



**LATVIJAS REPUBLIKA**  
**KRUSTPILS NOVADA PAŠVALDĀ**

Reģ. Nr. 90009118116

Rīgas ielā 150a, Jūkabpilī, LV-5202, Tālrunis 65237610, Fakss 65237611

Banka: SEB banka Jūkabpils filiāle, konts LV55 UNLA 0050 0143 2307 5

APSTIPRINĀTI  
ar Krustpils novada domes  
2009. gada 8. decembra lēmumu  
(reģistrāts desmit protokols Nr. 13., 11. p.)

**Krustpils novada pašvaldības  
Iedzīvotāju iekšzīdņu datu aizsardzības noteikumi.**  
Jūkabpilī

Šie noteikumi ir izdoti saskaņā ar Fizisko personu datu aizsardzības likumu un Ministru Kabineta noteikumu Nr. 40 „Personas datu apstrādes sistēmas aizsardzības obligātās tehniskās un organizatoriskās prasības” 5. punktu.

**1. Vispārīgie noteikumi**

1.1. Šie noteikumi nosaka informatīvās sistēmas (ZZDATS.) personas datu apstrādes (turpmāk tekstā – Personas datu apstrāde) lietošanu un aizsardzību, nodrošinot Krustpils novada pašvaldības (turpmāk tekstā – pašvaldība) informācijas resursu un informācijas sistēmu drošību.

1.2. Personas datu apstrāde tiek veikta Krustpils novada pašvaldības telpās, kas atrodas Rīgas ielā 150a, Jūkabpilī un Atašienes pagasta pārvaldes telpās, juridiskā adrese Liepu ielā 14A, Atašiene, Atašienes pagasts, Krustpils novads, Mežres pagasta pārvaldes telpās, juridiskā adrese „Druvasnieki” 16A, Mežre Mežres pagasts, Krustpils pagasta pārvaldes telpās, juridiskā adrese Daugavieši, Spunīni, Krustpils pagasts, Krustpils novads, Kuku pagasta pārvaldes telpās, juridiskā adrese Laukezera ielā 5, Zilīni, Kuku pagasts, Krustpils novads, Variēšu pagasta pārvaldes telpās, juridiskā adrese „Variēši”, Variēšu pagasts, Krustpils novads, Vepes pagasta pārvaldes telpās, Neretas 6, Vepes pagasts, Krustpils novads.

1.3. Noteikumi ir saistoši visiem Pašvaldības Personālu datu apstrādes lietotājiem. Noteikumi ir attiecināmi uz visiem personālu datiem, kas attiecas uz identifikāciju vai identifikājamu fizisko personu.

1.4. Par informācijas drošību Pašvaldībā atbild Krustpils novada pašvaldības priekšsēdētājs.

1.5. Šie noteikumi ir paredzēti izmantošanai tikai Pašvaldības ietvaros un to izpaušana citām trešajām personām ir atļaujama tikai ar Krustpils novada pašvaldības priekšsēdētāja atļauju.

## **2. Informācijas klasifikācija**

2.1. Informācijas klasifikācijas līmeņi:

2.1.1. slepena – augstākais līmenis. Šīs informācijas izpaušana vai nozagšana var radīt ievērojamus vai ilgstošus zaudējumus un nopietni kaitēt Pašvaldības labajai slavai. Strādājot ar šo informāciju ir jāievēro vislielāko piesardzību un šo informāciju drīkst izpaust tikai rakstveidā nepieciešamības gadījumos.

2.1.2. ierobežotas piekļuves – ikdienas darbības paredzētā informācija, kas paredzēta tikai noteiktam darbinieku lokam. Šīs informācijas izpaušana vai nozagšana var radīt Pašvaldībai iekšējās vai ārējās nekaitības. Piekļuve šai informācijai piešķir tikai pilnvarotiem darbiniekiem.

2.1.3. neklasificēta – informācija, kas jau sabiedrībā zināma, ko brīvi izplata vai kas pieejama visiem Pašvaldības darbiniekiem un citām trešajām personām. Šīs informācijas izpaušana vai nozagšana neietekmē Pašvaldības darbu.

2.2. Dati, kas tiek izmantoti Personālu datu apstrādei, ir klasificējami kā ierobežotas piekļuves informācija, kurai ir tiesības piekļūt un veikt to apstrādi tikai pilnvarotiem darbiniekiem.

## **3. Lietotāju tiesību piešķiršana un administrācija**

3.1. Pašvaldības institūcijas, fiziskās un juridiskās personas, kas veic vai valdīs kā personas datu apstrādi, reģistrēto šajā likumā noteiktajā kārtībā.

3.2. Datu valsts inspekcija l mumu par personas datu aizsardz bas speci lista re istr ciju pie em 15 dienu laik p c visas š panta piektaj da min t s inform cijas iesniegšanas Datu valsts inspekcijai.

3.3. Datu valsts inspekcija, kontrol un uzrauga p rzi a veikt s personas datu apstr des atbilst bu likuma pras b m.

3.4. Personas datu aizsardz bas speci lista pien kums ir saglab t un bez tiesiska pamata neizpaust personas datus ar p c darba tiesisko vai dienesta attiec bu izbeigšanas.

3.5. Re istr jot personas datu apstr di, Datu valsts inspekcija izsniedz p rzinim vai vi a pilnvarotai personai personas datu apstr des re istr cijas apliec bu.

3.6. Ja main s p rzinis vai p rzi a darb ba tiek izbeigta, vi š iesniedz Datu valsts inspekcijai iesniegumu par personas datu apstr des izsl gšanu no personas datu apstr des re istra.

3.7. Pašvald bas instit cijas reizi divos gados iesniedz Datu valsts inspekcijai audita atzinumu par personas datu apstr di, ietverot taj ar riska anal zi, un p rskatu par inform cijas droš bas jom veiktajiem pas kumiem. Pras bas audita atzinumam nosaka Ministru kabinets.

#### **4. Lietot ju ties bas, pien kumi un atbild ba**

4.1. Lietot jiem ir ties bas izmantot vi am lietošan nodotos datorus un to programmat ru, k ar lietot jam ir ties bas piepras t lietot ju atbalstu gad jum , ja datoram vai t programmat rai ir radušies trauc jumi vai ar lietot jam ir pietiekams uzskats par iesp jamo draudu (apdraud jumu) esam bu.

4.2. Lietot ju pien kums ir iepaz ties ar Noteikumiem un iev rot tos ikdienas darb .

4.3. Lietot ju tiešie pien kumi, ties bas un atbild ba ir ietverti katra lietot ja amata (darba) aprakst .

4.4.Lietotājs nedrīkst izpaust ziņas par Pašvaldības datoru tīkla uzbūvi un konfigurāciju, kā arī atklāt klasifikāciju informāciju nepilnvarotām personām.

4.5.Lietotājs nedrīkst atļaut piekļūt personām datiem citām personām, ja to nevajag tiešo darba pienākumu pildīšanai un to pilnvarojumu ir devis Pašvaldības priekšdators.

4.6.Beidzot darbu lietotājam ir pienākums pilnīgi izslēgt datoru, bet, ja lietotājs atstāj datoru uz pietiekošu laiku, tad lietotājam ir jālieto ekrāna aizsardzība ar paroli.

4.7.Lietotājam ir pienākums informēt datu subjekta pārzini, sniegt tam visu informāciju, kas saistīta ar atbilstošo datu subjektu.

4.8.Lietotājs ir atbildīgs par datortehniku, kas nodota viņam, kā arī lietotājs atbild par darbu, kas tiek veikts ar viņam nodoto datortehniku.

4.9.Lietotājs apņemas saglabāt informācijas konfidencialitāti ar pārc darba tiesisko attiecību izbeigšanas.

4.10.Lietotājs iekrāj cauraklotu reģistrācijas žurnālu, kur veic reģistrāciju par sistēmas izmantošanas dienu, laiku un fiziskās personas vārdu, uzvārdu un iemeslu sistēmas izmantošanai.

## **5. Informācijas sistēmas paroles uzbūve un lietošana**

5.1.Informācijas sistēmas aizsardzība tiek nodrošināta ar datora paroli.

5.2.Parolei operētājsistēmā jāatbilst sekojošiem prasībām:

5.2.1.minimālam paroles garumam jābūt vismaz 8 simboliem.

5.2.3.paroles uzbūvē jābūt komplicētai, izmantojot burtus, ciparus un pašo rakstzīmju kombināciju.

5.2.3. nedrīkst atkārtot nevienu no 6 (sešiem) iepriekšējiem parolēm.

5.3.Pašvaldības informatīvās sistēmas lietotāju paroli izveido un piešķir lietotājiem Iedzīvotāju reģistrācijas departaments.

5.4.Lietotājs nedrīkst izpaust savu paroli citiem lietotājiem vai jebkuram citam trešajam personam.

5.5.Lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

5.6.Ja lietotājam rodas aizdomas, ka viņa paroli ir uzzinājis jebkura cita persona, lietotājam ir pienākums pēc iespējas ātrāk mainīt šo paroli.

## **6. Datortehnikas uzstādīšana, programmas lietošana un informācijas saglabāšana**

6.1.Datortehnikas un programmatras uzstādīšanu, un to administrāšanu nodrošina Pašvaldības darbinieks, ar kuru Pašvaldība ir noslēgusi atsevišķu līgumu.

6.2.Lietotājiem ir aizliegts jebkādu veidmainīt lietošanā saistīt datortehnikas un programmatras konfigurāciju, kā arī instalēt programmatru uz to.

## **7. Rezerves kopiju veidošana**

7.1.Pašvaldības informatīvās sistēmas centrālās datubāzes rezerves kopiju nodrošināšanu un veidošana veic SIA „Dats”.

## **8. Rīcība problēmu gadījumā**

Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem utt.) lietotājiem ir nekavējotīgi jāpaziņo Pašvaldības priekšdatoram vai tā pilnvarotai personai.

Domes priekšdatoram

K.Pabrzis

