APSTIPRINĀTS

ar biedrības „DIA+LOGS”

valdes priekšsēdētājas

2018.gada 15.decembrī rīkojumu Nr. 06/18-R

PERSONAS DATU APSTRĀDES AIZSARDZĪBAS IEKŠĒJIE NOTEIKUMI

1. Vispārīgie jautājumi

1.1. Biedrības „DIA+LOGS” (turpmāk tekstā – Biedrība) personas datu apstrādes aizsardzības iekšējie noteikumi (turpmāk – Noteikumi) nosaka personu datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības, nodrošinot Biedrībā personu datu apstrādes drošību atbilstoši Fizisko personu datu apstrādes likuma, 2016.gada 27.aprīļa Eiropas parlamenta un padomes regulas (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (turpmāk – Regulas), citu normatīvo aktu prasībām, kas attecināmi uz šo jautājumu.

1.2. Noteikumu mērķis ir noteikt Biedrības organizatorisko pasākumu un nepieciešamo tehnisko līdzekļu kopumu, kas nodrošina godprātīgu un likumīgu fizisko personu (turpmāk tekstā – personas dati) datu apstrādi un izmantošanu tikai paredzētajiem mērķiem, to glabāšanas, atjaunošanas, labošanas un dzēšanas veidu, nodrošinot ikvienas fiziskas personas tiesības uz savu personas datu aizsardzību.

1.3. Saskaņā ar Regulu uz personas datu apstrādi ir attiecināmi šādi termini:

1.3.1. **datu subjekts** – fiziska persona, kuru var tieši vai netieši identificēt;

1.3.2. **datu subjekta piekrišana** – datu subjekta brīvi, nepārprotami izteikts gribas apliecinājums, ar kuru viņš sniedz piekrišanu savu personas datu apstrādei;

1.3.3. **personas dati** – jebkāda informācija, kas attiecas uz identificētu vai neidentificējamu fizisku personu;

1.3.4. **personas datu apstrāde** – jebkuras ar fiziskas personas datiem vai personas datu kopumiem veiktas darbības, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un izpaušanu, bloķēšanu vai dzēšanu;

1.3.5. **personas datu apstrādes sistēma** – jebkādā formā fiksēta strukturizēta personas datu kopa, kas ir pieejama, ievērojot attiecīgus personu identificējošus kritērijus;

1.3.6. **personas datu apstrādātājs** – pārziņa pilnvarota persona, kas veic personas datu apstrādi pārziņa uzdevumā;

1.3.7. **personas datu saņēmējs** – fiziskā vai juridiskā persona, kurai tiek izpausti fiziskas personas dati;

1.3.8. **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;

1.3.9. **pārzinis** – Biedrība, 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;

1.3.10. **trešā persona** – jebkura fiziskā vai juridiskā persona, izņemot datu subjektu, pārzini, personas datu apstrādātāju un personas, kuras tieši pilnvarojis pārzinis vai personas datu apstrādātājs;

1.3.11. **drošības incidents** – ir kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas resursu saņemšana, uzglabāšana, pieejamība vai konfidencialitāte.

1.4. Personas datu apstrāde tiek veikta Biedrības biroja telpās, tās struktūrvienībās un/vai Biedrības pārvaldībā esošajās informācijas sistēmās un programmās.

1.5. Noteikumi ir saistoši Biedrības darbiniekiem, kuri apstrādā personas datus, kā arī citām juridiskām vai fiziskām personām, ja līgumā starp Biedrību un šīm citām juridiskām vai fiziskām personām ir atsauce uz šiem Noteikumiem.

1.6. Noteikumi ir attiecināmi uz visiem personas datiem, kas attiecas uz identificētu vai neidentificētu fizisko personu.

1.7. Personu datu apstrādi Biedrībā veic tikai datu apstrādei pilnvarotās personas un pilnvarojumā noteiktajā kārtībā un apjomā.

1.8. Biedrībai ir pienākums nodrošināt, ka katram personas datu veidam ir noteikts un skaidrs apstrādes mērķis, ka ir noteikts, kādos gadījumos personas dati var tikt nodoti citām personām un iestādēm, kā arī jānodrošina, ka personas dati ir drošībā un aizsargāti.

1.9. Personu datu apstrāde Biedrībā notiek, ievērojot šādus pamatprincipus:

1.9.1. godprātīga un likumīga datu apstrāde;

1.9.2. datu apstrāde tiek veikta atbilstoši paredzētajam mērķim un tikai saskaņā ar to;

1.9.3. dati ir adekvāti (ne pārmērīgi);

1.9.4. dati ir precīzi;

1.9.5. dati netiek, glabāti ilgāk, nekā nepieciešams (datu apstrādes ilgumam ir jābūt saistītam ar noteiktu personas datu apstrādes mērķi);

1.9.6. dati tiek apstrādāti saskaņā ar datu subjekta tiesībām;

1.9.7. dati ir drošībā;

1.9.8. dati netiek pārsūtīti uz citām organizācijām, iestādēm vai ārvalstīm bez drošas adekvātas aizsardzības.

1.10. Lai aizsargātu personas intereses, datu apstrādei pilnvarotā persona nodrošina:

1.10.1. godprātīgu un likumīgu personas datu apstrādi;

1.10.2. personas datu apstrādi tikai atbilstoši paredzētajam mērķim un tam nepieciešamajā apjomā;

1.10.3. tādu personas datu glabāšanas veidu, kas datu subjektu ļauj identificēt attiecīgā laika posmā, kurš nepārsniedz paredzētajam datu apstrādes mērķim noteikto laika posmu;

1.10.4. personas datu pareizību un to savlaicīgu atjaunošanu, labošanu vai dzēšanu, ja par datu apstrādi nozīmētā persona ir informēta, vai tai vajadzēja būt informētai par to, ka personas dati ir nepilnīgi vai neprecīzi saskaņā ar personas datu apstrādes mērķi.

1.11. Par personas datu aizsardzību, informācijas drošības un pilnveidošanas procesu kopumā atbild Biedrības valdes priekšsēdētājs, kurš pats vai ar norīkoto personu starpniecību kontrolē personas datu apstrādes sistēmu drošību (turpmāk tekstā – Valdes priekšsēdētājs).

1.12. Valdes priekšsēdētājs var bez brīdinājuma liegt pilnvarotai personai piekļuvi personas datu apstrādes sistēmai, ja pilnvarotā persona pārkāpj Latvijas Republikas normatīvos aktus un/vai Biedrības iekšējos normatīvos aktus.

1.13. Valdes priekšsēdētājs ir tiesīgs pieprasīt no pilnvarotās personas rakstveida apliecinājumu par šo noteikumu un konfidencialitātes prasību ievērošanu darbā ar personas datiem un personas datu apstrādes sistēmu, kā arī veikt citas darbības, kuras uzskata par nepieciešamu, lai tiktu ievērotas normatīvo aktu prasības personu datu aizsardzības jomā.

1.14. Valdes priekšsēdētāja pienākums ir rūpēties par personas datu apstrādes sistēmas darbību, nodrošinot pilnvaroto personu drošu piekļuvi tai, kā arī iespēju datu subjektam iepazīties ar saviem personas datiem.

2. Vispārīgas personu datu apstrādes prasības

2.1. Uzsākot datu apstrādi (t.sk. vākšanu), datu subjekts jāinformē par to, ka:
- 2.1.1. tiks apstrādāti personas dati;
- 2.1.2. datus apstrādās Biedrība;
- 2.1.3. personas datu apstrādes mērķis.

2.2. Ja datu subjekts pieprasa, ir jāsniedz informācija par:
- 2.2.1. iespējamiem personu datu saņēmējiem;
- 2.2.2. datu subjekta tiesībām piekļūt saviem datiem un izdarīt tajos labojumus;
- 2.2.3. vai datu subjekta atbildes sniegšana ir obligāta vai brīvprātīga, kā arī iespējamās sekas par atbildes nesniegšanu;
- 2.2.4. personas datu apstrādes tiesiskais pamats.

2.3. Biedrība reģistrē sniegto informāciju.

2.4. Personas dati ir jāglabā, ievērojot vispārīgās datu glabāšanas un drošības prasības, t.sk., ar tehniskiem un organizatoriskiem līdzekļiem jānodrošina, ka personas datus nevar sagrozīt, bojāt un tiem nepiekļūst nepilnvarotās personas (datiem ir nodrošināta kontrolēta piekļuve slēgtās telpās, slēgtiem skapjiem, vietnēm un informācijas tehnoloģiju sistēmām).

2.5. Pirms personas datu izpaušanas vai nodošanas citām personām, t.sk., citiem darbiniekiem, jāpārliecinās, vai tam ir tiesisks pamats un likumīgs mērķis.

2.6. Personas dati bez šīs personas atļaujas netiek izpausti trešajām personām, izņemot, ja datu izpaušanu paredz normatīvie akti.

2.7. Personas dati tiek izpausti tikai tām personām vai iestādēm, kuras pirms datu izpaušanas ir identificētas, pamatojoties uz rakstveida iesniegumu vai vienošanos, norādot datu izmantošanas mērķi. Personas datu pieprasījumā norādama informācija, kas ļauj identificēt datu pieprasītāju un datu subjektu, kā arī pieprasāmo personas datu apjoms (aizliegts izpaust datus pa tālruni vai personas klātbūtnē, ja tā nav identificēta).

3. Personas datu apstrādes sistēmas nodrošinājums

3.1. Personas datu obligāto tehnisko aizsardzību īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret drošības incidenta radītu personas datu apdraudējumu.

3.2. Dati, kas tiek izmantoti personas datu apstrādē, ir klasificējami kā ierobežotas pieejamības informācija, kas paredzēta tikai noteiktam Biedrības darbinieku lokam. Informācijas sistēmas datus drīkst izmantot tikai Biedrības darbinieks, kuram valdes priekšsēdētājs ir devis atļauju ar attiecīgiem piekļuves datiem (turpmāk tekstā – Pilnvarotā persona).

3.3. Personas datu apstrādes sistēmas datortehnikas un programmatūras tehniskā uzstādīšana un tās administrēšana tiek nodrošināta atbilstoši vispārējiem IT drošības un IT lietošanas noteikumiem, un saskaņā Biedrības un SIA "DPS" vienošanos.

3.4. Datorizētās informācijas sistēmām (turpmāk – Informācijas sistēma) tiek nodrošināta autentifikācija atbilstoši IT drošības noteikumiem.

3.5. Apstrādājot personas datus Informācijas sistēmā, tiek nodrošināta tikai pilnvarotu personu piekļūšana pie tehniskajiem līdzekļiem un informācijas.

3.6. Biedrība personas datu saturošas programmatūras apstrādei lieto šādas ierīces:
- 3.6.1. darbstacijas un portatīvās iekārtas ar operētājsistēmu;
- 3.6.2. citas licencētas iekārtas un programmatūru pēc vajadzības.

3.7. Informācijas sistēmas personas datu apstrādes loģisko drošību nodrošina Biedrības resursu administrators kopā ar IT drošības pārvaldnieku, organizējot drošības iestatījumus tā, lai iespējamie riski tiktu novērsti pirms to iestāšanās.

4. Personas datu apstrādes organizatoriskā procedūra, aizsardzība pret ārkārtējiem apstākļiem un datu drošības pasākumi

4.1. Personas datu apstrāde Biedrībā ir atļauta tikai tad, ja normatīvajos aktos nav noteikts citādi un ja ir vismaz viens no šādiem nosacījumiem:
- 4.1.1. saņemta personas datu subjekta piekrišana;
- 4.1.2. datu apstrāde izriet no datu subjekta līgumsaistībām vai, ievērojot datu subjekta lūgumu, datu apstrāde nepieciešama, lai noslēgtu attiecīgu līgumu;
- 4.1.3. datu apstrāde nepieciešama Biedrības likumā noteikto funkciju veikšanai;
- 4.1.4. datu apstrāde neiecieš̆ama, lai aizsargātu datu subjekta vitāli svarīgas intereses, tajā skaitā dzīvību un veselību;
- 4.1.5. datu apstrāde nepieciešama, lai nodrošinātu sabiedrības interešu ievērošanu vai realizētu publiskās varas uzdevumus, kuru veikšanai personas dati ir nodoti Biedrībai vai pārraidīti trešajai personai;
- 4.1.6. datu apstrāde ir nepieciešama, lai, ievērojot datu subjekta pamattiesības un brīvības, realizētu Biedrības vai tās trešās personas likumiskās intereses, kurai personas dati atklāti.

4.2. Biedrība nodrošina, ka katram datu veidam ir noteikts un skaidrs apstrādes mērķis un ir noteikts, kādos gadījumos personas dati var tikt nodoti citām personām un iestādēm, kā arī jānodrošina, ka personu dati ir drošībā un aizsargāti.

4.3. Biedrība nodrošina tehnisko resursu fizisku aizsardzību pret ārkārtas apstākļiem (ugunsgrēks, plūdi u.c. apstākļi). Pasākumi pret ārkārtas apstākļiem tiek īstenoti

saskaņā ar Biedrības ugunsdrošības noteikumiem, kā arī vispārējām normatīvo aktu prasībām par elektroiekārtu drošu ekspluatāciju un to aizsardzību.

4.4. Lai izvairītos no tehnisko resursu tīšas bojāšanas radītām sekām, Biedrība rūpējas, lai tehnisko resursu pārvaldība notiktu atbilstoši Biedrības IT drošības un IT lietošanas noteikumiem.

4.5. Personas datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes pakāpei tiek iedalīta, pielikums Nr.2:

4.5.1. **Konfidenciāli dati** ir sensitīvi personas dati – atbilst augstākajam konfidencialitātes līmenim *(saskaņā ar normatīvajiem aktiem tie ir 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)*. Šie dati tiek iegūti un apstrādāti tikai tad, ja persona ir devusi rakstveida piekrišanu savu sensitīvo datu apstrādei un šādu datu apstrādi nosaka normatīvie akti;

4.5.2. **Iekšējas lietošanas dati** ir visi personas lietā iekļautie vai iekļaujamie dati – atbilst vidējam konfidencialitātes līmenim *(piem., personas kods, dzimšanas dati, identifikācijas dokumenta dati, adrese, privātais tālrunis, privātais e-pasts, sekmes, darba snieguma novērtējums, ģimenes stāvoklis)*;

4.5.3. **Brīvi iekšējās lietošanas dati** – ir personas *vārds, uzvārds, amats, darba vietas e-pasta adrese, darba vietas tālrunis, struktūrvienības nosaukums*, šie dati atbilst zemākajam konfidencialitātes līmenim.

4.6. Konfidenciālie dati tiek apstrādāti tikai, ja to nosaka normatīvie akti un tajos noteiktajā apmērā. Sensitīviem personas datiem tiek piemērots augstākais konfidencialitātes līmenis. Tie tiek izpausti tikai personām, normatīvajos aktos noteikto fiziskās personas tiesību vai pienākumu īstenošanai. Augstākā līmeņa konfidenciālie dati uzglabājami slēgtā telpā vai arī šifrētā veidā, ja tie ir elektroniskā formātā un tiem var piekļūt tikai iepriekš reģistrējoties. Ja konfidenciālie dati tiek izmantoti koleģiālo institūciju lēmuma pieņemšanā, publiskojamā lēmuma daļā, konfidenciālie dati tiek ar fiziskiem un tehnoloģiskiem līdzekļiem slēpti.

4.7. Iekšējās lietošanas dati tiek apstrādāti, ievērojot datu apstrādes principus, ir pieejami noteiktiem Biedrības darbiniekiem.

4.8. Brīvi iekšējās lietošanas dati, ievērojot datu apstrādes principus, ir pieejami ikvienam Biedrības darbiniekam, un ir publicējami Biedrības mājaslapā un citos sociālajos tīklos.

4.9. Biedrība savas darba organizācijas un darbības nodrošināšanai nosaka personas datu apstrādes mērķi, kā arī paredzēto datu apstrādes apjomu, kas nepieciešams datu apstrādes mērķa sasniegšanai.

4.10. Katram noteiktajam datu apstrādes mērķim ir jāidentificē datu subjekts, personas datu apstrādes veids un lietotāji vai trešās personas, kuras veic personas datu apstrādi.

4.11. Uzsākot jaunus projektus, ir jādefinē paredzamie datu apstrādes mērķi un paredzamais datu apstrādes apjoms, kas nevar būt lielāks par personas datu apstrādes mērķa sasniegšanai nepieciešamo.

4.12. Ne retāk kā reizi gadā ir jāveic personas datu apstrādes mērķa un ar to saistīto datu apjoma izvērtējums, ko veic datu aizsardzības speciālists sadarbībā ar Biedrības atbildīgām personām (pielikums Nr.1).

4.13. Personas datu apstrādāto informācijas resursu uzglabāšana un iznīcināšana notiek atbilstoši Biedrības Dokumentu apgrozības shēmai un lietu nomenklatūrai. Lietu nomenklatūra tiek regulāri aktualizēta.

4.14. Ja tiek saņemts pieprasījums no datu subjekta par informācijas iegūšanu par personu datu apstrādi, kas saistīta ar viņu, tad pilnvarotā persona apkopo visu informāciju, kas saistīta ar datu subjekta personu datu apstrādi tālāk noformējot to izziņas veidā un izsniedz datu subjektam.

4.15. Par personas datu apstrādes aizsardzības uzraudzību un nodrošināšanu atbilstoši šiem Noteikumiem ir atbildīgi Biedrības darbinieki, kuru pārziņā tiek organizēta datu apstrāde, un par attiecīgo datu apstrādi pilnvarotais darbinieks.

4.16. Biedrībai aizliegts nodot trešajām personām tehniskos resursus, ja tie satur personas datus. Šis aizliegums jāievēro arī gadījumos, kad tehnika tiek nodota utilizācijai.

4.17. Par jebkuru personas datu apstrādes incidentu Biedrības darbiniekam, kas to konstatējis, ir nekavējoties jāpaziņo informācijas resursu un tehnisko resursu turētājam:

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

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

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

5. Pilnvarotās personas tiesības, pienākumi un atbildība

5.1. Pilnvarotā persona ir atbildīga par datortehniku, kas nodota personas rīcībā, kā arī par dokumentiem, kas nepieciešami personas darba pienākumu pildīšanai.

5.2. Pilnvarotai personai ir tiesības izmantot lietošanā nodotos datorus un to programmatūru tikai darba vajadzībām.

5.3. Pilnvarotā persona nedrīkst izpaust ziņas par biedrības datoru tīklu uzbūvi un konfigurāciju, kā arī atklāt ierobežotas pieejamības informāciju nepilnvarotām personām. Personas datus var izpaust, pamatojoties uz rakstveida iesniegumu, norādot datu izmantošanas mērķi, ja normatīvajos aktos nav noteikts citādi. Personas datu pieprasījumā norādāma informācija, kas ļauj identificēt pieprasītāju un datu subjektu, kā arī personas datu apjomu.

5.4. Pilnvarotā persona nedrīkst atļaut piekļūt personas datiem nepiederošām personām, ja tas nav nepieciešams tiešo darba pienākumu veikšanai.

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

5.6. Pilnvarotās personas pienākums ir lietot nepieciešamos tehniskus un organizatoriskus līdzekļus, lai aizsargātu personas datus un novērstu to pretlikumīgu apstrādi.

5.7. Pilnvarotai personai ir aizliegts izmantot nelicencētu programmatūru.

5.8. Biedrībā ir aizliegta jebkāda nešifrēta bezvadu datortīkla izmantošana.

5.9. Pilnvarotā persona nedrīkst izdarīt darbības, kas būtu vērstas pret informācijas sistēmas drošību, izmantojot neparedzētas pieslēgšanās iespējas.

5.10. Beidzot (pārtraucot) darbu ar informācijas sistēmu, pilnvarotā persona aizver pārlūkprogrammu.

5.11. Pilnvarotā persona nedrīkst 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.

5.12. Ja ir aizdomas par tīšiem bojājumiem, kas radušies informācijas sistēmas paroles publiskošanas rezultātā vai citu iemeslu dēļ, pilnvarotā persona par to nekavējoties ziņo Pārzinim (biedrības vadībai).

6. Datu subjekta tiesības

6.1. Datu subjektam ir tiesības iegūt visu informāciju, kas par viņu savākta Biedrības personu apstrādes sistēmā, iesniedzot iesniegumu Pārzinim (Biedrības vadībai), ja vien šo informāciju izpaust nav aizliegts ar likumu.

6.2. Datu subjektam ir tiesības iegūt informāciju par tām fiziskām un juridiskām personām, kuras ir saņēmušas informāciju par šo datu subjektu, pēdējos divus gadus, iesniedzot iesniegumu Pārzinim (Biedrības vadībai).

6.3. Datu subjektam ir tiesības pieprasīt, lai viņa personas datus papildina, izlabo vai dzēš (iznīcina).

1. pielikums
pie Noteikumiem par personu datu apstrādes aizsardzību

PAR BIEDRĪBĀ "DIA-LOGS"

APSTRĀDĀTAJIEM FIZISKĀS PERSONAS DATIEM

Aizpildot tabulu par attiecīgajā struktūrvienībā apstrādātajiem fiziskās personas datiem, vēlams norādīt vismaz šādu informāciju (tabula var tikt precizēta gan izdodot rīkojumu par datu apstrādi, gan struktūrvienību vadītājiem aizpildot pārskatu par iepriekšējo gadu):

1.	Personu kategorija (klienti, studenti, darbinieki, apmeklētāji utt.).	
2.	Personas datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes pakāpei.	
3.	Personas dati – precīzi jānorāda, tieši kādi (piemēram: vārds, uzvārds, tālrunis, vecums, personas kods utt.).	
4.	Ar datiem veicamās darbības (vākšana, glabāšana, sistematizēšana – elektroniski, papīra formātā, publiskošana u.c.).	
5.	Datu apstrādes pamatojums (likuma pants/ līgumsaistības/ personas piekrišana u.c.).	
6.	Datu apstrādes mērķis.	
7.	Kur un cik ilgi dati tiek glabāti.	
8.	Kādā veidā tiek organizēta personas piekrišanas izteikšana datu apstrādei un glabāšanai (vai piekrišana izteikta rakstveidā).	
9.	Kādā veidā (ar fiziskiem vai programmatūras līdzekļiem) tiek nodrošināta datu aizsardzība.	
10.	Kas šos datus apstrādā (amats).	
11.	Kam ir piekļuve datiem un cik lielā apjomā.	
12.	Kādos gadījumos personas datus izsniedz trešajām personām.	
13.	Kādā veidā notiek personas datu aktualizēšana un cik bieži.	
14.	Kādā veidā dati tiek iznīcināti.	
15.	Personas tiesības piekļūt saviem personas datiem un izdarīt tajos labojumus.	
16.	Cita nozīmīga informācija (ja nepieciešams).	

2. pielikums
pie Noteikumiem par personu datu apstrādes aizsardzību

FIZISKO PERSONU DATU VEIDI

A. **Konfidenciāli dati** ir sensitīvi personas dati – kas atbilst augstākajam konfidencialitātes līmenim:

- personas rase;
- etniskā izcelsme;
- reliģiskā, filozofiskā un politiskā pārliecība;
- dalība arodbiedrībās;
- informācija par personas veselību vai seksuālo dzīvi.

B. **Iekšējas lietošanas dati** ir visi personas lietā iekļautie vai iekļaujamie dati – kas atbilst vidējam konfidencialitātes līmenim:

- personas kods;
- dzimšanas dati;
- dzimums;
- vecums;
- darba pieredze;
- izglītība;
- kvalifikācija;
- ziņas par valodas prasmēm;
- papildus izglītības un kursi;
- informācija par obligātās veselības pārbaudēm;
- audio/video ieraksti;
- fotogrāfijas;
- bērna vārds, uzvārds;
- bērna personas kods;
- ģimenes locekļu tālruņa numurs;
- ģimenes locekļu e-pasta adrese;
- identifikācijas dokumenta dati;
- deklarētā dzīves vietas adrese;
- faktiskā (korespondences) adrese;
- privātā tālruņa numurs (t.sk., mobilā);
- privātais e-pasts;
- bankas norēķinu konts;
- sekmes;
- darba snieguma novērtējums;
- ģimenes stāvoklis;
- u.c..

C. **Brīvi iekšējās lietošanas dati**, kas atbilst zemākajam konfidencialitātes līmenim:

- vārds, uzvārds;
- amats;
- darba vietas e-pasta adrese;
- darba vietas tālrunis;
- struktūrvienības nosaukums.