



Latvijas Republika

Jelgavas valstspilsētas pašvaldība

Lielā iela 11, Jelgava, LV-3001, tālrunis: 63005535, 63005538, e-pasts: pasts@jelgava.lv

APSTIPRINĀTI

ar Jelgavas valstspilsētas pašvaldības
izpilddirektora vietnieka
28.11.2025. rīkojumu Nr. 341-ri

JELGAVAS VALSTSPILSĒTAS PAŠVALDĪBAS PERSONAS DATU APSTRĀDES NOTEIKUMI

Izdoti saskaņā ar Valsts pārvaldes
iekārtas likuma 72.panta pirmās daļas 2.punktu

1. Noteikumos lietotie termini

- 1.1. Noteikumos lietotie termini, kas ir saistīti ar personas datu apstrādi, atbilst tiem terminiem un jēdzieniem, kas norādīti Eiropas Parlamenta un Padomes Regulā (ES) 2016/679 (2016.gada 27.aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgo datu aizsardzības regulu), ciktāl tie nav definēti atšķirīgi šo noteikumu izpratnē.
- 1.2. *Pārzinis* ir Jelgavas valstspilsētas pašvaldība (turpmāk – Pašvaldība), konkrētās struktūrvienības vai iestādes personā, kas nosaka personas datu apstrādes nolūkus un līdzekļus, kā arī kopumā atbild par personas datu apstrādi saskaņā ar spēkā esošo nacionālo, starptautisko normatīvo aktu prasībām par fizisku personu datu apstrādi.
- 1.3. *Darbinieks* ir Pašvaldības darbinieks, amatpersona, fiziska persona, ar kuru noslēgts uzņēmuma līgums, kā arī Pašvaldības pilnvarotā persona (persona, kura uz pilnvarojuma, līguma vai cita juridiska dokumenta pamata ir tiesīga rīkoties Pašvaldības vārdā) un praktikants, kurš iziet praksi Pašvaldībā.
- 1.4. *Personas dati* ir Pārziņa uzdevumā vai pilnvarojumā, pildot darba pienākumus, līgumsaistības vai cita veida saistības pret Pašvaldību apstrādājami fiziskas personas dati - jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu (“datu subjekts”).
- 1.5. *Datu subjekts* ir fiziska persona, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.
- 1.6. *Īpašo kategoriju personas dati* ir personas dati, kuri atklāj datu subjekta rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, kā arī ģenētiskie dati, biometriskie dati, caur kuriem tiek veikta fiziskas personas unikāla identifikācija, veselības dati vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju.
- 1.7. *Personas datu 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, nosūtīt, izplatīt vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana.

- 1.8. *Apstrādātājs* ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas Pārziņa vārdā apstrādā personas datus, bet nav Pārziņa darbinieks.
- 1.9. *Trešā persona* ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā pilnvarotas apstrādāt personas datus.
- 1.10. *Pašvaldības datu aizsardzības speciālists* (turpmāk – DAS) ir Pārziņa darbinieks, kurš Pašvaldībā veic Vispārīgās datu aizsardzības regulas 39.panta pirmajā daļā noteiktos uzdevumus.
- 1.11. *Procesa īpašnieks* ir Pašvaldības darbinieks, amatpersona vai cita ar rīkojumu pilnvarota persona, kura personas datu apstrādes mērķa izpildes ietvaros atbild par tam pārziņā nodotu procesu (darbību, darbību kopumu).
- 1.12. *Drošība* ir informācijas, t.sk. personas datu, aizsardzība pret neatļautu vai nelikumīgu apstrādi, nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus.
- 1.13. *Drošības incidents* (turpmāk – Incidents) ir kaitīgs notikums vai nodarījums vai vairāki saistīti notikumi, kuru rezultātā tiek apdraudēta informācijas tehnoloģiju, t.sk. personas datu apstrādes sistēmu, integritāte, pieejamība vai konfidencialitāte.
- 1.14. *Integritāte* ir aktuālas, pareizas, pilnīgas un nemainītas informācijas, t.sk. personas datu, saglabāšana, pretrunu neesamība.
- 1.15. *Konfidencialitāte* ir informācijas, t.sk. personas datu, nodošana tikai tām personām, kuras ir pilnvarotas to saņemt un lietot, nepadarot to pieejamu vai atklātu nepilnvarotām personām un/vai Trešajām personām, sistēmām vai procesiem.
- 1.16. *Pieejamība* ir piekļuve informācijai, t.sk. personas datiem, noteiktā apjomā un laikposmā pēc pieprasīšanas.
- 1.17. *Personas datu aizsardzības pārkāpums* (turpmāk – Pārkāpums) ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

2. Noteikumu mērķis un piemērošana

- 2.1. Šie noteikumi (turpmāk – Noteikumi) ir izstrādāti, lai nodrošinātu fizisko personu datu, kas tiek apstrādi Pašvaldībā, drošību, ievērojot regulējošo normatīvo aktu prasības.
- 2.2. Noteikumu mērķis ir:
 - 2.2.1. noteikt Pašvaldības organizatoriskos pasākumus un nepieciešamo tehnisko līdzekļu kopumu, kas nodrošina godprātīgu un likumīgu fiziskas personas datu apstrādi, un tiesības uz savu personas datu aizsardzību ievērošanu;
 - 2.2.2. nodrošināt drošu un normatīvajos aktos noteiktajām prasībām atbilstošu Personas datu apstrādes sistēmu;
 - 2.2.3. nodrošināt vienotas dokumentu sagataves, pielāgojamas atbilstoši nepieciešamībai (izvietotas failu serverī *M:disks/Kopejie/Personu datu noteikumi*).
- 2.3. Noteikumi ir saistoši visiem Pašvaldības darbiniekiem vai citādi ar Pašvaldību saistītajām personām, kuras, veicot darba vai citu saistību pienākumus, apstrādā Personas datus.
- 2.4. Pašvaldības iestāžu vai struktūrvienību vadītāji ir atbildīgi par savā pakļautībā esošo Darbinieku iepazīstināšanu ar šiem Noteikumiem.
- 2.5. Noteikumu pārkāpums ir uzskatāms par līgumsaistību, darba vai amata pienākumu un darba kārtības pārkāpumu (neizpildi), kas var būt par pamatu Darbinieka atbildībai vai disciplināratbildībai saskaņā ar normatīviem aktiem, darba līgumu vai cita veida līgumu, kas noslēgts starp Pašvaldību un Darbinieku.

- 2.6. DAS nodrošina šo Noteikumu un to pielikumu pārskatīšanu atbilstoši nepieciešamībai.

3. Personas datu drošības pamatnosacījumi

- 3.1. Personas dati ir uzskatāmi par ierobežotas pieejamības informāciju, un Trešajām personām tie ir izpaužami vai pieejami apstrādei tikai pastāvot atbilstošam tiesiskajam pamatam un izvērtējot norādīto pamatojumu, kādam mērķim datus plānots izmantot.
- 3.2. Personas datu apstrāde Pašvaldībā netiek veikta bez atbilstoša tiesiskā pamata un apstrādāt atļauts tikai tos Personas datus, kuru apstrādes pamatojums, mērķis un citi parametri ierakstīti Personas datu apstrādes darbību reģistrā.
- 3.3. Pašvaldībā jānodrošina autorizēta piekļuve Personas datiem un iespēja, Datu subjekta pieprasījuma gadījumā, atlasīt informāciju par viņa datu apstrādi.
- 3.4. Pašvaldībā Personas datu apstrādi veic personas, kas ir kompetentas rīkoties un ir parakstījušas rakstveida apliecinājumu par Noteikumu un konfidencialitātes prasību ievērošanu darbā ar Personas datiem un informācijas sistēmām (Noteikumu 1.pielikums), kas tiek glabāts darbinieka lietā, pie pilnvarojuma dokumenta, līguma vai vienošanās.
- 3.5. Par Personas datu aizsardzības un drošības pasākumu ievērošanu atbild visi darbinieki, kam ir pieeja informācijas sistēmām un citā formātā glabātiem Personas datiem, savukārt par drošības procesa pilnveidošanu atbild Pašvaldības iestāžu vai struktūrvienību vadītāji, kuri paši vai ar atbilstoši norīkotu personu starpniecību kontrolē Personas datu apstrādes sistēmu drošību, t.sk, apstrāžu reģistrēšanu atbilstoši Pārzinim noteiktajiem uzdevumiem.
- 3.6. Pašvaldības iestādes vai struktūrvienības vadītājs vai augstākstāvošas institūcijas vadītājs/amatpersona, ja apstrādē iesaistītas vairākas Pašvaldības iestādes ir tiesīgs pieprasīt informāciju par pienākumu izpildi no personām, kuras iesaistītas datu apstrādē un nekavējoties ierobežot piekļuvi informācijas sistēmām vai citā formātā glabātiem Personas datiem, ja persona pārkāpj normatīvos aktus.
- 3.7. Pašvaldībā jānodrošina, ka tiek uzskaitīti un izskatīti Incidenti, kas ir apdraudējuši Pašvaldības informācijas sistēmas vai citā formātā glabātos Personas datus un, ka tiek apstiprinātas galvenās aktivitātes, kas paaugstina Personas datu drošības līmeni.
- 3.8. Ja Pašvaldības funkciju un uzdevumu izpildei ir nepieciešams padarīt pieejamu daļu no Personas datus saturošiem resursiem, šo pieeju jākontrolē, ja iespējams, veicot datu pseidonimizēšanu (personas identifikatoru aizstāšana ar sasaistes kodiem) un padarot pieejamu iespējami minimālu Personas datu apjomu.
- 3.9. Personas datus, kas vairs nav nepieciešami noteiktā mērķa sasniegšanai, jāiznīcina vai jāveic to anonimizēšana (personas identifikatoru neatgriezeniska iznīcināšana vai pārveidošana par anonīmiem datiem), elektronisku informāciju iznīcinot tā, lai nebūtu iespējams atjaunot informācijas failus, savukārt informāciju papīra formātā iznīcina tā, lai nebūtu atjaunojama tajos esošā informācija.
- 3.10. Izpaužot datus Trešajām personām, jānodrošina informācijas glabāšana par datu izpaušanas laiku, apjomu, personu, kas tos pieprasījusi, nodevusi, saņēmusi.
- 3.11. Pašvaldībā jānodrošina, ka Personas datu vākšanu, ierakstīšanu, ierakstītās informācijas sakārtošanu, saglabāšanu, kopēšanu, pārrakstīšanu, pārveidošanu, labošanu, dzēšanu, iznīcināšanu, arhivēšanu, rezerves kopēšanu, bloķēšanu veic tikai kompetentās personas un/vai personas datu apstrādātājs, ar ko noslēgts rakstveida līgums, kā arī nodrošina iespēju noteikt tos Personas datus, kuri ir bijuši apstrādāti bez attiecīgā pilnvarojuma, kā arī apstrādes laiku un personu, kas to veikusi.
- 3.12. Pašvaldībai kā darba, prakses devējam jāveic darbinieku, pilnvaroto personu, praktikantu informēšana un apmācības pirms attiecīgo pienākumu uzsākšanas, nodrošinot, ka tie apzinās Personas datu drošības nozīmību un iespējamos draudus un ir pietiekami kvalificēti, lai ievērotu noteiktās drošības prasības.
- 3.13. Darbiniekiem veicot darba pienākumus ir pēc iespējas jāsamazina risks, ka Personas dati viņa rīcības dēļ var nonākt citu personu rīcībā: kļūda, zādzība, neuzmanība informācijas nodošanā vai nepareiza informācijas resursu lietošana.

4. Tiesības un pienākumi veicot Personas datu apstrādi

- 4.1. Darbiniekam veicot fizisko personu datu apstrādi ir šādas tiesības un pienākumi:
- 4.1.1. apstrādāt Personas datus tikai savas kompetences ietvaros uzdoto uzdevumu izpildei, ievērojot šajos Noteikumos un citos saistošajos normatīvajos aktos noteikto kārtību;
 - 4.1.2. lietot atbilstošus tehniskos un organizatoriskos līdzekļus, kas nodrošina datu aizsardzību un novērš to nelikumīgas iegūšanas iespējamību;
 - 4.1.3. ievērot Pašvaldībā apstiprinātos dokumentus, dokumentu paraugus attiecībā uz Personas datu apstrādi;
 - 4.1.4. lūgt tiešajam vadītājam skaidrot jautājumus attiecībā uz amata, darba pienākumu izpildes ietvaros veicamo Personas datu apstrādi, to pamatojumu, raksturu, apjomu, kā arī patstāvīgi sazināties par Personas datu apstrādes jautājumiem ar DAS un lūgt konsultāciju;
 - 4.1.5. pēc tiešā vadītāja vai DAS pieprasījuma sniegt pilnīgu, visaptverošu informāciju par amata pienākumu vai uzdevumu izpildes ietvaros veicamo Personas datu apstrādi un ievērot DAS norādījumus Personas datu apstrādē;
 - 4.1.6. nodot jautājuma risināšanu, lēmuma pieņemšanu tiešajam vadītājam, ja Darbinieks nepiekrīt DAS norādījumiem vai pienākumu izpildes procesā Personas datu apstrāde notiek atšķirīgi no DAS norādītā un Darbiniekam nav iespējas veikt izmaiņas;
 - 4.1.7. nekavējoties informēt tiešo vadītāju, ja konstatē vai ir pamatotas aizdomas, ka Personas datu apstrādē ir neatbilstības vai pretrunas ar normatīvajiem aktiem vai Personas datu apstrādes darbību reģistrā, noteiktajam;
 - 4.1.8. pieprasīt tehnisko nodrošinājumu un piekļuvi informācijas resursiem, kas nepieciešami darba pienākumu pildīšanai un šo Noteikumu realizēšanai;
 - 4.1.9. Personas datu apstrādes laikā nodrošināt, ka apstrādājamie dati nav pieejami Trešajām personām un bez tiesiska pamata neizpaust tos, t.sk. arī pēc darba tiesisko attiecību vai līgumattiecību izbeigšanas ar Pašvaldību. Šādam pienākumam ir beztermiņa raksturs;
 - 4.1.10. reģistrēt Personas datu nodošanas un saņemšanas faktu Pašvaldības noteiktā kārtībā, izņemot ja šāda datu nodošana tiek reģistrēta ar automātiskiem līdzekļiem;
 - 4.1.11. ierosināt jaunas informācijas iekļaušanu vai attiecīgu izmaiņu veikšanu Personas datu apstrādes reģistrā;
 - 4.1.12. aizliegts izpaust ziņas par izmantojamās informācijas sistēmas uzbūvi un konfigurāciju, fiziskās un loģiskās Personas datu aizsardzības līdzekļiem, kā arī atklāt Personas datus nepilnvarotām personām un/vai Trešajām personām, izņemot šajos Noteikumos noteiktos gadījumos. Pirms Personas datu izpaušanas nepieciešams veikt informācijas saņēmēja identificēšanu, pārliecināties par informācijas saņēmēja pilnvarojumu vai tiesībām saņemt Personas datus, šaubu gadījumā neveicot Personas datu saturošas informācijas izplatīšanu un ziņojot par nepamatotiem Personas datu saturošas informācijas pieprasījumiem Pašvaldības vadībai un DAS;
 - 4.1.13. nest atbildību par informācijas sistēmās un citā formātā glabātiem Personas datiem, kas nodoti viņa rīcībā, kā arī par citiem dokumentiem, kas nepieciešami darba pienākumu vai citu saistību pildīšanai;
 - 4.1.14. aizliegts darbiniekam nodotos informācijas resursos izmantot nelicencētu Informācijas tehnoloģiju programmatūru un izdarīt pret informācijas sistēmu drošību vērstas darbības un izmantot neparedzētas pieslēgšanās iespējas;
 - 4.1.15. pārtraucot darbu ar informācijas resursiem, informācijas sistēmām, kurās apstrādā Personas datus, tiek aizvērta pārlūkprogramma, savukārt, ja Personas datu apstrāde notiek, izmantojot papīra dokumentus, - tos novietot atbilstošā glabāšanas vietā;

- 4.1.16. ja nav uzdots konkrēts pienākums, aizliegts saņemt Personas datus pārveidot, atsavināt, reproducēt to kopumā vai tās daļas, izmantot to citu datu apstrādes sistēmu izveidei, kā arī glabāt publiski pieejamās vietās bez uzraudzības;
- 4.1.17. bez kavēšanās ziņot Pašvaldībai Noteikumos norādītā kārtībā, ja ir aizdomas par riskiem informācijas sistēmai un citā veidā apstrādātiem personas datiem, par bojājumiem informācijas sistēmai, par paroles iespējamu nonākšanu Trešo personu rīcībā un citām situācijām, kas var radīt riskus Personas datu drošībai;
- 4.1.18. aizliegts veikt personas datu apstrādi, t.i. izpaust, nodot Personas datus ārpus Eiropas Savienības vai Eiropas Ekonomiskās Zonas (trešajās valstīs vai starptautiskās organizācijās) bez papildus izvērtējuma un Vispārīgā datu aizsardzības regulā noteiktā pamatojuma esamības (piem., personas datu saņēmēja valsts nodrošina adekvātu personas datu aizsardzības līmeni; noslēgts sadarbības līgums ar Eiropas Komisijas apstiprinātu standarta klauzulām, saņēmējs sniedz adekvātas garantijas Personas datu aizsardzībai, t.sk. 'Binding Corporate Rules' esamība, saņēmējs pievienojies rīcības kodeksam vai sertifikācijas mehānismiem, saņemta datu subjekta piekrišana, nodošana izriet no ar datu subjektu noslēgta līguma, nepieciešama tiesvedībā u.c.). Personas datu nodošana ārpus Eiropas Savienības (trešajās valstīs vai starptautiskās organizācijās) rakstiski saskaņojuma ar pašvaldības DAS;
- 4.1.19. izteikt priekšlikumus Personas datu aizsardzības sistēmas uzlabošanai, pilnveidošanai un tās atbilstības nodrošināšanai normatīvajos aktos noteiktajām prasībām, par to informējot Pašvaldības vadību un DAS.
- 4.2. Struktūrvienības, iestādes vadītājam papildus Darbinieka tiesībām un pienākumiem ir šādas tiesības un pienākumi:
 - 4.2.1. nodrošināt veicamās datu apstrādes atbilstību normatīvajos aktos noteiktajām prasībām, t.sk. veikt nepieciešamās izmaiņas darba organizācijas dokumentos;
 - 4.2.2. Personas datu apstrādes jautājumu risināšanā piesaistīt citus speciālistus, struktūrvienību, iestāžu darbiniekus, vadītājus, to kompetences ietvaros;
 - 4.2.3. sniegt atbildes uz padotībā esošo Darbinieku jautājumiem par datu apstrādi un savas kompetences ietvaros iesaistīties Personas datu apstrādes jautājumu risināšanā, t.sk. arī, ja izteikts citas struktūrvienības vai iestādes pamatots lūgums;
 - 4.2.4. atbilstoši Noteikumos noteiktajai procedūrai, nodrošināt pakļautībā esošā Darbinieka sagatavotās informācijas par jaunu datu apstrādi vai izmaiņām iekļaušanu Personas datu apstrādes darbību reģistrā, pirms tam izvērtējot to un attiecīgi saskaņojot vai pamatoti noraidot piedāvātos papildinājumus, izmaiņas;
 - 4.2.5. vismaz reizi gadā pārvērtēt Personas datu apstrādes darbību reģistrā fiksēto apstrāžu atbilstību faktiskajiem Personas datu apstrādes procesiem.
- 4.3. Procesa īpašniekam, papildus Darbinieka tiesībām un pienākumiem ir šādas tiesības un pienākumi attiecībā uz pārziņā nodotiem procesiem:
 - 4.3.1. nodefinēt/ pārskatīt atbildībā nodoto datu apstrāžu mērķus (to būtiskumu, nepieciešamību utt.);
 - 4.3.2. izveidot/ pārskatīt atbildībā nodoto apstrāžu regulējošās procedūras/ instrukcijas/ politikas;
 - 4.3.3. izveidot/pārskatīt datu subjektu informēšanas mehānismus (piem., datu apstrādes paziņojumus, veidlapas, noteikumi);
 - 4.3.4. izvērtēt saņemtos datu subjektu pieprasījumus (dzēst, labot, iebilst, saņemt informāciju u.c.) un nodrošināt atbilžu sniegšanu uz tiem;
 - 4.3.5. izvērtēt saņemtās Personas datu apstrādes sūdzības un nodrošināt atbilžu sniegšanu;
 - 4.3.6. izvērtēt un nodrošināt atbilstošu sadarbības partneru (apstrādātāju) izvēli, līguma noslēgšanu un uzraudzību;
 - 4.3.7. piedalīties Incidentu izvērtēšanā, risku identificēšanā, seku minimizēšanā un nākotnes pasākumu izstrādē, lai nepieļautu turpmāku risku iestāšanos, kā arī sekot šo veicamo darbu izpildei;

- 4.3.8. sekot līdzi apstākļu un normatīvo aktu izmaiņām, kas varētu ietekmēt Personas datu apstrādi attiecīgajam mērķim, un izmaiņu gadījumā pārbaudīt apstrādājamo Personas datu veidu aktualitāti un, ja nepieciešams, veikt nepieciešamās izmaiņas;
- 4.3.9. sava procesa ietvaros, nodrošināt iesaistīto personu apmācību nodrošināšanu;
- 4.3.10. pēc nepieciešamības iniciēt un nodrošināt Novērtējuma par ietekmi uz datu aizsardzību veikšanu;
- 4.3.11. noteikt darbinieku kategorijas, kurām ir tiesības piekļūt konkrētiem Personas datiem;
- 4.3.12. sadarbībā ar citām struktūrvienībām izstrādāt atbildībā nodotajai datu apstrādei atbilstošus tehniskos un organizatoriskos pasākumus.

5. Personas datu apstrādes organizēšana

5.1. Personas datu apstrādes reģistrs.

- 5.1.1. Pašvaldībā jānodrošina ar Personas datiem veikto darbību uzskaiti, izmantojot informācijas sistēmas funkcionalitāti vai nodrošinot vispārīgu uzskaiti Personas datu apstrādes darbību reģistrā (turpmāk - Reģistrs), kur elektroniski uzskaita gan Pašvaldības kā Pārziņa veiktās datu apstrādes, gan apstrādes, kas Pašvaldībā tiek veiktas kā Personas datu apstrādātāja uzdevumā. Reģistrā norādāma vismaz tā informācija, kas uzskaitīta Noteikumu 2.pielikuma parauga formā.
- 5.1.2. Par šāda Reģistra uzturēšanu, t.i. par informācijas apkopošanu, ievadīšanu un regulāru pārskatīšanu, papildināšanu atbilstoši faktiskai apstrādei ir atbildīgs iestādes vai struktūrvienības vadītājs vai viņa norīkots atbildīgais darbinieks.
- 5.1.3. DAS nepieciešamības gadījumā sniedz ieteikumus Reģistra uzlabošanai.

5.2. Personas datu apstrādes uzsākšana jauniem mērķiem vai grozījumu veikšana esošajos.

- 5.2.1. Pirms Personas datu apstrādes uzsākšanas jauniem mērķiem iestādes vai struktūrvienības vadītājs vai augstākstāvošas institūcijas vadītājs/amatpersona, ja apstrādē iesaistītas vairākas Pašvaldības iestādes, atbilstoši Noteikumu 3.pielikuma paraugam, ar rīkojumu nosaka:
 - 5.2.1.1. datu apstrādes mērķi/us un tiesisko pamatu;
 - 5.2.1.2. par personas datu apstrādi atbildīgās personas, t.sk. Procesā īpašnieku/us, kas atbild par konkrētiem datu apstrādes procesiem, izvērtē un uzskaita riskus apstrādei, un, ja nepieciešams, organizē, ka tiek veikts novērtējums par datu apstrādes ietekmi uz datu aizsardzību (turpmāk – Novērtējums), atbilstoši Noteikumu 4.pielikuma paraugam un pārziņa leģitīmās intereses izvērtējums, atbilstoši Noteikumu 5.pielikuma paraugam, ja tiesiskais pamats datu apstrādei ir leģitīmā interese;
 - 5.2.1.3. personu loku, kurai būtu nepieciešams piekļūt informācijai;
 - 5.2.1.4. datu glabāšanas termiņus/ dzēšanas kritērijus;
 - 5.2.1.5. datu apstrādē izmantojamus tehniskos resursus un organizatoriskos pasākumus risku mazināšanai, ja tie atšķiras no kopējiem pasākumiem.
- 5.2.2. Procesā īpašnieki regulāri, bet ne retāk kā reizi gadā, pārvērtē datu apstrādes riskus un nodrošina, ka par apstrādes izmaiņām tiek veikts ieraksts Reģistrā.
- 5.2.3. Jaunu, Reģistrā neuzskaitītu personas datu apstrādes mērķu ieviešana vai grozījumu veikšana esošos mērķos ir jāsaskaņo ar DAS. Savstarpējai saskaņošanai iespējams izmantot Noteikumu 6.pielikuma reģistrācijas veidlapas paraugu.
- 5.2.4. Personas datu apstrāde tiek veikta Pašvaldības telpās, vai citā vietā saskaņā ar Pašvaldības vajadzībām un norādījumiem, nepieciešamības gadījumā, pirms apstrādes uzsākšanas, noslēdzot rakstveida līgumu ar Personas datu apstrādātāju.

5.3. Novērtējuma par ietekmi uz datu aizsardzību veikšanas kārtība.

- 5.3.1. Pirms apstrādes uzsākšanas (plānošanas/ izstrādes procesā) jānodrošina plānotās datu apstrādes ietekmes uz fizisko personu datu aizsardzību novērtēšana, ja jaunais apstrādes veids, jo īpaši, izmantojot inovatīvas tehnoloģijas un ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, varētu radīt augstu risku fizisku personu

- tiesībām un brīvībām, vai šī apstrāde ir minēta Datu valsts inspekcijas sarakstā kā datu apstrāde, kurai obligāti jāveic Novērtējums, tostarp:
- 5.3.1.1. datu saistībā ar sodāmību, noziedzīgiem nodarījumiem apstrāde un sensitīvu datu apstrāde, t.i. īpašo kategoriju personas datu, t.sk. biometrijas datu apstrāde ar mērķi identificēt fizisku personu;
 - 5.3.1.2. sistematiska uzraudzība, lai novērotu, novērtētu, uzraudzītu vai kontrolētu datu subjektus, tostarp tīmeklī iegūtus datus (sīkdatnes), publiski pieejamas zonas sistematiskas uzraudzības datus (videonovērošana), u.tml.;
 - 5.3.1.3. datu apstrāde attiecībā uz īpaši aizsargājamiem datu subjektiem (bērni, sociāli mazāk aizsargātas cilvēku kategorijas) plašā mērogā;
 - 5.3.1.4. personas datu apstrāde plašā mērogā un automatiska datu apstrāde, profilēšana;
 - 5.3.1.5. datu apstrāde izmantojot inovatīvas tehnoloģijas, mehānismus un metodes kopā ar kādu citu kritēriju;
 - 5.3.1.6. datubāžu apvienošana, automatizēta lēmumu pieņemšana, kuru pamato ar juridisku vai līdzīgu būtisku ietekmi u.c.
- 5.3.2. Novērtējumā iekļaujama vismaz šāda informācija:
- 5.3.2.1. plānoto apstrādes darbību un apstrādes nolūku, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistematisks apraksts;
 - 5.3.2.2. novērtējums par darbību nepieciešamību un samērīgumu attiecībā uz nolūkiem;
 - 5.3.2.3. novērtējums par iespējamiem riskiem datu subjektu tiesībām un brīvībām;
 - 5.3.2.4. pasākumi, kas paredzēti risku novēršanai, tostarp garantijas, drošības pasākumi un mehānismi, ar ko nodrošina personas datu aizsardzību un uzskatāmi parāda, ka ir ievērots normatīvais regulējums, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses.
- 5.3.3. Pēc iespējas Novērtējumā iekļauj arī trūkumu būtiskuma novērtējumu, iedalot trūkumus ‘Augsta riska’, ‘Vidēja riska’, ‘Zema riska’ kategorijās.
- 5.3.4. Pēc Novērtējuma veikšanas Novērtējuma veicējs sagatavo kopsavilkumu, kur norāda konstatētos trūkumus, kā arī trūkumu novēršanas plānu, ko pirms iesniegšanas vadībai saskaņo ar DAS.
- 5.3.5. Ja pēc Novērtējuma veikšanas un papildus datu aizsardzības pasākumu ieviešanas, joprojām datu apstrādei saglabājas augsts risks, Pašvaldībai jāinformē par šādu datu apstrādi nacionālā uzraudzības iestādē – Datu valsts inspekcija un jāapspriežas par apstrādes veikšanas apstākļiem, pieteikumā norādot:
- 5.3.5.1. pārziņa, kopīgo pārziņu un piesaistīto apstrādātāju attiecīgos pienākumus;
 - 5.3.5.2. paredzētās apstrādes nolūkus un līdzekļus;
 - 5.3.5.3. pasākumus, garantijas datu subjektu tiesību/brīvību aizsardzības nodrošināšanai;
 - 5.3.5.4. DAS kontaktinformāciju;
 - 5.3.5.5. sagatavoto Novērtējumu par ietekmi uz datu aizsardzību u.c. nepieciešamo informāciju.
- 5.3.6. Pašvaldībā Novērtējuma veikšanu organizē, to glabā un kontrolē noteikto trūkumu novēršanu, kā arī izvērtē un nosaka laika periodu pēc kura Novērtējums ir jāveic atkāroti konkrētās datu apstrādes Procesa īpašnieks, vai cits darbinieks, ko noteicis Pašvaldības iestādes/ struktūrvienības vadītājs vai augstākstāvošas institūcijas vadītājs/amatpersona, ja apstrādē iesaistītas vairākas Pašvaldības iestādes.
- 5.4. Personas datu nodošana un saņemšana.
- 5.4.1. Pašvaldībā ir aizliegts kopēt Personas datus saturošus failus uz ārējiem datu nesējiem, izņemot, ja tam ir saņemta tiešā vadītāja vai citas kompetentās personas atļauja.
 - 5.4.2. Personas datu pārsūtīšanu, pēc iespējas, veic šifrētā veidā, nodrošinot pārsūtāmās informācijas aizsardzību izmantojot atbilstošus tehniskos rīkus, kā, piemēram, unikālu paroli, kura pieejama tikai informācijas adresātam.
 - 5.4.3. Personas datus, kas fiksēti papīra formātā, Pašvaldībā glabā slēgtā dokumentu glabātuvē, kurai nodrošināta pieeja tikai kompetentajām personām.

- 5.4.4. Aizliegts personas datus saturošus dokumentus vai to projektus atstāt vietās, kur tiem var piekļūt citi darbinieki, personas, kas nav tiesīgi apstrādāt datus, piemēram, atstājot dokumentus nekontrolēti uz savas darba vietas galda, kopējā printerī, u.tml.
- 5.5. Personas datu glabāšana.
- 5.5.1. Iestādes, struktūrvienības vadītājs nosaka savā atbildībā esošo Personas datu glabāšanas termiņus, atbilstoši normatīvajos aktos noteiktajām prasībām un principam, ka Personas dati tiek glabāti tikai konkrētā mērķa sasniegšanai nepieciešamo minimālo laika periodu un minimālā apjomā, kamēr ir pamatota nepieciešamība to glabāšanai.
- 5.5.2. Personas datus, kas iekļauti elektroniskos un papīra formāta dokumentos, glabā atbilstoši lietu nomenklatūrā noteiktajiem glabāšanas termiņiem, kas tiek regulāri pārskatīti, lai nodrošinātu atbilstoša un pamatota glabāšanas termiņa noteikšanu.
- 5.5.3. Izvērtējot Personas datu glabāšanas termiņus ņem vērā vismaz šādus aspektus:
- 5.5.3.1. dati tiek glabāti tik ilgi, cik tie nepieciešami datu apstrādes nolūka sasniegšanai;
 - 5.5.3.2. dati tiek glabāti atbilstoši normatīvajos aktos noteiktajiem glabāšanas termiņiem;
 - 5.5.3.3. dati tiek uzglabāti noteikto noilguma periodu, kamēr nepieciešams nodrošināt pierādījumu saglabāšanu;
 - 5.5.3.4. datus no dokumentiem nedrīkst dzēst, ja tādējādi tiek ietekmēts dokumenta juridiskais spēks;
- 5.5.4. Pēc glabāšanas termiņa beigām Personas datus saturoši dokumenti tiek iznīcināti vai atsevišķos gadījumos nodoti valsts arhīvam. Par datu dzēšanas īstenošanu atbild katra Procesa īpašnieks vai Pašvaldības iestādes vai struktūrvienības vadītājs, vai Apstrādātājs, kura pārziņā atrodas atbilstošie dati.
- 5.6. Personas datu dzēšana.
- 5.6.1. Darbinieks vai Apstrādātājs nav tiesīgs turpināt veikt Personas datu apstrādi, ja vairs nepastāv Personas datu apstrādes tiesiskais pamats.
- 5.6.2. Aizliegts nodot (atsavināt) Trešajām personām informācijas tehnoloģiju iekārtas, ja tās satur Personas datus. Ja informācijas tehnoloģiju iekārtai nepieciešams garantijas remonts, pirms nodošanas remontā ir jānodrošina tajā esošo Personas datu drošība.
- 5.6.3. Personas datus, kas ir kļuvuši nepilnīgi, novecojuši, nepatiesi, pretlikumīgi apstrādāti (bez tiesiskā pamatojuma) vai arī tie vairs nav nepieciešami Pašvaldībā noteiktajam apstrādes mērķim, nekavējoties labo, precizē vai dzēš un par to, pēc iespējas, informē personas, kurām iepriekš nosūtīti apstrādātie Personas dati.
- 5.6.4. Izbeidzot Personas datu apstrādi un iestājoties glabāšanas termiņa beigām, Personas dati no informācijas sistēmām ir neatgriezeniski jādzēš vai, ja to nav iespējams veikts, sadarbībā ar informācijas tehnoloģiju speciālistu jānodrošina Personas datu anonimizācija.
- 5.6.5. Personas datus saturoši papīra dokumenti vai to projekti pēc datu apstrādes un glabāšanas termiņa beigām tiek iznīcināti izmantojot papīra griezēju vai nodoti centralizētais dokumentu iznīcināšanai.
- 5.6.6. Personas datus saturoši tehniskie resursi (USB, CD, HDD u.c.) pēc to izmantošanas nepieciešamības beigām, tiek nodoti informācijas tehnoloģiju speciālistam, kas iznīcina tehniskos resursus tā, lai nebūtu iespējama uzglabātās un dzēstās informācijas atjaunošana.
- 5.7. Personas datu izpaušana.
- 5.7.1. Personas datu izpaušanu Trešajām personām Pašvaldībā veic tikai atbilstoša tiesiskā pamata un motivēta pieteikuma esamības gadījumā.
- 5.7.2. Izpaužot Personas datus, t.sk., valsts un pašvaldību amatpersonām un darbiniekiem, pirms tam jāveic personu identificēšana, izvērtējot norādīto Personas datu izmantošanas mērķi, ja normatīvajos aktos nav noteikts citādi.

- 5.7.3. Aizliegts bez attiecīga pilnvarojuma pavairot dokumentus, kuri satur Personas datus. Pavairošanas gadījumā fakta fiksēšanu nodrošina informācijas sistēma vai persona, kuras pārraudzībā ir nodota attiecīgo datu pārraudzība.
- 5.7.4. Ja Personas dati tiek izpausti saņēmējam, kurš atrodas ārpus Eiropas Savienības vai Eiropas Ekonomiskās Zonas, jānodrošina papildus izvērtējumus, identificējot papildu Vispārīgā datu aizsardzības regulā noteiktā pamatojuma esamību (piem., Personas datu saņēmēja valsts nodrošina adekvātu personas datu aizsardzības līmeni, saņēmējs sniedz adekvātas garantijas Personas datu aizsardzībai, t.sk. 'Binding Corporate Rules' esamība, ar Eiropas Komisijas apstiprinātu standarta klauzulām noslēgts sadarbības līgums, saņēmējs pievienojies rīcības kodeksam vai sertifikācijas mehānismiem, saņemta datu subjekta piekrišana, nodošana izriet no ar datu subjektu noslēgta līguma, nepieciešama tiesvedībā u.c.).

6. Personas datu nodošana Apstrādātājam

- 6.1. Personas datu apstrādi var uzdot veikt Personas datu apstrādātājam (turpmāk – Apstrādātājs), ja sadarbība tiek veikta ievērojot šajos Noteikumos noteikto kārtību un citus personas datu apstrādi regulējošos normatīvos aktus.
- 6.2. Pirms sadarbības uzsākšanas ar Apstrādātāju, atbildīgie darbinieki pārliecinās par apstrādes tiesiskā pamatojuma esamību un Apstrādātāja spējām nodrošināt nodoto Personas datu drošību, nepieciešamības gadījumā izmantojot Noteikumu 7.pielikuma izvērtēšanas anketas paraugu un, ņemot vērā Apstrādātājam nodoto personas datu raksturu, apjomu un apstrādes būtību, veic pārbaudes, lai pārliecinātos, kā tās ievēro Pašvaldības kā Pārziņa dotos norādījumus drošas apstrādes nodrošināšanai.
- 6.3. Pirms Personas datu apstrādes nodošanas Apstrādātājam, vienmēr slēdzams rakstveida līgums, kurā pēc iespējas iekļaujami normatīvajos aktos noteiktie Apstrādātāja pienākumi, tostarp nosacījumi, kas uzskaitīti šo Noteikumu 8. pielikuma paraugā "Tipveida noteikumi par personas datu apstrādi", pielāgojot tos konkrētajam līgumam. Pakalpojuma sniedzēja piedāvātais līgums ir izmantojams, ja tajā iekļautie nosacījumi nav pretrunā Pašvaldības un normatīvo aktu prasībām.
- 6.4. Nav pieļaujama neizvērtētu apakšapstrādātāju piesaiste, izņemot gadījumus, kad, ar Procesu īpašnieka piekrišanu, līgumā ar Apstrādātāju nosaka, ka Pašvaldība tiks informēta pēc apakšapstrādātāja piesaistes, paredzot iespēju Pašvaldībai nepieciešamības gadījumā vienpusēji izbeigt līgumu pirms termiņa.
- 6.5. Pašvaldībā jāuzskaita Apstrādātājiem nodotās apstrādes, atbilstoši Noteikumu 9.pielikuma paraugam, uzskaitot vismaz Apstrādātāja nosaukumu, reģistrācijas numuru, adresi, kontaktpersonas, datu veidus un informāciju par līguma termiņu ievērošanas kontroli, datu apstrādes vietu un noteiktajām tehniskajām un organizatoriskajām prasībām, kā arī atbildīgo personu par sadarbību ar konkrēto Apstrādātāju.
- 6.6. Ja Personas dati tiek izpausti Apstrādātājam, kurš atrodas vai apstrādā datus ārpus Eiropas Savienības vai Eiropas Ekonomiskās Zonas, jānodrošina izvērtējums, identificējot papildu Vispārīgā datu aizsardzības regulā noteiktā pamatojuma esamību (piem., Personas datu saņēmēja valsts nodrošina adekvātu personas datu aizsardzības līmeni, saņēmējs sniedz adekvātas garantijas Personas datu aizsardzībai, t.sk. 'Binding Corporate Rules' esamība, ar Eiropas Komisijas apstiprinātu standarta klauzulām noslēgts sadarbības līgums, saņēmējs pievienojies rīcības kodeksam vai sertifikācijas mehānismiem, saņemta datu subjekta piekrišana, nodošana izriet no ar datu subjektu noslēgta līguma, nepieciešama tiesvedībā u.c.).

7. Datu subjektu pieprasījumu apstrāde

7.1. Vispārīgie Datu subjekta pieprasījumu apstrādes noteikumi:

- 7.1.1. Respektējot normatīvajos aktos noteiktās Datu subjektu tiesības, Pašvaldībā tiek pieņemti rakstiski iesniegumi no identificējamiem Datu subjektiem par Personas datu saturošas informācijas sniegšanu, nodrošinot Datu subjektam pieejamu standartizētu tipveida Datu subjekta pieprasījuma veidlapu (Noteikumu 10.pielikums) vai arī iespēju pieprasījumus saņemt citās formās.
- 7.1.2. Visa komunikācija ar Datu subjektu, t.sk. informācijas izsniegšana ir veicama bez maksas, izņemot, ja pieprasījums ir acīmredzami nepamatots vai pārmērīgs. Šādā gadījumā var atteikt izpildīt pieprasījumu vai pieprasīt izmaksās pamatotu saprātīgu maksu, kas saistīta ar informācijas sniegšanas nodrošināšanu.
- 7.1.3. Atbilde uz Datu subjekta pieprasījumu tiek sniegta ne vēlāk kā 1 (viena) mēneša laikā, izņemumu gadījumā, par to informējot Datu subjekta pieprasījuma iesniedzēju, termiņu var pagarināt līdz 3 (trīs) mēnešiem, ja pieprasījums ir sarežģīts un nav izpildāms 1 (viena) mēneša laikā.
- 7.1.4. Katra Pašvaldības iestāde, izmantojot informācijas sistēmas funkcionalitāti vai Noteikumu 11.pielikuma paraugu, nodrošina Datu subjektu pieprasījumu un to izpildes uzskaiti - reģistrēšanu, tādējādi kontrolējot atbilžu sagatavošanas termiņus un fiksējot tos pieprasījumus, kuriem iespējams pieprasīt izmaksās balstītu samaksu. Ik gadu līdz attiecīgā kalendārā gada beigām, neminot pieprasītāja identitāti un citus personas datus, iestādes, struktūrvienības vadītājs vai viņa norīkots atbildīgais darbinieks informē DAS par fiksētiem Datu subjektu pieprasījumiem un to izpildi.

7.2. Datu subjekta identifikācija un pieprasījumu iesniegšanas un atbildes sniegšanas veidi.

- 7.2.1 Datu subjekts pieprasījumu var iesniegt Pašvaldībā personīgi klātienē, nosūtot pa pastu vai elektroniski - izmantojot iestādes e-pastu vai Vienotajā valsts un pašvaldību pakalpojumu portālā www.latvija.lv aktivizētu e-adreses kontu.
- 7.2.2. Papīra formātā (klātienē vai pa pastu) iesniegtam pieprasījumam jābūt jābūt pašrocīgi parakstītam, elektroniskā veidā iesniegtam pieprasījumam - ar drošu elektronisko parakstu, klāt pievienojot pārstāvību apliecinājošu dokumentu, kurā paredzētas Trešās personas tiesības pieprasīt šādu informāciju, ja pieprasījumu Datu subjekta vārdā iesniedz Trešā persona.
- 7.2.3. Atbildīgais darbinieks pārliecinās par tās personas identitāti par kuru ir iesniegts Datu subjekta pieprasījums. Ja Datu subjektu nav iespējams identificēt, iesniedzējam tiek lūgts sniegt papildus informāciju, lai Datu subjektu identificētu.
- 7.2.4. Saņemot Datu subjekta pieprasījumu par pieprasījuma izpildi atbildīgais darbinieks pārbauda vai Pašvaldības rīcībā ir attiecīgā Datu subjekta personas dati un, ja netiek konstatēts, ka Pašvaldības rīcībā ir Datu subjekta personas dati, sagatavo atbildi, norādot, ka Pašvaldībā nav konstatēta Datu subjekta datu apstrāde.
- 7.2.5. Ņemot vērā atbildes saturā ietvertos Personas datus un to sensitivitāti, atbilde uz Datu subjekta pieprasījumu var tikt izsniegta Pašvaldībā klātienē, personu identificējot, vai nosūtot pa pastu, ierakstītā vēstulē, lai nodrošinātos, ka atbildi saņem attiecīgā persona, vai elektroniski, izmantojot e-pastu vai Vienotajā valsts un pašvaldību pakalpojumu portālā www.latvija.lv aktivizētu e-adresi.
- 7.2.6. Lai izvairītos no Personas datu nonāksšanas Trešo personu rīcībā, jāizvērtē Datu subjekta norādītais atbildes saņemšanas veids, ņemot vērā sniegtās informācijas apjomu, personas identifikācijas iespējamību un datu saņemšanas kanāla drošumu.

7.3. Saņemot Datu subjekta pieprasījumu piekļūt saviem datiem jeb iegūt par sevi informāciju:

- 7.3.1. atlasa Pašvaldības rīcībā esošos personas datus, t.sk. pārbauda Pašvaldības datu bāzēs esošo informāciju, uz serveriem un papīra formātā esošo informāciju (piemēram, klienta vai darbinieka lietu) un citas informācijas glabāšanas vietas;
- 7.3.2. pārliecinās, ka apkopotā informācija nesatur Trešo personu (citu Datu subjektu) datus, ja nepieciešams sagatavot Datu subjekta pieprasīto datu kopijas. Šajā gadījumā šie dati būtu dzēšami un nebūtu izsniedzami Datus subjektam šo tiesību ietvaros.
- 7.4. Saņemot Datu subjekta pieprasījumu labot savus datus:
 - 7.4.1. pārbauda vai norādītie dati ir atšķirīgi no Pašvaldības apstrādē esošajiem datiem.
 - 7.4.2. pārbauda vai iesniegtie dati ir precizējami, t.i., vai informācija ir patiesi kļūdaina. Ja datu labošanas pieprasījums nav pietiekami pamatots vai labojumus nav tehniski iespējams veikt, Datu subjektam sniedz atbildi, kurā norāda apsvērumus tam, kāpēc dati netiks laboti.
 - 7.4.3. nodrošina labojumu veikšanu pēc iespējas īsākā laikā, ja tiek konstatēts, ka patiesi ir nepieciešams veikts labojumus Personas datus.
 - 7.4.4. pārbauda vai konkrētos Personas datus tā nav nodevusi kādai Trešajai personai un, ja tas neprasa pārmērīgas pūles, par labojumiem informē arī attiecīgos datu saņēmējus, ja tiek veikti Datu subjekta Personas datu labojumi.
- 7.5. Saņemot Datu subjekta pieprasījumu dzēst savus datus, pirms pieprasījuma izpildes un Datu subjekta informēšanas, izvērtē vai datus nav nepieciešams saglabāt, jo šādu datu apstrādi pieprasa veikt normatīvie akti, tie nepieciešami arhīva vajadzībām vai Pašvaldības leģitīmo interešu aizsardzībai, t.sk. tiesvedībai un dzēš datus, ja konstatē kādu no šādiem gadījumiem:
 - 7.5.1. pieprasījumā norādītie personas dati Pašvaldībai vairs nav nepieciešami nolūkiem, kādiem tie bija vākti un apstrādāti, izņemot gadījumus, ja šādu datu apstrādi ilgāk pieprasa veikt normatīvie akti vai tie nepieciešami arhīva vajadzībām vai Pašvaldības leģitīmo interešu aizsardzībai, t.sk. tiesvedībai;
 - 7.5.2. ja datu apstrāde ir veikta uz Datu subjekta piekrišanas pamata un tā tiek atsaukta;
 - 7.5.3. ja attiecīgo datu apstrāde tiek veikta pamatojoties uz Pašvaldības leģitīmām interesēm un Datu subjekts pamatoti iebilst šādai datu apstrādei, norādot uz būtiskiem iemesliem pārtraukt šādu apstrādi;
 - 7.5.4. ja Datu subjekta attiecīgo datu apstrāde tiek veikta nelikumīgi;
 - 7.5.5. ja dati ir jādzēš saskaņā ar spēkā esošajiem normatīvajiem aktiem;
 - 7.5.6. pārbauda vai dzēstie dati nav nodoti kādai Trešajai personai un, ja tas neprasa pārmērīgas pūles, par dzēšanas faktu informē arī attiecīgos datu saņēmējus.
- 7.6. Saņemot Datu subjekta pieprasījumu ierobežot savus datus:
 - 7.6.1. ierobežo datu apstrādi šādos gadījumos:
 - 7.6.1.1. uz laiku, kamēr tiek pārbaudīta pieprasījuma pamatotība, ja tiek apstrīdēta datu precizitāte;
 - 7.6.1.2. uz Datu subjekta norādīto laiku, ja Datu subjekts ir iebildis datu dzēšana un tiek konstatēta nelikumīga datu apstrāde;
 - 7.6.1.3. uz Datu subjekta norādīto laiku, ja Pašvaldībai ir beigusies nepieciešamība glabāt datus, savukārt Datu subjektam tie ir nepieciešami, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
 - 7.6.1.4. uz laiku, kamēr tiek pārbaudīti Datu subjekta būtiskie iemesli datu apstrādes, kas pamatojas uz Pašvaldības leģitīmām interesēm, pārtraukšanai.
 - 7.6.2. ja datu apstrāde ir ierobežota, nodrošina, ka attiecīgie dati netiek izmantoti citiem mērķiem, kā tikai glabāšanai, Pašvaldības vai Trešās personas likumīgu prasību īstenošanai un aizstāvēšanai, dalībvalstu noteiktu svarīgu interešu dēļ vai atsevišķos gadījumos, ja Datu subjekts ir izteicis piekrišanu savu ierobežoto personas datu apstrādei;
 - 7.6.3. ja ierobežojums tiek atcelts, pirms tam informē Datu subjektu;

- 7.6.4. pārbauda vai dzēstie Personas dati nav nodoti Trešajai personai un, ja tas neprasa pārmērīgas pūles, par datu ierobežošanas faktu informē attiecīgos datu saņēmējus.
- 7.7. Saņemot Datu subjekta pieprasījumu nodrošināt savus datu pārnēsamību:
- 7.7.1. pārbauda vai dati ir pakļauti pārnēsamībai, t.i. pārbauda vai attiecīgie dati tiek apstrādāti uz Datu subjekta piekrišanas pamata, pamatojoties uz līgumsaistību izpildi vai tie tiek apstrādāti elektroniskā vidē;
- 7.7.2. ja Pašvaldības rīcībā ir konstatēti dati, kuriem piemērojama pārnēsamība, par pieprasījuma izpildi atbildīgais darbinieks sagatavo attiecīgos datus elektroniskā (*.xml, *.doc, *.csv) formātā un izsniedz datu subjektam vai viņa norādītai Trešajai personai;
- 7.7.3. ja Datu subjekts norādījis, ka Personas dati pārsūtāmi tiešā veidā Trešajai personai, izvērtē nosūtāmo datu apjomu un saturu un lemj par atbilstošiem drošības pasākumiem pieprasītās informācijas nosūtīšanā, informāciju kriptējot, aizsargājot ar paroli vai izmantojot citus risinājumus drošas informācijas nosūtīšanai;
- 7.7.4. pārliecinās, ka realizējot Datu subjekta tiesības, netiek aizskarts citu personu privātums, t.i. netiek izsniegti citu Datu subjektu dati, kuru sniegšanai nav pamata.
- 7.8. Saņemot Datu subjekta iebildumus pret savu datu apstrādi par pieprasījuma izpildi atbildīgais darbinieks, ja attiecīgi personas dati Pašvaldībā tiek apstrādāti Pašvaldības leģitīmo interešu ietvaros, vērsas pie attiecīgā Procesa īpašnieka, lai tas kopā ar DAS izvērtē Datu subjekta norādītos iemeslus, un ja tie ir būtiskāki un svarīgāki par Pašvaldības leģitīmām interesēm, nodrošina, ka tiek pārtraukta attiecīgā Datu subjekta datu apstrāde, par to paziņojot Datu subjektam un informējot Datu subjektu arī gadījumā, ja tiek pieņemts lēmums turpināt datu apstrādes veikšanu.
- 7.9. Saņemot Datu subjekta pieprasījumu nebūt automatizētu lēmumu subjektam:
- 7.9.1. pārtrauc automatizētu lēmumu pieņemšanu attiecībā uz Datu subjektu, ja attiecībā uz Datu subjektu tiek pieņemti pilnībā automatizēti lēmumi, kas Datu subjektam rada tiesiskas sekas vai līdzīgā veidā ietekmē Datu subjektu, izņemot šādus gadījumus:
- 7.9.1.1. ja lēmums ir vajadzīgs, lai noslēgtu, izpildītu līgumu starp Datu subjektu un Pārzini;
- 7.9.1.2. ja lēmuma pieņemšanu, nosaka normatīvie akti;
- 7.9.1.3. ja lēmums pamatojas uz Datu subjekta piekrišanu, kas nan atsaukta.
- 7.9.2. atteikuma gadījumā pārtraukt automatizētu lēmumu pieņemšanu, nodrošina lēmuma manuālu (ar cilvēka līdzdalību) pārskatīšanu, izņemot ja lēmuma pieņemšana ir noteikta normatīvajos aktos.

8. Personas datu apstrādes prasības informācijas tehnoloģijām

- 8.1. Lai nodrošinātu aizsardzību pret fiziskās iedarbības radītu Personas datu apdraudējumu un aizsardzību, Pašvaldībā ar informācijas tehnoloģiju līdzekļiem īsteno Personas datu obligāto tehnisko aizsardzību. Izvēloties veidu, kā tiks uzglabāti Personas dati, ņem vērā iespēju, ka bojājumus var nodarīt arī uguns, plūdi, eksplozijas, kā arī citi dabas, informācijas tehnoloģiju un cilvēku izraisīti Incidenti, tostarp, ņemot vērā jebkurus iespējamus draudus drošībai no līdzās esošajām telpām/ēkām/būvēm.
- 8.2. Datu apstrādes tehniskās un organizatoriskās drošības prasības informācijas tehnoloģijām nosaka Pašvaldības informācijas sistēmu drošības politika un tai pakārtotie noteikumi, kārtības, procedūras, plāni, rīkojumi un citi uz informācijas drošību attiecināmie Pašvaldības dokumenti.
- 8.3. Darbinieka pienākums pirms Personas datu apstrādes uzsākšanas elektroniskā vidē ir iepazīties ar Pašvaldības informācijas tehnoloģiju drošību reglamentējošiem dokumentiem, jautājumu gadījumā vērošoties pie tiešā vadītāja vai informācijas tehnoloģiju speciālista.

- 8.4. Pašvaldībā informācijas tehnoloģijām jānodrošina, vismaz šādu Personas datu apstrādes tehnisko un organizatorisko drošības prasību ievērošana:
- 8.4.1. Fiziskie drošības pasākumi:
- 8.4.1.1. tehniskie resursi, kas tiek izmantoti tiešo darba pienākumu veikšanai un satur Personas datus (stacionārie un portatīvie datori, ārējie cietie diski, planšetes, telefoni), laikā, kad tie netiek lietoti, tiek glabāti slēdzamās telpās un/vai skapjos;
 - 8.4.1.2. drošības pasākumi pret ārkārtas apstākļiem tiek īstenoti saskaņā ar ugunsdrošības noteikumiem Pašvaldībā, kā arī normatīvo aktu prasībām par elektroiekārtu drošu ekspluatāciju un to aizsardzību. Personas datus saturoši dokumenti ir glabājami pret uguns risku aizsargātos skapjos;
 - 8.4.1.3. telpas, kurās atrodas Personas datus saturoši tehniskie resursi un dokumentācija, ir nodrošinātas ar funkcionējošu apsardzes signalizāciju, dūmu detektoriem un ugunsdzēsamo aparātu.
- 8.4.2. Prasības informācijas tehnoloģiju lietotājiem:
- 8.4.2.1. piekļuves informāciju tehnoloģijām, kurās ir izvietoti Personas dati, nodrošināt atbilstoši Darbinieku kompetencei;
 - 8.4.2.2. beidzot darbu, izslēdz datoru (piem., izslēgšanas procedūra: Start => Shut Down => Ok). Atstājot datoru uz īsu laiku, lieto ekrāna saudzētāju ar paroli vai bloķē pieeju datora informācijai, noslēdzot datora klaviatūru ar attiecīgas (piem., Ctrl-Alt-Del) funkcijas palīdzību;
 - 8.4.2.3. datoros ir aizliegts izmantot nelicencētu programmatūru, kā arī instalēt jebkādu programmatūru bez Pašvaldības atļaujas. Programmatūrai jābūt nodrošinātai ar visiem pieejamajiem atjauninājumiem;
 - 8.4.2.4. aizliegts pieslēgties informācijas sistēmām, kurā tiek veikta Personas datu apstrāde, izmantojot neaizsargātu bezvadu datortīklu (Unencrypted Wireless Networks).
 - 8.4.2.5. bez Pašvaldības vadības attiecīgi pilnvarotu personu atļaujas aizliegts pieslēgt informācijas tehnoloģijām jebkādas ārējās atmiņas ierīces;
 - 8.4.2.6. datoriem, kas tiek izmantoti Personas datu apstrādē ir parole vismaz operētājsistēmas līmenī. Portatīvā datora cietajam diskam ir jābūt pilnīgi šifrētam vai tiek nodrošināti citi mehānismi, kā garantēt tajā esošo Personas datu drošību.
 - 8.4.2.7. informācijas tehnoloģiju aizsardzība un Pilnvaroto personu identifikācija tiek nodrošināta ar datora paroli, kura atbilst Pašvaldības informācijas tehnoloģiju resursu lietošanas noteikumos noteiktajām prasībām, t.sk.:
 - 8.4.2.7.1. paroli aizliegts veidot, izmantojot ar darbinieku, Pilnvarotu personu tieši saistītu informāciju (piemēram, vārdus, uzvārdus, dzimšanas dienas, tālruņa numurus, mājdzīvnieku un tuvinieku vārdus u.tml.);
 - 8.4.2.7.2. aizliegts izpaust savu paroli Trešajām personām;
 - 8.4.2.7.3. ja ir aizdomas, ka paroli zina Trešā persona, tai ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt to izdarīt komitetentajiem darbiniekiem, ziņot par paroles nokļūšanu Trešo personu rīcībā;
 - 8.4.2.7.4. ja gadījumā parole ir kļuvusi zināma Trešajām personām, darbinieks, Pilnvarotā persona vai cita persona, kurai par to ir kļuvis zināms, nekavējoties ziņo Pašvaldības nozīmētai personai Noteikumos noteiktajā kārtībā;
 - 8.4.2.7.5. nodrošinot piekļuves tiesības Pašvaldības izsniedz sākotnējo paroli, kura jānomaina pie pirmās autentifikācijas un sistēmas lietošanas.
- 8.4.3. Informācijas sistēmu aizsardzības vispārīgie nosacījumi:
- 8.4.3.1. informācijas sistēmas tiek pielāgotas Personas datu aizsardzības prasībām;
 - 8.4.3.2. tiek nodrošinātas informācijas sistēmas darbība, tās darbības atjaunošana (nomaiņa), ja noticis informācijas tehnoloģiju bojājums vai arī informācijas sistēmas darbība ir tikusi traucēta citu iemeslu dēļ;

- 8.4.3.3. informācijas sistēmām, kuras tiek izmantoti Personas datu apstrādē, tiek nodrošināta auditācijas pierakstu esamība;
- 8.4.3.4. tiek nodrošināti regulāri pasākumi pret drošības apdraudējumiem, t.sk. antivīrusu programmatūru uzstādīšana, ugunsdrošības konfigurēšana, darbinieku instruēšana, u.c.;
- 8.4.3.5. tiek organizēti fiziskās aizsardzības pasākumi pret drošības apdraudējumiem, t.sk. slēgtas telpas, ierobežotas piekļuves, u.tml.;
- 8.4.3.6. tiek nodrošināta informācijas sistēmu darbības nepārtrauktība un Personas datu atjaunošanas iespējamība, t.sk. rezerves kopiju veidošana, ja ir notikusi nesankcionēta Personas datu dzēšana vai labošana.
- 8.4.3.7. uz Pašvaldības serveriem ir uzstādīts nepārtrauktās barošanas avots (UPS), kas nodrošina nepārtrauktu elektrības padevi un iespēju izmantot sistēmu vēl pēc elektroenerģijas padeves atslēgšanas.

9. Incidentu/Pārkāpumu pārvaldība

- 9.1. Par jebkuru Personas datu apdraudējumu apstrādē iesaistītajai personai, kas to konstatējusi, nekavējoties jāziņo tiešajam vadītājam (kurš tālāk ziņo uz turpmāk norādīto e-pastu) vai uzreiz uz e-pastu: dati@jelgava.lv un tālruni +371 63005444, gadījumos, kad apdraudējums ir saistīts ar informācijas tehnoloģijām arī uz e-pastu: it@jelgava.lv un tālruni +371 63005555, t.sk. gadījumos, ja konstatēts jebkāda veida apdraudējums:
 - 9.1.1. tehniskajiem resursiem, t.sk. informācijas tehnoloģiju (elektroenerģijas padeves pārtraukums, šķidrumu vai svešķermeņu iekļūšana, bojājumi fiziska trieciena, uguns vai ūdens iedarbības rezultātā, datoru un citu tehnisko resursu nozaudēšana vai zādzība u.c.);
 - 9.1.2. informācijas resursiem (Trešajām personām kļuvusi zināma pieejas parole, konstatēta nesankcionēta piekļuve Personas datiem, t.sk. informācijas nesēju – USB, CD nozaudēšana, kā arī Personas datus saturoša e-pasta nosūtīšana neparedzētiem adresātiem, konstatēti informācijas sistēmas darbības pārtraukumi, Personas dati ir neautorizēti izdzēsti vai laboti u.c.);
 - 9.1.3. Personas datiem papīra formā (pārāk augsts mitrums telpās, metāla skapja vai telpu durvju slēdzenes nefunkcionēšana, signalizācijas nefunkcionēšana, Trešo personu piekļūšana dokumentiem, dokumentu nozaudēšana u.c.).
- 9.2. Apdraudējuma gadījumā Personas datu apstrādē iesaistītajam Darbiniekam savu iespēju un kompetences ietvaros ir jānodrošina personas datu un informācijas sistēmas drošība līdz Pašvaldības atbildīgā pārstāvja iesaistes brīdim.
- 9.3. Gadījumos, kad tiek konstatēts Incidents, datu apstrādē iesaistītajai personai vai citai personai, kurai ir kļuvis zināms par Incidenta iestāšanos, primāri nekavējoties jāsniedz informācija iepriekš minētajos veidos, kā arī, nepieciešamības gadījumā, jāaizpilda Incidenta ziņojums (Noteikumu 12.pielikums) nosūtot to uz e-pastu: dati@jelgava.lv.
- 9.4. DAS nekavējoties pēc informācijas par Incidentu saņemšanas pirmšķietami izvērtē vai ir noticis Personas datu pārkāpums, nepieciešamības gadījumā pieprasot papildus informāciju un savas kompetences ietvaros nosakot pasākumus seku mazināšanai un līdzīgu incidentu novēršanai.
- 9.5. Ja DAS pirmšķietami konstatē, ka ir noticis Personas datu pārkāpums, t.i. incidenta rezultātā ir notikusi nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto Personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem, veic šādas darbības:
 - 9.5.1. apkopo un uzskaita informāciju par Pārkāpumu un tā sekām;
 - 9.5.2. informē Informācijas tehnoloģiju nodaļas vadītāju, ja ir ietekmētas Pašvaldības informācijas sistēmas, un citas saistītās personas;
 - 9.5.3. ne vēlāk kā 48 stundu laikā no informācijas saņemšanas brīža sniedz informāciju par Pārkāpumu, tā faktiskajiem apstākļiem, personas datu aizsardzības pārkāpumu

- izmeklēšanas komisijas, kas izveidota ar Pašvaldības izpilddirektora rīkojumu (turpmāk – Komisija), priekšsēdētājam.
- 9.6. Komisijas priekšsēdētājs nekavējoties pēc informācijas saņemšanas sasauc Komisijas sēdi un, ja nepieciešams, viedokļa sniegšanai pieaicina konkrētās datu apstrādes Procesa īpašnieku/us un citas kompetentās personas.
- 9.7. Komisija veic šādas darbības:
- 9.7.1. izvērtē, kuras personas ir nepieciešams informēt par Pārķāpumu, lai nekavējoties pārtrauktu to, samazinātu sekas, ierobežotu ietekmi, novērstu atķārtošanos;
 - 9.7.2. izvērtē īstenojamās darbības, lai pārtrauktu Pārķāpumu (ja tas nav beidzies), ierobežotu nelabvēlīgo ietekmi uz datu subjektiem, samazinātu iespējamās zaudējumus un nekavējoties uzsāk to realizēšanu;
 - 9.7.3. izvērtē vai nepieciešams par Pārķāpumu ziņot Valsts policijai (ja saskatāmas noziedzīga nodarījuma pazīmes);
 - 9.7.4. novērtē Pārķāpuma radīto risku iesaistīto fizisko personu privātumam ņemot vērā:
 - 9.7.4.1. Kādi Personas dati ir skarti?
 - 9.7.4.2. Cik sensitīvi ir Pārķāpumā ietekmētie dati (t.sk. vai ir Īpašās kategorijas dati)?
 - 9.7.4.3. Kuras personas var tikt/ ir ietekmētas Pārķāpuma rezultātā (t.sk. ietekmēto personu skaitu un kategorijas)?
 - 9.7.4.4. Kā un kāpēc Pārķāpums iestājās?
 - 9.7.4.5. Ja dati ir tikuši nozaudēti vai nozagti, vai no attiecīgiem Personas datiem Trešā persona var ko uzzināt par attiecīgo Datu subjektu?
 - 9.7.4.6. Kādu ietekmi/sekas Pārķāpums atstās uz iesaistītām personām (t.sk. vai varētu tikt apdraudēta to fiziskā drošība, nodarīts materiāls zaudējums, nodarīts kaitējums reputācijai vai nodarīts emocionāls kaitējums)?
 - 9.7.4.7. Ja dati ir tikuši nozaudēti vai nozagti, vai dati bija pseidonimizēti, šifrēti, aizsargāti ar paroli vai citādi aizsargāti?
 - 9.7.4.8. Ja dati ir nozagti/pazaudēti, vai tie varētu tikt izmantoti noziedzīgiem mērķiem?
 - 9.7.4.9. Kādu ietekmi/sekas Pārķāpums atstās uz Pašvaldību (t.sk. vai varētu tikt apdraudēta Pašvaldības, to darbinieku/pakalpojumu saņēmēju drošība, nodarīts materiāls zaudējums vai kaitējums, t.sk. administratīvo iestāžu sodi, Datu subjektu prasījumi, nodarīts kaitējums reputācijai)?
 - 9.7.4.10. Kādas ir Pārķāpumā ietekmēto Datu subjektu identitātes un kontaktinformācija, lai nepieciešamības gadījumā būtu iespējams sazināties?
 - 9.7.5. ne vēlāk kā 12 stundu laikā no informācijas saņemšanas brīža, ziņo par Pārķāpumu, uzskaitot seku mazināšanas pasākumus un ieteikumus Pārķāpuma novēršanai, Pašvaldības vadībai, kas pieņem lēmumu par Datu subjekta un uzraudzības iestādes, t.i. Datu valsts inspekcijas, informēšanu.
- 9.8. Pašvaldības vadība pēc Pārķāpuma konstatēšanas nekavējoties informē ietekmētos Datu subjektus, ja Pārķāpuma sekas var radīt augstu risku fizisku personu tiesībām un brīvībām, un ne vēlāk kā 72 stundu laikā pēc Pārķāpuma konstatēšanas ziņo uzraudzības iestādei - Datu valsts inspekcijai, izņemot gadījumus, ja pēc izvērtēšanas ir konstatējams, ka Pārķāpums maz ticams, ka varētu radīt risku fiziskas personas privātumam.
- 9.9. Paziņojumā datu subjektiem un uzraudzības iestādei par datu apstrādes aizsardzības pārķāpumu iekļauj šādu informāciju:
- 9.9.1. Pārķāpuma fakts un īss apraksts;
 - 9.9.2. iesaistīto datu subjektu kategorijas un aptuvenais skaits, aptuveno ierakstu skaits (skarto datu apjoms);
 - 9.9.3. Pašvaldības DAS vārds, uzvārds un kontaktinformācija;
 - 9.9.4. izraisītās vai iespējamās sekas;
 - 9.9.5. Pašvaldības jau veiktos vai plānotos pasākumus, lai mazinātu iespējamās nelabvēlīgās sekas un nepieļautu šādu Pārķāpumu iestāšanos nākotnē.

- 9.10. Ne retāk kā reizi gadā DAS sagatavo kopsavilkumu par pārskata periodā fiksētiem Pārņēmumiem un to iemesliem, kā arī uzskaita veiktos pasākumus drošības uzlabošanai un ziņo par to Pašvaldības vadībai.

10. Sadarbība ar uzraudzības iestādi

- 10.1. Pašvaldības vārdā ar Datu valsts inspekciju vai ar citu uzraudzības iestādi Personas datu aizsardzības jomā mutvārdos un rakstveidā komunicē DAS. Šīs prasības neattiecas uz tādiem gadījumiem, kad uzraudzības iestāde uz normatīvā akta pamata pieprasa komunikāciju ar konkrētu Darbinieku.
- 10.2. Rakstveida komunikācija ar uzraudzības iestādi notiek atbilstoši Pašvaldībā noteiktai rakstveida korespondences aprites kārtībai. Ja Darbinieks saņem personificētu pieprasījumu no uzraudzības iestādes, Darbinieks nekavējoties par to informē DAS un savu tiešo vadītāju. Darbinieka tiešais vadītājs nodrošina pieprasījuma reģistrāciju Pašvaldības lietvedības sistēmā.
- 10.3. Ja uzraudzības iestāde veic pārbaudes Darbinieka darba vietā, tiem Darbiniekiem, kuri tajā brīdī atrodas darba vietā, ir pienākums nekavējoties informēt par šādu pārbaudi DAS un tiešo vadītāju. No Pašvaldības puses nepieciešamās darbības pārbaudes veikšanā organizē struktūrvienības vai iestādes vadītājs.

11. Darbinieku apmācība

- 11.1. Darbiniekiem tiek nodrošinātas apmācības un informēšana par datu aizsardzības pasākumiem veicot sākotnēju apmācību uzsākot darba attiecības (ievadinstruktaža) un veicot regulāro apmācību.
- 11.2. Sākotnējā apmācība tiek nodrošināta:
- 11.2.1. iepazīstinot ar šiem Noteikumiem un citiem ar personas datu apstrādi saistītiem normatīvajiem aktiem, dokumentiem (informācijas tehnoloģiju drošība, ierobežotas pieejamības informācijas saraksts);
 - 11.2.2. iepazīstinot ar darbinieku datu apstrādes paziņojumu;
 - 11.2.3. izpildot testu saistībā ar datu aizsardzības jautājumiem.
- 11.3. Regulārā apmācība notiek periodiski, bet ne retāk kā reizi trīs gados, darbiniekiem piedaloties klātienē vai tiešsaistes lekcijā, seminārā, apmācībās vai tiem tiek nosūtīts lekcijas, semināra, apmācību ieraksts vai prezentācija, uzlabotas procedūras, vai testa jautājumi, uz kuriem tiem jāvar veiksmīgi atbildēt.

Pašvaldības datu aizsardzības speciālists

Everita Širaka



Latvijas Republika

Jelgavas valstspilsētas pašvaldība

Reģ.Nr. 40900039904, Lielā iela 11, Jelgava, LV-3001, tālrunis: 63005531, 63005538, e-pasts: pasts@jelgava.lv

1.pielikums

Jelgavas valstspilsētas pašvaldības
Personas datu apstrādes noteikumiem
(apstiprināti ar Jelgavas valstspilsētas
pašvaldības izpilddirektora vietnieces
28.11.2025. rīkojumu Nr. 341-ri)

APLIECINĀJUMS

Es,

(vārds, uzvārds)

(amats/praktikants)

apņemos, atbilstoši Jelgavas valstspilsētas pašvaldības (turpmāk – Pašvaldība) spēkā esošajiem noteikumiem, kas regulē personas datu apstrādi, aizsardzību un informācijas drošību, Eiropas Parlamenta un Padomes regulai (ES) 2016/679 par fizisko personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46 EK (Vispārīgā datu aizsardzības regula) un citu saistošo normatīvo aktu regulējumam:

1. saglabāt un neizpaust amata/prakses pienākumu veikšanas laikā iegūto ierobežotas pieejamības informāciju, konfidenciālo informāciju, personas datus trešajām personām bez tiesiska pamatojuma un Pašvaldības saskaņojuma, t.sk. arī pēc tiesisko attiecību izbeigšanas;
2. ievērot personas datu apstrādi, aizsardzību un informācijas drošību regulējošos noteikumus un nekavējoties informēt Pašvaldību par konstatētajiem pārkāpumiem un nesankcionētu piekļuvi manā rīcībā esošajai ierobežotas pieejamības informācijai, konfidenciālajai informācijai, personas datiem, kas iegūti veicot pienākumus Pašvaldībā;
3. pārtraucot tiesiskās attiecības ar Pašvaldību, nekavējoties nodot Pašvaldībai manā rīcībā esošo Pašvaldības aprikojumu, kas izmantots personas datu apstrādei, kā arī manā rīcībā esošo ierobežotas pieejamības informāciju, konfidenciālo informāciju, personas datus, to saturošus dokumentu oriģinālus un kopijas, kas ir saņemti pienākumu izpildes laikā vai, kas ir manā rīcībā vai valdījumā.

Ar šo apliecinu, ka esmu brīdināts(-a), ka ierobežotas pieejamības, konfidenciālas informācijas, personas datu nelikumīgas izpaušanas un personas datu apstrādi un informācijas drošību regulējošo noteikumu pārkāpumu gadījumā var tikt nodarīts būtisks kaitējums datu subjektiem un zaudējumi Pašvaldībai, ko var lūgt man atlīdzināt. Esmu informēts(-a), ka par šī apliecinājuma un noteikumu pārkāpumu varu tikt saukts(-a) pie normatīvajos aktos noteiktās atbildības, t.sk. administratīvās un kriminālatbildības.

Parakstot šo apliecinājumu, apstiprinu, ka esmu iepazinies(-usies) un man ir izskaidroti Pašvaldības noteikumi, kas regulē personas datu apstrādi, aizsardzību un informācijas drošību un esmu informēts(-a) par nepieciešamību iziet Datu valsts inspekcijas izstrādāto bezmaksas tiešsaistes apmācību kursu e-vidē <https://e-kurss.dvi.gov.lv/>, par kursa apguvi un sertifikāta iegūšanu rakstveidā informējot pašvaldību uz e-pastu dati@jelgava.lv.

(datums)

(paraksts)

2.pielikums

Jelgavas valstspilsētas pašvaldības
Personas datu apstrādes noteikumiem
(apstiprināti ar Jelgavas valstspilsētas
pašvaldības izpilddirektora vietnieces
28.11.2025. rīkojumu Nr. 341-ri)

Personas datu apstrādes darbību reģistrs

Pārziņa nosaukums		
Reģistrācijas nr.		
Juridiskā adrese		
Par datu apstrādi atbildīgās personas	Vārds, uzvārds	
	tālrunis	
	e-pasts	
Personas datu aizsardzības speciālista kontaktinformācija - dati@jelgava.lv, 63005444		
Aktualizēšanas datums:		. .20 .

Apstrādes nolūki/ mērķi	Tiesiskais pamatojums Regulas 6.panta 1.p./9.panta 2.p. apakšp. likumi,MK not.	Datu subjektu kategorijas	Datu veidi	Datu saņēmēju kategorijas	Datu glabāšanas termiņi/ kritēriji dzēšanai	Datu nodošanas ārpus ES/EEZ		Loma (atzīmē ar “X”)		Īpaši noteiktie tehniskie / organizatoriskie drošības pasākumi
						Valsts uz kuru dati nodoti	Drošības pasākumi Regulas 49.panta 1.p.(2)	Pārzinis	Apstrāde datājs	
1.										
1.1.										
1.2.										
2.										
2.1.										

Rīkojums
Jelgavā

par personas datu apstrādi

Pamatojoties uz _____, kas nosaka _____, uzliekot par pienākumu Jelgavas valstspilsētas pašvaldībai (turpmāk – Pašvaldība) _____, noteikt šādu personas datu apstrādi:

1. Datu apstrādes nolūks:

2. Tiesiskais pamatojums:

3. Apstrādes apraksts, datu plūsmas (shēma):

4. Par personas datu apstrādi atbildīgās personas:

Procesa īpašnieks/i (atbildīgās personas amats, vārds, uzvārds):

Informācijas resursu turētājs:

Par tehniskajiem resursiem atbildīgais:

Procesā iesaistītās struktūrvienības/iestādes/pakalpojumu sniedzēji, kas apstrādās datus:

Nosaukums	Darbības ar personas datiem (<i>saņemšana, pārbaude, ievade, glabāšana, uzturēšana, izpildes kontrole, admin. pārkāpuma procesa veikšana</i>)

5. Personas datu apstrādes uzsākšanas datums:

6. Datu subjektu kategorijas un datu veidi:

Dati par _____ :

Identificējoša informācija:

Kontaktinformācija, u.c.:

7. Personas datu glabāšanas vieta, termiņš, dzēšanas kritēriji:

Elektroniski: _____ gadi.

Papīrā: _____ gadi. Nomenklatūras lietas Nr.:

Informācija par datu nosūtīšanu uz trešo valsti (ārpus ES/EEZ) vai starptautisku organizāciju:

8. Datu apstrādes sistēmas:

9. Datu subjektu informēšana par personas datu apstrādi:

Pašvaldības saistošie noteikumi _____

Pieteikuma veidlapa.

Pašvaldības tīmekļa vietnes www.jelgava.lv sadaļā: “Personas datu apstrāde”, “Pakalpojumi”,...

Uzraugošo, kontrolējošo institūciju sniegtā informācija pārkāpumu gadījumā, u.c.

10. Personas datu apstrādes vieta un datu apstrādē izmantojamie resursi:

Datu apstrādes vieta un tehniskie resursi:

Informācijas apmaiņas kanāli:

Iespēja pašam datu subjektam veikt datu labošanu/dzēšanu:

11. Apstrādē izmantojamie tehniskie un organizatoriskie pasākumi (risku mazināšanai)¹:

Datu apstrādes sistēma:

Datu ieguves veids:

Datu precizitātes pārbaudes/atjaunošanas/labojšanas procesa apraksts:

Riski, to mazināšanas pasākumi:

(amats, vārds, uzvārds, paraksts)

¹ **Tehnisko un organizatorisko pasākumu piemēri:** datu integrēšana no sistēmas, datu pieejamības minimizācija, konfidencialitātes nodrošināšana, pseidonimizācija, integritāte (pilnīguma saglabāšanai), rezerves kopijas, tehnisko un organizatorisko pasākumu efektivitātes izvērtēšana un risku analīzes veikšana, ierobežota piekļuve, dubultā verifikācija, noteikumi, kārtības, lietošanas instrukcijas, apmācības.

4.pielikums

Jelgavas valstspilsētas pašvaldības
Personas datu apstrādes noteikumiem
(apstiprināti ar Jelgavas valstspilsētas
pašvaldības izpilddirektora vietnieces
28.11.2025. rīkojumu Nr. 341-ri)

Novērtējums par ietekmi uz datu aizsardzību

iestādes nosaukums

Jautājumi	Atbildes	Piezīmes/ Trūkumi
I. Vispārīgie jautājumi		
1. Procesa jeb plānotās personas datu apstrādes (turpmāk – Process) nosaukums.		
2. Īss paredzētās datu apstrādes apraksts. Sniedziet informāciju par visu personas datu apstrādes ciklu (no datu ievākšanas/saņemšanas līdz datu iznīcināšanai, sadalot tos par apstrādes posmiem un norādiet konkrētas apstrādes darbības²), iespējams, izmantojot procesa datu plūsmu diagrammas (t.i. no kurienes/kura tiks vākti dati, ar ko tas tiks darīts, kur tiks glabāti dati, kam tiks nodoti dati, pievienojot novērtējuma pielikumā), un detalizēti aprakstot plānoto datu apstrādi. Ja paredzētas izmaiņas esošajā sistēmā, norādiet galvenās izmaiņas, kas tiek iniciētas. Sniedziet informāciju, ko vēlaties sasniegt ar Procesu (informācijas sistēmu, programmu) jeb plānoto apstrādi.	Resursi: <i>Aparatūra,</i> <i>programmatūra,</i> <i>tīkli,</i> <i>informācijas</i> <i>apmaiņas kanāli</i>	
3. Norādiet personas datu apstrādes nolūku Procesā. Norādiet detalizētu apstrādes nolūka (-u) aprakstu: paskaidrojiet Procesu soli pa solim, vajadzības gadījumā nošķirot nolūkus.		
4. Vai Procesā norādītais personas datu apstrādes nolūks ir reģistrēts pašvaldības Personas datu apstrādes darbības reģistrā vai arī tas ir saistīts ar kādu no nolūkiem, kas ir reģistrēts pašvaldības Personas datu apstrādes darbības reģistrā? Ja jā, norādiet reģistrēto Nolūku.		
5. Kādas pašvaldības struktūrvienības/iestādes ir iesaistītas Procesā? Lūdzu, norādiet tās. Vai tiks iesaistītas citas institūcijas ārpus pašvaldības? Lūdzu norādīt tās. Vai ir		

² 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, nosūtīt, izplatīt vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana

Jautājumi	Atbildes	Piezīmes/ Trūkumi
iegūts viņu viedoklis par plānoto apstrādi? Ja ir, tad kāds ir to viedoklis.		
6. Kādu datu subjektu kategoriju personas datus plānots apstrādāt Procesa ietvaros?		
7. Vai apstrādei pakļauto datu subjektu skaitā varētu būt īpaši aizsargājamas datu subjektu kategorijas (piem., bērni, seniori, darbinieki, pacienti)? Ja jā, vai viņi tiek informēti par viņu datu apstrādi viegli saprotamā un pārredzamā veidā?		
8. Kādi personas dati tiks apstrādāti Procesa ietvaros (uzskaitiet datu veidus/kategorijas)? Informējam, ka šim uzskaitījumam ir jāsakrīt ar tiesību aktos un dokumentos (ja tādi ir) uzskaitītajām datu kategorijām. Katrai datu kategorijai (veidam) ir jābūt vajadzīgai datu apstrādes nolūka sasniegšanai.		
9. Vai apstrādāti tiks Īpašu kategoriju personas dati (piem., veselības dati, biometriskie dati, etniskā piederība) vai dati par sodāmībām? Ja jā, norādiet: - to veidus/kategorijas; - Vai to apstrāde ir nodalīta no pārējo personas datu apstrādes? (ja jā, raksturojiet procedūru, kas tiek nodrošināta, ja nē, norādiet iemeslus) - Vai to apstrādei ir noteikts lielāks (augstāks) datu aizsardzības līmenis? (ja jā, raksturojiet aizsardzības līmeni).		
10. Vai datus ievāks no citas pašvaldības struktūrvienības vai iestādes/juridiskas personas? Ja jā, norādiet, struktūrvienības/iestādes/juridiskas personas un datu veidus, kādus saņems no tām.		
11. Vai datus ievāks (iegūs) no citas pašvaldības sistēmas? Ja jā, norādiet no tieši no kuras sistēmas/lietojumprogrammas un kādi personas dati. Vienlaicīgi norādiet, kurš ir attiecīgās sistēmas/lietojumprogrammas informācijas resursu turētājs.		
12. Vai datus ievāks (iegūs) no citām pašvaldībām, valsts institūcijām, juridiskām personām? Ja jā, norādiet no kādām un kādus personas datus saņems.		
13. Vai šajā Procesā apstrādātie personas dati tiks atkārtoti izmantoti citos procesos?		
14. Vai datus iegūs no paša datu subjekta? Ja, jā kādus datus.		
15. Kurš būs atbildīgs par personas datu apstrādi Procesā jeb, kas būs		

Jautājumi	Atbildes	Piezīmes/ Trūkumi
Procesa īpašnieks ³ plānotajai personas datu apstrādei? Norādiet amatu un dokumentu, kas nosaka, ka attiecīgā persona ir Procesa īpašnieks.		
16. Kurš būs atbildīgs par informācijas un tehniskajiem resursiem, kas tiks iesaistīti, Informācijas resursu turētājs un Tehnisko resursu turētājs. Norādiet amatus un dokumentu, kas nosaka attiecīgos resursu turētājus.		
17. Kam tiks izpausti dati? Kas saņems personas datus? Norādiet kurus personas datus katrs datu saņēmējs ⁴ iegūs. Jautājums attiecas gan uz iekšējiem, gan ārējiem datu saņēmējiem, kam tiks izpausti dati.		
18. Kur plānots glabāt datus?		
II. Apstrādes darbību nepieciešamības un samērīguma attiecībā uz nolūkiem novērtējums		
19. Vai esat identificējuši visus sava procesa nolūkus?		
20. Vai personas datu apstrādes nolūks Procesā ir saderīgs ar sākotnējo personas datu apstrādes nolūku?		
21. Kā nodrošināsiet, ka dati tiks izmantoti tikai noteiktajam nolūkam?		
22. Vai datu apstrādes nolūks ir konkrēts, skaidrs un leģitīms? Paskaidrojiet jeb pamatojiet, kāpēc uzskatiet, ka apstrādes nolūks ir konkrēts, skaidrs un leģitīms.		
23. Vai iegūtie personas dati būs adekvāti, atbilstīgi un ietvers tikai to, kas nepieciešams to apstrādes nolūkos, kam tie ir tikuši apstrādāti (“datu minimizēšana”)? Aprakstiet kāpēc katrs personas datu veids/kategorija ir nepieciešama Jūsu apstrādes nolūka sasniegšanai, t.i., norādiet katram datu veidam/kategorijai, kā tas palīdzēs sasniegt Procesa (procesu) nolūkus. Piemēram, klienta vārds, uzvārds – personas identifikācijai.		
24. Vai ir citi veidi kā sasniegt tos pašus Procesa (procesu) nolūkus? Pamatojiet atbildi.		
25. Vai personas datus plānots publiskot vai izpaust trešajām personām ⁵ (piem., sadarbības partneriem, citām valsts un pašvaldības (ne Jelgavas valstspilsētas pašvaldības), iestādēm/kapitālsabiedrībām)? Norādiet konkrēti kam, ja tiek plānots.		

³ Procesa īpašnieks ir Pašvaldības noteikta persona, kura atbild par pārziņā nodotiem procesiem datu apstrādēm, kas veicamas noteiktu mērķu ietvaros (piemēram, atbildīgā persona par datu apstrādes reģistra vešanu, atbildīgā persona par datu apstrādi informācijas sistēmā, par datu apstrādi mērķa sasniegšanu atbildīgās personas, u.tml.).

⁴ Personas datu saņēmējs ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai izpauž personas datus – neatkarīgi no tā, vai tā ir trešā persona vai nav. Tomēr publiskas iestādes, kas var saņemt personas datus saistībā ar konkrētu izmeklēšanu saskaņā ar Savienības vai dalībvalsts tiesību aktiem, netiek uzskatītas par saņēmējiem.

⁵ “trešā persona” ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņā vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus.

Jautājumi	Atbildes	Piezīmes/ Trūkumi
26. Vai nolūku varētu sasniegt, apstrādājot anonīmu informāciju ⁶ ? Pamatojiet atbildi. Ja atbilde ir "Jā", vai ir iespējams nodrošināt, ka persona nav identificējama? Kā tas tiktu nodrošināts?		
27. Ja apstrādās Īpašu kategoriju personas datus ⁷ vai datus par sodāmību un pārkāpumiem, vai nolūkus varētu sasniegt neapstrādājot Īpašu kategoriju personas datus vai datus par sodāmību un pārkāpumiem?		
28. Ja nolūku nevar sasniegt bez Īpašu kategoriju personas datu vai datu par sodāmību un pārkāpumiem apstrādes, aprakstiet kā izpaudīsies trūkumi nolūku sasniegšanā, ja Īpašu kategoriju personas dati vai dati par sodāmību un pārkāpumiem netiks apstrādāti?		
29. Vai lai sasniegtu nolūku, ir nepieciešams apstrādāt visus datus? Pamatojiet atbildi. Ja visi dati nav nepieciešami, tad norādiet tos datu veidus bez kuru apstrādes varētu iztikt? Pamatojiet atbildi.		
30. Vai būs iespējams Procesa ietvaros mainīt (t.i., palielināt, samazināt) apstrādei pakļauto datu apjomu? Pamatojiet atbildi.		
31. Cik ilgi uzglabās apstrādātos personas datus, lai sasniegtu nolūku? ⁸ Norādiet katram datu veidam/kategorijai (vai to grupai) glabāšanas termiņu, nolūku un termiņa pamatojuma skaidrojumu ⁹ . Pamatojiet kāpēc datu glabāšanas termiņi ir pamatoti ar normatīvo aktu prasībām un/vai apstrādes nepieciešamību, ja ir.		
32. Vai personas datus arhivēs? Pozitīvas atbildes gadījumā, norādiet, cik ilgi glabās arhivētos datus? Pamatojiet termiņu. Norādiet, kas glabās arhivētos datus.		
33. Kā tiks nodrošināta datu neatgriezeniska dzēšana pēc glabāšanas termiņa beigām? Kas un kā to nodrošinās? Norādiet informāciju atsevišķi uz elektroniskā formā esošiem datiem un papīra formā esošiem datiem. Ja elektroniskā veidā dati glabāsies vairākās		

⁶ informācija, kura neattiecas uz identificētu vai identificējamu fizisku personu, vai personas datiem, ko sniedz anonīmi tādā veidā, ka datu subjekts nav vai vairs nav identificējams.

⁷ Informācija, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētisko datu, biometrisku datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimundzīvi vai seksuālo orientāciju apstrāde

⁸ Personas dati jāglabā veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā; personas datus var glabāt ilgāk, ciktāl personas datus apstrādās tikai arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos.

⁹ Saskaņā ar Vispārīgās datu aizsardzības regulas 13.panta 2.punkta a) apakšpunktu un 14.panta 2.punkta a) apakšpunktu datu subjektam ir sniedzama informācija par laikposmu, cik ilgi tiks glabāti dati, vai ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai.

Jautājumi	Atbildes	Piezīmes/ Trūkumi
vietās, tad norādiet iepriekš minēto informāciju atsevišķi attiecībā uz katru glabāšanas vietu.		
34. Kādu labumu no šādas datu apstrādes varētu iegūt datu subjekts ¹⁰ jeb fiziskās personas, kuru dati tiks apstrādāti?		
35. Kādu labumu no šādas datu apstrādes varētu iegūt pašvaldība vai sabiedrība kopumā?		
36. Cik liels datu subjektu skaits tiks pakļauts datu apstrādei?		
37. Vai datu subjektam var iestāties kādas negatīvas sekas šādas apstrādes rezultātā? Ja Jā, norādiet kādas. Piemēram, diskriminācija, jebkura tiesiska darbība, kas cilvēkiem liek vilcināties izmantot likumīgas tiesības (vārda brīvība vai kā citādi), baidoties no tiesiskām sekām.		
38. Vai datu subjekti varētu paredzēt, ka Procesā paredzētā apstrāde notiks, pat ja viņi nelasītu informāciju, kura viņiem tiks sniegta?		
39. Ja dati tiks saglabāti arī statistikas vajadzībām, vai šim nolūkam tiks izmantoti anonimizēti dati, kā arī kā tiks nodrošināts, ka datu subjekti netiks atkārtoti identificēti?		
III. Tiesisko pamatu izvērtējums		
40. Vai personas datu apstrādes nepieciešamību (jeb pienākumu apstrādāt datus) nosaka ārējie normatīvie akti? Ja atbilde ir "Jā", tad norādiet, kādi normatīvie akti (minot arī konkrētus pantus un punktus, kas paredz <u>pienākumu</u> apstrādāt personas datus).		
41. Vai plānotā personas datu apstrāde ir nepieciešama līguma, kura līgumslēdzējuse ir datu subjekts, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanai?		
42. Vai personas datu apstrāde ir nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses? Pozitīvas atbildes gadījumā norādiet vitālās intereses.		
43. Vai personas datu apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim (pašvaldībai likumīgi piešķirtās oficiālās pilnvaras? Pozitīvas atbildes gadījumā, norādiet, kādas pilnvaras/pienākumus/uzdevumus?		
44. Ja personas datu apstrādes tiesiskais pamats ir datu subjektu		

¹⁰ Identificēta vai identificējama fiziska persona.

Jautājumi	Atbildes	Piezīmes/ Trūkumi
piekrišana, norādiet kādā veidā (elektroniski, rakstiski, mutiski) tiek iegūta datu subjektu piekrišana.		
45. Ja plānots apstrādāt īpašas kategorijas personas datus, lūdz norādiet tiesisko pamatu no Vispārīgās datu aizsardzības regulas 9.panta un 6.panta.		
46. Vai datu apstrādi var organizēt <u>pirms</u> tās uzsākšanas, saņemot datu subjekta brīvu un aktīvu <u>piekrišanu</u> ¹¹ ? Aprakstiet kā šāda piekrišanas iegūšana varētu tikt organizēta?		
47. Kādi būs trūkumi, ja datu subjektam ļautu brīvi izvēlēties vai pakļauties datu apstrādei vai nē?		
48. Vai datu apstrādi var organizēt tādējādi, ka uzsāk to automātiski, bet dod iespēju datu subjektam atteikties no turpmākas datu apstrādes šim nolūkam?		
49. Ja tas būtu iespējams, kādā veidā varētu organizēt atteikšanās iespēju?		
50. Ja datu apstrādes tiesiskais pamats ir pārziņa vai trešās personas leģitīmās intereses, vai ir veikts un dokumentēts <u>interesešu līdzsvarošanas tests jeb līdzsvarošanas pārbaude</u> ¹² ? Atcerieties, ka šo tiesisko pamatu (pārziņa leģitīmās intereses) nevar izmantot pašvaldība, pildot <u>savus uzdevumus vai funkcijas</u> .		
51. Cik bieži pārbaudīs/pārskatīs apstrādājamo personas datu apjoms un tā atbilstība personas datu apstrādes nolūkam? Vai ir izveidota jeb noteikta kārtība šādai regulārai pārskatīšanai? Ja ir noteikta kārtība, lūdz norādiet kārtības nosaukumu, datumu un numuru.		
IV. Datu subjekta tiesību nodrošināšana		
52. Vai datus ievāks no datu subjekta/trešās personas? Norādiet tieši no kā.		
53. Kā/kādā veidā (rakstiski, elektroniski, standartizētu ikonu veidā vai mutiski) datu subjektus informēs par viņu personas datu apstrādi pirms datu iegūšanas ? Ja datu subjektus neinformēs, sniedziet atbildi, kāpēc netiks datu subjekts informēti (Vispārīgās datu aizsardzības regulas 12., 13. un 14.pants).		

¹¹ datu subjekta "piekrišana" ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei.

¹² Skatīt 29. panta darba grupas 2014. gada 9. aprīļa atzinumu 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu 3.1. punktu (pieejams: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lv.pdf)

Jautājumi	Atbildes	Piezīmes/ Trūkumi
Kādā gadījumā un kad datu subjekts tiek/tiks informēts par datu apstrādi konkrētam nolūkam?		
54. Kāda satura informācija tiek/tiks sniegta datu subjektam? Norādiet vai arī pievienojiet pielikumā, kāda informācija tiks sniegta datu subjektam par viņa personas datu apstrādi.		
55. Kā pārliecināties, vai sniegtā informācija patiešām nonāk pie attiecīgajām personām?		
56. Vai sniegtā informācija ir/būs pilnīga un viegli saprotama?		
57. Vai šim nolūkam apstrādātie dati ir pietiekami kvalitatīvi?		
58. Kādas varētu būt sekas datu subjektam, ja šajā procesā tiktu apstrādāti neprecīzi dati?		
59. Kā pārliecināties, ka iegūtie dati ir precīzi?		
60. Kā pārliecināties, ka no trešajām pusēm iegūtie dati ir precīzi?		
61. Vai tiks izmantoti rīki/resursi, ka ļauj atjaunināt/labot datus, ja nepieciešams? Ja jā, norādiet kādi.		
62. Vai neprecīzi dati varētu radīt zaudējumus datu subjektam un/vai pašvaldībai? Norādiet konkrēti kādus zaudējumus var radīt.		
63. Vai un kā tiks nodrošinātas datu subjekta piekļuves tiesības saviem datiem (tiesības saņemt informāciju par saviem datiem un datu kopijas) saistībā ar plānoto konkrēto nolūku jeb Procesu? (Vispārīgās datu aizsardzības regulas 15. pants)		
64. Vai un kā tiks nodrošinātas datu subjekta tiesības labot un dzēst datus? (Vispārīgās datu aizsardzības regulas 16., 17. un 19. pants)		
65. Vai un kā tiks nodrošinātas datu subjekta tiesības iebilst un ierobežot apstrādi? (Vispārīgās datu aizsardzības regulas 18., 19. un 21. pants)		
66. Vai datu subjektam būs pienākums par sevi sniegt datus un kādas var būt sekas tam, ja dati netiks sniegti? (Vispārīgās datu aizsardzības regulas 13.panta 2.punkta e) apakšpunkts, 14.panta 2.punkta e) apakšpunkts).		
67. Vai datu subjektam būs tiesības uz datu pārnesamību? (Vispārīgās datu aizsardzības regulas 20.pants) ¹³ Ja "Jā", norādiet kā tās tiks nodrošinātas.		
68. Vai pirms datu apstrādes uzsākšanas ir notikusi vai tiek plānota apspriešanās ar Datu valsts inspekciju?		

¹³ 29.panta Datu aizsardzības darba grupas izdotās "Pamatnostādnes par tiesībām uz datu pārnesamību".
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Jautājumi	Atbildes	Piezīmes/ Trūkumi
69. Vai personas datus izmantos profilēšanai ¹⁴ ?		
70. Vai attiecībā uz datu subjektu tiks pieņemti individuāli adresēti lēmumi, balstoties uz šo apstrādi? Kā izpaudīsies iespējamās tiesiskās sekas datu subjektam?		
71. Vai datu subjekts tiks pakļauts pilnībā automatizētai datu apstrādei? Paskaidrojiet detalizēti. Norādiet, kāda būs šī apstrādes loģika.		
V. Apstrādātāju piesaiste		
72. Vai datu apstrādi uzticēs trešajai personai/apstrādātājam ¹⁵ (turpmāk – “Pakalpojumu sniedzējs”)? Ja Pakalpojumu sniedzēji būs vairāki, norādiet zemāk minēto informāciju par katru no tiem.		
73. Norādiet Pakalpojuma sniedzēja rekvizītus (nosaukums, reģistrācijas numurs, valsts, adrese, tālruņa numurs, elektroniskā pasta adrese).		
74. Kāda ir Pakalpojuma sniedzēja loma/iesaiste nolūka sasniegšanā?		
75. Vai pakalpojumu sniedzējs piesaistīs sniedzot Jums pakalpojumu vēl arī citus pakalpojumu sniedzējus? Ja jā, norādiet kādus, un kādiem nolūkiem tie tiks piesaistīti.		
76. Kādiem datu veidiem/kategorijām Pakalpojuma sniedzējs varēs piekļūt?		
77. Kādas darbības Pakalpojuma sniedzējs ar datiem varēs veikt? (uzglabāt, pārveidot, pārsūtīt utt.)		
78. Kurā valstī Pakalpojuma sniedzējs apstrādās datus (t.sk. uzglabās)?		
79. Vai ir iespējams norādīt Pakalpojumu sniedzējam cik ilgi dati būtu jāuzglabā?		
80. Vai līgumā ar Pakalpojumu sniedzēju ir ietvertas vai plānots ietvert pienākumu Pakalpojuma sniedzējam pēc līguma termiņa beigām dzēst viņa rīcībā nonākušos datus, izņemot gadījumu, ja atkārtoti tiek slēgts līgumu ar to pašu ārpuspakalpojuma sniedzēju par to pašu līguma priekšmetu?		
81. Vai Pakalpojuma sniedzējs ir apliecinājis (sniedzis garantijas) atbilstību Vispārīgajai datu aizsardzības regulai? Norādiet, kā tas ir noticis vai vēl notiks.		
82. Vai Pakalpojuma sniedzējs ir definējis savas atbildības ierobežojumus? Kādus?		

¹⁴ 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

¹⁵ “apstrādātājs” ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus.

Jautājumi	Atbildes	Piezīmes/ Trūkumi
83. Vai pakalpojuma līgumā var ietvert nepieciešamos līguma grozījumus, lai kontrolētu datu apstrādi pie Pakalpojuma sniedzēja?		
84. Vai Pakalpojuma sniedzējs pievienojies kādiem rīcības kodeksiem, sertifikācijas mehānismiem vai standartiem (piem., ISO) saistībā ar datu aizsardzības aspektiem. Kādiem?		
85. Ja datus pārsūtīs, izmantojot elektroniskos sakaru kanālus, kādi pasākumi tiek veikti, lai nodrošinātu datu drošību?		
VI. Citi jautājumi		
86. Kā tiks kontrolēta un uzskaitīta datu izpaušana/nodošana iekšējiem (pašvaldības) datu saņēmējiem (darbiniekiem) un trešajām personām?		
87. Vai paredzēta datu nodošana ārpus ES/EEZ? Pozitīvas atbildes gadījumā, norādiet valsti.		
88. Kāds būs papildus tiesiskais pamats datu nodošanai ārpus ES/EEZ jeb kā tiks nodrošināts pietiekams aizsardzības līmenis? Kurš no pasākumiem tiks ieviests datu nodošanas gadījumā: 1. datu aizsardzība atbilstoši ES Komisijas lēmumam par datu nodošanu uz valstīm, kas neietilpst ES/EEZ; 2. aizsardzības pasākumi (līgums, vienošanās ar ietvertām ES līguma standartklausulām vai apstiprināti noteikumi, sertifikācijas mehānismi); 3. izņēmumi (juridiska pienākuma izpilde, tiesisku prasījumu īstenošana, būtiska sabiedrības interese, personas piekrišana, ar personu noslēgta līguma izpilde, līguma noslēgšana personas interesēs, izpilde).		
89. Vai ir identificējami vēl kādi citi riski, kas netika iekļauti iepriekšējās atbildēs?	Papildus drošības riskus, kurus var izvērtēt atbilstoši situācijai, var atrasts šeit: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf	

Ziņas par konsultēšanos ar uzraudzības institūciju (ja nepieciešams):

Ziņošanas datums:	
DVI atbilde:	
Pārziņa veiktās korektīvās darbības:	
DVI lēmums:	

Novērtējuma noslēguma informācija:

Novērtējuma veicējs:	
Novērtējuma veikšanas datums:	
Pašvaldības iestāde/struktūrvienība:	
Ziņas par trūkumu novēršanu/termiņš:	
Iepazīstinātas ar novērtējuma rezultātu sekojošas personas:	

Novērtējuma veicēja paraksts:	
-------------------------------	--

Riska vērtējums* un riska mazināšanas pasākumi

Riska Nr. (Jautāju mu sadaļas nr.)	Riska apraksts	Iespējamais Regulas pārkāpums	Riska vērtējums pirms korektīvām darbībām			Rekomend ācijas risku minimizēš anai	Atbildīgā persona (datumi)
			Riska iestāšanās iespējamība	Riska ietekme	Kopējais risku vērtējums (pēc tabulas)		
			☐ Zema ☐ Mērena ☐ Augsta ☐ Ļoti augsta ☐ Nenovēršama	☐ Zema ☐ Vidēji zema ☐ Vidēja ☐ Augsta ☐ Ļoti augsta	☐ Zema ☐ Vidēja ☐ Augsta		

Riska atkārtots vērtējums pēc riska mazināšanas pasākumiem (ja nepieciešams)

Riska Nr. (Jautāju mu sadaļas nr.)	Veiktās korektīvās darbības	Riska vērtējums pēc korektīvām darbībām		Atlikušās ietekmes vērtējums
		Riska iestāšanās iespējamība	Riska ietekme	
		☐ Zema ☐ Mērena ☐ Augsta ☐ Ļoti augsta ☐ Nenovēršama	☐ Zema ☐ Vidēji zema ☐ Vidēja ☐ Augsta ☐ Ļoti augsta	☐ Zema ☐ Vidēja ☐ Augsta

***Risku vērtējumu apraksts**

Iespējamības riska apraksts:

IESPĒJAMĪBA					
Skaitliskais novērtējums	1	2	3	4	5
Vārdiskais novērtējums	Zems risks	Mērens risks	Augsts risks	Ļoti augsts risks	Nenovēršams
Riska apraksts	Reti	Maz ticams	Iespējams	Ļoti iespējams	Gandrīz noteikti
	Šis risks iespējams nekad neiestāties	Nav sagaidāms, ka risks iestāties, tomēr iestāšanās ir iespējama	Risks var iestāties un pietiekoši regulāri	Risks visticamāk iestāties, neatkarīgi no apstākļiem.	Risks iestāties ar izteiktu regularitāti

Ietekmes riska apraksts:

IETEKME					
Skaitliskais novērtējums	1	2	3	4	5
Vārdiskais novērtējums	Zema	Vidēji zema	Vidēja	Augsta	Ļoti augsta
Riska apraksts	Datu subjekta tiesības nevar tikt apdraudētas	Atsevišķa ietekme uz datu subjekta privātumu būs, bet tā būs nebūtiska.	Datu subjekta privātums var tikt ietekmēts un radīt datu subjektam jūtamas sekas	Risks, radīs būtisku privātuma aizskārumu, bet kura ietekme var tikt kontrolēta	Risks, radīs būtisku privātuma aizskārumu, kura ietekmi samazināt datu subjektam iespējams neizdosies (t.sk. īpašu kategoriju datu izmantošana).

Augsta/vidēja/zema riska identifikācijas tabula:

IETEKME	Ļoti augsta (5)	V	A	A	A	A
	Augsta (4)	V	V	A/V	A	A
	Vidēja (3)	Z/V	V	V	A/V	A
	Vidēji zema (2)	Z	Z/V	Z/V	V	A/V
	Zema (1)	Z	Z	Z	Z	Z
	Zems risks (1)	Mērens risks (2)	Augsts risks (3)	Ļoti augsts risks (4)	Nenovēršams (5)	
IESPĒJAMĪBA						

Legitīmās intereses izvērtējums

Jautājumi	Komentāri
1. Vispārīga informācija:	
1.1. Plānotās datu apstrādes mērķis un vispārīgs apraksts:	
1.2. Izvērtējuma veicējs (vārds, uzvārds, amats):	
1.3. Izvērtējuma saskaņošanas procesā iesaistītās personas:	
1.4. Kādi datu veidi tiek pakļauti apstrādei:	
2. Tiesiskā pamata konceptuāla izvēle:	
2.1. Vai datu apstrādei varētu tikt izmantojama datu subjekta piekrišana [VDAR 6.p.1.d.(a) apakšpunkts]? Kādas identificētas problēmas šī tiesiskā pamata izmantošanai?	
2.2. Vai varētu dati būt nepieciešami līgumsaistību izpildei [VDAR 6.p.1.d.(b) apakšpunkts]? Kādas identificētas problēmas šī tiesiskā pamata izmantošanai?	
2.3. Vai datu apstrāde izriet no juridiska pienākuma [VDAR 6.p.1.d.(c) apakšpunkts]? Kādas identificētas problēmas šī tiesiskā pamata izmantošanai?	
2.4. Vai varētu datu apstrāde pamatota ar Datu subjekta vai trešās personas vitāli svarīgām interesēm [VDAR 6.p.1.d.(d) apakšpunkts]? Kādas identificētas problēmas šī tiesiskā pamata izmantošanai?	
2.5. Vai varētu datu apstrāde pamatota ar sabiedrības interesēm un/vai pārvaldes uzdevumu izpildi [VDAR 6.p.1.d.(e) apakšpunkts]? Kādas identificētas problēmas šī tiesiskā pamata izmantošanai?	
2.6. Vai datu apstrāde varētu tikt pamatota ar pārziņa vai trešās personas legītīmām interesēm [VDAR 6.p.1.d.(f) apakšpunkts]. Ja šis tiesiskais pamats tiek apsvērts aizpildiet novērtējuma turpmākos punktus.	
3. Pārziņa intereses likumības novērtēšana	
3.1. Vai kādā normatīvā aktā ir noteikts aizliegums vai ierobežojums apstrādāt šāda veida datus?	
3.2. Vai kāds normatīvais akts pieļauj/piešķir tiesības pārzinim apstrādāt šāda veida datus? Kādi ir priekšnoteikumi datu apstrādei?	
3.3. Vai interese ir nedefinēta pietiekami konkrēta, precīzi atspoguļojot problēmu? Sniedziet izvērtējumu.	
3.4. Vai interese ir pašreizēja un reāla (Vai nepieciešamība apstrādāt datus ir tūlītēja vai nākotnē noteikta)? Sniedziet izvērtējumu.	
3.5. Kādas būtu sekas, ja datu apstrāde netiktu veikta?	
4. Alternatīvu apstrādes veidu identificēšana un adekvātuma izvērtēšana	
4.1. Uzskaitiet alternatīvus veidus kā varētu sasniegt nepieciešamo mērķi, kā arī katra alternatīvā veida trūkumus un pozitīvās puses.	I alternatīva: Apraksts: _____ Pozitīvie efekti: _____ Trūkumi: _____ II alternatīva: Apraksts: _____ Pozitīvie efekti: _____ Trūkumi: _____ [...]
4.2. Vai mērķi nevar sasniegt ar mazāk datu apstrādi? Pamatojiet izmantojamo datu veidu nepieciešamību pakļaut apstrādei?	

4.3. Vai datu apstrādē tiek izmantoti īpašas kategorijas dati? Ja atbilde ir "Jā", pamatojiet papildus tiesiskā pamata esamību?	
5. Datu subjekta interešu novērtējums	
5.1. Kādu datu subjektu kategoriju dati tiks izmantoti apstrādē?	
5.2. Vai datu apstrādei var tikt pakļauti mazāk aizsargātu datu subjektu dati (piem., bērni, darbinieki, seniori)? Pamatojiet kādi papildus pasākumi tiks veikti šo datu subjektu tiesību aizsardzībai?	
5.3. Cik liels (skaitliski) datu subjektu skaits varētu tikt pakļauts apstrādei?	
5.4. Vai datus plānots publiskot?	
5.5. Vai datu subjekts apzināsies vai varētu apzināties, ka viņa dati tādā veidā varētu tikt apstrādāti (t.sk. iegūti)?	
5.6. Vai datu subjekts piespiedu kārtā ir pakļauts datu apstrādei vai ir dota izvēles brīvība attiecībā uz savu personas datu pakļaušanu apstrādei?	
5.7. Vai plānots veikt 'slēptu' datu apstrādi?	
5.8. Vai datu apstrāde notiek telpās un vietās ar paaugstinātu privātuma aizsardzību (WC, dušas telpas, pārgērbšanās kabīnes, darbinieku/klientu atpūtas telpas)	
5.9. Vai dati var saturēt informāciju, kuru datu subjekts vēlētos pastiprināti aizsargāt (neatkarīgi no tā vai tie ir Īpašas kategorijas dati), <i>piemēram, informācija par ienākumiem, privātas fotogrāfijas, paroles.</i>	
5.10. Vai dati tiks nodoti ārpus ES/EEZ? Kā tas var ietekmēt datu drošību?	
6. Papildus līdzsvarošanas pasākumi:	
6.1. Vai ir iespējams datu apstrādi nošķirt no citu mērķu datu apstrādes (funkcionālais nošķīrums)?	
6.2. Vai ir iespējams piešķirt datu subjektam neapstrīdamu atteikšanās tiesību?	
6.3. Vai datu apstrādē ir iespējams izmantot pseidonimizācijas rīkus, <i>piemēram identifikatoru piešķiršanu?</i>	
6.4. Kā tiks nodrošināta datu subjektu informēšana par veicamo apstrādi?	
6.5. Kādi varētu tikt noteikti glabāšanas termiņi?	
6.6. Izvērtējums par nepieciešamību pēc Novērtējuma par datu apstrādes ietekmi uz datu aizsardzību:	
6.7. Kāda būs Pārziņa rīcība datu subjektu iebildumu saņemšanas gadījumā?	
7. Citi konstatētie apsvērumi, kas var ietekmēt izvērtējamo datu apstrādi.	
8. Gala lēmums (vai izvirzītais datu apstrādes mērķis ir samērīgs ar personu privātumu):	
Datums:	
Paraksts:	

Veidlapa personas datu apstrādes darbību reģistrācijai

Jelgavas valstspilsētas pašvaldības

Datu apstrāde Nr. ____

Reģistra informācija	Apraksts:
Apstrādes nolūks/mērķis	
Apstrādes tiesiskais pamatojums (likumi, noteikumi, piekrišana, līgums ar personu, u.c.)	
Datu subjektu kategorijas (personas, kuru datus apstrādās)	
Personas datu veidi (identif.i.- vārds, uzvārds, p.k., kontaktinfo. – tālrunis, e-pasts, u.c.)	
Datu saņēmēju kategorijas (sadarbības partneri, pakalpojumu sniedzēji u.c., kas pieklūs datiem – sist. uzturēšana, datu glabāšana)	Nosaukums, apstrādes būtība:
Datu glabāšanas termiņi /dzēšanas kritēriji	
Informācija par datu nosūtīšanu uz trešo valsti (ārpus ES/EEZ) vai starptautisku organizāciju	Ir / Nav plānota datu nodošana uz trešo valsti vai starptautisku organizāciju. Ja IR plānota, atzīmēt, kuru no pasākumiem ieviešīs: ☐ datu aizsardzība atbilstoši ES Komisijas lēmumam par datu nodošanu uz valstīm, kas neietilpst ES/EEZ; ☐ aizsardzības pasākumi (līgums, vienošanās ar ietvertām ES līguma standartklauzulām vai apstiprināti noteikumi, sertifikācijas mehānismi); ☐ izņēmumi (juridiska pienākuma izpilde, tiesisku prasījumu īstenošana, būtiska sabiedrības interese, personas piekrišana, ar personu noslēgta līguma izpilde, līguma noslēgšana personas interesēs, izpilde)
Loma (atzīmēt ar "X")	☐ Pārzinis ☐ Apstrādātājs
Īpaši noteikto tehnisko/ organizatorisko drošības pasākumu apraksts (instrukcijas, kārtības, datu šifrēšana, pseidonimizēšana, auditācijas pieraksti, ierobežotas piekļuves, dubultā verifikācija)	Datu apstrādes sistēma: Datu ieguves veids: Datu precizitātes pārbaudes/atjaunošanas/labojšanas procesa apraksts: Drošības pasākumi:

(vārds, uzvārds, amats)

(paraksts)

Sadarbības partnera izvērtēšanas anketa

Anketas apraksts:

Šīs anketas mērķis ir novērtēt sadarbības partnera - pašreizējo gatavību un atbilstību Eiropas Parlamenta un Padomes Regulai (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), turpmāk – VДАР, un Mākslīgā intelekta aktam, turpmāk - MI akts, kas nosaka pienākumus attiecībā uz mākslīgā intelekta risinājumu izmantošanu datu apstrādē.

Anketā izmantotie termini:

Personas dati - jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu, kuru tieši vai netieši var identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, vārdu/uzvārdu, personas kodu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem faktoriem, kas raksturīgi šīs personas fiziskajai, fizioloģiskajai, ģenētiskajai, garīgajai, ekonomiskajai, kultūrvēsturiskajai, ekonomiskajai, kultūras vai sociālajai identitātei.

Personas datu apstrāde attiecas uz jebkuru darbību vai darbību kopumu, ko veic, izmantojot personas datus vai personas datu kopas, neatkarīgi no tā, vai tie ir vai nav automatizēti līdzekļi, piemēram, savākšana, reģistrēšana, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, izguve, apspriešana, izmantošana, izpaušana, pārraidot, izplatot vai citādi padarot pieejamus, saskaņojot vai apvienojot, ierobežojot, dzēšot vai iznīcinot.

Datu pārkāpums ir drošības pārkāpums, kas izraisa nejaušu vai nelikumīgu iznīcināšanu, nozaudēšanu, pārgrozīšanu, neatļautu izpaušanu vai piekļuvi tiem, ko pārraida, glabā vai citādi apstrādā.

ES/EEZ – attiecas uz ES/EEZ līgumā noteikto jomu, kurā ietilpst 27 Eiropas Savienības dalībvalstis un trīs EBTA valstis (Eiropas Brīvās tirdzniecības asociācija), kurām ir saistošs nolīgums par Eiropas Ekonomisko zonu (EEZ). 27 dalībvalstis ir Austrija, Beļģija, Bulgārija, Horvātija, Kipra, Čehija, Dānija, Igaunija, Somija, Francija, Vācija, Grieķija, Ungārija, Īrija, Itālija, Latvija, Lietuva, Luksemburga, Malta, Nīderlande, Polija, Portugāle, Rumānija, Slovākija, Slovēnija, Spānija, Zviedrija. EBTA valstis, kurām arī ir saistošs datu aizsardzības regulējums, ir Islande, Lihtenšteina un Norvēģija.

Piemērojamība — VДАР attiecas uz personas datu apstrādi, ko veic organizācijas (darbojoties kā pārzinis vai apstrādātājs) ES/EEZ neatkarīgi no tā, vai apstrāde notiek ES/EEZ vai nē. VДАР attiecas arī uz tādu personas datu apstrādi, kuru ES/EEZ veic pārzinis vai apstrādātājs, kas nav reģistrēts ES/EEZ, ja apstrādes darbības ir saistītas ar:

- preču vai pakalpojumu piedāvāšanu, neatkarīgi no tā, vai ir nepieciešams datu subjekta maksājums, šādiem datu subjektiem ES/EEZ; vai
- datu subjektu uzvedības uzraudzība, ciktāl to rīcība notiek ES/EEZ.

Vārds, uzvārds, amats personai, kura aizpilda šo anketu:

Pakalpojuma sniedzēja/piegādātāja organizācijas/uzņēmuma nosaukums:

Datums:

Vispārēja informācija	
1. Datu apstrādes apraksts <i>Piemēram, ja videonovērošanas sistēmas uzturēšana, tad - kas paredzēts uzturēšanas ietvaros utt.</i>	
2. Datu apstrādes procesa apraksts <i>Aprakstiet, kā dati tiks iegūti, glabāti, apstrādāti. Kādas informācijas sistēmas tiks izmantotas.</i>	
3. Drošības pasākumu apraksts <i>Aprakstiet, uz kādiem resursiem tiks glābti dati, kā šie dati tiks aizsargāti.</i>	

Tēma	Jautājums	Atbilde
4. Pārskatatbildība (VDAR, 5 (2))	Vai spējat uzskatāmi parādīt atbilstību sniegt garantijas, ka tiks īstenoti atbilstoši tehniskie un organizatoriskie pasākumi tādā veidā, ka apstrādē tiks ievērotas VDAR prasības un tiks nodrošināta datu subjekta tiesību aizsardzība? Ja atbilde ir “Jā”, tad uzskaitiet procedūras un politikas, kas ir izstrādātas un ieviestas: 4.1. Personas datu apstrādes kārtība 4.2. Datu aprites un glabāšanas kārtība vai datu dzēšanas process 4.3. Informācijas tehnoloģiju drošības politika 4.4. Sertifikācijas mehānismi, kas apliecina personas datu apstrādes drošību (piemēram, 27001) 4.5. Personas datu apstrādes reģistrs 4.6. Iekšēja kārtība personas datu pārkāpumu identificēšanai un ziņošanai 4.7. Datu subjektu pieprasījumu izskatīšanas kārtība	☐ Jā ☐ Nē ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir

	Citas procedūras vai politikas:	
5. Tiesības labot (VDAR, 16)	Vai ir dokumentēta procedūra neprecīzu datu subjekta personas datu labošanai, ja to pieprasa Pārzinis? Ja atbilde ir "Nē", tad aprakstiet, kā paredzēts organizēt datu labošanu:	☐ Jā ☐ Nē
6. Tiesības uz dzēšanu / tiesības „tikt aizmirstam” (VDAR, 17)	Vai ir dokumentēta procedūra personas datu dzēšanai, ja to pieprasa Pārzinis? Ja atbilde ir "Nē", tad aprakstiet kā paredzēta datu dzēšana/iznīcināšana:	☐ Jā ☐ Nē
7. Tiesības ierobežot apstrādi (VDAR, 18)	Vai pastāv iespēja veikt personas datu apstrādes ierobežošanu (uzglabātu personas datu iezīmēšana ar mērķi ierobežot to apstrādi nākotnē), ja to pieprasa Pārzinis?	☐ Jā ☐ Nē
8. Tiesības uz datu pārnēsamību (VDAR, 20)	Vai pastāv iespēja nodrošināt Pārziņa personas datu pārnēsamību? Tas ir, vai spējat, pēc Pārziņa pieprasījuma, nodrošināt personas datu izsniegšanu strukturētā, plaši izmantotā un mašīnlasāmā formātā, un, vai spējat minētos datus nodot citam Pārzinim vai Apstrādātājam?	☐ Jā ☐ Nē
9. Datu apstrādes līgums - DAL (VDAR, 28)	Vai ir dokumentēta procedūra Pārziņa informēšanai par jebkādam iecerētajām pārmaiņām saistībā ar papildu apstrādātāju (apakšapstrādātāju) vai apstrādātāja aizstāšanu? Vai nodrošināt, ka iesaistītie papildus apstrādātāji sniedz pietiekamas garantijas, īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai apstrāde saglabātu noteikto Pārziņa personas datu aizsardzību?	☐ Jā ☐ Nē ☐ Jā ☐ Nē
10. Apstrāde Pārziņa vai Apstrādātāja pakļautībā (VDAR, 28, 29)	Vai visiem darbiniekiem (iekšējie un ārējie), kas strādā ar Pārziņa personas datiem, ir saistības ievērot datu aizsardzību un konfidencialitāti? (<i>piemēram, iegūts saistībraksts, darba pienākumi, konfidencialitātes apliecinājumi utt.</i>) Vai informējat par konfidencialitātes prasībām un apmācāt darbiniekus, kuri strādā ar Pārziņa personas datiem? Ja atbilde ir "Jā", lūdzu norādīt, cik bieži un kādā formā:	☐ Jā ☐ Nē ☐ Jā ☐ Nē

11. Personas datu apstrādes drošība (VDAR, 24,32)	Kādi organizatoriskie un tehnoloģiskie aizsardzības līdzekļi ir ieviesti personas datu aizsardzības nodrošināšanai? 11.1. Izveidota paroļu pārvaldība ar noteiktu sarežģītības līmeni un atjaunošanas kārtību. 11.2. Pieejas tiesību pārvaldība konkrētiem darbiniekiem noteiktu pienākumu veikšanai. 11.3. Darbību logošana. 11.4. Ugunsmūris. 11.5. VPN. 11.6. Šifrēšana. 11.7. Tiek veidotas rezerves kopijas. 11.8. Ieviests process personas datu drošības pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai. 11.9. Datorsistēmā izmanto tikai licencētas programmatūras, ko atjauno, kategoriski aizliedzot datu apstrādē izmantot nelicencētas programmatūras. 11.10. Ir ieviesta tīrā galda politika. 11.11. Ir aizliegts izpaust personas datus ar procesu nesaistītām trešajām personām. 11.12. Aizliegts apspriest ar darbu saistītus jautājumus sabiedriskās vietās, citiem dzirdot. 11.13. Spēja nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību. 11.14. Atjaunošana un iespēja savlaicīgi piekļūt personas datiem fiziska vai tehniska rakstura incidenta gadījumā. 11.15. Procesi, lai regulāri pārbaudītu, novērtētu un novērtētu tehnisko un organizatorisko pasākumu efektivitāti apstrādes drošības nodrošināšanai. 11.16. Citi (lūgums norādīt):	☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir ☐ Ir
12. Personas datu aizsardzības pārkāpumu (PDAP) procedūra (VDAR, 33)	Vai PDAP gadījumiem ir dokumentēta procedūra: 12.1. lai, tiklīdz kļuvis zināms PDAP, bez nepamatotas kavēšanās paziņotu Pārzinim? 12.2. lai dokumentēt visus faktus, kas attiecas uz PDAP, tā ietekmi un veiktajām koriģējošām darbībām? 12.3. lai saglabātu digitālos pierādījumus PDAP izskatīšanas vajadzībām? 12.4. lai darbinieki ir iepazīstināti ar kārtību rīcībai personas datu aizsardzības pārkāpuma gadījumā? Lūgums precizēt, kas to apliecina:	☐ Jā ☐ Nē ☐ Jā ☐ Nē ☐ Jā ☐ Nē ☐ Jā ☐ Nē

13. Personas datu nosūtīšana uz trešām valstīm vai starptautiskām organizācijām (VDAR, 5.nodaļa)	Vai uzņēmums apstrādā personas datus ārpus Eiropas Savienības vai EZZ (attiecas arī uz personas datu glabāšanu, izmantojot mākoņu pakalpojumus)? Lūgums precizēt serveru atrašanās vietas:		☐ Jā ☐ Nē
14. Personas datu nosūtīšana uz trešām valstīm vai starptautiskām organizācijām (VDAR, 5.nodaļa)	Ja uzņēmums apstrādā personas datus ārpus Eiropas Savienības vai EZZ, kādi drošības mehānismi tiek izmantoti? Līguma standartklauzulas Lēmums par aizsardzības līmeņa pietiekamību Saistošie uzņēmuma noteikumi Citi (lūgums norādīt):		☐ ☐ ☐
15. Datu aizsardzības speciālista (DAS) iecelšana (VDAR, 37,38, 39)	Vai jūsu organizācijā ir iecelts DAS, kurš ir pienācīgi iesaistīts un savlaicīgi informēts par visiem jautājumiem, kas attiecas uz personas datu aizsardzību? Ja atbilde ir „Jā”, lūdzu, norādiet DAS vārdu, uzvārdu un kontaktdatus:		☐ Jā ☐ Nē
16. Mākslīgā intelekta risinājumu izmantošana (MI akts, 3)	Mākslīgā intelekta (sistēma, kura projektēta darboties ar dažādiem autonomijas līmeņiem, kura var pēc ieviešanas būt adaptīva, un kura secina no informācijas, ko tā saņem, kā ģenerēt iznākumus, piemēram, prognozes, saturu, ieteikumus vai lēmumus) izmantošana		
	16.1. Vai jūsu organizācija izmanto MI risinājumus pakalpojumu sniegšanā?	☐ Jā ☐ Nē	
	16.2. Vai jūsu organizācija izmanto MI risinājumus persona datu apstrādē sniegto pakalpojumu ietvaros?	☐ Jā ☐ Nē	
	16.3. Vai izmantotais MI risinājums ir organizācijas pašas izstrādāts?	☐ Jā ☐ Nē ☐ Daļēji	
	16.4. Ja izmantojat MI risinājumu ārpalpojumu, lūdzu, norādiet nosaukumu:		

17. Mākslīgā intelekta risinājuma atbilstība (MI akts, 5, 6)	17.1. Vai kāds no izmantotajiem MI risinājumiem izmanto paņēmienus, lai būtiski iespaidotu personas uzvedību?	☐ Jā ☐ Nē
	17.2. Vai kāds no MI risinājumiem izmanto kādu no šīm fiziskas personas (vai grupas) iezīmēm: vecumu, invaliditāti, sociālo stāvokli vai ekonomisko stāvokli?	☐ Jā ☐ Nē
	17.3. Vai kāds no izmantotajiem MI risinājumiem izvērtē vai klasificē fiziskas personas noteiktā laikposmā, pamatojoties uz viņu sociālo uzvedību vai personas īpašībām un tas rada kaitējošu vai nelabvēlīgu attieksmi pret personu?	☐ Jā ☐ Nē
	17.4. Vai kāds no izmantotajiem MI risinājumiem prognozē fiziskas personas risku izdarīt noziedzīgu nodarījumu?	☐ Jā ☐ Nē
	17.5. Vai kāds no izmantotajiem MI risinājumiem izveido vai paplašina sejas atpazīšanas datubāzes, nemērķorientēti rasmojot sejas attēlus no interneta vai videonovērošanas sistēmu video?	☐ Jā ☐ Nē
	17.6. Vai kāds no izmantotajiem MI risinājumiem izsecina fiziskas personas emocijas?	☐ Jā ☐ Nē
	17.7. Vai kāds no izmantotajiem MI risinājumiem kategorizē fiziskās personas pēc biometriskajiem datiem, lai izsecinātu viņu rasi, politiskos uzskatus, dalību arodbiedrībās, reliģiskos vai filozofiskos uzskatus, dzimumdzīvi vai seksuālo orientāciju?	☐ Jā ☐ Nē
	17.8. Vai tiek izmantota reāllaika biometriskās tālidentifikācijas sistēma publiskās vietās?	☐ Jā ☐ Nē

Aizpildītāja paraksts _____

Tipveida noteikumi par personas datu apstrādi

1. Personas datu apstrāde

- 1.1. Ņemot vērā, ka Līguma izpildes ietvaros _____ kā Apstrādātājs sniedz _____ kā Pārzinim _____ pakalpojumu, kas ir saistīts ar personas datu apstrādi, Puses apņemas apstrādāt iegūtos fizisko personu datus minimālajā apjomā atbilstoši apstrādes nolūkam un ievērojot personas datu aizsardzības normatīvo aktu prasības, t.sk. Eiropas Parlamenta un Padomes regulas Nr.2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), turpmāk - Regula, Nacionālā kiberdrošības likuma un uz tā pamata izdoto Ministru kabineta noteikumu noteiktās prasības, t.sk. attiecībā uz informācijas sistēmu atbilstību minimālajām kiberdrošības prasībām, veicamajiem pasākumiem informācijas sistēmu konfidencialitātes, integritātes un pieejamības nodrošināšanai, datu atjaunošanai, dzēšanai, datu glabāšanai un izvietojšanai, tostarp, nodrošinot, ka personas dati:
 - 1.1.1. tiks apstrādāti likumīgi, godprātīgi un datu subjektiem pārredzamā veidā, lai izpildītu noteiktos pienākumus un kontroles institūciju prasības, neveicot apstrādi ar Līguma izpildi nesavietojamā veidā;
 - 1.1.2. ir precīzi un nepieciešamības gadījumā tiks atjaunināti un tiek glabāti veidā, kas pieļauj personu identifikāciju ne ilgāk, kā nepieciešams konkrētā mērķa sasniegšanai Līguma izpildē;
 - 1.1.3. tiks apstrādāti tādā veidā, lai nodrošinātu normatīvajiem aktiem atbilstošu datu drošību, t.sk. aizsardzību pret neatļautu vai nelikumīgu apstrādi un nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, fiziskās iedarbības radītu personas datu apdraudējumu;
 - 1.1.4. ir izstrādājis iekšējās, darbiniekiem saistošās procedūras, veicis savu darbinieku apmācīšanu, iepazīstināšanu ar līguma nosacījumiem, nodrošina sistēmas pierakstu veidošanu (ietverot informācijas sistēmas žurnālfailu un tīkla plūsmas žurnālfailus informācijas sistēmām un to darbību nodrošinotām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām, kas saistīti ar personas datu apstrādi).
- 1.2. Puses ievieš attiecīgas tehniskās un organizatoriskās prasības un pasākumus, kas nepieciešami personas datu apstrādes drošībai, uzņemas atbildību par attiecīgo personas datu apstrādi, t.sk. prasību ieviešanu un pārskatīšanu, saskaņā ar normatīvajos aktos noteikto kārtību un paredz šo prasību nepārtrauktu pārskatīšanu, lai nodrošinātu nepārtrauktu apstrādes sistēmu un pakalpojumu konfidencialitāti, integritāti, pieejamību un noturību.
- 1.3. Jaunu, būtisku datu apstrādes līdzekļu ieviešanu informācijas sistēmās Apstrādātājs veic tikai ar rakstisku Pārziņa piekrišanu.
- 1.4. Apstrādātājs veic _____ personu datu apstrādi ar mērķi _____.
- 1.5. Personas datu apstrādes ilgums ir _____ vai līdz brīdim, kad pēc Pārziņa paziņojuma nepieciešams izbeigt konkrēta datu subjekta personas datu apstrādi.
- 1.6. Līguma izpildes ietvaros tiks apstrādāti šādi personas dati: _____.
- 1.7. Līguma ietvaros tiks veiktas šādas darbības ar personas datiem:
 - 1.7.1. Pārzinis: _____.
 - 1.7.2. Apstrādātājs (t.sk. norāda apakšapstrādātājus, ja tādi ir): _____.
- 1.8. Personas datu nodošana tiek veikta izmantojot: _____, Apstrādātājam apstrādājot personas datus _____.
- 1.9. Pušu pienākumi un tiesības:
 - 1.9.1. Apstrādātājs veic apstrādi saskaņā ar Līguma nosacījumiem, Pārziņa norādījumiem un Regulas prasībām.
 - 1.9.2. Apstrādātājs pieklūst Pārziņa nodotajiem personas datiem ir tiesīgi tikai identificējamī Apstrādātāja darbinieki, kurus Apstrādātājs ir pilnvarojis konkrētās datu apstrādes veikšanai, nodalot piekļuvi informācijai un ievērojot nosacījumus un, kuri ir rakstveidā apņēmušies nelikumīgi neapstrādāt personas datus, t.sk., bet ne tikai: nelikumīgi neizpaust, nepārrunāt, nenodot datus citām personām, nelikumīgi neglabāt, kā arī neveikt jebkuras darbības ar personas datiem, kas ir ārpus piešķirtā pilnvarojuma, t.sk. arī pēc darba vai citu tiesisko attiecību izbeigšanas.
- 1.9.3. Apstrādātājs veic pasākumus personas datu apstrādes informācijas sistēmu un pakalpojumu nepārtrauktas konfidencialitātes, integritātes, pieejamības un noturības nodrošināšanai un aizsardzībai pret fiziskās iedarbības radītu personas datu apdraudējumu, tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai, lai nodrošinātu apstrādes drošību, saskaņā ar iekšējiem un apstrādi regulējošiem ārējiem normatīvajiem aktiem un, gadījumā, ja noticis incidents, nodrošina nekavējošu personas datu pieejamības un piekļuves atjaunošanu.

- 1.9.4. Apstrādātājs dara Pārzinim pieejamu visu informāciju, kas nepieciešama, lai apliecinātu, ka tiek pildīti šajā Līgumā un Regulā paredzētie Apstrādātāja pienākumi, t.sk. Regulas 28.pantā, 32. līdz 36. pantā noteiktie pienākumi attiecībā uz datu drošību, palīdzību Pārzinim atbildēt uz datu subjekta pieprasījumiem par to tiesību īstenošanu, paziņošanu par datu aizsardzības pārkāpumiem uzraudzības iestādei un/vai datu subjektam, datu aizsardzības novērtējuma veikšanu un pienākumu iepriekš konsultēties saskaņā ar normatīvajos aktos noteiktajiem Apstrādātāja pienākumiem, ņemot vērā datu apstrādes būtību un Apstrādātājam pieejamo informāciju.
- 1.9.5. Apstrādātāja pienākums ir veikt tikai tādu datu apstrādi, kas nepieciešama konkrētajam nolūkam, nodrošinot apstrādes drošības līmeni, kas atbilst novērtētam riskam attiecībā uz fizisko personu tiesībām un brīvībām, tostarp atbilstoši Regulas 32.pantam, t.sk. nodrošinot, ka viņa tehniskie līdzekļi ļauj veikt ierakstus par apstrādes darbībām un nodrošina ugunsmūra funkcionalitāti, datu rezerves kopiju veidošanu, veic regulāras to atjaunošanas pārbaudes un, ja iespējams, datu pseidonimizāciju un šifrēšanu.
- 1.9.6. Apstrādātājs uztur visus uzskaites ierakstus, kuri nepieciešami atbilstoši normatīvajiem aktiem attiecībā uz Apstrādātāja veikto personas datu apstrādi, un padara šos ierakstus pieejamus Pārzinim, saņemot attiecīgu Pārziņa pieprasījumu.
- 1.9.7. Pārzinim ir tiesības ierosināt un veikt neatkarīgas drošības pārbaudes attiecībā uz tādu netieši identificējamo personas datu apjomu, ko Apstrādātājs apstrādā Pārziņa uzdevumā. Pārzinim vai Pārziņa ieceltam revidentam ir tiesības pārbaudīt apstrādes darbības, īpaši attiecībā un tehniskajiem un organizatoriskajiem pasākumiem, lai apstiprinātu to atbilstību šim Līgumam un Vispārīgai datu aizsardzības regulai.
- 1.9.8. Apstrādātājs saprātīgā termiņā nodrošina Pārzinim visus nepieciešamos materiālus, dokumentus, vērtējumus un citu informāciju, lai veicinātu ar personas datiem saistīto apstrādes darbību visaptverošu pārskatīšanu vai pierādītu Apstrādātāja darbības atbilstību Vispārīgai datu aizsardzības regulai un informācijas drošības un kiberdrošības prasībām.
- 1.9.9. Pārzinis nodrošina, ka Apstrādātājam tiek nodoti tikai tādi personas dati, kuru apstrāde ir leģitīma.
- 1.10. Rīcība datu aizsardzības pārkāpuma/incidenta gadījumā:
- 1.10.1. Apstrādātājam ir pienākums informēt Pārzini par personas datu aizsardzības pārkāpumu (drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem) un drošības incidenta (kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte) gadījumu, ja tas notiek apstrādājot Pārziņa fizisko personu datus, izņemot gadījumus, kad maz ticams, ka varētu tikt radīts risks fizisku personu tiesībām, brīvībām vai Pārzinim.
- 1.10.2. Ja iestāties kāds no drošības incidentiem vai datu pārkāpumiem, Apstrādātājam pēc iespējas ātrāk, bet ne vēlāk kā 24 stundas pēc atklāšanas vai sūdzības saņemšanas jāinformē Pārzinis, darot zināmu šādu informāciju: pārkāpuma vai incidenta apraksts, t.sk. ietekmētie datu subjekti un aptuvenais skaits, ietekmētie personas datu ieraksti un aptuvenais skaits; datu aizsardzības speciālista vārds, uzvārds un kontaktinformācija vai norāda citu kontaktpersonu ar mērķi iegūt papildus informāciju par pārkāpumu vai incidentu; iespējamo seku apraksts; pasākumu, ko Apstrādātājs veicis vai ierosinājis veikt, lai novērstu pārkāpumu, apraksts, tostarp pasākumi, lai mazinātu iespējamās nelabvēlīgās sekas par:
- 1.10.2.1. drošības incidentiem uz it@jalgava.lv un pa tālruni +371 63005555;
- 1.10.2.2. personas datu pārkāpumiem uz dati@jalgava.lv un pa tālruni +371 63005444.
- 1.10.3. Ja Apstrādātājam nav iespējams sniegt visu iepriekš norādīto informāciju par pārkāpumu vai incidentu vienlaikus, tad informāciju var sniegt daļām. Informāciju sniedz bez nepamatojamas kavēšanās.
- 1.10.4. Apstrādātāja kontaktinformācija datu aizsardzības pārkāpuma/incidenta konstatēšanas gadījumā:
- 1.10.4.1. e-pasts _____,
- 1.10.4.2. tālrunis _____.
- 1.10.5. Apstrādātājs, ņemot vērā apstrādes raksturu un pieejamo informāciju, apņemas palīdzēt Pārzinim pārkāpumu fiksēšanā un paziņošanā uzraudzības iestādei un/vai datu subjektam, kā arī, ja nepieciešams, novērtējuma par ietekmi uz datu aizsardzību veikšanā un tā iepriekšējā apspriešanā ar uzraudzības iestādi.
- 1.10.6. Apstrādātājs nodrošina iekšējo kārtību rīcībai personas datu aizsardzības pārkāpuma gadījumā – noteiktas atbildības, noteiktas pārkāpumu ziņošanas un risināšanas procedūras, izstrādāta instrukcija, apmācīti darbinieki.
- 1.10.7. Pārkāpumu novēršanas gadījumā Apstrādātājam ir pienākums saglabāt pierādījumus par to, kādi tehniskie pasākumi un uzlabojumi tika veikti, lai tiku novērsts risks, ka pārkāpums iestājas atkārtoti.
- 1.10.8. Ja tiek konstatēts, ka veicot datu apstrādi ir noticis kiberdrošības incidents, Apstrādātājs apņemas informēt par notikušo incidentu ne tikai Pārzini šī Līguma noteiktajā kārtībā, bet arī valsts kiberdrošības iestādes (tajā skaitā, CERT), ja tas ir nepieciešams saskaņā ar Nacionālā kiberdrošības likuma prasībām vai citiem piemērojamiem tiesību aktiem, vai Pārziņa norādījumiem, kā arī sniegt detalizētu pārskatu Pārzinim par veiktajiem pasākumiem pārkāpuma pārvaldīšanai un nodrošināt pilnu notikumu žurnālu.
- 1.10.9. Pārzinim ir tiesības bez iepriekšēja brīdinājuma uzdot Apstrādātājam apturēt fizisko personu datu apstrādi, ja tam rodas šaubas par fizisko personu datu apstrādes atbilstību normatīvo aktu prasībām.
- 1.11. Citu apstrādātāju piesaiste, sadarbība un atbildība:

- 1.11.1. Ja Apstrādātājs izmanto personas datu apstrādei citas juridiskās vai fiziskas personas, Apstrādātājs nodrošina, ka pie Pašvaldības nodotajiem personas datiem var piekļūt tikai tie darbinieki, kas ir iesaistīti Līguma izpildē, nodrošinot to pienācīgu informēšanu par Līgumā noteikto prasību ievērošanu, neapstrādājot datus citādi, kā noteikts Līgumā un saistošajos norādījumos, kā arī uzrauga un nodrošina iesaistīto personu regulāru informēšanu un apmācību par drošības un aizsardzības prasībām personas datu apstrādē.
- 1.11.2. Apstrādātājs personas datu apstrādē iesaistītajam personālam nosaka un līgumā ar apakšapstrādātāju iekļauj identiskas konfidencialitātes un personas datu aizsardzības prasības, kādas noteiktas šajā Līgumā. Apstrādātājs ir tieši atbildīgs par apakšapstrādātāja veiktās personas datu apstrādes atbilstību Līgumā noteiktajām un Regulas prasībām savas kompetences ietvaros.
- 1.11.3. Par Līgumā noteiktajai datu apstrādei piesaistītajiem apakšapstrādātājiem, Apstrādātājam rakstveidā jāinformē Pārzinis pirms Līguma noslēgšanas vai 10 (desmit) darbdienu laikā pēc līguma ar apakšapstrādātāju noslēgšanas. Ja Pārzinis konstatē, ka konkrētā apakšapstrādātāja piesaiste neatbilst noteiktajām drošības prasībām, Pārzinis pārtrauc datu nodošanu un nepieciešamības gadījumā vienpusēji izbeidz Līgumu, par to 3 darbdienu iepriekš brīdinot Apstrādātāju.
- 1.11.4. Puses pēc otras Puses rakstiska pieprasījuma atbilstoši savai kompetencei sniedz informāciju, kas nepieciešama atbildot uz datu subjekta pieprasījumu par viņa datu apstrādi Līguma ietvaros un, lai pierādītu, ka personas datu apstrāde tiek veikta saskaņā ar Līgumu un saistošajiem normatīvajiem aktiem.
- 1.11.5. Pārzinis bez papildus atlīdzības var pieprasīt Apstrādātājam iesniegt pārskatu par apakšuzņēmējiem, kas veic personas datu apstrādi saskaņā ar Līgumu.
- 1.11.6. Katra no Pusēm Līguma izpildes ietvaros savstarpēji apmainoties ar Pušu pilnvaroto pārstāvju, nodarbināto identificējošo informāciju un kontaktinformāciju, kas satur personas datus informē par to, kādi viņu dati tiek nodoti otrai Pusei, norādot otras Puses nosaukumu, kontaktinformāciju un mērķi, kādiem nodotie personas dati varētu tikt izmantoti, un to, kādas ir viņu kā datu subjektu tiesības apstrādes ietvaros.
- 1.11.7. Apstrādātājs ir atbildīgs par zaudējumiem, kas radušies Pārzinim un datu subjektam nodarīto kaitējumu, kas nodarīts ar apstrādi, ja Apstrādātājs vai tā pilnvarotās personas nav izpildījušas šajā Līgumā, Regulā paredzētos Apstrādātāja pienākumus un Pārziņa likumīgus norādījumus.
- 1.11.8. Apstrādātājs par katru personas datu aizsardzības pārkāpumu, kas radies Apstrādātāja, vai tā pilnvarotās personas dēļ, maksā Pārzinim līgumsodu 10% (desmit procenti) apmērā no Līguma summas un atlīdzina pārkāpuma rezultātā Pārzinim nodarītos zaudējumus, t.sk. atmaksā izmaksāto kompensāciju vai tās daļu Pārzinim, soda sankcijas, ja tādas piemērotas. Līgumsoda samaksa neatbrīvo Izpildītāju no visu zaudējumu atlīdzināšanas pienākuma un pārējo Līguma saistību izpildes.
- 1.12. Personas datu apstrādes labošana vai apstrādes ierobežošana un izbeigšana:
- 1.12.1. Pēc Apstrādes pabeigšanas vai pārtraukšanas Apstrādātājs pēc Pārziņa izvēles pusēm vienojoties par termiņu nodod atpakaļ vai dzēš, iznīcina visus Pārziņa sniegtos Personas datus un personas datu saturošas informācijas kopijas, ja vien noteiktu datu glabāšanu nepieprasa saistošie normatīvie akti.
- 1.12.2. Apstrādātājam ir pienākums dokumentēt dzēšanas procesu un sniegt Pārzinim pierādījumus par datu dzēšanu, iesniedzot rakstveida apliecinājumu 10 (desmit) kalendāro dienu laikā pēc datu iznīcināšanas, kā arī iespēju veikt dzēšanas procesu neatkarīgu pārbaudi, ja Pārzinis devis Apstrādātājam norādījumus dzēst datus saskaņā ar Līgumā noteikto kārtību.
- 1.12.3. Apstrādātājam ir pienākums sniegt Pārzinim ne vēlāk kā 5 (piecu) dienu laikā visu informāciju par Līguma ietvaros apstrādājamo fizisko personu datu pieprasījumiem no datu subjekta vai trešo personu puses, ja Apstrādātājs tādus saņēms.
- 1.12.4. Apstrādātājs tikai ar iepriekšēju rakstisku Pārziņa piekrišanu var sūtīt personas datus ārpus Eiropas Savienības, Eiropas Ekonomiskās Zonas vai uz citu valsti, kas saskaņā ar Eiropas Komisijas viedokli garantē pietiekamu datu aizsardzības līmeni.
- 1.12.5. Apstrādātājs nav tiesīgs turpināt veikt personas datu apstrādi, t.sk. glabāšanu, pēc Līguma izbeigšanas vai datu apstrādes mērķa sasniegšanas, vai datu subjekta pieprasījuma par viņa personas datu apstrādes izbeigšanu saņemšanas, atkarībā, kurš nosacījums iestājas ātrāk.
- 1.12.6. Jebkuri grozījumi, labojumi un papildinājumi stājas spēkā, ja tie noformēti rakstveidā un tos parakstījušas abas Puses. Tie kļūst par šī Līguma neatņemamu sastāvdaļu no parakstīšanas brīža.

9.pielikums
 Jelgavas valstspilsētas pašvaldības
 Personas datu apstrādes noteikumiem
 (apstiprināti ar Jelgavas valstspilsētas
 pašvaldības izpilddirektora vietnieces
 28.11.2025. rīkojumu Nr. 341-ri)

Apstrādātāju reģistrs

Apstrādātājs <i>Nosaukums, reģ.nr., adrese, kontakinfo.</i>	Apstrādātāja kontaktpersona <i>Amats, vārds, uzvārds, kontakinfo.</i>	Pašvaldības atbildīgā persona par sadarbību <i>[vārds, uzvārds, amats, strukturvienī ba]</i>	Līguma Nr., datums un termiņš	Sadarbības apraksts	Nodoto datu subjektu kategorijas	Nodoto datu veidi	Apstrādes vieta <i>[valsts, adreses, kur atrodas dati]</i>	Datu nodošanas ārpas ES/EEZ gadījumā:		Īpaši noteiktie tehniskie / organizāto riskie drošības pasākumi
								Valsts uz kuru dati nodoti	Drošības pasākumi Regulas 49.panta 1.p.(2)	

10.pielikums

Jelgavas valstspilsētas pašvaldības
 Personas datu apstrādes noteikumiem
*(apstiprināti ar Jelgavas valstspilsētas
 pašvaldības izpilddirektora vietnieces
 28.11.2025. rīkojumu Nr. 341-ri)*

PĀRZINIM:

Jelgavas valstspilsētas pašvaldībai
 adrese: Lielā iela 11, Jelgava, LV-3001

Jelgavas valstspilsētas iestādes nosaukums, kam pieprasījums
 adresēts

DATU SUBJEKTA PIEPRASĪJUMS

I. INFORMĀCIJA PAR DATU SUBJEKTU	
Vārds uzvārds:	
Personas kods (vai dzimšanas datums, ja nav personas koda):	
Tālruņa numurs saziņai:	
Personu apliecinoša dokumenta numurs, izdošanas gads, izdevējiestāde (Nenorāda, ja identifikācija veikta klātienē vai pieprasījums parakstīts izmantojot drošu elektroniskās identifikācijas līdzekli)	
II. INFORMĀCIJA PAR PĀRSTĀVI	
AIZPILDA, JA PIEPRASĪJUMU IESNIEDZ CITA PERSONA DATU SUBJEKTA INTERESĒS	
Vārds uzvārds:	
Personas kods (vai dzimšanas datums, ja nav personas koda):	
Tālruņa numurs saziņai:	
Personu apliecinoša dokumenta numurs, izdošanas gads, izdevējiestāde (Nenorāda, ja identifikācija veikta klātienē vai pieprasījums parakstīts izmantojot drošu elektroniskās identifikācijas līdzekli)	
Pārstāvību apliecinoša dokumenta numurs, izdošanas gads, izdevējiestāde (Nenorāda, ja identifikācija veikta klātienē, uzrādot apliecinošus dokumentus)	
III. ATBILDES SAŅEMŠANAS VEIDS	
☐ Klātienē (norādīt Jūsu kontakttālruni saziņai par atbildes saņemšanu)	
☐ Uz e-pastu (norādiet Jūsu e-pastu)	
☐ Uz dzīvesvietas vai uzturēšanās vietas adresi (norādiet Jūsu adresi)	
☐ Uz e-adreses kontu aktivizētu Vienotajā valsts un pašvaldību	

pakalpojumu portālā www.latvija.lv (norādiet Jūsu e-adresi)	
<i>Esmu informēts, ka Pārzinis izvērtēs iepriekš norādītos saziņas kanālus un atbilstoši izsniedzamās informācijas sensitivitātei un apjomam var noteikt atšķirīgus saziņas kanālus, par ko Jūs tiksiet atsevišķi informēts.</i>	
IV. DATU SUBJEKTA PIEPRASĪJUMA BŪTĪBA	
AIZPILDA NEPIECIEŠAMO PIEPRASĪJUMA SADAĻU	
☐ VĒLOS PIEKĻŪT SAVIEM PERSONAS DATIEM JEB IEGŪT PAR SEVI INFORMĀCIJU	
Lūdzu norādiet kādiem personas datiem vēlaties piekļūt?	
Lūdzu norādiet kādā statusā Jūsu personas dati varētu tikt pie mums apstrādāti <i>(piem., darbinieks, apmeklētājs)</i>	
Ja vēlaties piekļūt foto/video ierakstos esošiem personas datiem, norādiet papildus identificējošu informāciju par sevi <i>(piem., aprakstiet savu izskatu, uzvedību attiecīgajā vietā u.c.)</i>	
Ja vēlaties piekļūt video ierakstos esošiem personas datiem lūdzu norādiet datumu un aptuvenu laiku, kad Jūs varējāt būt iekļuvis video novērošanas ierakstos	
☐ VĒLOS SAŅEMT INFORMĀCIJU PAR SAVU PERSONAS DATU APSTRĀDI	
Lūdzu norādiet par kādiem personas datiem vēlaties saņemt informāciju?	
Lūdzu atzīmējiet Jūs interesējošo informāciju:	☐ Apstrādes nolūki; ☐ Apstrādāto personas datu kategorijas; ☐ Personas datu saņēmēji vai saņēmēju kategorijas, kam personas dati ir izpausti vai kam tos plānots izpaust; ☐ Personas datu glabāšanas laika posms vai kritēriji laika posma noteikšanai; ☐ Informāciju par datu subjekta tiesību izmantošanas iespējām, t.sk. par tiesībām uz datu labošanu, dzēšanu, datu apstrādes ierobežošanu un tiesībām iebilst; ☐ Informācija par tiesībām iesniegt sūdzību uzraudzības iestādei; ☐ Informācija par personas datu ievākšanas avotiem; ☐ Informācija par automatizētu lēmumu pieņemšanu (ja tāda ir), tajā ietverto loģiku un paredzamajām sekām.
☐ VĒLOS LABOT SAVUS PERSONAS DATUS	
Lūdzu norādiet kādus personas datus vēlaties labot:	
Lūdzu norādiet iemeslu personas datu labošanai:	
Lūdzu norādiet personas datus kādi tie būtu pēc labojumiem:	
☐ VĒLOS DZĒST SAVUS PERSONAS DATUS	
Lūdzu norādiet kādus personas datus vēlaties dzēst:	
Lūdzu norādiet iemeslu personas datu dzēšanai:	☐ personas dati vairs nav nepieciešami saistībā ar nolūkiem, kādos tie tika vākti un apstrādāti; ☐ atsaucu savu iepriekš doto piekrišanu, uz kuras pamata tika veikta šāda apstrāde: <i>(norādiet apstrādi, kurai tika sniegta piekrišana):</i> _____ _____ ☐ personas dati ir apstrādāti nelikumīgi;

		Pamatojums: ☐ cits iemesls vai plašāks skaidrojums: 	
☐ VĒLOS IEROBEŽOT SAVU PERSONAS DATU APSTRĀDI			
Lūdzu norādiet kādu personas datu apstrādi vēlaties ierobežot:			
Lūdzu norādiet iemeslu personas datu apstrādes ierobežošanai:		☐ apstrāde ir nelikumīga, bet es nevēlos, lai dati tiktu dzēsti, bet ierobežoti sekojošu iemeslu dēļ: Ierobežojumu noteikt līdz: 20 .gada . . ☐ apzinoties, ka Pārzinim dati varētu nebūt vairs vajadzīgi, bet man tie varētu būt nepieciešami nākotnē sekojošu iemeslu dēļ: Ierobežojumu noteikt līdz: 20 .gada . . 	
Papildus informējam, ka datu apstrāde tiks ierobežota automātiski sekojošos gadījumos: - ja ir apstrīdēta arī personas datu precizitāte (uz laiku, kamēr precizitāte tiek pārbaudīta); - ja Jūs esat iebildis pret Pārziņa leģitīmo interešu nozīmīgumu un pārkumu pār savām leģitīmām interesēm (uz laiku, kamēr Pārzinis pārbauda argumentus un pārvērtē interešu līdzsvaru).			
☐ VĒLOS IZMANTOT TIESĪBAS UZ PERSONAS DATU PĀRNESAMĪBU			
Norādiet personas datu veidus, kurus vēlaties pārnest:			
Ja vēlaties, lai dati tiktu pārsūtīti tieši citam pārzinim, lūdzu norādiet informāciju par saņēmēju:		Nosaukums: _____ Reģ. Nr.: _____ Juridiskā adrese: _____ _____ _____ E-pasta adrese: _____ Kontakttālrunis: _____ _____	
Esmu informēts, ka saskaņā ar Vispārīgo datu aizsardzības regulu tiesības uz personas datu pārnēsāšanu attiecas tikai uz tādiem personas datiem, kas attiecas uz datu subjektu, tiek apstrādāti ar automatizētiem līdzekļiem un to pārņemšanas iespējas īstenojamas ar tehniskiem līdzekļiem, apstrāde pamatota uz piekrišanu un/vai ar datu subjektu noslēgta līguma izpildi. Esmu informēts, ka Pārzinis izvērtēs iepriekš norādītos saziņas kanālus un atbilstoši izsniedzamās informācijas sensitivitātei un apjomam var noteikt atšķirīgus saziņas kanālus, par ko Jūs tiksiet atsevišķi informēts. Sākotnēji lūdzam aplūkot Pārziņa pašapkalpošanās portālos pieejamo informāciju un iespējas to iegūt un saglabāt elektroniskā formātā.			
☐ VĒLOS IEBILST SAVU PERSONAS DATU APSTRĀDEI			
Lūdzu norādiet kādai personas datu apstrādei vēlaties iebilst:			
Norādiet iebildumu būtību:		☐ iebilstu pret Pārziņa leģitīmo interešu (sabiedrības interešu, valsts pārvaldes uzdevumu veikšanai nepieciešamo datu apstrādes) nozīmīgumu un pārkumu pār manām leģitīmām interesēm, jo: ☐ iebilstu 	
☐ VĒLOS ATTEIKTIES NO SAVU DATU IZMANTOŠANAS AUTOMATIZĒTA INDIVIDUĀLA LĒMUMA PIENĒMŠANĀ VAI LŪGT PĀRSKATĪT AUTOMATIZĒTU INDIVIDUĀLA LĒMUMA PIENĒMŠANU			

Lūdzu norādiet kādā automatizētā personas datu apstrādē nevēlaties, lai Jūsu dati tiktu izmantoti:	
<i>Esmu informēts, ka saskaņā ar Vispārīgo datu aizsardzības regulu atteikšanās tiesības neattiecas uz tādām datu apstrādēm, kura:</i> ▪ rada tiesiskas sekas man; ▪ ir vajadzīga, lai izpildītu līgumu starp mani un Pārziņi (šajā gadījumā varu pieprasīt manuālu lēmuma pārskatīšanu); ▪ ir atļauta vai uzlikta kā pienākums ar Pārziņim piemērojamiem normatīvajiem aktiem; ▪ pamatota ar datu subjekta pieprasījumu (šajā gadījumā es varu pieprasīt manuālu lēmuma pārskatīšanu)	
Lūdzu norādiet, kurus automatizētus lēmumus vēlaties pārskatīt:	
Lūdzu norādiet papildus argumentus, kādēļ Jūsprāt automatizēts lēmums ir neprecīzs:	
V. PARAKSTA REKVIZĪTI	
<i>Esmu informēts, ka saskaņā ar Vispārīgo datu aizsardzības regulu atbilde tiks sniegta 1 (viena) mēneša laikā pēc pieprasījuma saņemšanas. Noteiktos gadījumos šis periods var tikt pagarināts vēl uz 2 (diviem) mēnešiem, ņemot vērā pieprasījuma sarežģītību un skaitu, informējot par pagarināšanas iemesliem 1 (viena) mēneša laikā pēc pieprasījuma saņemšanas.</i>	
(vārds, uzvārds) (paraksts)* (datums)*	
*Datums un paraksts nav nepieciešams, ja dokuments parakstīts ar drošu elektronisku parakstu, kas satur laika zīmogu.	
AIZPILDA PĀRZINIS	
VI. ZIŅAS PAR PIEPRASĪJUMA IZPILDES GAITU	
Atbildīgā darbinieka vārds, uzvārds, amats:	
Veikto darbību apraksts:	
Atbildes izsūtīšanas laiks:	
Jautājuma atrisināšanas statuss:	
Paraksts:	

11.pielikums

Jelgavas valstspilsētas pašvaldības
Personas datu apstrādes noteikumiem
(apstiprināti ar Jelgavas valstspilsētas
pašvaldības izpilddirektora vietnieces
28.11.2025. rīkojumu Nr. 341-ri)

Datu subjektu pieprasījumu un izpildes reģistrs

iestādes nosaukums

Nr.p. k.	Datums, kad saņemts	Pieprasītāja identitāte (t.sk.veids kā persona identificēta)	Pieprasījuma būtība	Izpildes termiņš	Izpildes kontrole		
					Izpildes datums, apjoms, veids un veiktās darbības izpildes nodrošināšanai (kad, kā, kur nosūtīta atbilde)	Vai par šīm darbībām ziņots citiem datu subjekta datu saņēmējiem (kad, kādiem)?	Izpildes statuss (‘Nav sākts’, ‘procesā’, ‘pabeigts’)
1.							
2.							
3.							
4.							

12.pielikums

Jelgavas valstspilsētas pašvaldības
 Personas datu apstrādes noteikumiem
*(apstiprināti ar Jelgavas valstspilsētas
 pašvaldības izpilddirektora vietnieces
 28.11.2025. rīkojumu Nr. 341-ri)*

Personas datu drošības incidenta ziņojums*

Ziņotāja vārds uzvārds		amats		Iestāde/ Struktūrvienība	
Ziņojuma aizpildīšanas datums		Incidentā iestāšanās datums, laiks (ja zināms)		Vai Incidents ir pārtraukts vai vēl turpinās?	
Kādos apstākļos Incidents notika un kā izpaudās?					
Kādi dati tikuši vai var tikt ietekmēti Incidentā?					
Incidentā iesaistīto datu apjoms?					
Kā Jūsaprāt šāds incidents var ietekmēt Incidentā cietušo personu?					
Kas Jūsaprāt izraisīja Incidentā iestāšanos?					
Kādi pasākumi ir veikti, lai Incidentu pārtrauktu un ietekmētos datus atgūtu vai minimizētu sekas?					
Kur Incidentā iesaistītie dati atrodas tagad un cik daudz personu tiem var/varētu piekļūt (redzēt)?					
Ja iespējams, uzskaitiet personas (vai personu grupas), kuru dati ir ietekmēti Incidentā					
Kādi Jūsaprāt varētu būt vēl Incidenti iestājušies vai ar zināmu ticamību varētu iestāties nākotnē?					

* ziņojums pēc incidenta konstatēšanas NEKAVĒJOTIES jānosūta uz e-pastu: dati@jelgava.lv, informējot arī telefoniski **63005444**.