KURZEMES PLĀNOŠANAS REĢIONS
Reģ. Nr.. 90002183562
Juridiskā adrese: Avotu iela 12, Saldus, LV-3801, Administrācijas adrese: Eksporta iela 12-212 Rīga, LV 1045
pasts@kurzemesregions.lv

Kurzemes plānošanas reģiona
KĀRTĪBA, KĀDĀ TIEK IEVĒROTA FIZISKO PERSONU DATU AIZSARDZĪBA

Šie noteikumi ir izdoti saskaņā ar Fizisko personu datu aizsardzības likumu un Ministru Kabineta 2001.gada 30.janvāra noteikumiem Nr.40 "Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības".

Terminu skaidrojums:

1) **datu subjekts** — fiziskā persona, kuru var tieši vai netieši identificēt;
2) **personas dati** — jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu;
3) **personas datu apstrāde** — jebkuras ar personas datiem veiktas darbības, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un izpaušanu, bloķēšanu vai dzēšanu;
4) **personas datu apstrādes sistēma** — jebkādā formā fiksēta strukturizēta personas datu kopa, kas ir pieejama, ievērojot attiecīgus personu identificējošus kritērijus;
5) **personas datu operators** — pārziņa pilnvarota persona, kas veic personas datu apstrādi pārziņa uzdevumā;
6) **personas datu saņēmējs** — fiziskā vai juridiskā persona, kurai tiek izpausti personas dati;
7) **sensitīvi personas dati** — personas dati, kas norāda personas rasi, etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi;
8) **pārzinis** — fiziskā vai juridiskā persona, valsts vai pašvaldības institūcija, kura pati vai kopā ar citiem nosaka personas datu apstrādes mērķus un apstrādes līdzekļus, kā arī atbild par personas datu apstrādi saskaņā ar Fizisko personu datu aizsardzības likumu;
9) **trešā persona** — jebkura fiziskā vai juridiskā persona, izņemot datu subjektu, pārzini, personas datu operatoru un personas, kuras tieši pilnvarojis pārzinis vai personas datu operators;

1. **Vispārējie noteikumi:**
   1.1. Kurzemes plānošanas reģiona iekšējie datu apstrādes aizsardzības noteikumi (turpmāk – noteikumi) nosaka personas datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības Kurzemes plānošanas reģionā.
   1.2. Noteikumi ir saistoši visām personas datu apstrādē iesaistītajām personām, tai skaitā personas datu operatoriem un to darbiniekiem.
   1.3. Apstrādāt sensitīvus personas datus ir atļauts tikai pilnvarotām vai ar Kurzemes plānošanas reģiona administrācijas vadītājas vai Attīstības padomes priekšsēdētājas rīkojumu norīkotām personām (turpmāk tekstā – pilnvarotā persona).
   1.4. Vārds, uzvārds, tālruņa numuri, e-pasti – vajadzīgi, lai reģistrētu dažādu Kurzemes plānošanas reģiona pasākumu dalībniekus.
   1.5. Dzimums, etniskā piederība, deklarētās dzīvesvietas adrese, faktiskās dzīvesvietas adrese, informācija par veselību pamatā vajadzīga projekta "Kurzeme visiem" ietvaros. To paredz Labklājības ministrijas (LM) izstrādātās „Pamatnostādnes sociālo pakalpojumu attīstībai 2014.-2020.gadam". Ministru kabineta 2015. gada 16.jūnija noteikumi Nr.313 "Darbības programmas „Izaugsme un nodarbinātība" 9.2.2.specifiskā atbalsta mērķa „Palielināt kvalitatīvu institucionālai aprūpei alternatīvu sociālo pakalpojumu dzīvesvietā un ģimeniskai videi pietuvinātu pakalpojumu pieejamību personām ar invaliditāti un bērniem" 9.2.2.1.pasākuma "Deinstitucionalizācija" īstenošanas noteikumi". Sensitīvo personas datu apstrāde tiek veikta saskaņā ar Fizisko personu datu aizsardzības likuma 11.panta 11.punktu - personas datu apstrāde ir nepieciešama, pildot valsts pārvaldes funkcijas.
   1.6. Personas datu apstrāde tiek veikta tikai konkrētiem mērķiem un saskaņā ar tiem.
2. **Par tehniskajiem resursiem un personas datu aizsardzību atbildīgām personām un to pienākumiem:**
   2.1. Par tehniskajiem resursiem (darbinieku datortehnikas uzturēšanu un izmantošanu) ir atbildīgs tehnisko resursu turētājs – Kurzemes plānošanas reģions.
   2.2. Tehnisko resursu turētājs:
      2.2.1. nodrošina fiziskās aizsardzības pasākumus;
      2.2.2. nodrošina tehnisko resursu darbspēju;
      2.2.3. nodrošina tehnisko resursu atjaunošanu vai nomaiņu, ja tie ir bojāti.
   2.3. Par personas datu aizsardzību Kurzemes plānošanas reģionā atbild ar Kurzemes plānošanas reģiona administrācijas vadītājas vai Attīstības padomes priekšsēdētājas rīkojumu norīkota persona.
   2.4. Atbildīgais par personas datu aizsardzību:
      2.4.1. organizē un kontrolē personas datu apstrādes atbilstību Fizisko personu datu aizsardzības likuma un citu saistīto likumu prasībām.
   2.5. Personas, kuras tiek iesaistītas personas datu apstrādē, rakstveidā apņemas saglabāt un nelikumīgi neizpaust personas datus. Šo personu pienākums ir neizpaust personas datus arī pēc darba tiesisko vai citu līgumā/-os noteikto attiecību izbeigšanās.
   2.6. Visām iesaistītajām personas datu apstrādes procesā personām pienākums ir iepazīties ar šiem noteikumiem un ievērot tos ikdienas darbā.

3. **Personas datu aizsardzības klasifikācija:**
   3.1. Ierobežotas piekļuves informācija – tā ir tāda informācija, kurai piekļūt var tikai pilnvarots darbinieks un/vai uzraudzības un kontroles iestādes atbilstoši to kompetencei. Šādi klasificēti tiek jebkuri sensitīvi personas dati. Šo datu izpaušana vai nozagšana var radīt ievērojamus vai ilgstošus zaudējumus vai cita veida kaitējumu datu subjektam un/vai Kurzemes plānošanas reģionam. Ar šiem datiem drīkst veikt tikai tādas darbības, kas atbilst projekta mērķiem un uzdevumiem.
   3.2. Vispārējās piekļuves informācija– tā ir informācija, kas ir pieejama bez ierobežojuma visiem Kurzemes plānošanas reģiona darbiniekiem. Šādi tiek klasificēti dati, ar kuru palīdzību identificēt fizisko personu nav iespējams.
4. **Personas datu apstrādes organizācija:**
   4.1. Personas datu apstrāde tiek veikta Kurzemes plānošanas reģiona telpās, kas atrodas Eksporta ielā 12-212, Rīgā.
   4.2. Personas datu apstrāde tiek veikta šajā adresē darba dienās laikā no 8:30 līdz 17:00.
   4.3. Sensitīvie personas dati papīra formā ir jāglabā slēgtā skapī, kuram var piekļūt tikai pilnvarotās personas. Aizliegts tos atstāt vietās, kas varētu būt pieejamas trešajām personām.
   4.4. Aizliegts bez nepieciešamības pavairot sensitīvos personas datus papīra formā. Kad kopija vairs nav nepieciešama darbam, tā ir jāiznīcina.
   4.5. Sensitīvajie dati elektroniskā veidā tiek glabāti šifrētā veidā un tiem var piekļūt tikai pilnvarotās personas.
   4.6. Aizliegts kopēt personu datus saturošus failus uz ārējiem datu nesējiem, kam netiek lietota parole vai citi aizsardzības līdzekļi.
   4.7. Gadījumos, kad ir nepieciešams pārsūtīt failus, kas satur sensitīvus personas datus, to drīkst darīt tikai šifrētā veidā vai datni noslēdzot ar paroli.
   4.8. Datu subjekta pieprasījuma gadījumā, mēneša laikā no pieprasījuma izsniegšanas dienas Fizisko personu datu aizsardzības likumā noteiktajā kārtībā ir jāsniedz tam pieprasītā informācija vai pamatots rakstveida atteikums.
   4.9. Ja datu subjekts pieprasa, lai viņa personas datus papildina vai izlabo, kā arī pārtrauc to apstrādi vai iznīcina tos, tad mēneša laikā no pieprasījuma izsniegšanas dienas Fizisko personu datu aizsardzības likumā noteiktajā kārtībā ir rakstiski jāinformē datu subjekts par saistībā ar viņa pieprasījumu veiktajām darbībām.
   4.10. Ja datu subjekts var pamatot, ka personas dati ir nepilnīgi, novecojuši, nepatiesi, pretlikumīgi apstrādāti vai arī tie vairs nav nepieciešami vākšanas mērķim, pārziņa pienākums ir nekavējoties novērst šo nepilnību vai pārkāpumu un par to paziņot trešajām personām, kas iepriekš ir saņēmušas apstrādātos datus.
   4.11. Fizisko personu datu aizsardzības likumā noteiktajos gadījumos Kurzemes plānošanas reģionam ir pienākums izpaust personas datus valsts un pašvaldību amatpersonām, kas pirms datu izpaušanas ir jāidentificē. Personas datus var izpaust, pamatojoties uz rakstveida iesniegumu vai vienošanos, norādot datu izmantošanas mērķi, ja likumā nav noteikts citādi.

5. **Tehniskie resursi, ar kuriem tiek nodrošināta personas datu apstrāde:**
   5.1. Personas datu apstrādei norīkotajiem darbiniekiem izdalītie stacionārie un portatīvie datori ar Windows 7 vai Windows 10 operētājsistēmām.
   5.2. Visiem datoriem ir uzstādīta antivīrusa programmatūra.
   5.3. Punktā 6.7. paredzētajiem mērķiem izmantojamais ārējais cietais disks.
   5.4. Saņemot personas datus, tiek saglabāta informācija: par personas datu saņemšanas laiku, personu, kas novedusi personas datus, personu, kas saņēmusi personas datus. Nododot personas datus, tiek saglabāta informācija: par personas datu nodošanas laiku, personu, kas nodevusi datus, personu, kas saņēmusi datus, personas datiem, kas tikuši nodoti. KPR visu informāciju glabā sistēmā EDUS.
   5.5. Visas darbības ar personas datiem tiek uzskaitītas – tiek uzskaitīts apstrādes laiks un persona, kas to veikusi.
6. **Pasākumi, kas veicami tehnisko resursu aizsardzībai:**
   6.1. Lai nodrošinātos pret nesankcionētu fizisku piekļuvi, tehniskie resursi (datori un ārējais cietais disks) novietoti slēdzamā, ar signalizāciju aprīkotās telpās. Pie datoriem ir aizliegts atrasties trešajām personām.
   6.2. Beidzot darbu lietotājiem ir pienākums pilnīgi izslēgt datoru, bet, ja lietotāji atstāj datoru uz pietiekošu īsu laiku, tad lietotājiem ir jālieto ekrāna saudzētājs ar paroli.
   6.3. Datoros ir aizliegts izmantot nelicencētu programmatūru, kā arī vispār instalēt jebkādu programmatūru bez tehnisko resursu turētāja ziņas. Esošajai datoros programmatūrai ir jābūt uzliktiem visiem pēdējiem atjauninājumiem.
   6.4. Aizliegts pieslēgties personas datu apstrādes sistēmai izmantojot Wi-Fi bezvadu tīklu.
   6.5. Tehnisko resursu turētājs iespēju robežās nodrošina tehnisko resursu aizsardzību pret dabas stihijām, ugunsgrēka, plūdiem u.tml.
   6.6. Telpās, kurās atrodas personas datus saturošie tehniskie resursi un dokumentācija, ir jābūt funkcionējošai signalizācijai, kā arī ugunsdzēšamajam aparātam.
   6.7. Katra mēneša sākumā atbildīgais par personas datu aizsardzību, datoros esošos personas datus kopē uz ūdensizturīgu un ugunsizturīgu ārējo cieto disku, kas pārējo laiku tiek glabāts slēgtajā metāla skapī.
   6.8. Jebkuru cieto disku, uz kura notika personas datu apstrāde, pēc tā kalpošanas beigām pirms tā nodošanas utilizācijā tehnisko resursu turētājs fiziski iznīcina rūpīgi sadauzot to ar āmuru tā lai tā darbības atjaunošana vai datu iegūšana no tā būtu neiespējama saprāta robežās.
   6.9. Aizliegts nodot trešajām personām tehniskos resursus, ja tie satur personas datus. Šis aizliegums jāievēro arī gadījumos, kad tehnika tiek nodota utilizācijai. Ja tehnikai nepieciešams garantijas remonts, pirms tās nodošanas garantijā ir jāizņem cietais disks.
7. **Paroles garums un uzbūves nosacījumi:**
   7.1. Parolēm ir jābūt ne mazāk kā 10 simbolus garām, un tām ir jāsatur vismaz 1 lielais burts, viens mazais burts, viens cipars, un viens simbols (t.i. izsaukuma zīme, jautājuma zīme, domu zīme, iekavas, utt.).

7.2. Paroli aizliegts veidot, izmantojot ar sistēmas lietotāju saistītu informāciju (piemēram, vārdus, uzvārdus, dzimšanas dienas, tālruņa numurus, mājdzīvnieku un tuvinieku vārdus u. tml.).

7.3. Aizliegts izmantot jau iepriekš izmantotas paroles.

7.4. Paroles obligāti jāmaina reizi trijos mēnešos. Gadījumā, ja pastāv iespēja, ka parole kļuvusi zināma trešajām personām, tai jātiek nomainītai nekavējoties.

7.5. Parole nedrīkst būt pieejama trešajām personām. Paroli nedrīkst uzglabāt pierakstītu uz papīra vai arī elektroniskā formā, ja tas rada apdraudējumu parolei nokļūt trešās personas rokās. Elektroniskā formā paroles drīkst glabāt tikai šifrētā veidā.

8. Datu operatoru tiesības un pienākumi:

8.1. Pēc tam, kad datu operators ir veicis visas nepieciešamās darbības ar datiem, tie ir jāizdzēš vai fiziski jāiznīcina, ja tie ir papīra formā.

8.2. Datu operators drīkst glabāt datus tikai tik ilgi, cik ilgi tie ir nepieciešami konkrētā mērķa sasniegšanai.

9. Darbības incidentu gadījumā:

9.1. Par jebkuru personas datu apstrādes incidentu darbiniekam, kas to konstatējis, ir nekavējoties jāpaziņo tehnisko resursu turētājam un atbildīgajam par personas datu aizsardzību:

9.1.1. ja konstatēts jebkāda veida apdraudējums tehniskajiem resursiem (elektroenerģijas padeves pārtraukums, šķidrumu vai svešķermeņu iekļūšana, bojājumi fiziska trieciena, uguns iedarbības vai plūdu rezultātā u.c.);

9.1.2. ja konstatēts jebkāda veida apdraudējums informācijas resursiem (trešajām personām kļuvusi zināma pieejas parole, konstatēta nesankcionēta piekļuve, konstatēti darbības pārtraukumi u.c.);

9.1.3. ja konstatēts jebkāda veida apdraudējums sensitīvos personas datiem papīra formā (pārāk augsts mitrums telpās, metāla skapja vai telpu durvju slēdzenes nefunkcionēšana, signalizācijas nefunkcionēšana, trešo personu piekļūšana dokumentiem, u.c.).

9.2. Incidentu gadījumā darbiniekam savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt tehnisko un informācijas resursu drošību līdz attiecīgo resursu turētāja ierašanās brīdim.

9.3. Gadījumā, ja tiek konstatēta datu noplūde, ir nekavējoties tas jāpaziņo atbildīgajam par personas datu aizsardzību, jāatrod tās avots un noplūde ir jānovērš.

10. Informācijas sniegšana Datu valsts inspekcijai:

10.1. Pirms izmaiņu izdarīšanas personas datu apstrādē šīs izmaiņas jāreģistrē Datu valsts inspekcijā.

10.2. Ja mainās personas datu apstrādes tehniskie un organizatoriskie pasākumi, kas būtiski ietekmē personas datu apstrādes aizsardzību, informācija par to gada laikā jāiesniedz Datu valsts inspekcijai.

10.3. Ja mainās pārzinis vai pārziņa darbība tiek izbeigta, ir jāiesniedz Datu valsts inspekcijai iesniegumu par personas datu apstrādes izslēgšanu no personas datu apstrādes reģistra.

10.4. Gadījumā, kad Datu valsts inspekcija pieprasa, lai tiek uzrādīti dokumenti un sniegta cita informācija, kas attiecas uz pārbaudāmo personas datu apstrādi, tā ir nekavējoties jāiesniedz.