LATVIJAS REPUBLIKA
VALKAS NOVADA PAŠVALDĪBA
Reģ.Nr.90009114839, Beverīnas iela 3, Valka, Valkas novads, LV-4701,
tālr.64722238, e-pasts: novads@valka.lv, www.valka.lv

NOTEIKUMI
Valkā

2025.gada 27.novembrī Nr.12

APSTIPRINĀTI
ar Valkas novada pašvaldības domes
2025. gada 27.novembra sēdes lēmumu Nr. 326
(protokols Nr. 24, 4.§)

Personas datu apstrādes un aizsardzības risku pārvaldības noteikumi Valkas novada pašvaldībā

Izdoti saskaņā ar
Valsts pārvaldes iekārtas likuma
72.panta pirmās daļas 2.punktu,
Eiropas Parlamenta un padomes
2016.gada 27.aprīļa Regulas 2016/679
"par fizisku personu aizsardzību attiecībā uz
personas datu apstrādi un šādu datu brīvu apriti
un ar ko atceļ Direktīvu 95/46/EK" 35.pantu

I. Vispārīgie jautājumi

1. Šie noteikumi (turpmāk – Noteikumi) nosaka, kādos gadījumos un kādā kārtībā Valkas novada pašvaldībā (turpmāk – pašvaldība) veic datu apstrādes un aizsardzības risku analīzi, rezultātu novērtēšanu un atbilstošu drošības pasākumu īstenošanu.
2. Noteikumi ir saistoši pašvaldības amatpersonām, darbiniekiem, apstrādātājiem un apstrādātāja piesaistītiem apakšapstrādātājiem, ja tas noteikts līgumā. Ja datu aizsardzības speciālista uzdevumu izpildei ir piesaistīts ārpakalpojuma sniedzējs, Noteikumi ir saistoši arī datu aizsardzības speciālista pakalpojuma sniedzējam.

II. Novērtējums par ietekmi uz datu aizsardzību

3. Pašvaldības iestādes un/vai struktūrvienības vadītājs par plānotajām izmaiņām tā pārraudzībā esošajiem personas datu apstrādes procesiem vai jauniem personas datu apstrādes procesiem informē datu aizsardzības speciālistu, iesniedzot tam aizpildītu personas datu apstrādes aprakstu saskaņā ar Noteikumu 1. pielikumu.
4. Datu aizsardzības speciālists novērtē plānotās izmaiņas un to ietekmi uz datu subjekta tiesībām un brīvībām.
5. Ja apstrādes veids, jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, varētu radīt augstu risku datu subjekta tiesībām un brīvībām, datu aizsardzības speciālists par to informē pašvaldības direktoru.
6. Ja plānotās izmaiņas skar informācijas sistēmu, pašvaldībā veic informācijas sistēmas drošības risku analīzi.
7. Datu aizsardzības speciālists personas datu apstrādes aprakstā iekļauto informāciju vērtē saskaņā ar Noteikumu 2. pielikumu.

III. Personas datu apstrādes risku pārvaldības plāna izstrāde un izpilde

8. Datu aizsardzības speciālists pēc saņemtā personas datu apstrādes apraksta izvērtēšanas sagatavo novērtējuma par ietekmi uz datu aizsardzību risku analīzes un ieviešamo drošības līdzekļu ziņojumu saskaņā ar Noteikumu 3. pielikumu, kurā uzskaita identificētos riskus ar vērtību no 3 līdz 9, ko desmit darbdienu laikā iesniedz pašvaldības iestādes un/vai struktūrvienības vadītājam.
9. Pašvaldības iestādes un/vai struktūrvienības vadītājs, ņemot vērā datu aizsardzības speciālista sagatavoto novērtējuma par ietekmi uz datu aizsardzību risku analīzes un ieviešamo drošības līdzekļu ziņojumu, mēneša laika sagatavo drošības pasākumu ieviešanas plānu saskaņā ar Noteikumu 4. pielikumu, ko iesniedz pašvaldības izpilddirektoram apstiprināšanai.
10. Pašvaldības iestādes un/vai struktūrvienības vadītājs nodrošina personas datu drošības pasākumu ieviešanas plāna izpildi un aktualizāciju.

Valkas novada pašvaldības domes priekšsēdētājs V.A.Krauklis

I. Personas datu apstrādes vispārīgs apraksts	
Iestādes vai struktūrvienības nosaukums	
Novērtētājs (vārds, uzvārds, amats)	
Kontaktinformācija	
Novērtējuma veikšanas periods	
Pārzinis Ja personas datu apstrādei ir piesaistīta cita organizācija, kā pārzinis, tad norādiet informāciju par šo pārzini, tai skaitā, kāds ir datu apstrādes mērķis.	
Apstrādātājs Ja personas datu apstrādei ir piesaistīta citu organizāciju, kā apstrādātāju, tad norādiet informāciju par apstrādātāju, tai skaitā, kādus uzdevumus tas veic.	
Kādas iestādes un/vai struktūrvienības ir iesaistītas datu apstrādē, un kādus uzdevumus tās veic.	
Datu aizsardzības sistēmas apraksts. Aprakstiet kādi iekšējie kārtības noteikumi un procedūras tiek ievērotas konkrētajā datu apstrādē: • informāciju par ieviestajiem drošības pasākumiem; • informāciju pa ieviestajiem piekļuves kontroles un autentificēšanās mehānismiem; • informāciju par datu apstrādes kvalitātes kontroli. Ja ir veikta iepriekš NIDA, sniedziet info par identificējamajiem riskiem.	
Datu apstrādes dzīves cikla vizualizācija* Aprakstiet konkrētās datu apstrādes datu aprites dzīves ciklu.	
**** Organizācijas datu apstrādes sistēma**	
Kāds ir personas datu apstrādes mērķis? Norādiet normatīvos aktus, kas paredz datu apstrādi.	
Kādi personas dati tiek apstrādāti?	

Vai notiek automatizēta lēmumu pieņemšana? Ja atbilde ir "jā", raksturojiet procedūru, kā datu subjekts tiek informēts par to.	Jā/ Nē	
Vai īpašo kategoriju personas datu apstrāde ir nodalīta no pārējo personas datu apstrādes? Ja atbilde ir "jā", raksturojiet procedūru, kā tas tiek nodrošināts. Ja atbilde ir "nē", norādiet iemeslus.	Jā/ Nē	
Vai visi apstrādājamie dati ir nepieciešami personas datu apstrādes mērķa sasniegšanai? Ja atbilde ir "jā", uzskaitiet šos datus, norādot, kādēļ tie nepieciešami personas datu apstrādes mērķa sasniegšanai. Ja atbilde ir "nē", norādiet iemeslus.	Jā/ Nē	
Ja personas datu apstrādes tiesiskais pamats ir datu subjekta piekrišana, norādiet, kādā veidā (elektroniski, rakstiski, mutiski).		
Ja personas datu apstrādes tiesiskais pamats ir datu subjekta piekrišana, norādiet - kad tiek iegūta datu subjekta piekrišana un kāds ir tās saturs.		
Vai tiek apstrādāti nepilngadīgu personu, kas jaunāki par 13 gadiem, personas dati uz piekrišanas pamata. Ja atbilde ir "jā", norādiet kārtību, kā tiek iegūta nepilngadīgās personas likumisko aizgādņu piekrišana.	Jā/Nē	
II. Datu subjekta tiesības un brīvības		
1. Personas datu apstrāde atbilstoši personas datu apstrādes mērķim		
Kāda kārtība ir paredzēta, lai izvērtētu apstrādājamo personas datu apjomu un to atbilstību personas datu apstrādes mērķa sasniegšanai? Kā tiek nodrošināts, ka personas datu apjoms visā to apstrādes laikā nepārsniedz personas datu apstrādes mērķa sasniegšanai nepieciešamo?		

Vai ir noteiktas procedūras, kā identificē datu subjektu, informācijas sistēmas lietotāju, trešās personas, kuras apstrādā personas datus manuāli vai informācijas sistēmā? Ja atbilde ir "jā", raksturojiet kārtību vai procedūru.	Jā/ Nē	
2. Adekvāta personas datu apstrāde		
Kā tiek nodrošināta pareizu (precīzu, aktuālu) personas datu apstrāde?		
Cik bieži veic pārbaudes vai apstrādāti tiek pareizi (precīzi, aktuāli) dati? Norādiet pamatojumu, kādēļ ir izvēlēts šāds periodiskums un vai tas nodrošina tikai pareizu (precīzu, aktuālu) personas datu apstrādi.		
3. Personas datu glabāšana atbilstoši personas datu apstrādes mērķim		
Kāds ir personas datu glabāšanas termiņš? Analizējiet un raksturojiet personas datu glabāšanas termiņu, atbilstoši datu apstrādes nolūkam. Analīze jāveic attiecībā uz izvēlētajiem datu glabāšanas risinājumiem gan datu dzīvescikla apstrādes, gan dzīvescikla glabāšanas fāzēs.		
4. Datu subjekta tiesību nodrošināšana		
4.1. Datu subjekta informēšana par viņa personas datu apstrādi		
Vai ir nodrošināta datu subjekta informēšana par viņa personas datu apstrādi neatkarīgi no tā, vai personas dati ir vai nav iegūti no datu subjekta? Ja atbilde ir “jā”, norādiet, kādā veidā un kādā gadījumā datu subjekts tiek informēts par viņa personas datu apstrādi un kāda satura informācija tiek sniegta. Ja atbilde ir “nē”, norādiet, kādēļ datu subjekts netiek informēts.	Jā/ Nē	

Vai datu subjektam tiek nodrošināta iespēja iegūt informāciju par personām, kuras ir saņēmušas informāciju par šo datu subjektu? Ja atbilde ir "jā", norādiet, par kādu laikposmu šāda informācija tiek sniegta. Ja atbilde ir "nē", norādiet, kādēļ informācija netiek sniegta.	Jā/Nē	
Vai informācija par datu subjektu tiek saņemta no trešajām personām? Ja atbilde ir "jā", norādiet informācijas saņemšanas kārtību un tiesisko pamatu šādas informācijas saņemšanai.	Jā/ Nē	
4.2. Datu subjekta tiesības piekļūt saviem personas datiem		
Vai datu subjektam ir nodrošinātas tiesības piekļūt saviem personas datiem? Ja atbilde ir “jā”, raksturojiet kārtību, kādā tiek nodrošinātas datu subjekta piekļuves tiesības saviem personas datiem. Ja atbilde ir “nē”, norādiet, kāpēc datu subjekta piekļuves tiesības nav nodrošinātas.	Jā/ Nē	
Kā tiek nodrošināta personas datu atrašana pēc datu subjekta pieprasījuma?		
Vai pārzinim ir tiesības atteikt datu subjektam piekļuvi viņa personas datiem? Ja atbilde ir "jā", norādiet, kādā gadījumā.	Jā/ Nē	
Vai notiek automatizēta lēmumu pieņemšana, pamatojoties uz apstrādātajiem personas datiem? Kādā gadījumā pārzinis pārskata šādus lēmumus?	Jā/ Nē	
5. Personas datu nodošana valstīm, kas nav Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstis, vai valstīm, kuras nav saņēmušas Eiropas Datu aizsardzības kolēģijas atzinumu par adekvātu datu aizsardzības līmeni		

Vai personas dati tiek nodoti valstij, kas nav Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalsts, vai starptautiskajai organizācijai? Ja atbilde ir "jā", norādiet pamatojumu šādai personas datu apstrādei, valsti, kurai dati tiek nodoti, un personas datu veidus, kas tiek nodoti.	Jā/ Nē	
III. Personas datu aizsardzība un drošība		
Kā datu apstrādes procesā tiek nodrošināta konfidencialitāte? Veiciet analīzi attiecībā uz sistēmas darbības ilgtspēju un tās ietekmi uz datu subjekta tiesībām un brīvībām. Ja apstrādē tiek plānots piesaistīt apstrādātājus ,izanalizējiet katru apstrādātāju atsevišķi .		
Raksturojiet aizsardzības pasākumus, kas ir ieviesti pēc neautorizētas un prettiesiskas piekļuves personas datiem, kas ir apstrādāti automatizēti vai manuāli.		
Vai ir izstrādātas informācijas sistēmu piekļuves kontroles procedūras? Ja atbilde ir "jā", kā iestāde pārvalda informācijas sistēmu lietotāju kontus?	Jā/ Nē	
Kādas ir prasības lietotāju kontu parolēm vai citiem kontu aizsardzības rīkiem?		
Vai ir noteikti pienākumi informācijas sistēmu lietotājiem? Kādi?		
Vai pirms informācijas sistēmas nodošanas ekspluatācijā veic drošības atbilstības pārbaudi? Ja atbilde ir "jā", norādiet pārbaudes norises kārtību un personas datu apstrādes pamatus.	Jā/ Nē	
Raksturojiet kārtību, kā tiek nodrošināta datu rezerves kopiju veidošana un pārbaude.		

Vai datu apstrādē izmanto ārējas informācijas sistēmas, kas savienotas ar iestādes informācijas sistēmām? Ja atbilde ir "jā", kāda ir kārtība un nosacījumi, saskaņā ar kuriem izveido sadarbību ar citām iestādēm?	Jā/ Nē	
Kādas tehnoloģijas un rīki tiek izmantoti, lai savienotu sistēmas?		
Vai informācijas sistēmām var piekļūt attālināti? Ja atbilde ir "jā", kāda ir attālinātas piekļuves procedūra un nosacījumi?	Jā/ Nē	
Vai informācijas sistēmā ir nodefinētas lietotāju piekļuves tiesības. Ja atbilde ir "jā", raksturojiet to.	Jā/Nē	
Vai bojātiem datu nesējiem, kas satur personas datus, tiek izdzēsta informācija pirms nesēja nodošanas trešajām personām?		
Vai informācijas sistēmās tiek izmantota datu šifrēšana? Ja atbilde ir "jā", raksturojiet to.	Jā/ Nē	
Vai pirms informācijas publiskošanas tiek izvērtēts tās konfidencialitātes līmenis un iespējamie riski? Ja atbilde ir "jā", raksturojiet to.	Jā/ Nē	

*** Datu apstrādes dzīvescikla dažādo posmu raksturojums**

- **Radi vai saņem**

Šajā fāzē personas dati nonāk organizācijas (pārziņa) rīcībā. Visbiežāk datu avoti ir pats datu subjekts 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.

- **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.

- **Izmantošana**

Pēc izplatīšanas fāzes, kad dati ir nonākuši tiem paredzētajā izmantošanas vietā, tiek uzsākta datu izmantošana atbilstoši to iegūšanas nepastarpinātajam nolūkam. 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.
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);
- arhivē.

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.

**** 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.

Apdraudējumu novērtējums

Nr. p. k.	Apdraudējums	Apraksts	Konfidencialitāte	Integritāte	Pārmērīga pieejamība	Varbūtība	Ietekme	Riska līmenis
Personas datu apstrāde								
1.	Personas datu apstrāde bez likumīga pamata	Personas datu apstrādei nepastāv neviens no Vispārīgās datu aizsardzības regulas 6.pantā noteiktajiem likumīgajiem pamatiem	X		X			
2.	Īpašo kategoriju personas datu apstrāde bez likumīga pamata	Personas datu apstrādei nepastāv neviens no Vispārīgās datu aizsardzības regulas 9.pantā noteiktajiem likumīgajiem pamatiem	X		X			
3.	Personas datu nodošana trešajai personai bez likumīga pamata	Aģentūras rīcībā esošie persona dati tiek nodoti trešajai personai nekonstatējot likumīgu pamatu atbilstoši Vispārīgās datu aizsardzības regulas 6. un/ vai 9. pantam	X		X			
4.	Pārmērīga personas datu apstrāde	Tiek ievākts un apstrādāts lielāks persona datu apjoms nekā tas ir nepieciešamas nolūka sasniegšanai	X	X	X			
5.	Datu subjekta neinformēšana par personas datu apstrādi, ja personas dati tiek iegūti no datu subjekta	Iegūstot datus no datu subjekta, tam netiek sniegta Vispārīgās datu aizsardzības regulas 13. pantā noteiktā informācija.	X		X			
6.	Datu subjekta neinformēšana par personas datu apstrādi, ja dati nav iegūti no datu subjekta	Datu subjektam netiek sniegta Vispārīgās datu aizsardzības regulas 14. pantā noteiktā informācija, ja dati tiek iegūti no trešās personas	X		X			
7.	Personas datu apstrāde neatbilstoši Vispārīgās datu aizsardzības regulas principiem	Personas datu apstrāde tiek veikta, neievērojot šādus principus: 1. likumīgums, godprātība, pārredzamības princips; 2. nolūku ierobežojuma princips; 3. datu minimizēšanas princips; 4. precizitātes princips; 5. glabāšanas ierobežojumu princips; 6. integritāte un konfidencialitātes princips.	X	X				
8.	Nepilnīga personas	Personas dati papīra un	X	X	X			

	datu iznīcināšana	elektroniskā veidā tiek iznīcināti nepilnīgi, kā rezultātā tie var nonākt trešās personas rīcībā						
9.	Personas datu apstrādātāja piesaiste bez pārziņa -apstrādātāja līguma	Ar piesaistīto ārpakalpojumu, kas veic personas datu apstrādi aģentūras uzdevumā nav noslēgts pārziņa – apstrādātāja līgums atbilstoši Vispārīgās datu aizsardzības regulas 28.pantam	X	X	X			
10.	Datu subjekts netiek informēts par automatizētu lēmuma pieņemšanu	Datu subjektam atbilstoši Vispārīgās datu aizsardzības regulas 3. nodaļas ceturtajai iedaļai ir tiesības iebilst pret automatizētu lēmumu pieņemšanu		X	X			
11.	Neatbilstoša datu subjekta piekrišana	Datu subjekta iegūtā piekrišana nav atbilstoša Vispārīgās datu aizsardzības regulas 7. panta prasībām	X		X			
12.	Aģentūrai nav iespējas identificēt informācijas sistēmas lietotāju, kas ir piekļuvis un veicis datu subjekta personas datu apstrādi	Aģentūrai nav iespējas izsekot nodarbināto veiktajām darbībām ar personas datiem, kā arī nav iespējas sagatavot un sniegt atbildi datu subjektam gadījumos, kad datu subjekts ir vērsies pie aģentūras ar informācijas pieprasījumu	X	X				
13.	Neprecīzu personas datu apstrāde	Iegūtie persona dati no datu subjekta vai citas trešās personas ir neprecīzi, kas noved pie nepilnībām aģentūras sniegtajā pakalpojumā datu subjektam		X				
14.	Datu subjekta tiesību neievērošana	Datu subjektam netiek sniegt atbilde uz datu subjekta informācijas pieprasījumu mēneša laikā no pieprasījuma saņemšanas brīža			X			
15.	Personas datu nosūtīšana uz trešām valstīm vai starptautiskām organizācijām bez pietiekamām garantijām	Apstrādātie personas dati tiek nosūtīti uz trešajām valstīm vai starptautiskām organizācijām, neievērojot Vispārīgās datu aizsardzības regulas 45., 46.pantā noteikto.	X		X			
16.	Nepietiekamas nodarbināto zināšanas par personas datu aizsardzību	Netiek nodrošinātas drošības apmācības personām, kas veic datu apstrādi informācijas sistēmās	X	X	X			
Citi								
17.	Nepietiekama kontrole	Nepietiekamas kontroles (tai skaitā, neveikta audita) dēļ laicīgi netiek konstatēti drošības pārkāpumi	X	X	X			
18.	....							

1. Lai noteiktu apdraudējumu, datu aizsardzības speciālistam jānovērtē katra tabulā minētā apdraudējuma varbūtība un apdraudējuma iespējamā ietekme katrai ar „X” apzīmētajai drošības kategorijai atsevišķi.
2. Ja kāds no tabulā iekļautajiem apdraudējumiem nav aktuāls konkrētajai personas datu apstrādei, tad ailē „Varbūtība” ieraksta „0” (nulle) un apdraudējuma novērtējumu neveic.
3. Ja personas datu apstrādes apraksta analīzes laikā tiek identificēti apdraudējumi, kas nav iekļauti

tabulā, novērtē apdraudējumu īstenošanās varbūtību un ietekmi, un apdraudējumu novērtējumu iekļauj risku analīzes rezultātu apkopojumā.

4. Personas datu apstrādes un tās drošības apdraudējuma iestāšanās varbūtības novērtēšanai pielieto skalu no 1 līdz 3:

Vērtība	**Apraksts**
1	Maz ticams, ka apdraudējums īstenosies gada laikā. Esošie pasākumi vai procedūras Personas datu aizsardzības un IS drošības risku novēršanai ir pietiekoši, vai arī apdraudējuma iestāšanās varbūtība ir ļoti zema.
2	Varbūt apdraudējums īstenosies gada laikā. Esošie pasākumi vai procedūras Personas datu aizsardzības un IS drošības risku novēršanai ir vai ir nepilnīgi, vai arī apdraudējuma iestāšanās varbūtība ir vidēja.
3	Iespējams, ka apdraudējums īstenosies gada laikā. Esošie pasākumi vai procedūras Personas datu aizsardzības un IS drošības risku novēršanai ir nepilnīgi vai neeksistē, vai arī apdraudējuma iestāšanās varbūtība ir augsta.

5. Personas datu apstrādes un drošības apdraudējuma ietekmes novērtēšanai pielieto skalu no 1 līdz 3:

Vērtība	**Apraksts**
1	Personas datu apstrādes un tās drošības apdraudējuma iestāšanās gadījumā ietekme uz resursu integritāti, konfidencialitāti, pieejamību, un personas datu apstrādes likumību atbilstoši Vispārīgās datu aizsardzības regulas prasībām ir niecīga.
2	Personas datu apstrādes un tās drošības apdraudējuma iestāšanās gadījumā ietekme uz resursu integritāti, konfidencialitāti, pieejamību, un personas datu apstrādes likumību atbilstoši Vispārīgās datu aizsardzības regulas prasībām ir jūtama.
3	Personas datu apstrādes un tās drošības apdraudējuma iestāšanās gadījumā ietekme uz resursu integritāti, konfidencialitāti, pieejamību, un personas datu apstrādes likumību atbilstoši Vispārīgās datu aizsardzības regulas prasībām ir būtiska.

6. Riska līmeni nosaka sareizinot apdraudējuma iestāšanās varbūtību ar apdraudējuma ietekmes pakāpi:

Riska līmenis	**Apraksts**
No 1 līdz 2	Nenozīmīgs risks. Nav nepieciešama papildus uzmanība. Riska atkārtota novērtēšana jāveic katru gadu.
No 3 līdz 4	Pieņemams risks. Risks jāuzrauga, pēc gada jāveic atkārtota novērtēšana, ieteicams piemērot drošības pasākumus.
No 6 līdz 9	Ievērojams risks. Jāpiemēro pasākumi riska mazināšanai, 6 mēnešu laikā pēc riska mazinošo pasākumu ieviešanas jāveic riska atkārtota novērtēšana.

Novērtējuma par ietekmi uz datu aizsardzību risku analīze

Nr. p.k.	Apdraudējums	Apraksts	Konstatētie fakti	Konfidencialitāte	Integritāte	Pieejamība	Varbūtība	Ietekme	Riska līmenis

Ieviešamie drošības līdzekļi

Nr. p.k.	Apdraudējums	Riska līmenis	Ieviešamais drošības līdzeklis

Risku analīzi <datums> veica:
Amats, vārds, uzvārds _____
Tālr. nr., e-pasts

<*Persona datu apstrādes procesa nosaukums***> drošības pasākumu ieviešanas plāns**

Nr.	Apdraudējums*	Uzdevumi/ Aktivitātes	Rezultāts	Rādītājs	Izpildes termiņš	Finansējums (EUR, KK)	Atbildīgais

* Apdraudējums, kuram riska analīzes laikā sniegti priekšlikumi papildus drošības līdzekļu piemērošanai

Iestādes vai struktūrvienības vadītājs:
Amats, vārds, uzvārds _____
Tālr. nr., e-pasts