RĪGAS PLĀNOŠANAS REĢIONS

Reģ.Nr. 90002222018, Zigfrīda Annas Meierovica bulvārī 18, Rīga, LV – 1050,
tālr.: +371 67226430, fakss: +371 67226431, e-pasts: rpr@rpr.gov.lv, www.rpr.gov.lv

IEKŠĒJIE NOTEIKUMI

Rīgā

2016.gada 16.novembrī Nr. 2

Apstiprināti ar Rīgas plānošanas reģiona attīstības padomes 2016.gada 16.novembra sēdes lēmumu Nr.8

Rīgas plānošanas reģiona fizisko personu datu apstrādes aizsardzības noteikumi

Izdoti saskaņā ar Valsts pārvaldes iekārtas likuma 72.panta pirmās daļas 2. punktu un Ministru kabineta 2001.gada 30.janvāra noteikumu Nr.40 "Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības" 5.punktu

1. VISPĀRĪGIE NOTEIKUMI

1.1. Iekšējie noteikumi "Rīgas plānošanas reģiona fizisko personu datu apstrādes aizsardzības noteikumi" (turpmāk - Noteikumi) nosaka personas datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības, nodrošinot Rīgas plānošanas reģionā (turpmāk – Iestāde) informācijas sistēmu drošību.

1.2. Noteikumu mērķis ir:

1.2.1. noteikt Iestādes organizatorisko pasākumu un nepieciešamo tehnisko līdzekļu kopumu, kas nodrošina godprātīgu un likumīgu personas datu apstrādi un lietošanu tikai paredzētajiem mērķiem, to glabāšanas, atjaunošanas, labošanas un dzēšanas veidu, nodrošinot ikvienas fiziskas personas tiesības uz savu personas datu aizsardzību;

1.2.2. nodrošināt drošu un normatīvajos aktos noteiktajām prasībām atbilstošu personas datu apstrādes aizsardzības sistēmu;

1.2.3. nodrošināt vienādu un sistemātisku pieeju personas datu apstrādes jomas jautājumu risināšanai.

1.3. Noteikumi ir saistoši visām personas datu apstrādē iesaistītajām personām Iestādē.

1.4. Iestāde apstrādā un uzkrāj personas datus par Eiropas Sociālā fonda projekta "Deinstitucionalizācija un sociālie pakalpojumi personām ar invaliditāti un bērniem" (projekta identifikācijas numurs 9.2.2.1./15/I/002) ietvaros atbalstu saņēmušajām fiziskajām personām.

2. LIETOTIE TERMINI

2.1. **Datu subjekts** - fiziskā persona, kuru var tieši vai netieši identificēt;

2.2. **Personas dati -** jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisko personu;

2.3. **Pārzinis** – Iestāde, kas nosaka personas datu apstrādes mērķus un apstrādes līdzekļus, kā arī atbild par personas datu apstrādi saskaņā ar normatīvajiem aktiem par fizisko personu datu aizsardzību;

2.4. **Personas datu apstrādes sistēma** - jebkādā formā fiksēta strukturizēta personas datu kopa, kas ir pieejama, ievērojot attiecīgus fiziskas personas identificējošus kritērijus;

2.5. **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;

2.6. **Personas datu operators –** uz rakstveida līguma pamata veic personas datu apstrādi atbilstoši līgumā noradītajam apjomam, paredzētajiem mērķiem un Pārziņa norādījumiem;

2.7. **Trešā persona -** jebkura fiziskā vai juridiskā persona, izņemot datu subjektu, personas datu operatoru un personas, kuras tieši pilnvarojis pārzinis vai personas datu operators.

2.8. **Informācijas sistēma** (turpmāk - IS) **–** informācijas un tehnisko resursu kopums;

2.9. **Auditācijas pieraksti –** analīzei pieejami pieraksti, kuros reģistrēti dati par noteiktiem notikumiem (piekļūšana, datu ievade, mainīšana, dzēšana, izvade u.c.) IS;

2.10. **Informācijas resursi –** sistēmprogrammas, lietojumprogrammas, sistēmu un datu faili un cita informācija, ko izmanto informācijas apstrādei, pārraidei, glabāšanai un citu funkciju veikšanai;

2.11. **Tehniskie resursi –** datori, tīkla aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei un glabāšanai;

2.12. **Informācijas tehnoloģiju drošības incidents** (turpmāk – drošības incidents) – ir kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte.

3. PERSONAS DATU AIZSARDZĪBAS KLASIFIKĀCIJA

3.1. Iestādē tiek izmantoti ierobežotas pieejamības, neklasificējami un publiski dati.

3.2. Ierobežotas pieejamības dati (augsts līmenis) ir dati, kas tiek glabāti datu bāzēs un kas paredzēti ierobežotam darbinieku lokam. Pie ierobežotas piekļuves datiem pieder arī personas dati. To lietošanu nosaka Fizisko personu datu aizsardzības likums. Ierobežotas pieejamības datu izpaušana vai zādzība var radīt ievērojamus vai ilgstošus zaudējumus vai cita veida kaitējumu Iestādei un/vai datu subjektam.

3.3. Neklasificējami dati (zems līmenis) ir tie, kas sabiedrībai ir jau zināmi un ko izplatīšana Iestādei neradīs zaudējumus.

3.4. Publiski dati (zems līmenis) ir tie, ko Iestāde ar nodomu izplata publiski sabiedrības informēšanai. Šādu datu izplatīšana Iestādei neradīs zaudējumus.

3.5. Ar ierobežotas pieejamības datiem drīkst veikt tikai tādas darbības, kas atbilst Fizisko personu datu aizsardzības likumā un šajos Noteikumos noteiktajam.

4. TIESĪBAS UN PIENĀKUMI

4.1. Pārziņa tiesības un pienākumi:

4.1.1. Par personu datu aizsardzību, informācijas drošības un pilnveidošanas procesu kopumā atbild Iestādes vadītājs, kurš pats vai ar norīkotu personu starpniecību kontrolē personas datu apstrādes sistēmu drošību (turpmāk - Pārzinis);

4.1.2. Personas datu apstrādi Iestādē veic Pārziņa pilnvarotas personas (turpmāk – Pilnvarotā persona);

4.1.3. Pārzinis var uzdot personas datu apstrādi veikt Personas datu operatoram;

4.1.4. Pārzinis var bez brīdinājuma dzēst vai mainīt Pilnvarotās personas datus informācijas sistēmas piekļuvei, ja Pilnvarotā persona pārkāpj Noteikumus, kā arī citus ārējos normatīvos aktus un ētikas normas;

4.1.5. Pārzinis ir tiesīgs pieprasīt no Pilnvarotās personas rakstveida apliecinājumu (1.pielikums), par šo noteikumu un konfidencialitātes prasību ievērošanu darbā ar personas datiem un personas datu apstrādes sistēmu, kā arī veikt visas citas darbības, kuras uzskata par nepieciešamu, lai tiktu ievērotas visas normatīvo aktu prasības personas datu aizsardzības jomā. Apliecinājumu glabā darbinieka personas lietā;

4.1.6. Pārziņa pienākums ir rūpēties par personas datu apstrādes informācijas sistēmas darbību, nodrošinot Pilnvaroto personu drošu piekļuvi tai, kā arī iespēju datu subjektam iepazīties ar saviem personas datiem no personas datu apstrādes sistēmas;

4.1.7. Pārzinis iekārto, veic ierakstus un glabā IS reģistrācijas žurnālu atbilstoši 2.pielikumā noteiktajai formai;

4.1.8. Pārzinis iekārto un glabā personas datu apstrādes darbību reģistrācijas žurnālu atbilstoši 3.pielikumā noteiktajai formai;

4.1.9. Pārzinis ir tiesīgs pieprasīt informāciju no personām, kuras iesaistītas personas datu apstrādē par pienākumu izpildi.

4.2. Pilnvarotās personas tiesības un pienākumi:

4.2.1. Pilnvarotā persona apstrādā personas datus, ievērojot normatīvajos aktos noteikto kārtību un Noteikumu prasības;

4.2.2. Pilnvarotā persona personas datu apstrādes laikā nodrošina, ka apstrādājamie personas dati nav pieejami trešajai personai;

4.2.3. Pilnvarotā persona reģistrē personas datu nodošanas un saņemšanas faktu personas datu apstrādes darbību reģistrācijas žurnālā;

4.2.4. Pilnvarotā persona ne mazāk kā vienu reizi gadā pārbauda personas datu apstrādē esošo datu aktualitāti un atbilstību personas datu apstrādes mērķim;

4.2.5. Pilnvarotās personas lietošanā nodotās IS izmanto tikai darba vajadzībām;

4.2.6. Pilnvarotai personai aizliegts izpaust ziņas par Iestādes IS uzbūvi un konfigurāciju, kā arī atklāt ierobežotas pieejamības informāciju nepilnvarotām personām;

4.2.7. Pilnvarotās personas pienākums saglabāt un bez tiesiska pamata neizpaust personas datus arī pēc darba tiesisko attiecību izbeigšanas;

4.2.8. Pilnvarotās personas pienākums ir lietot nepieciešamos tehniskos un organizatoriskos līdzekļus, lai aizsargātu personas datus un novērstu to nelikumīgu apstrādi;

4.2.9. Pilnvarotā persona atbildīga par IS, kas nodota viņa rīcībā, kā arī par dokumentiem, kas nepieciešami viņa darba pienākumu pildīšanai;

4.2.10. Pilnvarotai personai aizliegts izmantot nelicencētu programmatūru;

4.2.11. Pilnvarotā persona nedrīkst izdarīt darbības, kas būtu vērstas pret IS drošību, izmantojot neparedzētas pieslēgšanās iespējas;

4.2.12. beidzot (pārtraucot) darbu ar IS, Pilnvarotā persona aizver pārlūkprogrammu;

4.2.13. Pilnvarotai personai aizliegts saņemto informāciju pārveidot, piedalīties tās pārdošanā vai cita veida atsavināšanā, reproducējot kopumā vai tās daļas, izmantot to citu datu apstrādes sistēmu izveidei, kā arī glabāt publiski pieejamās vietās;

4.2.14. ja ir aizdomas par tīšiem bojājumiem, kas ir radušies IS paroles publiskošanas rezultātā vai citu iemeslu dēļ, Pilnvarotā persona par to nekavējoties ziņo Pārzinim;

4.2.15. par prettiesisku nodarījumu Pilnvarotā persona atbild normatīvajos aktos noteiktajā kārtībā;

4.2.16. Pilnvarotai personai ir tiesības izteikt priekšlikumus aizsardzības sistēmas uzlabošanai, pilnveidošanai un tās atbilstības nodrošināšanai normatīvajos aktos noteiktajām prasībām.

5. PERSONAS DATU APSTRĀDES ORGANIZĀCIJA

5.1. Pārzinis pirms IS nodošanas personas datu apstrādē tos reģistrē IS reģistrācijas žurnālā (2. pielikums).

5.2. Personas datu apstrāde tiek veikta Iestādes telpās, datu operatoru telpās (saskaņā ar noslēgtu rakstveida pakalpojuma līgumu) un datu subjektu atrašanās vietās.

5.3. Personas datu apstrāde Iestādē tiek veikta darba dienās laikā no 8:30 līdz 18:00. Datu operatoru telpās un datu subjektu atrašanās vietās personas datu apstrāde tiek veikta atbilstoši pakalpojuma līgumā noteiktos laika periodos vai saskaņotā laika grafikā.

5.4. Personas datu apstrādi elektroniskā formā veic izmantojot tikai tos tehniskos resursus, kas reģistrēti tehnisko resursu reģistrācijas žurnālā.

5.5. **Personas datu nodošana un saņemšana**

5.5.1. Aizliegts kopēt personas datus saturošus failus uz ārējiem datu nesējiem, izņemot šo noteikumu 6.13. un 6.14.punktos minēto kopēšanu;

5.5.2. informāciju, kura satur personas datus, pārsūtīšanu veic šifrētā veidā. Pārsūtamās informācijas kopumu nodrošina ar aizsardzību, informācijas pieejai izmantojot unikālu paroli, kura pieejama tikai noteiktam personu lokam;

5.5.3. personas dati, kas fiksēti papīra formātā, Pārzinis glabā slēgtā dokumentu glabātuvē (skapī), kurai nodrošināta pieeja tikai Pilnvarotām personām. Aizliegts dokumentus vai to projektus, kuros ir fiksēti personas dati atstāt vietās, kur tie ir pieejami nesankcionēti un nekontrolēti trešajām personām.

5.6. **Personas datu glabāšana**

5.6.1. elektroniskie dokumenti tiek arhivēti normatīvajos aktos noteiktajā kārtībā;

5.6.2. Pārzinis glabā personas datu saturošus elektroniskos un papīra formāta dokumentus atbilstoši lietu nomenklatūrā noteiktajam glabāšanas laikam;

5.6.3. pēc glabāšanas termiņa beigām papīra un elektroniskie dokumenti tiek iznīcināti normatīvajos aktos noteiktajā kārtībā.

5.7. **Personas datu dzēšana**

5.7.1. aizliegts nodot trešajām personām tehniskos resursus, ja tie satur personas datus. Šis aizliegums jāievēro arī gadījumos, kad tehniskie resursi tiek nodoti utilizācijai. Ja tehnikai nepieciešams garantijas remonts, pirms tās nodošanas remontā ir jānodrošina tajā esošo personas datu drošība;

5.7.2. personas datus, kas ir kļuvuši nepilnīgi, novecojuši, nepatiesi, pretlikumīgi apstrādāti vai arī tie vairs nav nepieciešami noteiktajam personas datu apstrādes mērķim, nekavējoties labo, precizē vai dzēš un par to informē trešās personas, kurām Iestāde iepriekš nosūtījusi apstrādātos personas datus;

5.7.3. izbeidzot personas datu apstrādi Pārzinis vai Pilnvarotā persona neatgriezeniski dzēš personas datus no IS;

5.7.4. personas datu saturoši papīra dokumenti vai to projekti pēc nepieciešamības tiek iznīcināti normatīvajos aktos noteiktajā kārtībā.

5.8. **Personas datu izpaušana**

5.8.1. datu subjekta informācijas pieprasījumu Pārzinis izskata viena mēneša laikā no pieprasījuma saņemšanas dienas un Fizisko personu datu aizsardzības likumā

noteiktajā kārtībā sniedz pieprasīto informāciju vai pamatotu rakstveida atteikumu vai informē par veiktajām darbībām (papildina, labo vai dzēš) saistībā ar informācijas pieprasījumā izteikto prasību;

5.8.2. Fizisko personu datu aizsardzības likumā noteiktajos gadījumos Iestāde izpauž personas datus valsts un pašvaldību amatpersonām, kas pirms datu saņemšanas ir identificētas. Personas datus izpauž, pamatojoties uz rakstveida iesniegumu vai vienošanos, kurā norādīts personas datu izmantošanas mērķis, ja likumā nav noteikts citādi;

5.8.3. personas datu nodošanu trešajām personām veic Fizisko personu datu aizsardzības likumā noteiktajos gadījumos;

5.8.4. pavairot personas datus saturošu informāciju ir tiesības Pilnvarotai personai. Pavairošanas faktu reģistrē personas datu apstrādes darbību reģistrācijas žurnālā, kurš glabājas pie Pilnvarotās personas. Aizliegts bez tiesiska pamatojuma pavairot informāciju ar personas datiem.

6. INFORMĀCIJAS SISTĒMAS AIZSARDZĪBAS VISPĀRĪGIE NOSACĪJUMI

6.1. Pārzinis īsteno personas datu obligāto tehnisko aizsardzību ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret fiziskās iedarbības radītu personas datu apdraudējumu un aizsardzību, kuru realizē ar programmas līdzekļiem.

6.2. Pārzinis:

6.2.1. sagatavo (pielāgo) IS personas datu apstrādei un reģistrē to IS reģistrācijas žurnālā;

6.2.2. nodrošina antivīrusu programmatūras uzstādīšanu, ugunsmūra konfigurēšanu, darbinieku instruēšanu, u.c. nepieciešamās darbības;

6.2.3. nodrošina IS darbspēju, tās darbības atjaunošanu (nomaiņu), ja noticis tehnisko resursu bojājums vai arī IS darbība ir tikusi traucēta citu iemeslu dēļ;

6.2.4. nodrošina auditācijas pierakstu esamību IS, kuri tiek izmantoti personas datu apstrādē;

6.2.5. nodrošina IS drošību pret drošības incidentiem, incidentu gadījumā veic nepieciešamos pasākumus nelabvēlīgo seku mazināšanai;

6.2.6. organizē IS fiziskās aizsardzības pasākumus.

6.3. Tehniskie resursi, kas satur personas datus (stacionārie un portatīvie datori, ārējie cietie diski), laikā, kad tie netiek lietoti, tiek glabāti slēdzamās telpās.

6.4. Bez Pārziņa atļaujas aizliegts pieslēgt tehniskajiem resursiem jebkādas ārējās atmiņas ierīces.

6.5. Lietot tehniskos resursus, kuri reģistrēti IS reģistrācijas žurnālā, atļauts tikai Pilnvarotām personām.

6.6. Beidzot darbu, Pilnvarotā persona izslēdz datoru (izslēgšanas procedūra: Start =>Shut Down =>Ok), bet, ja Pilnvarotā persona atstāj datoru uz īsu laiku, lieto ekrāna saudzētāju ar paroli vai bloķē pieeju datora informācijai, noslēdzot datora klaviatūru ar Ctrl-Alt-Del funkcijas palīdzību.

6.7. Datoriem, kas tiek izmantoti personas datu apstrādē ir parole vismaz operētājsistēmas līmenī. Portatīvā datora cietajam diskam ir jābūt pilnīgi šifrētam.

6.8. Datoros ir aizliegts izmantot nelicencētu programmatūru, kā arī instalēt jebkādu programmatūru bez Pārziņa atļaujas. Programmatūrai jābūt nodrošinātai ar visiem pieejamajiem atjauninājumiem.

6.9. Aizliegts pieslēgties IS, kurā tiek veikta personas datu apstrāde, izmantojot bezvadu datortīklu (Unencrypted Wireless Networks).

6.10. Tehniskajiem resursiem, kurus izmanto personas datu apstrādē, aizliegts izmantot bezvadu peles, tastatūras un printerus.

6.11. Drošības pasākumi pret ārkārtas apstākļiem tiek īstenoti saskaņā ar ugunsdrošības noteikumiem Iestādē, kā arī normatīvo aktu prasībām par elektroiekārtu drošu ekspluatāciju un to aizsardzību.

6.12. Telpas, kurās atrodas personas datu saturošie tehniskie resursi un dokumentācija, ir nodrošināta ar funkcionējošu apsardzes signalizāciju, dūmu detektoriem un ugunsdzēšamo aparātu.

6.13. Katra mēneša pirmajā pirmdienā, vai nākamajā darba dienā ja pirmdiena ir svētku diena, tehniskajos resursos esošos personas datus kopē uz ārējo cieto disku, kas tiek glabāts aizslēdzamā skapī.

6.14. Pilnvarotās personas, kuras veic personas datu apstrādi, izmantojot portatīvos datorus, darba dienas laikā uzkrātos personas datus, pēc iespējas ātrākā laikā, no portatīvā datora, izmantojot reģistrētu ārējo cieto disku, pārsūta uz stacionāro datoru, kas reģistrēts IS reģistrācijas žurnālā, nesaglabājot kopijas portatīvajā datorā.

6.15. Ārējo cieto disku, kuru izmanto personas datu apstrādei aizliegts iznest ārpus Iestādes telpām, un tas tiek glabāts slēdzamā glabātuvē (skapis vai atvilktne).

7. PAROĻU VEIDOŠANAS UN GLABĀŠANAS NOSACĪJUMI

7.1. Tehnisko resursu aizsardzība un Pilnvaroto personu identifikācija tiek nodrošināta ar datora paroli, kura atbilst sekojošām prasībām:

7.1.1. minimālais paroles garums ir 8 simboli;

7.1.2. maksimālais paroles maiņas periods nav ilgāks par 60 dienām;

7.1.3. paroles uzbūve ir komplicēta, to veido izmantojot burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+);

7.1.4. veidojot paroli, tā nav vienāda ar trīs iepriekšējām parolēm.

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

7.3. Pilnvarotai personai aizliegts izpaust savu paroli.

7.4. Ja Pilnvarotai personai ir aizdomas, ka paroli zina trešā persona, tai ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt Pārzini to izdarīt savā vietā.

8. PERSONU RĪCĪBA APDRAUDĒJUMA GADĪJUMOS

8.1. Par jebkuru personas datu apstrādes apdraudējumu personas datu apstrādē iesaistītajai personai, kas to konstatējusi nekavējoties jāziņo Pārzinim, tai skaitā gadījumos:

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

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

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

8.2. Apdraudējuma gadījumā personas datu apstrādē iesaistītajai personai savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt IS drošību līdz Pārziņa ierašanās brīdim.

8.3. Gadījumos, kad tiek konstatēta prettiesiska personas datu nokļūšana trešo personu rīcībā (datu noplūde), personas datu apstrādē iesaistītajai personai nekavējoties jāinformē Pārzinis.

Rīgas plānošanas reģiona
Attīstības padomes priekšsēdētājs D. Straubergs

1. pielikums
2016.gada 16.novembra iekšējiem noteikumiem Nr.2
"Rīgas plānošanas reģiona fizisko personu datu
apstrādes aizsardzības noteikumi"

APLIECINĀJUMS

Es,

Vārds Uzvārds: _____ _____

Iestādes nosaukums: _____

Amats:

Personas kods: | | | | | | | — | | | | | |

E-pasts: _____

Tālrunis _____

apņemos saskaņā ar Fizisko personu datu aizsardzības likumu:

1. saglabāt un prettiesiski neizpaust amata (darba) pienākumu veikšanas laikā iegūtos personas datus trešajām personām;

2. amata (darba) pienākumu veikšanas laikā iegūtos personas datus prettiesiski neizpaust trešajām personām pēc darba tiesisko attiecību izbeigšanas;

3. nekavējoties informēt Rīgas plānošanas reģionu (Pārzinis) par nesankcionētu piekļuvi manā rīcībā esošiem personu datiem, kas iegūti veicot amata (darba) pienākumus RPR.

Ar šo apliecinu, ka esmu brīdināts (a), ka personas datu izpaušanas gadījumā varu tikt saukts (a) pie normatīvajos aktos noteiktās atbildības un uzņemos atbildību par savas darbības rezultātā pieļautajām kļūdām un radītajiem zaudējumiem saistībā ar dalību personas datu apstrādē.

Ar šo apliecinu, ka esmu iepazinies un man ir izskaidroti Rīgas plānošanas reģiona ____.____._____ iekšējie noteikumi "Rīgas plānošanas reģiona fizisko personu datu apstrādes aizsardzības noteikumi".

Pilnvarotā persona:

20__.gada _____

/paraksts un tā atšifrējums/

Pārzinis:

20__.gada _____

/paraksts un tā atšifrējums/

2. pielikums
2016.gada 16.novembra iekšējiem noteikumiem Nr.2
"Rīgas plānošanas reģiona fizisko personu datu
apstrādes aizsardzības noteikumi"

Rīgas plānošanas reģiona personas datu apstrādē izmantojamo Informācijas sistēmu reģistrācijas žurnāls

N.P.K.	Datums	Informācija par resursu			Saņēmēja		
		Tehniskie parametri, nosaukums	Izmantošanas veids	Atrašanās vieta	Paraksts	Atšifrējums	Datums
1.							
2.							
3.							
4.							

3. pielikums
2016.gada 16.novembra iekšējiem noteikumiem Nr.2
"Rīgas plānošanas reģiona fizisko personu datu
apstrādes aizsardzības noteikumi"

Rīgas plānošanas reģiona
Personas datu apstrādes darbību reģistrācijas žurnāls

N.P.K.	Datums	Darbības veicēja		Veiktās darbības apraksts	Datu subjekta	
		Vārds	Uzvārds		Vārds	Uzvārds
1.						
2.						
3.						
4.						

Sadaļā "Veiktās darbības apraksts" tiek norādīta informācija:

1. *Par personas datu **saņemšanu** – saņemšanas laiks, personu, kas nodevusi personas datus. Šo informāciju var aizvietot ar norādi uz pievienotu elektronisku vēstuli, pavadvēstuli vai citu dokumentētu informāciju, kas pievienota reģistrācijas žurnālam.*
2. *Par personas datu **nodošanu** – personas datu nodošanas laiks, personu, kas saņēmusi personas datus, personas datus, kas tika nodoti. Šo informāciju var aizvietot vai papildināt ar norādi uz pievienotiem dokumentiem, kas pievienoti reģistrācijas žurnālam.*
3. *Par citām darbībām, kas veiktas ar personas datiem, piemēram, kopēšana, pārrakstīšana, pārveidošana, labošana, dzēšana, iznīcināšana, rezerves kopēšana kādas darbības veiktas, veiktās darbības pamatojums vai mērķis. Šo informāciju var aizvietot vai papildināt ar norādi uz pievienotiem dokumentiem, kas pievienoti reģistrācijas žurnālam.*