SIA Eiropas Tālmācības centrs
Reģistrācijas Nr. LV43603089888
Profesionālās tālākizglītības centrs
"Eiropas Tālmācības centrs"
Reģistrācijas Nr. 4515802989

Juridiskā adrese: Baldones iela 27A-2, Iecava, Bauskas novads, LV 3913
Faktiskā adrese: Lomonosova iela 1 k-4, Rīga, LV-1019
Mob. tālr.: +371 22038287 • e-pasts: etc@eiropascentrs.lv, www.eiropascentrs.lv

IEKŠĒJIE NOTEIKUMI
Rīgā

APSTIPRINĀTS
ar Eiropas Tālmācības centrs
direktores L.Likas
02.09.2022. rīk.Nr.1-08/8

2022.gada 2.septembrī Nr. 1-19/16

Personas datu apstrādes aizsardzības noteikumi

1. SIA Eiropas Tālmācības centrs vienotais reģistrācijas Nr. 43603089888, tās struktūrvienības Profesionālās tālākizglītības centrs "Eiropas Tālmācības centrs", reģistrācijas Nr. izglītības iestāžu 4515802989 (turpmāk – Sabiedrība jeb Pārzinis) personas datu apstrādes aizsardzības noteikumi nosaka kārtību, kā:

1.1. notiek personas datu apstrāde, aprite, glabāšana, un iznīcināšana;

1.2. tiek nodrošināti minimālie tehnoloģiski un organizatoriskie pasākumi personas datu apstrādē;

1.3. datu subjekts, var piekļūt personas datiem, kas par to savākti, kādas ir datu subjekta tiesības uz savu personas datu labošanu un "tiesībām tikt aizmirstam", ja šādu personas datu glabāšana pārkāpj Vispārīgo datu aizsardzības regulu vai Eiropas Savienības, vai dalībvalsts tiesību aktus, kas ir piemērojamas pārzinim;

1.4. rīkoties gadījumos, kad tiek konstatēts drošības pārkāpums, kas izraisa nejaušu vai nelikumīgu personas datu, kas tiek pārsūtīti, glabāti vai citādi apstrādāti, bojāeju, zudumu, izmaiņas, neatļautu izpaušanu vai piekļuvi tiem.

Kārtības mērķis nodrošināt Sabiedrības fizisko personu datu apstrādes drošību atbilstoši Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 (2016. gada 27. aprīlis) par fizisko personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46 EK.

2. VISPĀRĪGIE NOTEIKUMI

2.1. Noteikumu mērķis nodrošināt 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.

2.2. Dati, kas tiek izmantoti personas datu apstrādē, ir klasificējami kā ierobežotas pieejamības informācija, kas paredzēta tikai noteiktam Sabiedrības darbinieku lokam (1.pielikums) un uz kuriem attiecināms dienesta noslēpuma ievērošanas pienākums.

2.3. Noteikumi ir saistoši viesiem Sabiedrības darbiniekiem, kuri apstrādā personas datus.

2.4. Personas datu apstrāde tiek veikta Sabiedrības telpās un/vai Sabiedrības pārvaldībā esošajās informācijas sistēmās.

2.5. Noteikumi attiecināmi uz visiem personas datiem, kas attiecas uz identificētu vai identificējamu fizisko personu.

2.6. Pārzinis var bez brīdinājuma dzēst vai mainīt darbinieka personas datus personas datu apstrādes sistēmas piekļuvei, ja darbinieks pārkāpj Latvijas Republikas normatīvos aktus un/vai saistošos normatīvos

aktus, un/vai Sabiedrības iekšējos normatīvos aktus.

2.7. Pārzinis ir tiesīgs pieprasīt no darbinieka 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 ievēroti spēkā esošie Latvijas Republikas normatīvie akti attiecībā uz prasībām par personas datu aizsardzību.

2.8. Pārziņa pienākums ir rūpēties par personas datu apstrādes sistēmas darbību, nodrošinot darbiniekiem drošu piekļuvi, kā arī iespēju datu subjektam iepazīties ar saviem personas datiem.

2.9. **Personas datu apstrāde Sabiedrībā notiek, ievērojot šādus pamatprincipus:**

1) godprātīga un likumīga datu apstrāde;
2) datu apstrāde tiek veikta atbilstoši paredzētajam mērķim un tikai saskaņā ar to;
3) dati ir adekvāti (ne pārmērīgi);
4) dati ir precīzi;
5) dati netiek glabāti ilgāk, nekā nepieciešams (datu apstrādes ilgumam ir jābūt saistītam ar noteiktu personas datu apstrādes mērķi);
6) dati tiek apstrādāti saskaņā ar datu subjekta tiesībām;
7) dati ir drošībā;
8) dati netiek pārsūtīti uz citām organizācijām, iestādēm vai ārvalstīm bez drošas adekvātas aizsardzības.

2.10. **Personas datu apstrādes nolūki:**

1) **līguma noslēgšana un izpilde** – lai Sabiedrība varētu noslēgt un izpildīt līgumu, pakalpojuma izpildīšanai, apkopojot un apstrādājot noteiktus personas dati, kas tiek savākti pirms līguma noslēgšanas vai jau noslēgtā līguma laikā;
2) **Sabiedrības leģitīmās intereses** – ievērojot Sabiedrības intereses, kuras pamatā ir kvalitatīva pakalpojuma nodrošināšana. Sabiedrībai ir tiesības apstrādāt personas datus tādā apjomā, kādā tas ir objektīvi nepieciešams un pietiekams norādīto nolūku īstenošanai;
3) **juridisko pienākumu izpilde** – Sabiedrība ir tiesīga apstrādāt personas datus, lai izpildītu spēkā esošos Latvijas Republikas normatīvos aktus, kā arī sniegtu atbildes uz valsts un pašvaldības likumīgiem pieprasījumiem;
4) **piekrišana** – personas datu subjekta piekrišanu personas datu vākšanai un apstrādei noteiktiem mērķiem. Datu subjektam tiesības jebkurā laikā atsaukt savu iepriekš sniegto piekrišanu, izmantojot norādītos saziņas kanālus ar Sabiedrību. Pieteiktās izmaiņas stājas spēkā 3 (trīs) darba dienu laikā pēc šāda paziņojuma saņemšanas. Piekrišanas atsaukums neietekmē apstrādes likumību, kas pamatojas uz piekrišanu pirms atsaukuma;
5) **vitālu interešu aizsardzība** – Sabiedrība ir tiesīga apstrādāt personas datus, lai aizsargātu datu subjektu, tā pārstāvju pārstāvju, Sabiedrības darbinieku vai citas fiziskas personas vitālās intereses, piem., ja apstrāde ir vajadzīga humanitāros nolūkos, dabas stihiju un cilvēka izraisītu, it īpaši, epidēmiju un to izplatīšanās monitoringam vai ārkārtas humanitārajās situācijās (terora akti, kibernoziegumi, tehnogēnās katastrofu situācijas un tml.);
6) **oficiālo pilnvaru izpilde vai Sabiedrības intereses** – Sabiedrība ir tiesīga apstrādāt personas datus, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot Sabiedrības likumīgi piešķirtās oficiālās pilnvaras. Šādos gadījumos pamats personas datu apstrādei ir iekļauts normatīvajos aktos. Par personas datu aizsardzību, informācijas drošības un pilnveidošanas procesu kopumā atbild Sabiedrības valdes loceklis, kurš pats vai ar norīkoto personu starpniecību kontrolē personas datu apstrādes sistēmu drošību.

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

2.12. **Sabiedrība izmanto personas datu apstrādē sekojošus personas datu veidus:**

1) **identifikācijas un kontaktinformācijas dati:** vārds, uzvārds, personas kods, dzimšanas datums, pases dati, dzimums, adrese, telefona numurs, e-pasta adrese, dzīvesvietas adrese;

2) **pakalpojuma sniegšanas laikā iegūtie dati**: pakalpojuma sniegšanas laikā iegūtie dati, tajā skaitā veselības dati (personas dati, kas saistīti ar fiziskas personas fizisko vai garīgo veselību, tostarp veselības aprūpes pakalpojumu sniegšanu, un kas atspoguļo informāciju par tās veselības stāvokli);

3) **ar pakalpojuma apmaksu saistītie dati:** apmaksas statuss, diagnozes kods, apdrošināšanas polises numurs;

4) **pilnvaroto personu dati:** pilnvarotās personas, kas normatīvajos aktos noteiktajā kārtībā pārstāv datu subjektu.

3. ATBILDĪGĀS PERSONAS PAR PERSONAS DATU APSTRĀDI

3.1. Sabiedrībā atbildīgās personas par personas datu apstrādi informācijas resursos, tehniskajos resursos un personas datu aizsardzību Sabiedrībā tiek noteikts ar Eiropas Tālmācības centra direktora rīkojumu.

3.2. Atbildīgā persona par informācijas resursiem:

1) nodrošina loģiskās aizsardzības pasākumus;
2) nodrošina informācijas resursu darbības atjaunošanu, ja noticis tehnisko resursu bojājums vai arī informācijas resursu darbība ir tikusi traucēta citu iemeslu dēļ.

3.3. Atbildīgā persona par tehniskajiem resursiem:

1) nodrošina fiziskās aizsardzības pasākumus;
2) nodrošina tehnisko resursu darbspēju;
3) nodrošina tehnisko resursu atjaunošanu vai nomaiņu, ja tie bojāti.

3.4. Atbildīgā par personu datu aizsardzību:

1) organizē un kontrolē personas datu apstrādes atbilstību likuma prasībām;
2) atbild par personāla dokumentācijas un ar to saistīto personas datu apstrādes atbilstību normatīvo aktu prasībām;
3) nodrošina un kontrolē personāla dokumentācijas un tajā iekļauto personas datu apstrādes atbilstību likuma prasībām;
4) nodrošina ar personāla vadību saistīto procesu atbilstību likuma prasībām, tajā skaitā attiecībā uz minētajos procesos veikto personas datu apstrādi.

4. VISPĀRĒJĀ PERSONAS DATU APSTRĀDES KĀRTĪBA

4.1. Pārzinis veic personas datu apstrādi gan manuāli (papīra formā, iekļaujot tos līgumos, vēstulēs un aktos u.c.dokumentos), gan elektroniski, apstrādājot personas datus Sabiedrības grāmatvedības uzskaites programmās.

4.2. Personas datu vākšana no datu subjektiem veic Sabiedrības darbinieki, kas strādā ar datu subjektu personas datiem, ievērojot šos Noteikumus, Regulas un citu personas datu apstrādi regulējošo normatīvo aktu prasības.

4.3. Personas dati no datu subjektiem tiek ievākti datu subjektam uzrādot personas apliecinošos dokumentus, savstarpējās pārrunās, no elektroniskās sarakstes, kā arī aizpildot un iesniedzot attiecīgus dokumentus saskaņā ar spēkā esošajiem Latvijas Republikas normatīvajiem aktiem.

4.4. Gatavojot līgumu projektus darbiniekiem ir tiesības un pienākums pieprasīt no datu subjekta, lai tiek uzrādīti personu apliecinoši dokumenti (pases, personas identifikācijas kartes u.c.) oriģināli. Nav atļauts izgatavot un glabāt minēto dokumentu kopijas.

4.5. Darbiniekam pirms personas datu saņemšanas ir jāinformē datu subjekts par paredzēto personas

datu apstrādes mērķi un pamatojums, kā arī jāpārliecinās, ka ir saņemta datu subjekta nepārprotama piekrišana personas datu apstrādei, ja šāda piekrišana nepieciešama.

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

4.7. Pārzinis nodrošina tehnisko resursu fizisku aizsardzību pret ārkārtas apstākļiem (ugunsgrēks, plūdi un citi ārkārtas apstākļi). Pasākumi pret ārkārtas apstākļiem tiek īstenoti saskaņā ar Sabiedrības ugunsdrošības noteikumiem, kā arī vispārējām normatīvo aktu prasībām par elektroiekārtu drošu ekspluatāciju un to aizsardzību.

4.8. Lai izvairītos no tehnisko resursu tīšas bojāšanas radītām sekām, Pārzinis rūpējas, lai tehnisko resursu pārvaldība notiktu atbilstoši Sabiedrības IT drošības noteikumiem un Sabiedrības IT lietošanas noteikumiem.

4.9. Sabiedrības personas datu aizsardzības sistēma tiek veidota tā, lai pēc iespējas izvairītos no vienu un to pašu datu apstrādes vairākās struktūrvienībās.

4.10. Personas datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes pakāpei tiek iedalīta šādi:

1) konfidenciāli dati ir īpašas kategorijas personas dati – šo datu apzīmējums Sabiedrībā risku klasifikatorā ir K1, kas atbilst augstākajam konfidencialitātes līmenim;
2) iekšējās lietošanas dati ir visi personas lietā iekļautie vai iekļaujamie dati – šo datu apzīmējums Sabiedrības risku klasifikatorā ir K2, kas atbilst vidējam konfidencialitātes līmenim;
3) brīvi iekšējās lietošanas dati ir personas vārds, uzvārds, amats, darba vietas e-pasts, darba vietas tālrunis, struktūrvienības nosaukums – šo datu apzīmējums Sabiedrības risku klasifikatorā ir K3, kas atbilst zemākajam konfidencialitātes līmenim.

4.11. Konfidenciālie dati tiek apstrādāti tikai, ja to nosaka normatīvie akti un tajos noteiktajā apmērā. Augstākā līmeņa konfidenciālie dati (K1) dati tiek marķēti ar apzīmējumu "SENSITĪVS" un tiem tiek piemērots augstākais konfidencialitātes līmenis. Tie tiek izpausti tikai personām, normatīvajos aktos noteikto fiziskās personas tiesību vai pienākumu īstenošanai. Augstākā līmeņa konfidenciālie dati (K1) 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 lēmumu pieņemšanā, publiskojamā lēmuma daļā, konfidenciālie dati tiek ar fiziskiem un tehnoloģiskiem līdzekļiem slēpti.

4.12. Iekšējās lietošanas dati un brīvi iekšējās lietošanas dati, tiek apstrādāti, ievērojot vispārējos datu apstrādes principus.

4.13. Pēc datu subjekta pieprasījuma darbiniekam ir pienākums sniegt šādu informāciju:

1) iespējamie personas datu saņēmēji;
2) datu subjekta tiesībām piekļūt saviem personas datiem un izdarīt tajos labojumus.

4.14. Darbinieks, kas atbild par grāmatvedības vajadzībām apstrādāto personas datu apstrādāšanu, apstrādā šos personas datus veicot to reģistrāciju, sakārtošanu, pārveidošanu, nodošanu, kopēšanu un cita veidi apstrādi. Pārējiem darbiniekiem piekļuves tiesības noteiktas Noteikumu 1.pielikumā, ar tiesībām vai bez tiesībām veikt jebkādus grozījumus vai izmaiņas tajos.

4.15. Darbinieki ir atbildīgi par personas datu pareizību un to savlaicīgu atjaunošanu, labošanu vai dzēšanu, ja personas dati ir nepilnīgi vai neprecīzi, kā arī nodrošina personas datu uzglabāšanu, sniegšanu, izpaušanu un nodošanu saskaņā ar Regulā, citos normatīvajos aktos un šajos noteikumos minētajām prasībām.

4.16. Darbinieki nododot personas datus, nodrošina informācijas saglabāšanu par:

1) personas datu nodošanas laiku;
2) personu, kas nodevusi personas datus;
3) personu, kas saņēmusi personas datus;
4) personas datiem, kas tikuši nodoti.

4.17. Informācija tiek saglabāta rakstveidā, saskaņā ar Sabiedrības lietu nomenklatūru.

4.18. Darbiniekiem ir pienākums nekavējoties ziņot Sabiedrības vadībai un tehnisko resursu turētājam par izmantojamās datu apstrādes sistēmas nepilnībām, drošības incidentiem, iespējamiem darbības traucējumiem, kā arī ziņot par iespējamo pārkāpumu personas datu apstrādē.

4.19. Darbiniekiem nav atļauts bez saskaņojuma ar Sabiedrības vadību veikt personas datu iznīcināšanu.

4.20. Faksu, skeneru un distances saziņas līdzekļu, kurus izmantojot iespējams individuāls kontakts ar datu subjektu, ir atļauts izmantot saziņai ar datu subjektu, tikai tādos nolūkos, kas noteikti šajos Noteikumos vai ja šādas tiesības noteiktas līgumā un/vai likumā. Izmantojot tālruni, atbildīgā darbinieka (pilnvarotā persona) pienākums ir sarunas sākumā informēt datu subjektu par savu identitāti un zvana mērķi. Sabiedrībā aizliegta šādu sarunu ierakstīšana, šādu ierakstu glabāšana un izmantošana.

4.21. Personas datus saturošie dokumenti jāglabā slēdzamā skapī (vēlams metāla). Atslēga tiek glabāta pie atbildīgā darbinieka.

4.22. Ne retāk kā reizi gadā ir jāveic personas datu apstrādes mērķa un ar to saistīto datu apjoma izvērtējums, ko veic Sabiedrības valde vai pilnvarotā persona.

4.23. Ja tiek saņemts pieprasījums no datu subjekta par informācijas iegūšanu par personu datu apstrādi, kas saistīta ar viņu, tad pēc Sabiedrības valdes locekļa pieprasījuma, atbildīgais darbinieks apkopo visu informāciju, kas saistīta ar datu subjekta personu datu apstrādi un nodod to Sabiedrības valdes loceklim, kas saņemto informāciju apkopo izziņas veidā un izsniedz datu subjektam.

4.24. Par personas datu apstrādes aizsardzības uzraudzību un nodrošināšanu atbilstoši šiem Noteikumiem ir atbildīgs Sabiedrības valdes loceklis, kuru pārziņā tiek organizēta datu apstrāde, un par attiecīgo datu apstrādi pilnvarotais darbinieks jeb pakalpojuma sniedzējs.

4.25. Darbinieks nedrīkst atļaut piekļūt personas datiem nepiederošām personām, ja tas nav nepieciešams tiešo darba pienākumu veikšanai.

4.26. Darbiniekam pienākums bez tiesiska pamata neizpaust personas datus arī pēc darba tiesisko attiecību izbeigšanas.

4.27. Darbiniekam pienākums ir lietot nepieciešamos tehniskos un organizatoriskos līdzekļus, lai aizsargātu personas datus un novērstu to pretlikumīgu apstrādi.

4.28. Noteikumos noteikto daru apstrādes pamatprincipu pārkāpšana, tai skaitā, jebkādā veidā iegūto personas datu neatļauta izpaušana, ir uzskatāma par Sabiedrības iekšējās kārtības noteikumu pārkāpumu.

5. PERSONAS DATU APSTRĀDE INFORMĀCIJAS RESURSOS

5.1. Informācijas sistēmās personas datu apstrādes loģisko drošību nodrošina Sabiedrības valdes loceklis, organizējot drošības iestatījumus tā, lai iespējamie riski tiktu novērsti pirms to iestāšanās.

5.2. Personas datu aizsardzību informācijas nesējos īsteno ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret drošības incidentu radītu personas datu apdraudējumu.

5.3. Personas datu apstrādes sistēmas datortehnikas un programmatūras tehniskā uzstādīšana un tās administrēšana tiek nodrošināta atbilstoši Sabiedrības IT drošības noteikumiem un Sabiedrības IT lietošanas noteikumiem.

5.4. Piekļuve informācijas resursiem tiek ierobežota ar paroli:

1) parole veidojama no vismaz astoņiem simboliem, starp kuriem ir vismaz viens latīņu alfabēta mazais burts, vismaz viens latīņu alfabēta lielais burts un vismaz viens cipars;

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

3) paroli ieteicams mainīt ne retāk kā reizi trijos mēnešos;

4) 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;

5) attālināta piekļuve informācijas resursiem caur internetu tiek aizsargāta ar lokālā tīkla maršrutētāju, kam ir ugunsmūra funkcija.

5.5. Datorizētās informācijas sistēmām tiek nodrošināta autentifikācija atbilstoši Sabiedrības IT drošības noteikumiem.

5.6. Apstrādājot personas datus informācijas sistēmā, tiek nodrošināta tikai atbilstošo darbinieku piekļūšana pie tehniskajiem līdzekļiem un informācijas.

5.7. Pārzinis personas datu saturošas programmatūras apstrādei lieto šādas ierīces:

1) darbstacijas un portatīvās iekārtas ar operētājsistēmu;
2) citas licencētas iekārtas un programmatūru pēc vajadzības.

5.8. Darbinieks ir atbildīga par datortehniku, kas nodota tās rīcībā, kā arī par dokumentiem, kas nepieciešami personas darba pienākumu pildīšanai.

5.9. Personas datu apstrādāto informācijas resursu uzglabāšana notiek atbilstoši Sabiedrības lietu nomenklatūrai. Par kuras aktualitāti atbilst Sabiedrības valdes loceklis.

5.10. Darbiniekam ir tiesības izmantot lietošanā nodotos datorus un to programmatūru tikai darba vajadzībām.

5.11. Darbinieks nedrīkst izpaust ziņas par Sabiedrības 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 datu pieprasītāju un datu subjektu, kā arī pieprasāmo personas datu apjomu. Jebkura informācijas sniegšana iepriekš saskaņojama ar Sabiedrības valdes locekli.

5.12. Darbiniekam ir aizliegts izmantot nelicencētu programmatūru.

5.13. Darbinieks nedrīkst izdarīt darbības, kas būtu vērstas pret informācijas sistēmas drošību, izmantojot neparedzētas pieslēgšanās iespējas.

5.14. Beidzot (pārtraucot) darbu ar informācijas sistēmu, darbinieks aizver pārlūkprogrammu.

5.15. Darbinieks 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.

5.16. Ja ir aizdomas par tīšiem bojājumiem, kas ir radušies informācijas sistēmai paroles publiskošanas rezultātā vai citu iemeslu dēļ, pilnvarotā persona par to nekavējoties ziņo Sabiedrības valdes loceklim.

5.17. Videonovērošana Sabiedrības telpās tiek veikta reālā laika režīmā un ieraksti tiek uzglabāti ne vairāk kā 30 dienas.

5.18. Pie ieejas Sabiedrības ēkās, kur notiek videonovērošana, tiek izvietota brīdinājuma zīme, kuras paraugs pievienots šiem noteikumiem kā pielikums Nr.2.

5.19. Videonovērošanas dati klasificējami kā ierobežotas piekļuves informācija, kurai drīkst piekļūt tikai pilnvaroti darbinieki.

5.20. Par datu dzēšanu no sistēmas (tajā skaitā – rezerves kopijām) pēc minētā termiņa beigām ir atbildīgs informācijas resursu turētājs.

5.21. Videonovērošanas datus nedrīkst kopēt ārējos datu nesējos (CD, DVD, USB diskos, zibatmiņas ierīcēs u.tml.), izņemot gadījumus, kad tas nepieciešams rezerves kopiju nodrošināšanai.

5.22. Videonovērošanas datu rezerves kopijām jānodrošina tāds pats drošības un aizsardzības

līmenis kā pašai videonovērošanas sistēmai atbilstoši šiem noteikumiem.

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

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.);

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

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

6. DATU SUBJEKTA TIESĪBAS

6.1. Datu subjektam ir tiesības iegūt visu informāciju, kas par viņu savākta Sabiedrībā personu datu apstrādes sistēmā, iesniedzot iesniegumu Sabiedrības valdes loceklim, 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, iesniedzot iesniegumu Sabiedrības valdes loceklim.

6.3. Datu subjektam ir tiesības pieprasīt arī šādu informāciju:

1) pārziņa nosaukums, adrese;
2) personas datu apstrādes mērķis, apjoms, veids;
3) datums, kad klienta personas datos pēdējo reizi ir izdarīti labojumi, dati dzēsti vai bloķēti;
4) personas datu ieguves avots;
5) automatizētajā apstrādes sistēmā izmantotās apstrādes metodes, par kuru piemērošanu tiek pieņemti individuāli automatizēti lēmumi.

6.4. Datu subjektam ir tiesības pieprasīt, lai viņa personas datus papildina vai izlabo, kā arī pārtrauc to apstrādi vai iznīcina tos, ja personas dati ir nepilnīgi, novecojoši, pretlikumīgi apstrādāti vai arī tie vairs nav nepieciešami vākšanas mērķim. Datu subjektam minētā prasība ir jāpamato. Ja šāda prasība izrādās pamatota, tad Sabiedrība ir pienākums nekavējoties novērst šo nepilnību vai pārkāpumu un par to paziņot trešajām personām, kas iepriekš ir saņēmušas apstrādātos datus.

6.5. Datu subjekta pieprasījums ir jāizskata un ir jāizsniedz rakstveida pamatota atbilde viena mēneša laikā no attiecīgā pieprasījuma iesniegšanas dienas.

6.6. Datu subjektam ir tiesības iepriekš norādīto informāciju bez maksas saņemt divas reizes gadā, iesniedzot iesniegumu.

7. PERSONAS DATU APSTRĀDES AIZSARDZĪBAS PĀRKĀPUMI

7.1. "Personas datu aizsardzības 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.

7.2. Paziņojumā apraksta personas datu aizsardzības pārkāpuma raksturu, tostarp, ja iespējams, attiecīgo datu subjektu kategorijas un aptuveno skaitu un attiecīgo personas datu ierakstu kategorijas un aptuveno skaitu; datu aizsardzības speciālista vārds un uzvārds un kontaktinformācija vai norādījumi uz citu kontaktpunktu, kur var iegūt papildu informāciju; apraksts par personas datu aizsardzības pārkāpuma iespējamām sekām; darbības vai pasākumi, ko pārzinis veicis vai ierosinājis veikt, lai novērstu personas datu aizsardzības pārkāpumu, tostarp attiecīgā gadījumā – pasākumus, lai mazinātu tā iespējamās nelabvēlīgās sekas.

7.3. Personas datu apstrādes aizsardzības pārkāpuma paziņojumu Datu valsts inspekcijai iesniedz Pārzinis.

7.4. Personas datu aizsardzības pārkāpuma gadījumā datu pārzinis bez nepamatotas kavēšanās un, ja

iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms iesniedz Personas datu apstrādes aizsardzības pārkāpuma paziņojumu.

7.5. Datu pārzinis var neiesniegt Paziņojumu gadījumos, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām.

7.6. Ja un ciktāl informāciju nav iespējams sniegt vienlaikus, informāciju var sniegt pa posmiem bez turpmākas nepamatotas kavēšanās. Ja paziņošana Datu valsts inspekcijai nav notikusi 72 stundu laikā, paziņojumam pievieno kavēšanās iemeslus.

7.7. Aizpildītu Paziņojuma formu var iesniegt elektroniski parakstītu nosūtot uz Datu valsts inspekcijas oficiālo e-pasta adresi info@dvi.gov.lv ar norādi "Paziņojums par personas datu aizsardzības pārkāpumu", ierakstītā sūtījumā vai personīgi Datu valsts inspekcijā, kā arī veicot autorizāciju valsts pārvaldes pakalpojumu portālā www.latvija.lv

Direktore Laura Lika

A.Puste
28358776