Saturs

IEVADS

Novērtējums par ietekmi uz datu aizsardzību (NIDA) ir jāuzskata par risku un to ietekmes uz fiziskas personas (datu subjekta) tiesībām un brīvībām apkopojumu, ko varētu radīt plānotā vai esošā datu apstrāde. Noteiktos gadījumos NIDA ir Datu regulā[1] noteikts pienākums, tomēr organizācijas var izvēlēties NIDA veikt arī, kad tas nav obligāti, tā lietderības kā risku vadības rīka dēļ. NIDA ir process, kas izveidots, lai aprakstītu apstrādi, novērtētu tās nepieciešamību un samērīgumu un palīdzētu pārvaldīt tādus riskus fizisku personu tiesībām un brīvībām, kas izriet no personas datu apstrādes, novērtējot tos, nosakot pasākumus to novēršanai[2].

Vienkāršojot, NIDA vērtē mijiedarbību starp datu subjekta tiesībām un brīvībām, ar riskiem ko rada plānotā vai esošā datu apstrāde, kas izraisa potenciālo iejaukšanos šajās tiesībās un brīvībās.

Šīs vadlīnijas ir rīks, kas palīdzēs NIDA izstrādē. Vadlīnijas skaidros gan to, kuros tieši gadījumos NIDA ir veicams, gan ļaus organizācijai novērtēt, vai NIDA būs iespējams veikt pašu spēkiem vai arī tomēr būs nepieciešama ārpakalpojuma piesaiste specifiska jautājuma novērtēšanai. Vadlīnijas izmantojamas, gan pirms jauna procesa ieviešanas, gan arī esošo procesu ietekmes uz datu aizsardzību novērtēšanai, pilnveidojot risku vadības sistēmu.

Atvieglojot šo vadlīniju piemērošanu, tās sakārtotas atbilstoši secīgiem soļiem, sākot no posma, kad notiek gatavošanās NIDA veikšanai (pirmsnida[3] posms), un beidzot ar posmu, kad NIDA jau ir veikts. Katrs vadlīniju posms var būt lasāms neatkarīgi un, ja organizācija skaidri spēj identificēt, kurā posmā tai nepieciešams atbalsts vai ieteikumi tālākai rīcībai, tad var koncentrēties tikai uz attiecīgās nodaļas izpēti. Vienlaikus, lai uzskatītu, ka veikts pilnvērtīgs NIDA ir jāveic visi vadlīnijās norādītie posmi. Atbilstoši vadlīniju struktūrai esam sagatavojuši arī NIDA veidlapu, kurā organizācija var iekļaut informāciju, kas attiecas uz konkrēto NIDA punktu. NIDA veidlapā tēmas ir sakārtotas atbilstoši vadlīniju nodaļām.

Vadlīniju nodaļas sākas ar aspekta teorētiskās puses skaidrojumu sniedzot pamatojumu kāpēc konkrētajā gadījumā iesakāma konkrēta rīcība, savukārt sadaļā, kas vadlīnijās apzīmēta ar "PRAKTISKI", ir sniegti ieteikumi jau konkrētai rīcībai, ar kuras palīdzību aizpildāma NIDA veidlapa.

Datu regula nenosaka tieši kādā veidā ir jāveic NIDA, līdz ar to šajās Vadlīnijās aprakstītām metodēm, paņēmieniem un ieteikumiem kā organizācijai rīkoties nav normatīvi saistoša rakstura. Ja organizācija saskata citu modeli NIDA veikšanai, kas ļauj sasniegt Datu regulā minēto rezultātu, tad organizācija var rīkoties arī savādāk un piemērot citas metodes un veidlapas.

Šīs vadlīnijas sniegs ieteikumus un ceļvedi, kādus soļus spert un kādiem procesiem pievērsties, veicot NIDA, tomēr nevienas vadlīnijas nespēj aizstāt Jūsu veselo saprātu un speciālās zināšanas par plānotajām apstrādes darbībām. Nevairieties pakārtot NIDA veikšanas metodiku un izmantotos palīglīdzekļus plānotās apstrādes loģikai.

Apzīmējumu skaidrojums:
Ņem vērā! – Informējam/pievērsiet uzmanību norādītājai informācijai!

[1] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 par fizisko personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK

[2] 29.panta datu aizsardzības darba grupas 2017.gada 4.aprīļa Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē, 4.lp. Pieejams: https://www.dvi.gov.lv/sites/dvi/files/novertejumu-par-ietekmi-uz-datu-aizsardzibu11.pdf

[3] Ar pirmsnida posmu šo vadlīniju kontekstā saprotamas darbības kas tiek veiktas lai noteiktu vai attiecīgai apstrādei ir veicams NIDA atbilstoši Datu regulas 35.panta 1.punktā noteiktajam. Ja tiek secināts, ka NIDA veicams, tad šajā posmā veiktās darbības ir iekļaujamas NIDA. Ja tiek secināts ka NIDA nav veicams šī posma ietvaros paveiktais saglabājams pārskatatbildības nodrošināšanai, bet tālākas šajās vadlīnijās paredzētās veicamās darbības NIDA veikšanai vairs nav veicamas.

I. nodaļa "NIDA veikšanas nepieciešamības novērtējums"

1.1. Kodolīgs datu apstrādes raksturojums

Pirmais solis organizācijai ir saprast, vai NIDA ir jāveic. Kodolīgs datu apstrādes[4] raksturojums ļaus veikt sākotnējo izvērtējumu par iespējamiem apdraudējumiem datu subjektu tiesībām un brīvībām, ko plānotā/veiktā datu apstrāde rada.

Šajā posmā organizācijai jāapraksta un jāizvērtē galvenie datu apstrādes raksturlielumi. Aprakstā iekļaujams izvērtējums par vismaz:

- Datu veidiem[5] un apjomu;
- Datu subjektu[6] kategoriju raksturojumu;
- Vai apstrāde paredz veikt datu subjektu novērtēšanu, vai profilēšanu[7];
- Datu apstrādē izmantotajiem tehniskajiem risinājumiem;
- Līguma vai tiesību akta veidu, kas nosaka personas datu apstrādes ietvaru;
- Pasākumiem, kas paredzēti, lai garantētu un pierādītu atbilstību Datu regulas prasībām (datu subjekta tiesību nodrošināšana);
- Vai/ja ir paredzēta datu nosūtīšana uz trešajām valstīm vai starptautiskas organizācijas.

Ja kodolīgs apstrādes apraksts nav pietiekams, lai veiktu sākotnējo izvērtējumu riskiem, kas var rasties datu subjektu tiesībām un brīvībām, organizācijai ir nepieciešams veikt strukturētu plānotās datu apstrādes analīzi, kas sevī ietver gan personas datu apstrādes vizualizāciju[8], gan tās funkcionālo aprakstu[9]. Minētie procesi palīdzēs organizācijai identificēt gan galvenos personas datu apstrādes raksturlielumus, gan arī dažādas darbības datu aizsardzībai, kāpēc tās ir nepieciešamas, un to savstarpējo mijiedarbību.

Ņem vērā! Šajā sadaļā organizācija veic plānotās datu apstrādes identifikāciju (piemēram, piešķir tai nosaukumu, kuru iekļauj "datu apstrādes reģistrā"), iekļaujot īsu un kodolīgu aprakstu. Apraksta plānoto datu apstrādi. Norāda datu apstrādes izmaiņas, ja tādas ir bijušas, vai kodolīgs datu apstrādes raksturojums tiek veikts par esošu datu apstrādi.

[4] "apstrāde" ir jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana

[5] Šo vadlīniju kontekstā ar līdzīgu nozīmi var tikt lietoti jēdzieni datu veidi un datu kategorijas.

[6] identificēta vai identificējama fiziska persona ("datu subjekts"); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;

[7] "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;

[8] Detalizētāk skatīt 5.3. Plānotās datu apstrādes analīze

[9] Detalizētāk skatīt 5.3. Plānotās datu apstrādes analīze

II. nodaļa "Galvenās ieinteresētās personas, jeb kam ir jāveic NIDA"

2.1. NIDA procesā iesaistītās personas un to pienākumi

Datu regula atbildību par NIDA veikšanu uzliek pārzinim, vienlaikus gadījumos, ja tiek iesaistīts apstrādātājs, tam ir 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. Tāpat, ja tāds ir iecelts, pārzinim ir pienākums uzklausīt datu aizsardzības speciālista (DAS) padomu NIDA izstrādes gaitā.

Pārzinis, kopīgie pārziņi vai apstrādātājs

Pārzinis[10] 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.

Atbilstoši Datu regulas 35. panta 1. punktam, pārzinis (vai kopīgi pārziņi) ir atbildīgs par NIDA un tas uzņemas atbildību par NIDA izstrādi, to īstenošanu. Tas nozīmē, ja gadījumā pārzinis uzdod NIDA izstrādāt kādai citai personai savas organizācijas iekšienē vai piesaista ārpakalpojumu sniedzēju, pārzinis jebkurā gadījumā būs atbildīgs par NIDA atbilstību Datu regulas prasībām.

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 jāvienojas un jānosaka noslēgtās vienošanās priekšmets un apstrādes ilgums, apstrādes raksturs un nolūks, personas datu veidi un datu subjektu kategorijas, kā arī abu pušu pienākumi un tiesības.

Ja datu apstrādi pilnībā vai daļēji veic apstrādātājs, tam ir pienākums palīdzēt pārzinim NIDA izstrādes procesā, sniedzot tam visu nepieciešamo informāciju.[11] Tas nozīmē, ka, pamatojoties uz starp pārzini un apstrādātāju noslēgto līgumu, apstrādātājam ir jāsniedz visa tam pieejamā informācija, piemēram, bet ne tikai, par ieviestajiem tehniskajiem un organizatoriskajiem pasākumiem datu apstrādes drošības nodrošināšanai.

Pārzinis	Kopīgi pārziņi	Apstrādātājs
Persona, vienpersoniski pieņem lēmumu, ka: 1. konkrētajā gadījumā ir nepieciešams veikt datu apstrādi; 2. kādā veidā un apjomā nepieciešams apstrādāt datus.	Ja lēmumu par personas datu apstrādes veidu un tās nepieciešamību kopīgi pieņem vairākas personas.	Nepieņem lēmumu par datu apstrādes veidu un tās nepieciešamību. Ir noslēgts līgums ar pārzini, ar kuru uzticēts veikt datu apstrādi kādas citas personas vārdā. Var izvēlēties tikai dažus praktiskākus īstenošanas aspektus ("nebūtiskus līdzekļus") vai arī līdzekļu izvēle ir liegta pilnībā.

Datu aizsardzības speciālists

DAS ir tā persona, kura ar savām speciālajām zināšanām datu aizsardzībā konsultē pārzini. DAS galvenā funkcija ir sniegt neatkarīgu viedokli par plānoto vai jau ieviesto datu apstrādes procesu atbilstību Datu regulai un citiem saistošiem normatīvajiem aktiem.[12]

[10] Vadlīniju kontekstā "pārzinis" ir nosaukts par "organizācija".
[11] Datu regulas 28. panta 3. punkta f) apakšpunkts.
[12] Datu regulas 37. pants Datu regula noteiktos gadījumos uzliek par pienākumu pārzinim iecelt datu aizsardzības speciālistu (piemēram, publiskas pārvaldes iestādes, organizācija, kura veic īpašu kategoriju datu apstrādi plašā mērogā)

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 izstrādāt NIDA veikšanas iekšējo formu. DAS novērtē, vai NIDA ir veikts atbilstoši un vai novērtējumā ietvertie secinājumi ir Datu regulai atbilstoši. Noslēgumā DAS var ieteikt pasākumus, kuri pārzinim jāievieš, lai mazinātu identificētos riskus personas tiesībām un brīvībām. Pārzinim ir pienākums nodrošināt, ka DAS veic neatkarīgu kvalitātes kontroli attiecībā uz citu piesaistīto ekspertu izstrādāto NIDA. Neatkarīgi no datu aizsardzības speciālista sniegtajiem ieteikumiem, atbildīgs par datu apstrādi un ar to saistītiem jautājumiem ir pārzinis.

DAS, saskaņā ar Datu regulas 39. panta 1. punkta c) apakšpunktu pārrauga NIDA īstenošanu organizācijā.

Ņem vērā! Noteiktos gadījumos organizācijai ir pienākums pieprasīt viedokli datu subjektam vai tā pilnvarotajam pārstāvim. Būtisks priekšnoteikums NIDA izstrādes procesā ir dokumentēt visu iesaistīto personu sniegtos viedokļus, padomus vai pieņemtos lēmumus.

PRAKTISKI

2.2. Personas datu apstrādē iesaistīto personu un to lomu uzskaitījums

Šajā sadaļā NIDA izstrādātājs apraksta un identificē pārzini, ja ir, tad iekļauj arī informāciju par kopīgajiem pārziņiem, kā arī citām datu apstrādē iesaistītajām personām (piemēram, apstrādātājs vai sadarbības partneris), nepārprotami definējot katras puses pienākumus un uzdevumus. Sadaļā aprakstāma pārziņa darbības joma un jāraksturo, kādi un kādā apjomā dati tiek apstrādāti (jāapraksta esošā situācija), kopēju pārziņu gadījumā apraksts jāsniedz par visiem partneriem.

Jānorāda NIDA veicējs, tā kvalifikācija un loma organizācijā, ja tam tāda ir. Jāsniedz informācija par organizācijas DAS un tā lomu NIDA veikšanā. Ja apstrādē iesaistītas citas puses (piemēram, kā apstrādātājs vai sadarbības partneris), tad jāsniedz gan tā uzdevumu, gan arī darbības sfēras apraksts.

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

III. nodaļa "Darbības joma un piemērojamība"

NIDA veicams gadījumos, kad apstrādes darbības varētu izraisīt augstu risku fizisku personu tiesībām un brīvībām. Likumdevējs ir tiešā veidā iezīmējis gadījumos, kuros īpaši apsverama paaugstinātu risku iestāšanās iespējamība.

Datu regula nosaka, ka uzraudzības iestādes definē jomas, kurās tās saskata paaugstinātus apdraudējumus datu subjekta tiesībām un brīvībām. Uzraudzības iestādes arī var definēt jomas, kurās šādus paaugstinātus apdraudējumus tās nesaskata.

Šī nodaļa ļaus saprast kā vērtēt NIDA veikšanas nepieciešamību Jūsu plānotajām datu apstrādes darbībām.

3.1. Kad veikt NIDA?

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;
- publiski pieejamas zonas uzraudzība plašā mērogā;
- īpašu kategoriju personas datu vai Datu regulas 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā;[13]
- apstrāde ir iekļauta Inspekcijas izstrādātajā sarakstā ar datu apstrādēm, kurām obligāti jāveic NIDA.

Ņem vērā! Organizācijai ir nepieciešams pievērst īpašu uzmanību identificētajiem riskiem un izvērtēt, vai apstrādes veids varētu radīt augstu risku fizisku personu tiesībām un brīvībām.

Ņem vērā! Inspekcijas saraksts izstrādāts, pamatojoties uz EDAK kritērijiem[4]. Kritēriju mērķis ir veidot sistēmisku pieeju organizācijas plānoto apstrāžu analīzei, lai novērtētu, kur iespējamā ietekme uz datu subjektu ir paaugstināta.
Sistēmiskā pieeja piemērojama arī attiecībā uz jomām, kas nav tieši uzskaitītas sarakstā. Ja organizācijas veiktā vai potenciālā apstrāde atbilst vismaz diviem kritērijiem, tad uzskatāms, ka ir jāveic NIDA.
Tomēr, dažos gadījumos NIDA būs jāveic 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.

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[14].

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

Svarīgi atcerēties, ka NIDA veikšana nav vienreizējs pasākums un to ir jāpārskata visa personas datu apstrādes procesa laikā, lai uzraudzītu jaunu risku rašanos, piemēram, mainoties apstrādes darbībām vai organizācijas darbības jomai. Vienlaikus NIDA periodiska pārskatīšana palīdzēs organizācijai novērtēt, kuras riska samazināšanas metodes darbojas.

3.2. Kad NIDA var neveikt?

[13] Datu regulas 35. panta 3. punkts
[14] Sīkāk par ietekmes uz fizisku personu noteikšanu lūdzam skatīt IX. nodaļu "Ietekmes uz datu subjektu raksturojums".

- **Nav riska datu subjektu tiesībām un brīvībām**

NIDA var neveikt, ja apstrādes loģika un iesaistīto datu apjoms neliecina par iespējamu augstu risku datu subjekta tiesībām un brīvībām. Šajā gadījumā izaicinājums ir veikt sākotnējo novērtējumu par pastāvošās ietekmes līmeni. Organizācijai ir jāizvērtē ne tikai to, kas uztrauc organizācijas klientus, bet arī kā datus ir iespējams izmantot potenciāla apdraudējuma radīšanai klienta tiesībām un brīvībām.

Veicot sākotnējo novērtējumu, attiecībā uz iespējamajiem apdraudējumiem ir jāvērtē ietekme uz visām datu subjekta tiesībām un brīvībām. Analizējot apdraudējumus, organizācijai ir jāpieņem to iespējami lielākā ietekme.

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

Ņem vērā! Organizācijai jāspēj uzskatāmi demonstrēt un pamatot savu pārliecību, ka apstrāde neradīs paaugstinātu apdraudējumu datu subjektu tiesībām un brīvībām.

- **NIDA jau ir veikts par līdzīgu datu apstrādi**

NIDA var neveikt, ja NIDA par analogām apstrādes darbībām pati organizācija (vai cita līdzīga organizācija[15]) 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.

Ņem vērā! Šādos gadījumos organizācijas rīcībā ir jābūt nerediģētam veiktam 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.

- **Ja novērtējums veikts juridiskā regulējuma izveides laikā**

Atsevišķos gadījumos likumdevējs veic NIDA vēl likumdošanas procesā, vai pirms tā. Nedrīkst izdarīt secinājumu, ka NIDA veikts likumdošanas procesā tikai tāpēc, ka apstrāde likumā paredzēta. Lai uzskatītu NIDA veikšanas pienākumu par izpildītu, organizācijai jāpārliecinās, ka likumdošanas procesā patiesi veikts iespējamās ietekmes uz personu tiesībām un brīvībām novērtējums, ko radītu plānotā personas datu apstrāde. 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.

Organizācijas veiktais mājasdarbs – secinājumi par to, vai likumdošanas procesā NIDA ir vai nav veikts, ir jādokumentē un jāsaglabā nepieciešamībai:

[15] Līdzīga organizācija – juridiskā statusa, struktūras, ieviesto tehnisko risinājumu un darbības jomas ziņā līdzīga. Piemēram, viena pašvaldība atbilstoši šiem kritērijiem var būt uzskatāma par līdzīgu citai pašvaldībai.

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

Organizācijai nevajadzētu uztvert NIDA par formalitāti – šī instrumenta pirmais un galvenais uzdevums ir palīdzēt novērtēt plānotās personas datu apstrādes ietekmi uz klientu/iedzīvotāju datu aizsardzību. Tāpēc gadījumos, kad normatīvais akts vai tā anotācija satur tikai vispārīgo aprakstu par datu apstrādi un ietekmes novērtējumu, organizācijai ir jāveic atsevišķs NIDA, vismaz, lai noteiktu 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.

- **NIDA "baltais saraksts"**

NIDA var neveikt, ja plānotā datu apstrāde ir iekļauta Inspekcijas "baltajā sarakstā". Inspekcijas izstrādātais "baltais saraksts" 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.**

Sekojiet informācijai Inspekcijas tīmekļa vietnē par saraksta apstiprināšanu.

PRAKTISKI

3.3. NIDA veikšanas nepieciešamības novērtējums

Šajā sadaļā NIDA izstrādātājs veic NIDA nepieciešamības analīzi. Tas nozīmē, ka ir jāņem vērā vai:

- saskaņā ar Datu regulas 35. pantu NIDA ir jāveic;
- *plānotās apstrādes darbības* ir iekļautas Inspekcijas izstrādātajā sarakstā ar datu apstrādēm, kurām obligāti jāveic NIDA;
- pastāv citi apstākļi, kādēļ organizācija uzskata par nepieciešamību veikt NIDA;
- vai apstrāde ir iekļauta sarakstā, kas izveidots saskaņā ar Datu regulas 35.pantu un nav jāveic NIDA - "baltais saraksts".

Organizācijai nepieciešams norādīt objektīvu informāciju, uz kuras pamata ir ierobežots NIDA tvērums attiecībā uz apstrādes nolūkiem un apjomu, tostarp norādīt tos aspektus, kas ir ārpus NIDA, un iespējamos saistītos riskus personu tiesībām un brīvībām, tostarp veidu, kādā tos varētu novērst, un to personu identificēšanu, kuras ir atbildīgas par attiecīgo risku pārvaldību.

Neatkarīgi no analīzes par pienākumu veikt NIDA, organizācija varētu izvērtēt nepieciešamību to veikt, lai pārliecinātos, ka plānotā datu apstrāde patiesi nerada riskus datu subjekta tiesībām un brīvībām.

Ja NIDA nepieciešamības novērtējuma laikā tiek secināts, ka NIDA nav veicams, tad tālāku NIDA izstrādi var pārtraukt, paveikto darbu sākotnējā izpētē saglabājot pārskatatbildības nodrošināšanas nolūkos.

VI. nodaļa "NIDA mijiedarbība ar citām Datu regulas prasībām"

Pareizi veikts NIDA tiks integrēts organizācijas datu aizsardzības sistēmā un tas savietosies ar visiem citiem datu aizsardzībai ieviestiem pasākumiem vienotā mehānismā. Pasākumi, ko pārzinis veic pārskatatbildības[16] principa vai citu Datu regulas izvirzīto prasību nodrošināšanai, neaizstāj NIDA. Vienlaikus darbs, kas ieguldīts attiecīgajos pasākumos, ir izmantojams un lielākajā daļā gadījumu organiski savietojas ar NIDA.

4.1. Organizācijas datu aizsardzības sistēma

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. Piemēram:

- Iekšējie kārtības noteikumi un procedūras: organizācija ir izstrādājusi datu apstrādes un aizsardzības politiku, procedūras un iekšējās kārtības noteikumus, kurās izklāstīts, kā organizācijā jārīkojas ar personas datiem un nodrošina to īstenošanu;
- Atbilstība tiesību aktiem: 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;
- Drošības pasākumi: organizācija ir izveidojusi un īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai aizsargātu personas datus pret nesankcionētu piekļuvi, izpaušanu, pārveidošanu un iznīcināšanu;
- Piekļuves kontrole un autentificēšanas mehānismi: organizācijas īstenotās kontroles, lai ierobežotu piekļuvi personas datiem, pamatojoties uz lietotāju lomām, atļaujām un autentifikācijas mehānismiem;
- Iepriekš veikts novērtējums par ietekmi uz datu aizsardzību: organizācija jau iepriekš (par citu datu apstrādi) veikusi novērtējumu, lai identificētu un mazinātu privātuma riskus, kas saistīti ar datu apstrādes darbībām;
- Izglītoti darbinieki: organizācija nodrošina darbiniekiem apmācības un izpratnes veidošanas programmas par datu aizsardzības principiem, privātuma praksi un viņu pienākumiem.

4.2. Datu apstrādes reģistrs

Datu apstrādes reģistra mijiedarbība ar NIDA ir tieša un nepastarpināta. Par labu praksi būtu uzskatāma apstrādes strukturēšana un aprakstīšana veidā, kas vēlāk ļautu to ietvert apstrādes reģistrā. Šāda informācija palīdzēs kartēt datu apstrādes dzīvesciklu. Tāpat informāciju varēs izmantot novērtējot apstrādāt paredzēto datu veidus un to tiesisko pamatu.

Savukārt, ja datu apstrāžu reģistra uzturēšana organizācijai nav obligāts no Datu regulas izrietošs pienākums, to var ieviest kā rīku, kas palīdzēs organizācijai pārskatīt savas aktivitātes datu aizsardzības jomā.

4.3. Līdzsvarošanas tests

Gadījumos, kad plānotā personas datu apstrāde balstīsies Datu regulas 6. panta 1. punkta f) apakšpunktā norādītajā tiesiskajā pamatā, ir jāveic plānotās personas datu apstrādes līdzsvarošanas tests. Līdzsvarošanas tests ir ne tikai neatņemams datu apstrādes likumības elements, bet tā veikšanā ir arī jāņem vērā un jāanalizē virkne elementu, kas ir būtiski apstrādes iespējamās ietekmes novērtēšanā un līdz ar to arī NIDA veikšanā.

[16] Datu regulas 5.panta 2.punkts – organizācija spēj uzskatāmi pierādīt, ka tiek ievēroti visi personas datu apstrādes principi.

No līdzsvarošanas testa īpaši aizgūstami tādi apstrādes elementi, kurus organizācija ieviesusi, lai garantētu datu loģisko un fizisko drošību, kā arī tādi elementi, kas paredzēti, lai sniegtu papildus garantijas datu subjektu tiesību aizsardzībai.

Ņem vērā! Līdzsvarošanas testa primārā funkcija ir novērtēt plānotās personas datu apstrādes likumību. Ja līdzsvarošanas tests ir negatīvs, tad apstrāde nav veicama dēļ neatbilstības datu aizsardzības principiem. NIDA par šo apstrādi ir nelietderīgs!

4.4. Personas datu pārkāpumu reģistrs

Personas datu pārkāpumu reģistrs ir būtisks apstāklis, lai organizācija varētu pieņemt, ka tai ir izveidota funkcionēt spējīga risku pārvaldības sistēma. NIDA veikšanas laikā var paredzēt šāda reģistra izveidi un uzturēšanu. Lai gan personas datu pārkāpumu reģistrs tieši nepalīdzēs NIDA veikšanas procesā, tomēr, šāda reģistra izveidošana ir risku identifikācijas un pārvaldības neatņemama sastāvdaļa, jo savlaicīgi izveidots pārkāpumu reģistrs palīdzēs, ne tikai novērst datu aizsardzības pārkāpumu, bet arī operatīvi uz to reaģēt.

Vienlaikus Inspekcija uzsver, ka organizatoriskie paņēmieni, ko katra organizācija izmanto risku pārvaldības sistēmas izveidei un uzturēšanai, tai skaitā vai organizācija vispār uzskata šāda reģistra izveidi par lietderīgu ir katras atsevišķās organizācijas pārziņā.

Ņem vērā! Nevajadzētu aizmirst par sistēmas izveidi apstrādes radīto risku vēlākai veiksmīgai pārvaldīšanai.

4.5. Tehnisko un organizatorisko pasākumu kopums

NIDA ir savstarpēji saistīts ar tehnisko un organizatorisko pasākumu kopumu, kas lielākoties kalpo, lai nodrošinātu datu apstrādes atbilstību precizitātes, integritātes un konfidencialitātes principiem. Tehnisko un organizatorisko pasākumu efektivitāte būs viens no primārajiem veidiem, kā organizācija mazinās identificēto risku ietekmi uz datu subjektu tiesībām un brīvībām. Jau ieviesto pasākumu novērtējums ir solis, kas organizācijai veicams pēc sākotnējās ietekmes uz datu subjekta tiesībām un brīvībām noteikšanas.

Ņem vērā! Visiem pasākumiem, ko organizācija veic pārskatbildības nodrošināšanai, būs nozīme arī NIDA. Tas sevī ietver arī organizācijas lēmumu par pasākumiem un soļiem, ko organizācija ir izlēmusi neveikt.

PRAKTISKI

Ieviešot jaunu personas datu apstrādes procesu organizācijai ir jāspēj novērtēt jaunā procesa mijiedarbība ar jau esošo sistēmu. Ir iespējams, ka esošā datu aizsardzības sistēma un datu apstrādes sistēma pati par sevi rada noteiktus riskus datu subjekta tiesībām un brīvībām.

Piemēram, ja plānots jauno Informācijas sistēmu izvietot uz jau pastāvošās infrastruktūras ir nepieciešams novērtēt gan esošās infrastruktūras kapacitāti un spēju uzturēt jauno informācijas sistēmu ievērojot tās esošo noslodzi, tāpat ir nepieciešams novērtēt jau ieviestos organizatoriskos aizsardzības pasākumus, kā lietotāju piekļuves tiesību piešķiršanas kārtība un šo pasākumu mijiedarbību ar jauno sistēmu.

Organizācijas esošās sistēmas aprakstīšana, veicot sākotnējo plānotās personas datu apstrādes drošības un atbilstības situācijas novērtējumu, ir nepieciešama, lai:

1) pārliecinātos vai attiecībā uz plānoto datu apstrādi ir piemērojami organizācijā jau ieviestie pasākumi un rīki, kā arī cik efektīvi tie būs;
2) kādi ir sākotnējie plānotās apstrādes radītie riski situācijā, ja netiek veiktas izmaiņas/papildinājumi organizācijas esošajā datu aizsardzības sistēmā;
3) kādu papildus pasākumu ieviešana nepieciešama esošajā sistēmā.

4.6. Organizācijas esošo pasākumu apraksts

Šajā sadaļā organizācijai vajadzētu īsumā aprakstīt esošo datu aizsardzības un apstrādes sistēmu. Veicot analīzi, jāņem vērā, ka:

- Organizācijas datu aizsardzības sistēma ir vērsta uz to, lai nodrošinātu atbilstību datu aizsardzības tiesību aktiem un aizsargātu personu tiesības uz privātumu, savukārt organizācijas datu apstrādes sistēma koncentrējas uz tehnisko infrastruktūru un operatīvajiem procesiem, kas saistīti ar personas datu pārvaldību.
- Datu aizsardzības sistēma ietver plašāku organizatorisko politiku, procedūras un atbilstības pasākumus, savukārt datu apstrādes sistēma īpaši attiecas uz datu pārvaldības tehniskajiem un operatīvajiem aspektiem.
- Datu aizsardzības sistēmas mērķis ir aizsargāt personu privātumu un nodrošināt atbildīgu datu apstrādi, savukārt datu apstrādes sistēma veicina efektīvu un drošu personas datu apstrādi saskaņā ar uzņēmējdarbības vajadzībām.

V. nodaļa "Datu apstrādes dzīves cikls"

Plānojot uzsākt jaunu personas datu apstrādi[17], vai arī, 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. Veicot NIDA, katrai atsevišķai personas datu apstrādei kā procesam plānoto personas datu apstrādi var uztvert par nepārtrauktu secīgu darbību kopumu. Šādu kopumu katra organizācija var definēt, izmantojot dažādas metodes un pieejas. Šajā vadlīnijās tiks izmantota sertificēti informācijas sistēmu drošības profesionāļu (CISSP) pieeja, kuri ir sadalījuši darbību kopumu definētās fāzēs[18]. Šī pieeja vienkāršo katrā apstrādes etapā pastāvošo datu aizsardzības risku identifikāciju, kā arī piemērojamo drošības pasākumu datu aizsardzībai noteikšanu, bet šīs fāzes kopā sauc par datu apstrādes dzīvesciklu. Kopumā tiek izdalītas piecas datu dzīvescikla fāzes.

5.1. Datu apstrādes dzīvescikla dažādo posmu raksturojums

- **Radi vai saņem**

Šajā fāzē personas dati nonāk organizācijas (pārziņa)[19] rīcībā. Visbiežāk datu avoti ir pats datu subjekts[20], valsts iestāžu vai privātas datu bāzes, no kurām par datu subjektu tiek iegūta papildinoša 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).

Šī fāze iezīmē sākuma punktu datu apstrādes darbībās organizācijā. Radi vai saņem fāze uzskatāma par noslēgtu, kad dati ir ievietoti lokācijā, no kuras tos var pārvirzīt uz to paredzēto atrašanās vietu, sākot nākošo 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 novēršot iespējamos integritātes un konfidencialitātes apdraudējumus.

- **Izplatīšana**

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 savi specifiski drošības apdraudējumi, 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 nākošā dzīvescikla fāze ir datu izmantošana atbilstoši to ieguves nolūkam.

---

[17] jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana; (Datu regulas 4. panta 2. punkts)

[18] https://www.pearsonitcertification.com/articles/article.aspx?p=3167978&seqNum=5

[19] "pārzinis" ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus; ja šādas apstrādes nolūkus un līdzekļus nosaka ar Savienības vai dalībvalsts tiesību aktiem, pārzini vai tā iecelšanas konkrētos kritērijus var paredzēt Savienības vai dalībvalsts tiesību aktos; (Datu regulas 4. panta 7. punkts)

[20] "Datu subjekts" ir identificētu vai identificējamu fizisku persona (Datu regulas 4. panta 1. punkts). Datu subjekts var būt … , klients

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**

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 veidā, 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.

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**

Datu uzturēšanas starpfāze ir brīdis, kad organizācija joprojām esot "izmantošanas" fāzē veic konkrētas darbības ar klientu datiem iepriekš noteikta mērķa sasniegšanai. Tas nozīmē, ka organizācija uzturēšanas starpfāzē novērtē, ne tikai to, vai mērķis 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.).

Šī starpfāze ļauj noteikt, kad dati ir kļuvuši veci, neprecīzi un vairāk nav izmantojami neviena godprātīga un likumīga datu apstrādes mērķa sasniegšanai. Konstatējot kādu no apsvērumiem, kas traucē ar datu palīdzību sasniegt plānoto mērķi – dati vai nu atgriežas iegūšanas/radīšanas fāzē (ja mērķis joprojām ir sasniedzams un tam pastāv likumīgs pamats) vai nonāk dzīvescikla noslēdzošajā fāzē.

- **Arhivēšana/dzēšana**

Noslēdzošais posms datu apstrādes dzīvesciklā ir organizācijas rīcībā esošo datu arhivēšana un dzēšana. Tas nozīmē, ka organizācija tās rīcībā esošos datus:

- padara par nelasāmiem trešajām personām (datu neatgriezenisku iznīcināšana vai anonimizācija[21]);

[21] 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.

- arhivē.

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 termiņiem 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.

Datu dzīvescikla apraksts/analīze – tieši NIDA veikšanas nepieciešamībai – ir jāveic vizualizācijas veidā. Respektīvi, labs 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.

5.2. Organizācijas datu apstrādes sistēma

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 uz vajadzīgo laiku un drošai iznīcināšanai, kad tie vairs nav vajadzīgi.

NIDA veicams, ja, analizējot datu apstrādes dzīvesciklu, tiek konstatēts, ka plānotās apstrādes darbības radīs riskus datu subjekta tiesībām.

PRAKTISKI

5.3. Plānotās datu apstrādes analīze

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

Analizējot (Vizualizējot) plānoto datu apstrādes modeli, jāataino 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 vēlamos rezultātus;
- datu apstrādes dzīvescikla vizualizācijas izstrāde;
- dažādu scenāriju testēšana, lai pārskatītu kā modelis varētu potenciāli darboties praksē.

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

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 – 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! Jāņem vērā, ka 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.

Ņem vērā! 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.

VI. nodaļa "Datu apstrādes atbilstība un likumība"

Neatņemama NIDA daļa ir datu apstrādes atbilstības un likumības novērtēšana. Jebkuras datu apstrādes analīze sākas ar datu apstrādes mērķa noteikšanu, kā arī analīzi, kādi tieši personas dati būs vajadzīgi konkrētā mērķa sasniegšanai. Datu apstrādes atbilstības un likumības novērtējums ir veicams visām datu apstrādes dzīvescikla apraksta laikā noteiktajām darbībām, par visiem datu veidiem ko organizācija plāno apstrādāt konkrētās personas datu apstrādes kontekstā.

Ņem vērā! NIDA ir veicams datu apstrādei, kas vēl tikai plānojas, savukārt datu apstrāžu reģistrs ir uzturams par apstrādēm, kuras organizācija jau īsteno.

6.1. Datu veidi

Nepieciešams klasificēt personas datus, kurus organizācija plāno apstrādāt. Visus personas datus nosacīti var iedalīt divās lielās grupās – personas dati un īpašu kategoriju personas dati. Tāpat būtu jāņem vērā, ka datiem par sodāmību un pārkāpumiem ir speciāla Datu regulā paredzēta kārtība un ar to apstrādi saistīti paaugstināti riski datu subjekta tiesībām un brīvībām. Ja tiek plānots apstrādāt šos datus, arī tas būtu norādams NIDA. Vērtējot ierobežojumus[22], īpašu kategoriju personas datu apstrādei, secināms, ka likumdevējs ir pieņēmis, ka šādu datu apstrāde pati par sevi ir ar potenciāli lielāku ietekmi uz datu subjektu.

Ņem vērā! Organizācijai dati ir jāklasificē atbilstoši to potenciālajai ietekmei uz datu subjektu.

Nosakot, plānotās datu apstrādes ietekmi, jāņem vērā vismaz šādus kritērijus:

- Vai tie ir dati, kuru neatbilstoša apstrāde var radīt tiešu ietekmi uz datu subjektu? Jo lielāks ir tiešas un nepastarpinātas ietekmes risks uz datu apstrādi, jo lielāks tiešas potenciālas ietekmes risks datu subjektam.
- Vai datu apjoms, ko apstrādā organizācija, atbilst datu subjekta gaidām?
- Kāda ir datu subjekta attieksme pret datu apstrādi? Vai tas uzskata, ka konkrētā datu apstrāde tam var radīt īpašu apdraudējumu?
- Novērtējums par datu turpmākas izmantošanas iespējām citu personu nolūku sasniegšanai. Respektīvi - vai konkrēti dati ir nepieciešami un lietderīgi citiem tirgus dalībniekiem, vai šo datu izmantošana ļauj gūt lielāku peļņu vai konkurences priekšrocības, vai arī dati var tikt izmantoti krāpniecības shēmās. Jo šie dati ir iekārojamāki trešām personām, jo lielākus riskus šo datu apstrādei rodas no mērķtiecīgu trešās puses uzbrukumu puses.

Plānotā personas datu apstrādes nolūka sasniegšanai tiks apstrādāti dažādi personas datu veidi. Apstrādājamo datu veidu kategorizēšana un sistematizēšana atvieglos plānoto apstrādes darbību apraksta izstrādi .

Kārtot datus grupās ir iespējams atbilstoši dažādām metodēm:

- atbilstoši datu plānotajam izmantošanas nolūkam (lai nodrošinātu uzņēmuma normatīvajos aktos noteiktos pienākumus attiecībā uz atbilstošas grāmatvedības kārtošanu, organizācijai jāglabā informācija par personas veiktajiem maksājumiem);
- atbilstoši datu raksturojumam (piemēram, viens no datu veidiem var būt datu subjekta kontaktinformācija).

Tomēr konkrētais sistematizācijas un kategorizācijas veids ir atkarīgs tieši no organizācijas un risinājumi iespējami visdažādākie.

[22] Datu regulas 9. panta 1. punkts. Ir aizliegta tādu personas datu apstrāde, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētisko datu, biometrisko datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju apstrāde.

Sistematizēti un kategorizēti dati izmantojami potenciālās datu apstrādes ietekmes uz datu subjektu tiesībām un brīvībām risku novērtējumā. 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[23] vērtību, kas tiks izmantota kopējās riska vērtības noteikšanā, izmantojot vienādojumu, kurš tiks skaidrots riska analīzes sadaļā.

6.2. Datu aizsardzības principi

Datu aizsardzības principu ievērošana ir neatņemami saistīta ar datu veidiem un plānoto datu apstrādes nolūku. Jāņem vērā, ka paaugstinātus riskus un ietekmi uz datu subjektu tiesībām un brīvībām personas datu aizsardzībā (ieskaitot privātās dzīves neaizskaramības nodrošināšanu) var radīt tieši tas, ka organizācija nespēs nodrošināt atbilstību kādam personas datu aizsardzības principam.

Ņem vērā! Kad nodrošināta atbilstība "datu minimizēšanas principam", ir nepieciešams pārliecināties, ka apstrādes laikā būs iespējams nodrošināt arī atbilstību pārējiem personas datu apstrādes principiem.

Vienlaikus paaugstinātus riskus un ietekmi uz datu subjekta tiesībām un brīvībām citu pamattiesību piemērošanas aspektos lielākoties radīs "integritātes un konfidencialitātes" principa neievērošana.

Formāla pieeja uzdevuma izpildei (aprakstam par atbilstību principiem), piemēram, tikai konstatējums, ka tiek izpildītas prasības, nav uzskatāmas par atbilstoši veikta NIDA elementu. Nepieciešama analīze par to, kā un kādiem līdzekļiem tiek plānota atbilstības datu aizsardzības principiem nodrošināšana.

6.2.1. "Likumīgums, godprātība un pārredzamība"

Nepieciešams noteikt kāds būs datu apstrādes tiesiskais pamats[24] atbilstoši Datu regulai. 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 sistēmiskākā veidā identificēt ieviešamos papildus pasākumus, ja tiks konstatēts, ka apstrādei jāpiemēro kādi risku mazināšanas pasākumi, kas saistīti ar tiesiskā pamata iegūšanu.

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

Godprātības elements paredz, ka plānotās apstrādes darbības netiks veiktas nelikumīgam mērķim, kā arī datu subjekts netiks maldināts attiecībā uz plānoto viņa personas datu apstrādi. Tas nozīmē, ka organizācijai ir jāņem vērā arī datu subjekta saprātīgās gaidas un principa pārkāpums būs datu apstrāde veidā, kas, vadoties no veselā saprāta viedokļa, ir bijis datu subjektam negaidīts.

Ja secināms, ka apstrādei nav iespējams nodrošināt atbilstošu tiesisko pamatu tā ir nelikumīga un tālāka NIDA veikšana nav lietderīga.

6.2.2. "Nolūka ierobežojumi"

Jānovērtē, vai tiek nodrošināts, ka personas dati tiks izmantoti tikai plānotā datu apstrādes nolūka vai ar to savietojamiem nolūkiem sasniegšanai. NIDA laikā jāanalizē, vai princips tiek ievērots visā datu dzīvescikla laikā un ir novērsta personas datu starpizmantošana neparedzētu un datu subjektiem nezināmu nolūku sasniegšanai.

[23] Sīkāk par riska faktoriem vadlīniju 7.2. nodaļā "risku iespējamības un ietekmes analīze".
[24] Datu regulas 6., 9. un 10. pants

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.

Nepieciešams veikt analīzi, 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 sistēmā attēlojums (skatīt iepriekš aprakstīto datu dzīvescikla vizualizāciju).

Šajā posmā pārzinis var nonākt arī pie secinājuma, ja apstrādē iesaistīti īpaši riskanti datu masīvi, šo principu iespējams nodrošināt, izveidojot 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.

Aprakstā būtu jāiekļauj vismaz organizācijas:

- iekšējo noteikumu attiecībā uz informācijas apstrādi analīze
- piešķirto sistēmas lietotāju lomu un datu izmantošanas monitoringa novērtējums.

Tas nodrošinātu, ka organizācijā nenotiek informācijas sistēmu izmantošana sākotnēji neparedzētiem mērķiem, un piekļuve personas datiem notiek tikai lietotājiem piešķirto piekļuvju apjomā.

Ņem vērā! NIDA laikā arī jāvērtē, vai un kā papildināsies darbinieku lomu apraksti, kā arī kurš veiks uzraudzību par nepieciešamo izmaiņu veikšanu.

6.2.3. "Datu minimizēšana"

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

6.2.4. "Precizitāte"

Jāveic gan analīze, kā neprecīzi dati iespaidos mērķa sasniegšanu, gan kādi pasākumi tiks īstenoti, lai nodrošinātu iespējami precīzu datu apstrādi. Arī šajā gadījumā princips jāpiemēro visam datu dzīvesciklam, vērtējot ietekmi uz katra atsevišķā dzīvescikla posma uzdevumu izpildi.

6.2.5. "Glabāšanas ierobežojums"

Jānovērtē ieviestie mehānismi, kā tiks nodrošināts, ka dati netiek glabāti ilgāk kā nepieciešams mērķa sasniegšanai; kā par principa izpildi iespējams pārliecināties pēc datu subjekta iesnieguma saņemšanas; kā arī kādi mehānismi ieviesti, lai pārbaudītu, ka automatizētu risinājumu izmantošanas gadījumā tiek veiktas pēcpārbaudes par prasību izpildi.

6.2.6. "Integritāte un konfidencialitāte"

Nepieciešams vērtēt:

a) datu apstrādes sistēmu tehniskos raksturlielumus un aizsardzības pasākumus,
b) iekšējos organizatoriskos pasākumus datu aizsardzībai,
c) kā arī minēto (a) un (b)) punktu, mijiedarbību.

Integritātes un konfidencialitātes principa efektīva piemērošana palīdzēs aizsargāt ne tikai organizācijas apstrādātos personas datus, bet arī organizācijas biznesa procesa datus no trešajām personām. Objektīva situācijas novērtēšana ir izšķiroša veiksmīgas sistēmas aizsardzības un atbilstošas funkcionēšanas pārraudzības izveidei.

Ņem vērā! Būtiski NIDA procesā ir neuzdot vēlamo par esošo, bet savu sistēmu novērtēt pēc iespējas objektīvāk.

Organizācijai jāpievērš uzmanība sistēmas darbības ilgtspējai un ietekmei uz datu subjekta tiesībām un brīvībām, respektīvi, kas notiek, ja sistēmā personas datu apstrāde kaut kādu iemeslu dēļ nenotiek:

a) Kā tas ietekmē plānotā personas datu apstrādes mērķa sasniegšanu?
b) Kā tas ietekmē datu subjektu un viņa gaidas?

Piemēram, ja organizācija izstrādā lietotni lietotāja pārvietošanās maršruta fiksācijai, lai balstoties uz saņemtajām ziņām piedāvātu lietotājam atlīdzību par veikto attālumu, bet saņemto informāciju izmantotu 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 mērķi; Tāpat lietotājs nesaņems gaidīto pakalpojumu – mērķētas reklāmas un atlīdzību par veikto attālumu.

6.2.7. "Pārskatatbildība"

Visas darbības un pasākumi, ko organizācija ir veikusi NIDA ietvaros, ir jādokumentē un jāsaglabā atsekojamā veidā organizācijas lietvedībā. Šis ne tikai palīdzēs efektīvi atsekot izmaiņu nepieciešamībai un pārvaldīt procesu, 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.

Pievērsiet uzmanību tieši ar NIDA veikšanu saistītās dokumentu aprites organizācijas ieteikumiem šo vadlīniju nodaļā XI. nodaļa "Dokumentācija".

PRAKTISKI

6.3. Plānotās datu apstrādes likumības analīze

Šajā sadaļā NIDA veicējs nodrošina esošas un/vai 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 mērķi un datu apstrādes dzīves cikla posmu.

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.

Ja plānotā datu apstrāde tiek balstīta uz datu subjekta "piekrišanu", šajā sadaļā ir jāanalizē arī piekrišanas nosacījumi, lai tā atbilstu Datu regulas 7. pantam.

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

VII. nodaļa "Riska novērtējums"

Riska pārvaldība ir organizācijas jebkuru procesu būtisks elements, lai apzinātu iespējamās problēmas un risinājumus, lai organizācijas vadītājs spētu pieņemt pamatotu lēmumu turpmākai rīcībai.

Datu regulā ir noteikta prasība organizācijām 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.

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

7.1. Kas ir risks?

Risks fizisku personu tiesībām un brīvībām ir saistāms ar fizisku, materiālu vai nemateriālu kaitējumu. 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 atņemta iespēja kontrolēt savus personas datus, kā arī, ja tiek apstrādāti īpašas kategorijas dati, vai dati par sodāmību.[25]

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**[26]". 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 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

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

Ņem vērā!

- riska avotiem var būt raksturīga mainība. Neskaidrības, kas saistītas ar vairākiem faktoriem, tostarp cilvēka uzvedības un organizatoriskām struktūrām vai sabiedrības ietekmēm, attiecībā uz kurām var būt grūti paredzēt kādu konkrētu notikumu, var būt neprognozējamas;
- 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.

[25] 75. apsvērums
[26] ISO 31000:2018 3.1. apakšpunkts

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 elektroskūtera nomu. Lai saņemtu pakalpojumu, iedzīvotājiem nepieciešams lejupielādēt aplikāciju, 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 īstenoto 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.

7.2. Riska iespējamības un ietekmes analīze

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".[27] 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.

Datu regulas 75. apsvērums skaidro "tiesību un brīvību apdraudējuma" jēdzienu, kā jebkādu neparedzētu ietekmi vai sekas attiecībā uz datu subjektiem kas var radīt kaitējumu personai.

Riska faktori[28] var izrietēt no pašas apstrādes, piemēram, apstrādes mērķa, 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 riska faktori:

Darbības, kas saistītas ar apstrādes nolūkiem	izriet no apstrādes mērķa
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 subjekta 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, mazumtirdzniecību u.c.
Datu izpaušana	izriet no konteksta, kādā personas dati tiek izpausti trešajām personām

[27] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf
[28] Riska faktors - Apstāklis kas palielina vai samazina riska iestāšanās iespējamību.

	datu apstrādes ietvaros;
Datu aizsardzības pārkāpums	izriet no personas datu aizsardzības pārkāpumu iespējamības, piemēram, darbinieki regulāri nosūta e-pastus citām personām;
Sekas, kas nav savietojamas ar sākotnējo datu apstrādes mērķi	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 NIDA veikt. 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.

7.3. Kāds ir riska apjoms, ko ir gatavs uzņemties?

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

Riska apjoms, ko ir gatava uzņemties organizācija 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	Iekšējai vai ārējie faktori ir mainījušies, tādēļ riska novērtēšanai jāveic papildu analīze vai risks ir jāpārvērtē

Sākotnējais risks --> Esošās kontroles --> Atlikušais risks --> Papildu mazinošās kontroles
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 papildus mazinošās kontroles.

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.

7.4. Riska izvērtēšana

Riska kritēriji, kas jāņem vērā, pieņemot lēmumu, 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.

Katram identificētajam riska faktoram pārzinis nosaka raksturīgo ietekmi. Ietekme būs atkarīga no kaitējuma, kas var tikt nodarīts atsevišķiem datu subjektiem un/vai sabiedrībai kopumā - tiesībām un brīvībām īsterminā, vidējā terminā un ilgterminā.

Attiecībā uz katru identificēto riska faktoru pārzinim ir jānosaka tam raksturīgā ietekme, t. i., iespējamie rezultāti. Ietekme būs atkarīga no kaitējuma, kas īsterminā, vidējā terminā un ilgterminā var rasties jo īpaši datu subjektiem un sabiedrībai kopumā.

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 īsterminā, vidēja terminā un ilgterminā ietekme ir tieši saistāma ar regularitāti cik bieži attiecīgā teritorija un datu centrs applūst. Savukārt 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 īsterminā, vidēja terminā un ilgterminā ietekmi ir jāvērtē arī plānotās datu apstrādes radītas noslodzes palielināšanās laika gaitā. Tehnoloģiju darbības ietekme uz plānotās personas datu apstrādes nolūka sasniegšanu.

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

Ņem vērā! Pirms riska novērtēšanas un novērtēšanas laikā jāiegūst attiecīga informācija. Dažos gadījumos lēmumu pieņēmēji šo informāciju var izmantot bez turpmākas (padziļinātas) analīzes.

7.5. Riska noteikšana

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

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").

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, bez matemātiskas kvantifikācijas.
- Kvantitatīvā risku novērtējuma metode ir pieeja riska novērtēšanai, kas 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.

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.
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.

7.6. Riska avotu un to cēloņu noteikšana

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.

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 mērķa un apjoma, kā arī analīzes metodes vai metodēm. Būtu jāizlemj, kā informācija jāvāc, jāglabā un jādara pieejama.

7.7. Risku mijiedarbības analīze

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.

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 mijiedarbību un to ietekmi uz apstrādes darbībām.

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.

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.

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

7.8. Riska novērtējums

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. Jānosaka kritērijus 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 mērķiem, garantiju pārkāpumi utt.

Apzinot un analizējot riska faktorus, ir jānosaka kaitējums, ko riska materializēšanās var radīt datu subjektiem.

7.9. Riska iespējamības analīze

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 1x gadā.

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.

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 nākošā gada laikā datu centrs applūdīs ir niecīga/teorētiska). Savukārt "ļoti ticams" risks ir tas, ka datu centra elementi pārstāj darboties tehniska nolietojuma dēļ (iespējamība, ka nākošā 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, utml.).

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, kur 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.

Ņem vērā! Kvalitatīvos un puskvantitatīvos paņēmienus var izmantot tikai, lai salīdzinātu riskus ar citiem riskiem, kas novērtēti tādā pašā veidā vai ar tādiem 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.

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 vairāki 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.

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.

Atgādinām, ka organizācijai uzsākot risku novērtējumu bija jānosaka pieņemamais riska apmērs[29]. Riska iespējamības novērtējuma rezultāts ir reālais datu apstrādes risku apmērs. Organizācijai pēc iespējamības novērtējuma veikšanas jāpārliecinās, ka noteiktais riska apmērs nepārsniedz pieņemamo līmeni.

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.

[29] Riska apmērs ir atkarīgs no pieņēmumiem par attiecīgo kontroļu esamību un efektivitāti (raksturīgais vai bruto risks (situācijā, kad tiek pieņemts, ka kontroles pasākumi var neizdoties) un atlikušais vai neto risks attiecībā uz riska līmeni, ja pieņem, ka kontroles darbojas tā, kā paredzēts).

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			

Riska ietekmes izvērtējuma piemērs:

Apraksts	**Ietekmes līmenis (kvalitatīvi)**	**Ietekmes līmenis (kvantitatīvi)**
Tas ietekmē noteikto pamattiesību īstenošanu, un radītās sekas ir neatgriezeniskas: • un/vai sekas ir saistītas ar īpašu datu kategorijām vai noziedzīgiem nodarījumiem un ir neatgriezeniskas; • un/vai tās rada būtisku sociālu kaitējumu, piemēram, diskrimināciju un ir neatgriezenisks; • 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 augsts attiecībā pret datu kategorijām vai 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

Varbūtības izvērtējums:

• 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: • un/vai ir pierādījumi, ka šāds risks pēdējā gadā ir materializējās; • 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: • un/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 perioda, piemēram, kas ir vecāks 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

7.10 Riska rādītāju apkopošana

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.

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 .

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.

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			

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.

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.

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.

7.11. Rezultātu pēcpārbaude un apstiprināšana

Organizācijas norīkotajai personai, kura pārskata veikto NIDA, ir jānovērtē rezultātu ticamība. Atbilstoši Datu regulai[30] viens no Datu aizsardzības speciālista uzdevumiem ir sniegt organizācijai viedokli par sagatavotu NIDA un tā konstatēto risku mazināšanas pasākumu lietderību.

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.

[30] Datu regulas 35. pants.

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

Izvērtējot izstrādāto NIDA, jāņem vērā:

- informācijas ieguves avotu: jāapsver - vai dati ir no uzticama avota, konsekventi un pietiekami, tāpat, piemēram, iespējams ir mainījušās datu iegūšanas metodes vai datu veidi;
- NIDA un risku izvērtēšanas metode: vai izvēlētā risku analīzes metode ļauj pienācīgi novērtēt plānotās datu apstrādes sarežģītību;
- Iesaistītās personas: 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, kas nav galvenā plānotās personas datu apstrādes mērķa auditorija, un/vai tiek iegūts viedoklis, kas nav reprezentatīvs, salīdzinot ar plānotās personas datu apstrādes mērogu.
- Informācijas kvalitāte: 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;
- Secinājumi: 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.

7.12. Lēmumu par riska nozīmīgumu pieņemšana

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.

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 pirmsnidas[31] laikā.

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 līmeni līdz atlikušais riska līmenis ir pieņemams.

7.13. Apspriešanās ar uzraudzības iestādi

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

[31] Ar pirmsnida posmu šo vadlīniju kontekstā saprotamas darbības, kas tiek veiktas, lai noteiktu, vai attiecīgai apstrādei ir veicams NIDA atbilstoši Datu regulas 35.panta 1.punktā noteiktajam. Ja tiek secināts, ka NIDA veicams, tad šajā posmā veiktās darbības ir iekļaujamas NIDA. Ja tiek secināts, ka NIDA nav veicams, šī posma ietvaros paveiktais saglabājams pārskatatbildības nodrošināšanai, bet tālākas šajās vadlīnijās paredzētās veicamās darbības NIDA veikšanai vairs nav veicamas.

ietvaros organizācijai ir jāiesniedz NIDA pilns saturs.

Inspekcija, izvērtējot visu saņemto informāciju, sniegs savu vērtējumu konkrētā situācijā. Pēc būtības pastāv iespējas, 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.

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

VIII. nodaļa "NIDA veikšanas metodoloģija"

Pirms atbilstošas metodoloģijas izvēles un risku novērtējuma veikšanas, organizācijai ir jādefinē skaidrs un saprotams novērtējuma tvērums un jāidentificē ieinteresētās personas.

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.

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

NIDA tiek veidots tā, lai analizētu kā incidentu un dažādu notikumu iespējamība varētu ietekmēt personas tiesības un brīvības, 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 jau bijuši līdzīgas datu apstrādes (arī ārpus konkrētās organizācijas).

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.

<u>NIDA nodrošinās, ka organizācijā notiek:</u>

- analīze par pārkāpuma iespējamajām sekām uz personu;
- analīze, vai datu kategorijas, kuras tiek apstrādātas, rada augstu risku, ka incidents var notikt.

<u>Izvēloties veidu kā veikt NIDA, ir jāņem vērā, ka tajā ir jāietver vismaz:</u>

- informāciju par organizācijas mērķiem, stratēģisko virziena mijiedarbību ar plānoto personas datu apstrādes izvērtēšanu;
- detalizētas informācijas aprakstu par organizācijas darbībām un darbībām, apstrādājot personas datus, tostarp par organizācijas procesiem, tai pieejamiem resursiem, sadarbību ar citām organizācijām u.c. ieinteresētām personām vai procesiem, kas varētu ietekmēt cilvēkus;
- seku (finansiālo, juridisko) izvērtēšanu, ko datu subjektiem varētu radīt incidenti (nozaudēšana, noplūde, kiberuzbrukums);
- tādu scenāriju kopumu, kuros ir augsts risks personas datu apstrādei;
- informāciju par nepieciešamajiem resursiem un darbībām, kuras jāveic, lai ierobežotu iespējamo ietekmi uz datu subjektiem.

Ņem vērā! Kad organizācijai nav pieredzes plānotai datu apstrādei līdzīgu darbību veikšanā vai ir maz pieejamās informācijas un/vai datu apstrādes darbības pēc būtības ir komplicētas - organizācijai vai tās pilnvarotajai personai ir attiecīgi jāpaplašina NIDA ietvars.

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

Ņem vērā! Tā nav universāla un katra organizācija to var pielāgot savām vajadzībām.

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. Atgādinām, ka šajā gadījumā piemēri ir ilustratīvi un nav jāuzskata par visaptverošu riska faktoru analīzi.

8.1. Datu veidi

Riska faktora noteikšana un riska līmeņa klasifikācija, kas izriet no datu apstrādē iesaistītajām datu kategorijām.

Riska faktors	Riska līmenis (kvalitatīvi)	Riska līmenis (kvantitatīvi)
Īpašo kategoriju dati	Ļoti augsts	4
Finanšu dati	Augsta	3
Personas apliecinošie dokumenti, dati, kuri izmantoti profilēšanai (nesatur īpašo kategoriju datus)	Vidējs	2
Personas vārds, uzvārds, dzīvesvietas adrese/kontaktinformācija	Zems	1

8.2. Datu apstrāde

Riska faktora noteikšana un riska līmeņa klasifikācija, kas izriet no plānotās datu apstrādes.

Riska faktors	**Riska līmenis (kvalitatīvi)**	**Riska līmenis (kvantitatīvi)**
Īpašo kategoriju datu apstrāde. Piemēram: • Ģenētiski novērtēts un/vai prognozēts 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

8.3. Datu avots

Riska faktora noteikšana un riska līmeņa klasifikācija, kas izriet no datu avota.

Riska faktors	**Riska līmenis (kvalitatīvi)**	**Riska 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

8.4. Datu apstrādes apjoms

Riska faktora noteikšana un riska līmeņa klasifikācija, kas izriet no datu apstrādes apjoma.

Riska faktors	Riska līmenis (kvalitatīvi)	Riska 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.	Augsta	3
Normatīvajā aktā noteiktas datu apstrādes veikšana, ja tiek izmantoti jauni tehnoloģiski risinājumi.	Vidējs	2
Datu apstrāde šaurā mērogā, neizmantojot privātumam invazīvus tehniskus risinājumus	Zems	1

8.5. Datu subjekta kategorijas

Riska faktora noteikšana un riska līmeņa klasifikācija, kas izriet no datu apstrādē iesaistītajām datu subjektu kategorijām.

Riska faktors	**Riska līmenis (kvalitatīvi)**	**Riska 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, redzes, dzirdes, kustību traucējumiem, sociāli atstumti cilvēki (arī, ja plānotā datu apstrāde varētu radīt šādu risku).	Augsta	3

Darbinieki (ja darba devēja darbības joma nav saistīta ar riska nozari); Organizācijas klienti (ja organizācijas uzņēmējdarbība nav saistīta ar riska nozari).	Vidējs	2
Datu subjekts (iedzīvotājs), kuram nav īpaša statusa attiecībās ar organizāciju	Zems	1

8.6. Datu apstrādē izmantotās tehnoloģijas

Riska faktora noteikšana un riska līmeņa klasifikācija, kas izriet no datu apstrādē izmantotajām tehnoloģijām.

Riska faktors	**Riska līmenis (kvalitatīvi)**	**Riska 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
Mobilās lietotnes; Videonovērošanas sistēmas; Informācijas sistēmas.	Vidējs	2
Tīmekļa vietne.	Zems	1

8.7. Pārziņa/apstrādātāja darbības jomas

Riska faktora noteikšana un riska līmeņa klasifikācija, kas izriet no organizācijas/apstrādātāja darbības jomas.

Risks	**Riska līmenis (kvalitatīvi)**	**Riska līmenis (kvantitaīvi)**
Slimnīcas/ biotehnoloģiju uzņēmums	Ļoti augsts	4
Finanšu iestāde	Augsts	3
Mārketinga uzņēmums	Vidējs	2
Pētniecības projekti	Zems	1

8.8. Datu izpaušana trešajām personām un/vai nosūtīšana uz trešajām valstīm vai starptautiskām organizācijām

Riska faktora noteikšana un riska līmeņa klasifikācija, kas izriet no datu nosūtīšanas uz trešo valsti.

Riska faktors	**Riska līmenis (kvalitatīvi)**	Riska līmenis (kvantitatīvi)
Datu nosūtīšana uz trešajām valstīm vai starptautiskām organizācijām, kur organizācijai ir pamatotas šaubas par aizsardzības pasākumu nodrošināšanas pietiekamību.	Ļoti augsts	4
Īpašo kategoriju datu vai datu nodošana trešajām personām, kas var radīt risku personas tiesībām un brīvībām.	Augsts	3
Nepārskatāma pārredzamības nodrošināšana attiecībā uz personas datu apstrādi (piemēram, publikācijas sociālajos tīklos).	Vidējs	2
Personas datu nodošana trešajām personām 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

8.9. Personas datu aizsardzības pārkāpuma iestāšanās riska novērtēšana

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 mērķiem, garantiju pārkāpumi utt.

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 mērķi, ja pārtrauc darboties klientu vadības sistēma).

Lai veiktu personas datu pārkāpuma riska līmeņa novērtēšanu, organizācija var modelēt dažādas personas datu aizsardzības pārkāpuma situācijas. Situācijas aprakstam organizācijai jāizmanto vismaz šādi elementi:

- Pārkāpuma veida apraksts.
- Personas datu kategoriju uzskaitījums un datu subjektu raksturojums, kuriem pārkāpuma rezultātā ir nodarīts kaitējums.
- Kāds kaitējums var tikt nodarīts datu subjekta tiesībām un brīvībām.

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

Piemērs:

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

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

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 vienu mēnesi no izvērtējuma veikšanas – īstermiņā, vidējā termiņā vai ilgtermiņā).

IX. nodaļa "Ietekmes uz datu subjektu raksturojums"

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 jā, tad kādā veidā.

To cik liela varbūtība ir, ka ietekme iestāsies, noteiks risku analīzes nodaļā. 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 nākošajā NIDA veikšanas posmā.

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

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.

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. [32]

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

9.1. Datu aizsardzības tiesības

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

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.

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, kas nebūtu 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 datu subjekta iesniegumu organizācijai iesniegt attālināti. Šādā gadījumā tiek radīts apdraudējums datu subjekta tiesībām no pārredzamības, saziņas un datu subjekta tiesību īstenošanas perspektīvas.

- **Informēšana**

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

[32] 2014. gada 29. panta darba grupas paziņojums par riskos balstīto pieeju.

Datu regulas 13. un 14. pantā norādīto obligāto informāciju. Gadījumā, ja, veicot datu subjektu tiesību aprakstu, tiek secināts, ka ar līdzšinējām metodēm datu subjekta informēšanas pienākumu organizācija jaunajā datu apstrādes procesā nespēs nodrošināt, tad jādomā par piemērotiem ietekmes mazināšanas pasākumiem – kā nodrošināt, ka datu subjekts informāciju par apstrādi tomēr saņems laicīgi.

Piemērs – 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**

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 jaunveidotās personas datu apstrādes sistēmas praktisko pusi. Atkarībā no plānotās datu apstrādes mainīsies arī datu subjekta tiesību īstenošanas procesi.

Piemērs - 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**

Izvērtējot tiesību uz datu labošanu īstenošanu, ir jāņem vērā, ka tas daļēji pārklājas ar risku novērtējumu. Tas ir būtisks elements, lai noteiktu gan datu vērtību, gan arī, lai apsvērtu kāda būs piemērotākā sistēma datu labošanai. Datiem atkarībā no to nozīmes datu apstrādē var būt atšķirīga loma tās darbības nodrošināšanā. Tie 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.

Šīs tiesības novērtējums būtu jāsāk ar:

- veida, kā dati tiek iegūti;
- 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.

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 arī veidojamo informācijas aprites sistēmu izstrādāt loģisku un efektīvu.

Piemērs – Organizācija veido iepazīšanās aplikāciju/portālu. Viena no pirmajām izvēlēm, kas datu subjektam ir jāveic, ir tā seksuālās orientācijas norādīšana, vēlāk datu subjektam jāsniedz arī tā identificējošā 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 attiecībā uz datu subjekta tiesību uz informācijas labošanu īstenošanu. Būtu jāievēro princips, ka informāciju, ko datu subjekts ir pats iesniedzis, pats arī var izlabot.

- **Datu dzēšana, iebilšana datu apstrādei un pārnesamība**

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 tās nodrošināt.
Šīs tiesības novērtējumā jāņem vērā:

- vai plānotajā datu apstrādē ir īstenojamas minētās tiesības;
- analīze par to, kādi tehniskie līdzekļi tiks izmantoti datu subjekta tiesību nodrošināšanai.

Pēc datu apstrādes procesu datu dzīvesciklā identifikācijas, kuros 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 uz iebilšanu datu apstrādei 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 ierobežošana**,

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).

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.

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.

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 atbilstošajā vietā sākotnējā datu kopā.

Piemēram, organizācija plāno uzsākt aizdevumu izsniegšanu, izmantojot aplikācijas starpniecību. Aplikācijā tiek ieintegrētas nepieciešamās "Zini savu klientu" darbības, tiek saglabāti darījuma pamatdati, kā arī informācija, kuru aplikācijai klients sniedz brīvprātīgi – gatavību saņemt komerciālos 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 tiesībām jāattiecas, 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 ieintegrēt), uzskatāms, ka apstrādē saglabājas augsti riski, kuru mazināšanai organizācijai jāatrod risinājumi.

- **Automatizēta individuālu lēmumu pieņemšana**

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 īpašas kategorijas datu apstrāde tiek veikta, ievērojot Datu regulas 22. panta 4. punktā noteikto.

Aprakstā jānovērtē, gan datu subjekta saprātīgās gaidas un izpratne par datu apstrādi, gan arī automatizētu lēmumu pieņemšanas nozīmi 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*[33]. 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! NIDA organizācijai ir jāvērtē arī iespējamība, kā datus varētu izmantot trešās personas gadījumā, ja organizācija zaudētu kontroli pār datiem. Viens no elementiem, kas jāņem vērā – vai trešās personas datus varētu izmantot profilēšanai vai automatizētai lēmumu pieņemšanai.

9.2. Citas tiesības un brīvības

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.

Līdz ar to, šajā gadījumā, vērtējot ietekmi uz personas pamattiesībām, ieteikumi tiks izteikti attiecībā uz izpausmēm, kur šī ietekme izpaužas netiešāk, vai pastāv tikai ietekmes risks. To cik liela varbūtība ir, ka ietekme iestāsies noteiks risku analīze. Šeit ir nepieciešams identificēt visas iespējamās arī hipotētiskās ietekmes uz datu subjektu. Tāpat atceramies, ka iespējamas ietekmes

[33] Atsauce uz Datu regulas 4. pantu - definīcija

pastāvēšana šajā brīdī nenozīmē, ka apstrāde būs neiespējama – drīzāk ietekmes pastāvēšana ļaus noteikt riskus, kas ir vērtējami nākošajā NIDA veikšanas posmā.

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

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.

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, kas ņemtu vērā dzimuma faktorus, 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.*

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, kura 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 tiesības pārkāpumu.

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

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.*

Netiešas ietekmes piemērs ir atrašanas vietas datu, kas liecina par datu subjektu pārvietošanās paradumiem, izgūšana un apstrāde dažādu nolūku dēļ. 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 pietiekoši precīzi, lai ietekmētu un manipulētu personas brīvu spēju pieņemt lēmumus.

- **Taisnīga tiesa:** *Katram cilvēkam ir tiesības uz godīgu tiesu un nekāda cilvēka nedrīkst pazemināt līdz nelikumīgam vai arbitrāram ieslodzījumam vai sodam.*

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.*

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.*

Šīs pamattiesības 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.*

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 uz augstu fizisko un garīgo veselību.*

Iespējama gan tieša, gan netieša ietekme. Tiešā veidā nosakot personai diagnozi 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, kuru īstenībā nav.

Cits piemērs varētu būt, ka, vērtējot personas apdrošināšanas prēmijas apmēru, personas saslimšanas varbūtības novērtējums paaugstina apdrošināšanas izmaksas līdz līmenim, kas personai apgrūtinātu iespēju apdrošināt savu veselību.

Abos gadījumos ir secināms, ka iespējama ietekme uz personas veselību pastāv – ietekmes riska apmērs ir nosakāms iepriekšējā nodaļā, kas veic iespējamo risku novērtējumu.

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

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 savādāks 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 vispārīgām pamattiesībām.

X. nodaļa "Risku pārvaldība"

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 šo darbu veikšanai budžetā līdzekļus, 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.

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.

10.1. Līgumiskie paņēmieni

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.

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:*

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 iesaistām kādu citu personu. Ar rīka starpniecību mazinām iespējamo kopējo ietekmi un riskus, jo novērš tos apdraudējumus, kas varētu izcelties, jo viena persona nav informēta par pasākumiem, kas jādara datu aizsardzībā.

- *Kontroles un auditu tiesības:*

Līgumā iekļautās tiesības vienai pusei veikt kontroles un auditus, lai pārliecinātos par otras puses ievēroto noteikumu un prasību izpildi. Kad apstrādē tiek iesaistīta vairāk par vienu personu, 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 tas palīdz arī mazināt kopējos riskus, kas noteikti NIDA attiecībā uz otras puses veiktas darbības neatbilstību.

- *Konfidencialitātes nosacījumi:*

Ietveriet konfidencialitātes noteikumus, 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:*

Iekļaujiet līgumā mehānismus 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.

10.2. Tehniski paņēmieni

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:*

Apsveriet iespēju veikt regulāras drošības pārbaudes, lai identificētu potenciālos iekšējos un ārējos drošības apdraudējumus. 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:*

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

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 resursus, kas var tikt aktivizēti nepieciešamības gadījumā, nodrošināšana.

- *Programmatūras pārbaudes*

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. Apsveriet pirmkoda izstrādes pārbaudes veikšanu un tā automatizētas testēšanas procedūras ieviešanu.

- *Datu šifrēšana:*

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.

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 trešai personai nav iespējams datus saistīt ar datu subjektu un netiek ietekmēts veids, kā cita persona izturas pret datu subjektu.

- *Ieguldījums drošības tehnoloģijās:*

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.

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.

10.3. Organizatoriskie paņēmieni

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:*

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

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:*

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.

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:*

Proaktīva un pārredzama komunikācijas sistēma 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:*

Apmācīts un informēts personāls par datu apstrādes un aizsardzības procedūrām nodrošina risku mazināšanu visas tās risku grupas, 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:*

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.

PRAKTISKI

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.

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

10.4. Esošo kontroļu efektivitātes izvērtējums

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.

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 paredzēts, 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.

Riskam var būt vairāk nekā viena kontrole, tā pat viena kontrole var ietekmēt vairāk nekā vienu risku. Būtu jānošķir kontroles, kas maina iespējamību, sekas vai abus. Tāpat ir jānodala ieviestās kontroles, kas ir sadalītas starp dažādām ieinteresētajām 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.

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

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 mērķi – ja datu apstrādes mērķis ir saistīts ar datu apstrādes centrā ievietotās informācijas aktīvu izmantošanu organizācijas ikdienas darbā.

XI. nodaļa "Dokumentācija"

Ņemot vērā, ka NIDA veikšanas laikā tiks izmantoti daudz 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.

Tāpat NIDA veikšana un iekļaušana organizācijas datu aizsardzības sistēmā ir saistīta ar NIDA ietvaros apstrādātās informācijas kategorizēšanu (piemēram, informācija, kas var būt nepieciešama pārskatatbildības principa nodrošināšanai), kā arī noteiktu jaunu dokumentu izstrādi (piemēram, DAS viedoklis par NIDA atbilstību).

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

11.1. Datu aizsardzības risku reģistrs

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.

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 divas vai vairāk NIDAs, 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.

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.

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.

Īsumā datu aizsardzības risku reģistrācijas un uzkrāšana vienuviet palīdzētu pārvaldīt NIDA laikā konstatētos riskus, to ietekmi un ietekmes mazināšanas pasākumus.

11.2. NIDA ziņojums

NIDA ziņojums ir NIDA procesa starprezultāts, kurā tiek apkopoti veiktā risku novērtējuma un plānotās personas datu apstrādes analīzes rezultāti. Šajā ziņojumā būtu jāapkopo katra NIDA procesa posma uzskaite un jāatzīmē secinājumi no katra procesa posma. 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 ko 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.

11.3. Lēmumu pieņemšanas dokumentācija

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.

Organizācijai ir jādokumentē pieņemtos lēmumus saistībā ar plānoto datu apstrādi. NIDA dokumentācijā var izmantot jebkurus līdzekļus, kas ir vispiemērotākie organizācijai un attiecīgajai apstrādei.

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.

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.

11.4. Risku pārvaldības plāns

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.

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.

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.

XII. nodaļa "Apspriešanās un komunikācija ar datu subjektu"

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.

Šāds viedoklis ir pieprasāms, organizācijai izmantojot dažādus sev pieejamos līdzekļus (piemēram, jautājumu formā organizācijas darbiniekiem, vai izmantojot vienkāršas aptaujas, ko dara pieejamus pārziņa klientiem).

12.1. Fokusa grupas diskusija

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:

- Grupas sastāvs: 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.

- Moderators: 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.

- Atklātais dialogs: 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..

- Datu analīze: 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.

Ieguvumi organizācijai:

- Ieskats datu subjekta perspektīvās: 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.

- Problēmu un to risinājumu apzināšana: organizācija var identificēt iespējamās bažas un problēmas saistībā ar datu apstrādi, kas, iespējams, nav konstatētas iekšējos novērtējumos. Fokusa grupas diskusijās var izcelt jomas, kurās datu subjekti jūtas neērti vai neskaidri attiecībā uz savu personas datu apstrādi.

- Komunikācija un pārredzamība: 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.

- Lēmumu pieņemšana: 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.

12.2. Strukturētas vai daļēji strukturētas intervijas

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 fokuss 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.

- Konsekvence un salīdzināmība: 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, padziļinātāk izpētot konkrētas tēmas, atklājot pamatā esošo datu subjektu attieksmi, kas saistīta ar datu apstrādi.

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

Ieguvumi organizācijai:

- Izpratne par datu subjekta perspektīvām: Intervijas ar datu subjektiem sniedz organizācijai tiešu ieskatu par to, kā konkrētā persona vērtē plānoto datu apstrādi, iegūstot dziļāku izpratni par to bažām, vēlmēm un gaidām attiecībā uz datu privātumu un drošību.

- Problēmu un to risinājumu apzināšana: 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.

- Komunikācija un pārredzamības: 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.

- Lēmumu pieņemšana: 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.

12.3. Aptaujas

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.

- Aptaujas anketa: organizācija var izstrādāt anketu, kas ietver virkni jautājumus saistībā ar plānoto datu apstrādi un citiem būtiskiem tematiem. Jautājumi var tikt veidoti ar vienu vai vairākiem atbilžu variantiem, izmantojot reitinga skalu, atvērtā tipa vai šo formātu kombinācija.

- Analīze un interpretācija: Organizācija iegūst plašākas sabiedrības daļas ieskatus par plānoto datu apstrādi.

Ieguvumi organizācijai:

- Plašāks sabiedrības ieskats: Izmantojot dažādus saziņas kanālus, aptaujas dod iespēju organizācijai iegūt un apkopot atsauksmes no daudziem datu subjektiem dažādās demogrāfiskajās un ģeogrāfiskajās vietās. Izmantojot šo metodi, organizācija var gūt plašu izpratni par datu subjektu domām, bažām un attieksmi pret plānoto datu apstrādi.

- Anonīma atgriezeniskā saite: Aptaujas nodrošina datu subjektiem platformu, kurā paust savu viedokli anonīmi, un tas var veicināt atklātākas atbildes. Dalībnieki var justies ērtāk dalīties savās domās, nebaidoties no sekām.

- Skaitliski izsakāmi dati: 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).

- Izmaksu efektivitāte: 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.

- Komunikācija un pārredzamība: 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 subjekta uzticēšanos.

- Lēmumu pieņemšana: No aptaujas atbildēm gūtās atziņas var izmantot uz datiem balstītu lēmumu pieņemšanu, 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.

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.

12.4. Ziņošana citām iesaistītajām personām un NIDA publicēšana

NIDA publicēšana demonstrē organizācijas atbildību par tās veikto datu apstrādi un nodrošina pārredzamību Datu regulas izpratnē. 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.

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.

XIII. nodaļa "Uzraudzība un pārskatīšana"

13.1. Integrācijas datu aizsardzības sistēmā

Kad NIDA ir pabeigts, nepieciešams īstenot 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.

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.

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, mērķis 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.

13.2. Apstrādes darbību pastāvīga uzraudzība

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

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 iespējamo datu apstrādes ietekmi.

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.

13.4. NIDA periodiska pārskatīšana

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.

NIDA periodiska pārskatīšanas biežums katrai organizācijai būs individuāls. Termiņš iekļaujams NIDA ziņojumā. NIDA periodiskās pārskatīšanas laikā ir jāpievērš uzmanība, vai identificētie riski un ietekmes novērtēti pareizi un vai praksē personas datu apstrādes radītā ietekme nav lielāka par NIDA laikā identificēto. NIDA, kur viens no kritērijiem ietekmes novērtējuma veikšanai bija tehnoloģisko inovāciju izmantošana, šim termiņam katrā ziņā vajadzētu būt īsākam. Rekomendējams šādu atkārtotu novērtēšanu veikt pēc personas datu apstrādes pirmā gada, ja vien apstrādē nav notikušas būtiskas izmaiņas ātrāk.

Ņem vērā! 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.

13.5. 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.

Pielikums Nr.1 – 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. Labajā pusē esošajā pusē norādīts ko konkrētajā veidlapas vietā apskatīt, savukārt kreisajā pusē slīprakstā tiek skaidrots kā apskatāmais jautājums risināms. *Aizpildot veidlapu slīprakstā esošais teksts ir dzēšams.*

Ja aizpildot veidlapas II nodaļu tiek secināts, ka NIDA nav veicams tad tālāku veidlapas aizpildīšanu var pārtraukt.

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 eadresi, elektroniskā pasta adresi vai juridisko adresi.*
Kopīgi pārziņi	*Ja lēmumu par personas datu apstrādes veidu un tās nepieciešamību kopīgi pieņem vairākas personas. Šajā sadaļā norāda informāciju par kopīgiem pārziņiem atbilstoši vadlīniju II. nodaļai "Galvenās ieinteresētās personas, jeb kam ir jāveic NIDA".*
Apstrādātājs	*Ja personas datu apstrādei pārzinis piesaista citu organizāciju, kā apstrādātāju, tad šajā sadaļā norāda informāciju par apstrādātāju atbilstoši vadlīniju II. nodaļai "Galvenās ieinteresētās personas, jeb kam ir jāveic NIDA".*
Citas iesaistītas personas	*Šajā sadaļā norāda informāciju, 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 kvalificēti 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 veikta NIDA.*
Datu aizsardzības speciālists	*Šajā sadaļā norāda informāciju par DAS, ja tāds ir norīkots.*
Nepieciešamības par datu aizsardzības speciālista iesaisti NIDA veikšanas procesā 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. Darbības joma un piemērojamība	

Šo sadaļu aizpilda atbilstoši vadlīniju III. nodaļai "Darbības joma un piemērojamība".	
NIDA veikšanas nepieciešamības novērtējums	*Šajā sadaļā organizācija norāda objektīvu informāciju, uz kuras pamata tiek pieņemts lēmums par nepieciešamību veikt vai neveikt NIDA atbilstoši vadlīniju III nodaļai "Darbības joma un piemērojamība". Vai plānotā datu apstrāde ietilpst Datu regulas 35. panta tvērumā? Vai plānotā datu apstrāde ir iekļauta Datu valsts 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, kas izveidots saskaņā ar Datu regulas 35. pantu un nav jāveic NIDA "baltais saraksts".*
Vai NIDA ir jāveic?	JĀ ☐ NĒ ☐ *Ja atbilde ir Nē – tad NIDA veikšanu var pārtraukt.*
III. NIDA mijiedarbība ar citām Datu regulas prasībām *Šo sadaļu aizpilda atbilstoši vadlīniju VI. nodaļai "NIDA mijiedarbība ar citām Datu regulas prasībām".*	
Pārziņa datu aizsardzības sistēmas apraksts	*Šajā sadaļā organizācija īsumā apraksta esošo datu aizsardzības sistēmu atbilstoši vadlīniju IV nodaļai, norādot:* • *organizācijas iekšējos kārtības noteikumus un procedūras;* • *informāciju par ieviestajiem drošības pasākumiem;* • *ieviestajiem piekļuves kontroles un autentificēšanās mehānismiem;* • *ja ir veikta, informāciju par iepriekš veiktu NIDA;* • *informāciju par darbinieku zināšanām par datu apstrādi un aizsardzību (piemēram, vai ir veiktas apmācības vai citādi instruēti darbinieki).*
Citi pasākumi, kurus pārzinis veicis pārskatatbildības principa vai citu Datu regulas izvirzīto prasību nodrošināšanai.	*Šajā sadaļā organizācija īsumā apraksta citus pasākumus, kas īstenoti atbilstoši vadlīniju IV. nodaļai, piemēram:* • *informāciju par datu apstrādes reģistru;* • *gadījumā, ja plānotā datu apstrāde balstīta uz Datu regulas 6. panta 1. punkta f) apakšpunktu, informāciju par veikto līdzsvarošanas testu un tā rezultātiem;* • *informāciju par personas datu apstrādes pārkāpumu reģistru (ja tāds ir izveidots);* • *informāciju par citu ieviesto tehnisko un organizatorisko pasākumu kopumu.*
IV. Informācija par plānoto apstrādi *Šo sadaļu aizpilda atbilstoši vadlīniju V. nodaļai "Datu apstrādes dzīves cikls".*	
Datu apstrādes dzīves cikla vizualizācija	*Šajā sadaļā apraksta konkrētas datu apstrādes datu aprites dzīves ciklu.*
Datu apstrādes funkcionāls apraksts	*Šajā sadaļā organizācija veic datu apstrādes funkcionālo aprakstu, kurā jāietver datu apstrādes darbību uzskaitījums; detalizēta faktisko informācijas aprites elementu analīze.*
V Datu apstrādes atbilstība un likumība *Šo sadaļu aizpilda atbilstoši vadlīniju VI. nodaļai "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:*

<table>
<tr><td></td><td colspan="3">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).</td></tr>
<tr><td>Datu aizsardzības principi</td><td colspan="3">Šajā nodaļā organizācija vērtē atbilstību visiem datu apstrādes principiem, kuri noteikti Datu regulas 5. pantā.</td></tr>
<tr><td colspan="4">“likumīgums, godprātība un pārredzamība”</td></tr>
<tr><td>Kāds ir plānotās personas datu apstrādes tiesiskais pamats?</td><td colspan="3">Šajā sadaļā organizācija nodrošina esošas un/vai 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 mērķi un datu apstrādes dzīves cikla posmu.
Tiesiskā pamata analīze jāveic saskaņā ar Datu regulas 6. pantu un gadījumos, kad tiek veikta īpašo kategoriju datu apstrāde – Datu regulas 9. pantu, savukārt, ja tiek apstrādāta informācija par personas sodāmību – Datu regulas 10. pantu.
Ja plānotā datu apstrāde tiek balstīta uz datu subjekta “piekrišanu”, šajā sadaļā ir jāanalizē arī piekrišanas nosacījumi, lai tā atbilstu Datu regulas 7. pantam.</td></tr>
<tr><td colspan="4">“datu minimizēšana”</td></tr>
<tr><td>Vai ir izvērtēts apstrādājamo personas datu apjoms un to atbilstība personas datu apstrādes mērķa sasniegšanai?</td><td colspan="3">JĀ ☐
NĒ ☐</td></tr>
<tr><td colspan="4">Ja atbilde ir "JĀ", uzskaitiet šos datus, norādot, kādēļ tie nepieciešami personas datu apstrādes mērķa 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 (mērķis)?</td><td colspan="3">Šeit tiek norādīts precīzi definēts personas datu apstrādes nolūks. Mērķis, 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/mērķim .</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 esošos personas datus, 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>
</table>

<table>
<tr><td colspan="3">“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="2">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>Resurss: *Piemēram, aparatūra, programmatūra, tīkli, cilvēki, informācijas apmaiņas kanāli papīra formāta informācijas apmaiņai u.c.</td></tr>
<tr><td colspan="3">“pārskatatbildība”</td></tr>
<tr><td>Vai organizācija spēj demonstrēt, ka plānotā datu apstrāde atbilst visām Datu regulas prasībām?</td><td colspan="2">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="3">VI. Risku datu subjekta tiesībām un brīvībām analīze
Šo sadaļu aizpilda atbilstoši vadlīniju VII. nodaļai “Risku novērtējums” un VIII. nodaļai “NIDA veikšanas metodoloģija”, ievērojot organizācijas izvēlēto riska novērtējuma metodoloģiju konkrētajā gadījumā.</td></tr>
<tr><td colspan="3">VII. “Ietekmes uz datu subjektu raksturojums”
Šo sadaļu aizpilda atbilstoši vadlīniju IX. nodaļa “Ietekmes uz datu subjektu raksturojums”.</td></tr>
<tr><td>Datu aizsardzības tiesības</td><td rowspan="8">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.</td></tr>
<tr><td>Informācijas pārredzamība, saziņa un datu subjekta tiesību īstenošanas kārtība</td></tr>
<tr><td>Informēšana</td></tr>
<tr><td>Piekļuve datiem</td></tr>
<tr><td>Datu labošana</td></tr>
<tr><td>Datu dzēšana, iebilšana datu apstrādei un pārnesamība</td></tr>
<tr><td>Datu ierobežošana</td></tr>
<tr><td>Automatizēta individuālu lēmumu pieņemšana</td></tr>
<tr><td>Citas pamattiesības</td><td rowspan="10">Šajā sadaļā organizācija apraksta kā plānotā datu apstrāde varētu ietekmēt vai ietekmē vispārējās pamattiesības.</td></tr>
<tr><td>Vienlīdzība un nediskriminācija</td></tr>
<tr><td>Dzīvības drošības tiesības</td></tr>
<tr><td>Brīvības tiesības</td></tr>
<tr><td>Taisnīga tiesa</td></tr>
<tr><td>Privātās un ģimenes dzīves ievērošana</td></tr>
<tr><td>Tiesības uz darbu, īpašumu un taisnīgu atalgojumu</td></tr>
<tr><td>Tiesības uz izglītību</td></tr>
<tr><td>Tiesības uz veselību</td></tr>
<tr><td>Piederība politiskai sabiedrībai</td></tr>
<tr><td colspan="3">VIII. “Risku pārvaldība un risku mazinošie pasākumi”
Šo sadaļu aizpilda atbilstoši vadlīniju X. nodaļai “Risku pārvaldība”.</td></tr>
<tr><td>Līgumiskie paņēmieni</td><td colspan="2">Šajā sadaļā organizācija veic analīzi attiecībā ieviesto</td></tr>
</table>

Tehniskie paņēmieni Organizatoriskie paņēmieni	*kontroļu efektivitāti, lai mazinātu identificētos riskus, kas noteikti šīs veidlapas VI. sadaļā "Risku datu subjekta tiesībām un brīvībām analīze".*
IX. "Cita papildus informācija"	
Vai NIDA veikšanas procesā ir pieprasīts datu subjektu vai viņu pārstāvju viedoklis?	*Šajā sadaļā organizācija norāda iegūto viedokli vai apsvērumus/apstākļus viedokļa neiegūšanai (skatīt vadlīniju XII. nodaļu "Apspriešanās un komunikācija ar datu subjektu").*
Lēmumu pieņemšanas dokumentācija	*Šajā sadaļā organizācija norāda vai un kā dokumentēti pieņemtie lēmumi saistībā ar plānoto datu apstrādi (skatīt vadlīniju XI. nodaļu "Dokumentācija").*
Risku pārvaldības plāns	*Šajā sadaļā organizācija apraksta identificēto risku pārvaldības plānu, ja tāds ieviests (skatīt vadlīniju XI. nodaļu "Dokumentācija").*
Ziņošana citām iesaistītajām personām un NIDA publicēšana	*Šajā sadaļā organizācija norāda, vai un kādā apjomā ir paredzēts publicēt veikto NIDA (skatīt vadlīniju XII. nodaļu "Apspriešanās un komunikācija ar datu subjektu").*
NIDA uzraudzība un pārskatīšana	*Šajā sadaļā organizācija norāda kāda ir izveidota NIDA uzraudzības un pārskatīšanas sistēma (skatīt vadlīniju XIII. nodaļu "Uzraudzība un pārskatīšana").*
X. "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 (skatīt vadlīniju VII. nodaļu "Riska novērtējums").*

Novērtētājs