komentāri	*Šajā sadaļā organizācija, ja ir, iekļauj datu aizsardzības speciālista sniegto viedokli vai ieteikumus par veikto NIDA.*

Nepieciešamība veikt iepriekšēju apspriešanos ar uzraudzības iestādi atbilstoši Datu regulas 36. pantam.	*Šajā sadaļā organizācija veic izvērtējumu par nepieciešamību veikt iepriekšēju apspriešanos ar Datu valsts inspekciju.*