SIA "DLV"

PERSONAS DATU APSTRĀDES UN AIZSARDZĪBAS NOTEIKUMI

Saturs

1. Noteikumu mērķis un termini **3**

2. Vispārīga informācija (Datu subjekti, apstrādāto Personu datu kategorijas (arī Īpašās Personas datu kategorijas) un veidi, Personas datu apstrādes mērķi, avoti, tiesiskais pamats, Profilēšana, Personas datu izpaušana, Personas datu glabāšana, Personas datu apstrādes ģeogrāfiskā teritorija, glabāšanas periods) **8**

3. Informācijas resursi, tehniskie resursi un par Personas datu aizsardzību atbildīgās personas, to tiesības un pienākumi **17**

4. Personas datu aizsardzības klasifikācija atbilstoši to Vērtības un Konfidencialitātes pakāpei **18**

5. Tehniksie resursi, ar kādiem tiek nodrošināta Personas datu apstrāde **18**

6. Personas datu apstrādes organizatoriskā procedūra **18**

7. Videonovērošana **19**

8. Datu subjekta (Darbinieka, Līgumslēdzēja, Klienta) tiesības **19**

9. Kārtība, kādā DLV nodrošina Datu subjektam garantētās tiesības un Personas datu drošības pasākumi **20**

10. Paroles uzbūve, tās lietošanas kārtība un piekļuve **23**

11. Pasākumi, kas veicami tehnisko resursu aizsardzībai pret ārkārtas apstākļiem, un līdzekļi, ar kādiem nodrošina tehniskos resursus pret tīšu bojāšanu un neatļautu iegūšanu **24**

12. Informācijas nesēju glabāšanas un iznīcināšanas kārtība **25**

13. Personas datu Lietotāju tiesības, pienākumi, ierobežojumi un atbildība **25**

14. Personas datu aizsardzības pārkāpumu procedūra **25**

Pielikums Nr.1 - Datu aizsardzības pārkāpumu reģistrācijas žurnāls .....

1. NOTEIKUMU MĒRĶIS UN TERMINI

Šo Personas datu apstrādes un aizsardzības noteikumu (turpmāk – **Noteikumi**) mērķis ir noteikt DLV:

- 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;

- veiktās Personas datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības, apstrādājot fizisko Personu datus un nodrošinot DLV Informācijas resursu un Informācijas sistēmu drošību;

- Personas datu aizsardzības pārkāpumu procedūru.

Šie Noteikumi ir izstrādāti saskaņā ar Regulas prasībām.

Šajā dokumentā tiek lietoti šādi termini:

Termins (saīsinājums)	**Definīcija**
Apdraudējums	Iemesli, kas var neļaut uzturēt Informācijas sistēmas drošību atbilstoši noteiktajām Informācijas resursu Konfidencialitātes, Pieejamības un Integritātes prasībām. Informācijas sistēmas drošības apdraudējums ir ar nodomu (tīši) vai aiz neuzmanības veikta darbība vai notikums, kas var izraisīt sistēmas bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kuru dēļ piekļūšana sistēmas Informācijas resursiem var būt traucēta vai neiespējama. Apdraudējumu iespējamību nosaka sistēmas ievainojamības.
Auditācijas pieraksti	Ieraksti Informācijas sistēmas atmiņā, kas izdarīti dažādās informācijas apstrādes procesa stadijās, lai šos ierakstus varētu vēlāk noteiktā secībā pārskatīt un izsekot aplūkojamā procesa norisi.
Augsti vērtīga informācija	Informācija, kuru lietojot nevietā, nesankcionēti mainot, sabojājot vai padarot nepieejamu pilnvarotām personām kādu laika periodu, var rasties nozīmīgi un ilgstoši zaudējumi, ciest DLV reputācija un izdarīts Personas datu aizsardzības pārkāpums.
Autentiskums	Īpašība, kas nodrošina, ka priekšmeta vai resursa identitāte ir tāda, kā tiek apgalvots.
Biometriskie dati	Personas dati, kas attiecas uz personas fiziskajām vai uzvedības pazīmēm, kas ļauj unikāli identificēt šo personu, piemēram, sejas attēli vai pirkstu nospiedumu dati.
Core HR Data	Darbinieka vārds, uzvārds, personas kods, dzimšanas datums, dzimums, fotogrāfija (caurlaides izgatavošanai), dzīvesvietas adrese, tālrunis, e-pasta adrese, norēķina konta numurs, personāla lieta (ieskaitot, darba pieteikuma informācija (CV; valsts valodas apliecības, izglītības dokumentu dati; atsauces), darba līgums, Obligātās veselības pārbaudes karte, darba vides risku novērtējums Darbinieka darba vietā, funkcija, apmācības, darbības novērtējumi, paaugstinājumi amatā, uzvedības un disciplīnas dati), departamentu / uzņēmējdarbības vienības, darba vietas dati, algas informācija, informācija par slimības datiem un pensionēšanās datiem (VID), nodokļu un sociālās apdrošināšanas dati, transportlīdzekļa numura zīmes detaļas, dati par Darbinieka bērnu vecumu (Darbinieka bērnu dzimšanas apliecības numurs un izsniegšanas datums papildatvaļinājumu piešķiršanai), dati par invaliditāti (papildatvaļinājumu piešķiršanai), atsevišķos gadījumos Personas dati darba atļaujas (uzturēšanās

	atļaujas kopija, trešās valsts Darbinieka pases dati) vai vīzu noformēšanai, viesnīcu rezervācijām, lēmuma/laulības reģistrācijas apliecības dati (uzvārda maiņas gadījumā)
Darbinieks	Esošie (~400), bijušie DLV darbinieki un darba pretendenti
Datu analīze	Dati tiek izmantoti veidā, kas analizē uzvedību un modeļus, un ļauj izdarīt secinājumus katrā gadījumā, lai uzlabotu produktivitāti, konkurētspēju un / vai peļņu.
Datu Apstrādātājs	Termins "Datu Apstrādātājs" atbilst Regulas 4. panta 8. punktā noteiktajai definīcijai. Sabiedrība, kas apstrādā Personas datus Datu Pārziņa vārdā. Ja sabiedrība glabā vai apstrādā Personas datus, bet nepārzina (nekontrolē) Personas datus un apstrādā Personas datus, kas ir balstīti saskaņā ar Datu Pārziņa norādījumiem, tad šī sabiedrība ir "Datu Apstrādātājs". Datu apstrādes procesā var ietilpt pakalpojumu sniedzēji (piemēram, algu sarakstu pakalpojumu sniedzējs, IT pakalpojumu sniedzējs).
Datu Pārzinis	Termins "Datu Pārzinis" atbilst Regulas 4. panta 7. punktā noteiktajai definīcijai. Sabiedrība, kas izlemj, kāpēc un kādā veidā (t.i., izlemj mērķus un līdzekļus, ar kuru palīdzību) tiek apstrādāti Personas dati. Lemjot, kurš pārzina Personas datus, nepieciešams atbildēt uz šādiem jautājumiem: - kurš izlemj, kāda informācija tiks uzglabāta? - kurš lemj par informācijas izmantošanu un mērķiem? - kurš lemj par Personas datu apstrādes līdzekļiem? Ja sabiedrība pārzina un ir atbildīga par tās rīcībā esošajiem Personas datiem, tā ir Datu Pārzinis.
DLV	SIA "DLV" - juridiska persona ar vienoto reģistrācijas Nr.40003227719, juridiskā adrese: Krīdenera dambis 9, Rīga, LV-1019 (tai piederošas interneta vietne: www.dlvbet.lv; DLV spēļu zāles: "Zilais Dimants", "Dimats Z" un "Dimanta Bingo"), kura rīkojas Personas datu Pārziņa statusā. Saraksts, kurā ir uzskaitītas DLV pakalpojumu sniegšanas vietas, ir pieejams tīmekļa vietnē www.dlvbet.lv.
Draudi	Jebkurš notikums, kura dēļ DLV var rasties zaudējumi. Draudi var būt visdažādākie – dažādas katastrofas, terorisms, budžeta finansējuma zaudējums, komunikāciju bojājumi, datu bojājumi, kļūdas, darbinieku prettiesiska vai ļaunprātīga darbība (arī bezdarbība) un citi.
Fiziskā aizsardzība	Informācijas resursu aizsardzība pret fiziskas iedarbības radītu informācijas nesēju Apdraudējumu (piemēram zādzība, sprieguma pazemināšanās, aparatūras bojājumi u.c.).
Ierobežotas pieejamības informācija	Iekšējās aprites informācija, kurai Informācijas resursu turētājs ir noteicis pieejas personu loku.
Ietekme	Informācijas drošības Incidenta rezultāts.
Ievainojamība	Informācijas sistēmas Nepilnība, kas ļauj kādam noteiktam Apdraudējumam īstenoties un ietekmēt sistēmas drošību.
Incidents	Gadījums, kurā Informācijas sistēmas Apdraudējumi ir negatīvi ietekmējuši Informācijas sistēmas darbību, izmantojot tās trūkumus.
Informācijas resursi, informācija	Datu faili, datu bāzes, arhīvi u.c. informācija (neatkarīgi no datu nesēja veida).

Informācijas resursu turētājs	Persona, kura ir atbildīga par Informācijas resursiem (to Pieejamību, Integritāti, Konfidencialitāti, lietošanu un lietošanas sekām) un kura pienākumi ir noteikti DLV normatīvos.
Informācijas sistēma/-as	Datu ievadīšanas, uzglabāšanas un apstrādes datorizēta sistēma, kas paredz Lietotāju pieeju tajā glabātajiem datiem vai informācijai, vai jebkādā formā fiksēta strukturizēta Personas datu kopa, kas ir pieejama, ievērojot attiecīgus personu identificējošus kritērijus.
Informācijas sistēmas administrators	Persona, kas plāno, vada un pārvalda sistēmas izmantošanu un kas ir atbildīga par tās funkcionēšanu.
Integritāte	Raksturo, cik lielā mērā informācija tiek uzglabāta un/vai pārraidīta pilnīga, precīza, patiesa un aktuāla.
Īpašās Personas datu kategorijas	Regulas 9. pantā noteiktie Personas datu veidi, kas atklāj kādu no tālāk norādītajām ziņām par personu: rasi vai etnisko izcelsmi, politiskos uzskatus, reliģiskos vai filozofiskos uzskatus vai dalību arodbiedrībās. Personas datu īpašās kategorijas attiecas arī uz ģenētiskiem datiem, biometriskiem datiem (piemēram, pirkstu nospiedumiem vai sejas attēliem), veselības datiem, datiem par seksuālo dzīvi vai seksuālo orientāciju, kā arī jebkādiem Personas datiem, kas attiecas uz notiesājošiem spriedumiem vai noziedzīgiem nodarījumiem.
Klasificēšana	Konfidencialitātes, Pieejamības un Vērtības līmeņa piešķiršana.
Klients	a) jebkura fiziska persona, kura izmanto, ir izmantojusi, vai ir izteikusi vēlēšanos izmantot jebkurus DLV sniegtos pakalpojumus vai ir jebkādā citā veidā saistīta ar tiem (tajā skaitā Klienti azartspēļu zālēs, interaktīvo interneta azartspēļu Klienti, apmeklētāji); b) jebkura fiziska persona, kura darbojas juridiskās personas, piegādātāja vai cita DLV biznesa partnera uzdevumā un pārstāv šādu juridisku personu.
Konfidencialitāte	Īpašība, ka informācija nav pieejama vai netiek atklāta nepilnvarotiem indivīdiem, sistēmām vai procesiem.
Leģitīmās intereses	Rodas, ja Personas datu apstrāde ir nepieciešama Datu Pārziņa vai Trešās personas Leģitīmo interešu nolūkos, izņemot gadījumus, kad Datu subjekta intereses vai pamattiesības un pamatbrīvības ir svarīgākas par šādām Leģitīmām interesēm. Leģitīmo interešu piemēri ir Personas datu apstrāde pētniecības nolūkos vai noziedzīgu nodarījumu novēršanai.
Lietotājs	Juridiskā vai fiziskā persona, kura noslēgusi līgumu ar DLV par datu lietošanu (t.sk. Darbinieki) vai kura uz pieprasījuma pamata saņem DLV vai normatīvajos aktos noteiktajā kārtībā.
Loģiskā aizsardzība	Datu vai Informācijas resursu aizsardzība, kuru realizē ar programmatūras līdzekļiem, piemēram, identificējot Informācijas sistēmas Lietotāju, pārbaudot viņa pilnvaru atbilstību attiecīgajām darbībām IS, pasargājot informāciju no tīšas vai nejaušas maiņas vai dzēšanas.
Līgumslēdzēji	Fiziskas personas (t.i., nevis sabiedrības), kas sniedz / ir snieguši DLV pakalpojumus, bet ne saskaņā ar darba līgumu.
Nepilnība	Raksturo sistēmas ievainojamības pakāpi, realizējoties konkrētam Draudam, piemēram, vāja administratīvā sistēma, nav precīzi definēti pienākumi, atbildība, netiek veikta piekļuves kontrole vai tā ir nepilnīga (gan fiziskā piekļuve, gan loģiskā), nav Informācijas sistēmas drošības noteikumu u. c.

Personas dati	Termins “Personas dati” atbilst Regulas 4. panta 1. punktā noteiktajai definīcijai. Jebkura informācija par dzīvu fizisku personu, kas tieši vai netieši ļauj identificēt šo personu. Personas dati var ietvert vārdu, uzvārdu, personas kodu, tiešsaistes identifikatoru, informāciju par personas atrašanās vietu vai jebkuru citu informāciju, kas ir raksturīga šai personai, un, kas ļautu personu identificēt, vai padara personu identificējamu. Regula attiecas gan uz automatizētiem Personas datiem, gan uz manuālajām datu reģistrēšanas sistēmām, kurās Personas dati ir pieejami saskaņā ar konkrētiem kritērijiem. Tās var ietvert hronoloģiski sakārtotus manuālo ierakstu saraktus, kas satur Personas datus. Personas dati, kas ir pseidonīmi - piem. ar paroli kodēti dati - var ietilpt Regulas darbības jomā atkarībā no tā, cik grūti ir piešķirt pseidonīmu konkrētai personai.
Personas datu apstrāde	Termins “Personas datu apstrāde” atbilst Regulas 4. panta 2. punktā noteiktajai definīcijai. Jebkura darbība vai darbību kopums, kas tiek veikts ar Personas datiem, piemēram, jebkāda veida Personas datu vākšana, izmantošana, reģistrēšana, organizēšana, pārveidošana, izpaušana, iznīcināšana, glabāšana vai jebkāda citāda Personas datu padarīšana par pieejamiem. Apstrāde var veikt vai nu manuāli, vai arī izmantojot automatizētas sistēmas, piemēram, informācijas tehnoloģiju sistēmas (attiecīgi jāinterpretē "apstrādāt" un "apstrāde").
Personas datu aizsardzības pārkāpums (turpmāk – Pārkāpums)	Termins “Personas datu aizsardzības pārkāpums” atbilst Regulas 4. panta 12. punktā noteiktajai definīcijai. Drošības pārkāpums, kurā rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto Personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.
Pieejamība	Raksturo, cik lielā mērā pilnvarotās personas var piekļūt nepieciešamajai informācijai ne vēlāk kā noteiktā laikā pēc Informācijas pieprasīšanas brīža.
Profilēšana	Termins “Profilēšana” atbilst Regulas 4. panta 4. punktā noteiktajai definīcijai. Automatizēta Personas datu apstrāde, lai novērtētu konkrētus ar fizisku personu saistītus personiskus aspektus, lai analizētu vai paredzētu personas sniegumu, lēmumus, vēlmes, attieksmi un / vai uzvedību (un attiecīgi jāinterpretē "Profils").
Regula	Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz Personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)
Risks (risks)	DLV varbūtēja nespēja pilnvērtīgi un kvalitatīvi veikt kādu savu saistību vai funkciju izpildi. Informācijas drošības kontekstā tiek aplūkoti tikai tie riski, kas ir saistīti ar Informācijas sistēmas funkcionēšanu.
Tehnoloģiskie resursi	Programmatūra (izpildāms programmas kods un konfigurācijas faili, kas nodrošina Informācijas sistēmas funkcionēšanu), datori, datortīklu aparatūra, komunikāciju līnijas u.c. tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei un glabāšanai.
Tehnoloģisko resursu turētājs	Persona, kura ir atbildīga par Tehnoloģisko resursu uzturēšanu un drošību.
Trešā persona	Jebkura persona vai sabiedrība, aģentūra vai cita organizācija (kas nav datu subjekts, Datu Pārzinis vai Datu Apstrādātājs), kas Datu Pārziņa vai Datu Apstrādātāja tiešā pakļautībā ir pilnvarota apstrādāt Personas datus.

Vērtība	Informācijas resursa nozīmīgums DLV, ko nosaka, izvērtējot iespējamos zaudējumus, kurus var radīt Informācijas zaudēšana, sabojāšana vai nonākšana nepiederošu personu rokās.
Vidēji vērtīga informācija	Informācija, kuru lietojot nevietā, nesankcionēti mainot, sabojājot vai padarot nepieejamu pilnvarotām personām kādu laika periodu, DLV var rasties jūtami zaudējumi, ciest DLV reputācija un izdarīts personas datu aizsardzības pārkāpums.
Vispārpieejamā informācija	Informācija, kas ir brīvi pieejama visiem DLV Darbiniekiem un jebkurai citai personai, kas šo informāciju ir pieprasījusi.
Zema riska informācija	Informācija, kuru lietojot nevietā, nesankcionēti mainot, sabojājot vai padarot nepieejamu pilnvarotām personām kādu laika periodu, DLV nerodas nopietni zaudējumi vai būtiski darbības traucējumi.

2. VISPĀRĪGA INFORMĀCIJA

Datu subjekti, apstrādāto Personu datu kategorijas (arī Īpašās Personas datu kategorijas) un veidi, Personas datu apstrādes mērķi, avoti, tiesiskais pamats, Profilēšana, Personas datu izpaušana, Personas datu glabāšana, Personas datu apstrādes ģeogrāfiskā teritorija, glabāšanas periods.

Datu subjekti:	**Darbinieki**	**Līgumslēdzēji**	**Klienti**
Apstrādāto Personu datu kategorijas, arī Īpašās Personas datu kategorijas, un veidi	- Attiecībā uz esošajiem Darbiniekiem Core HR Data, e-pasta sarakste, attēls (videonovērošana), attiecībā uz Darbiniekiem administratoriem – dati par sodāmību. - Attiecībā uz bijušajiem Darbiniekiem Core HR Data (bijušie Darbinieki var pieprasīt izziņa, raksturojumus u.tml.), e-pasta sarakste, attēls (videonovērošana) mazākā apjomā, neglabājot informāciju par slimības datiem un pensionēšanās datiem (VID). - Attiecībā uz darba pretendentiem: vārds, uzvārds, adrese, tālruņa numurs, CV, atsauces no iepriekšējiem darba devējiem un darba pretendentu intervēšanas piezīmes. **Īpašās Personas datu kategorijas:** - **dati par veselību** (Obligātās veselības pārbaudes, kā arī, lai veiktu nelaimes gadījuma darbā izmeklēšanu (no ārstniecības iestādes pieprasa šo izziņu par cietušā (Darbinieka) veselības traucējumu smaguma pakāpi)); - informācija par satiksmes noteikumu	Vārds, uzvārds, personas kods, adrese, tālruņa numurs, e-pasta adrese, PVN numurs, līgums, ja Līgumslēdzējs darbojas vietās, kur DLV veic videonovērošana, arī Līgumslēdzēja attēls **Īpašās Personas datu kategorijas**: netiek apstrādātas	**Identifikācijas dati**, piemēram: vārds, uzvārds, personas kods, dzimšanas datums, dzimums, fotogrāfija, personu apliecinoša dokumenta dati (piemēram: pases dati, ID kartes dati). **Kontaktinformācija**, piemēram: deklarētā un faktiskā dzīvesvietas adrese, tālruņa numurs, e-pasta adrese. **Finanšu dati**, piemēram:Klienta bankas kredītkartes informācija, lai iemaksātu naudas summu likmju izdarīšanai; Klienta konta numurs, uz kuru laimesta gadījumā tiks izmaksāts laimests. **Dati, kas iegūti un/vai radīti, pildot normatīvajos aktos paredzētus pienākumus**, piemēram: dati, kas izriet no informācijas pieprasījumiem, kas saņemti no izmeklēšanas iestādēm, zvērinātiem notāriem, nodokļu administrācijas iestādēm, tiesām un zvērinātiem tiesu izpildītājiem. **Saziņas dati**, kas tiek vākti, kad Klients apmeklē DLV spēļu zāles un tīmekļa vietnes, kur DLV sniedz pakalpojumus, vai sazinās ar DLV telefoniski, e-pasta

	pārkāpumiem; - dalība arodbiedrību organizācijās/darbinieku arodbiedrībās (darba līguma uzteikuma gadījumā). Attiecībā uz darba pretendentiem Īpašās Personas datu kategorijas netiek apstrādātas.		sarakste, ziņas un citi saziņas līdzekļi, piemēram: sociālie mediji, dati, kas iegūti, Klientam apmeklējot DLV tīmekļa vietnes vai sazinoties citos DLV kanālos, kā arī **vizuālie un/vai audioieraksti** (Klienta attēls, veicot videonovērošanu). **Ar pakalpojumiem saistītie dati**, piemēram: saņemtie pakalpojumi, izmaksātie laimesti, iesniegtie pieteikumi, pieprasījumi un sūdzības.
Apstrādes mērķi	Nodokļu un maksājumu nolūkos; vadības funkciju izpildei (biznesa stratēģija, mārketinga un reklāmas nolūki); noziedzīgu nodarījumu novēršanai vai atklāšanai saistībā ar DVL īpašumā vai lietošanā esošā īpašuma aizsardzību un, lai aizsargātu Darbinieka kā datu subjekta vitāli svarīgas intereses, tajā skaitā dzīvību un veselību; DLV Leģitīmo interešu ievērošanai (Klientu apkalpošanas un/vai pakalpojumu sniegšanas kvalitātes uzraudzības un pilnveidošanas nolūkos; produktivitātes novērtēšanai, veicināšanai; pierādījumu nodrošināšanai pret prasījumiem par pakalpojuma neatbilstību un/vai līgumsaistību izpildi, kā arī pierādījumu nodrošināšanai pret iespējamo prasījumu, kas izriet no delikta); ar DLV mājaslapu saistītiem mērķiem (piemēram, norādot Darbinieka	Nodokļu un maksājumu nolūkos; vadības funkciju izpildei (biznesa stratēģija, mārketinga un reklāmas nolūki); noziedzīgu nodarījumu novēršanai vai atklāšanai saistībā ar DVL īpašumā vai lietošanā esošā īpašuma aizsardzību un, lai aizsargātu Līgumslēdzēja kā datu subjekta vitāli svarīgas intereses, tajā skaitā dzīvību un veselību; lai nodrošinātu DLV kā Datu Pārziņa likumā noteikto pienākumu veikšanu un piemērojamo normatīvo tiesību aktu prasību izpildi; lai sankcionētu un kontrolētu piekļuvi digitālajiem kanāliem un to darbību, novērstu nesankcionētu piekļuvi un to negodprātīgu izmantošanu, un, lai nodrošinātu informācijas drošību, pamatojoties uz līguma izpildi vai, lai izpildītu juridisku pienākumu vai saskaņā ar Līgumslēdzēja piekrišanu vai DLV	**Juridisko pienākumu izpildei un Klienta identitātes pārbaudei:** lai pildītu piemērojamos likumus un normatīvos aktus (tajā skaitā, bet ne tikai DLV ir pienākums pārliecināties par kazino, spēļu zāles vai bingo zāles apmeklētāju vecumu, nepieļaut nepilngadīgu personu dalību interaktīvajās azartspēlēs vai interaktīvajās izlozēs un novērst no interaktīvajām azartspēlēm atkarīgo spēlētāju turpmāku dalību azartspēlēs (saskaņā ar personas iesniegumu, lai viņu neielaistu spēļu zālēs), tāpat DLV ir pienākums normatīvajos aktos noteiktajā kārtībā un apmērā samaksāt par laimestiem iedzīvotāju ienākuma nodokli (IIN); tāpat DLV ir pienākums normatīvajos aktos noteiktajā kārtībā (Azartspēļu un izložu likumā 36. panta trešā daļa) izmaksāt spēlētājam laimestu; tāpat DLV ir pienākums normatīvajos aktos noteiktajā kārtībā veikt

	kontaktinformāciju); lai nodrošinātu DLV kā Datu Pārziņa likumā noteikto pienākumu veikšanu un piemērojamo normatīvo tiesību aktu prasību izpildi; lai sankcionētu un kontrolētu piekļuvi digitālajiem kanāliem un to darbību, novērstu nesankcionētu piekļuvi un to negodprātīgu izmantošanu, un, lai nodrošinātu informācijas drošību, pamatojoties uz līguma izpildi vai, lai izpildītu juridisku pienākumu vai saskaņā ar Darbinieka piekrišanu vai DLV leģitīmajās interesēs kontrolētu DLV digitālo pakalpojumu autorizāciju, piekļuvi un darbību; lai pilnveidotu tehniskās sistēmas, IT infrastruktūru, pielāgotu pakalpojuma attēlošanu ierīcēs un attīstītu DLV pakalpojumus, piemēram: testējot un pilnveidojot tehniskās sistēmas un IT infrastruktūru, pamatojoties uz DLV leģitīmajām interesēm pilnveidot tehniskās sistēmas un IT infrastruktūru; prasījuma tiesību nodibināšanai, īstenošanai un aizstāvībai: lai nodibinātu, īstenotu, aizstāvētu un cedētu prasījuma tiesības, vai, lai izpildītu juridisku pienākumu, vai DLV leģitīmajās interesēs īstenotu prasījuma tiesības.	leģitīmajās interesēs kontrolētu DLV digitālo pakalpojumu autorizāciju, piekļuvi un darbību; lai pilnveidotu tehniskās sistēmas, IT infrastruktūru, pielāgotu pakalpojuma attēlošanu ierīcēs un attīstītu DLV pakalpojumus, piemēram: testējot un pilnveidojot tehniskās sistēmas un IT infrastruktūru, pamatojoties uz DLV leģitīmajām interesēm pilnveidot tehniskās sistēmas un IT infrastruktūru; prasījuma tiesību nodibināšanai, īstenošanai un aizstāvībai: lai nodibinātu, īstenotu, aizstāvētu un cedētu prasījuma tiesības, vai, lai izpildītu juridisku pienākumu, vai DLV leģitīmajās interesēs īstenotu prasījuma tiesības.	Klientu izpēti, lai sniegtu ziņas kompetentajām iestādēm, lai novērstu, atklātu, izmeklētu un ziņotu par iespējamu noziedzīgi iegūtu līdzekļu legalizēšanu, terorisma finansēšanu, ja Klients ir pakļauts finanšu sankcijām vai ir politiski nozīmīga persona), vai, lai DLV leģitīmajās interesēs nodrošinātu pārdomātu riska vadību un uzņēmuma pārvaldību. **Vispārīgai Klientu attiecību vadīšanai un pieejas pakalpojumiem nodrošināšanai un administrēšanai:** lai sniegtu pakalpojumu, lai nodrošinātu datu aktualitāti un pareizību, pārbaudot un papildinot datus, izmantojot ārējos vai iekšējos avotus, pamatojoties uz pakalpojuma izpildi vai, lai izpildītu juridisku pienākumu. **Klienta un/vai DLV interešu aizsardzībai:** lai aizsargātu Klienta un/vai DLV intereses un pārzinātu DLV sniegto pakalpojumu kvalitāti un, lai sniegtu pierādījumus, balstoties uz pakalpojuma izpildi vai, lai izpildītu juridisku pienākumu, vai Klienta piekrišanu, vai DLV leģitīmajās interesēs novērstu, ierobežotu un izmeklētu DLV pakalpojumu un produktu negodprātīgu vai prettiesisku izmantošanu vai traucējumu radīšanu tajos, iekšējai apmācībai vai pakalpojumu kvalitātes nodrošināšanai. Lai garantētu DLV un/vai Klienta drošību,

			aizsargātu Klienta dzīvību un veselību un citas DLV un Klienta tiesības, pamatojoties uz DLV leģitīmajām interesēm aizsargāt savus Klientus, un Klientu un DLV aktīvus. **Pakalpojumu negodprātīgas izmantošanas novēršanai un pakalpojumu pienācīgai nodrošināšanai**: lai sankcionētu un kontrolētu piekļuvi digitālajiem kanāliem un to darbību, novērstu nesankcionētu piekļuvi un to negodprātīgu izmantošanu, un, lai nodrošinātu informācijas drošību, pamatojoties uz līguma izpildi vai, lai izpildītu juridisku pienākumu vai saskaņā ar Klienta piekrišanu vai DLV leģitīmajās interesēs kontrolētu DLV digitālo pakalpojumu autorizāciju, piekļuvi un darbību. Lai pilnveidotu tehniskās sistēmas, IT infrastruktūru, pielāgotu pakalpojuma attēlošanu ierīcēs un attīstītu DLV pakalpojumus, piemēram: testējot un pilnveidojot tehniskās sistēmas un IT infrastruktūru, pamatojoties uz DLV leģitīmajām interesēm pilnveidot tehniskās sistēmas un IT infrastruktūru. **Prasījuma tiesību nodibināšanai, īstenošanai un aizstāvībai:** lai nodibinātu, īstenotu, aizstāvētu un cedētu prasījuma tiesības, vai, lai izpildītu juridisku pienākumu, vai DLV

			leģitīmajās interesēs īstenotu prasījuma tiesības.
Avoti	Darbinieka Personas dati var tikt vākti tieši no Darbinieka, no darba līguma attiecībām, kā arī no ārējiem avotiem, piemēram, nodarbinātības aģentūrām, darbinieku atlases uzņēmumiem, darbu sludinājumu portāliem, VID, publiskajiem reģistriem un publiski pieejamas informācijas.	Līgumslēdzēja Personas dati var tikt vākti tieši no Līgumslēdzēja, no līguma attiecībām, kā arī no ārējiem avotiem, piemēram, publiskajiem reģistriem un publiski pieejamas informācijas.	Klienta Personas dati var tikt vākti tieši no Klienta, no Klienta pakalpojumu izmantošanas un no ārējiem avotiem, piemēram, publiskajiem reģistriem un publiski pieejamas informācijas.
Tiesiskais pamats	- Darba līguma noslēgšanai un izpildei; - DLV juridisko pienākumu izpildei atbilstoši normatīvo aktu prasībām, kas nosaka darba devēja pienākumus saistībā ar Darbiniekiem (Darba likums, 2009. gada 25. augusta Ministru kabineta noteikumi Nr.950 "Nelaimes gadījumu darbā izmeklēšanas un uzskaites kārtība", likumi, kas nosaka valsts sociālo apdrošināšanu, grāmatvedības kārtošanu u.c.); - DLV Leģitīmo interešu nodrošināšanai; saskaņā ar Darbinieka piekrišanu.	- Līguma izpildei; - DLV juridisko pienākumu izpildei atbilstoši normatīvo aktu prasībām, (likumi, kas nosaka grāmatvedības kārtošanu u.c.); - DLV Leģitīmo interešu nodrošināšanai; - saskaņā ar Līgumslēdzēja piekrišanu.	- Līguma (pakalpojuma) izpildei; - DLV juridisko pienākumu izpildei atbilstoši Azartspēļu un izložu normatīvajiem aktiem (Azartspēļu un izložu likums un Ministru kabineta noteikumi Nr. 715 "Interaktīvo azartspēļu un interaktīvo izložu spēlētāju reģistrācijas un identitātes pārbaudes kārtība"), Patērētāju tiesību aizsardzības likumam, Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likumam, likumam "Par grāmatvedību", likumam "Par iedzīvotāju ienākumu nodokli", likumam "Par nodokļiem un nodevām", likumam "Par izložu un azartspēļu nodevu un nodokli", Arhīvu likumam un citiem Latvijas Republikas normatīvajiem tiesību aktiem; - DLV Leģitīmo interešu nodrošināšanai; saskaņā ar Klienta

			piekrišanu.
Profilēšana, personalizēti piedāvājumi un automatizēta lēmumu pieņemšana	Netiek veikta	Netiek veikta	Lai izvērtētu noteiktas Klienta personīgās pazīmes, Klienta Datu analīzes veikšanai un konsultēšanai, tiešā mārketinga nolūkos, automatizētai lēmumu pieņemšanai, piemēram: riska vadībai, attālināti sniegto pakalpojumu nodrošināšanai, t.sk. pakalpojumu uzraudzībai, lai novērstu krāpšanu, un tā ir pamatota uz DLV leģitīmajām interesēm, juridisku pienākumu pildīšanu, pakalpojuma (līguma) izpildi vai Klienta piekrišanu. Lai uzlabotu Klienta digitālo pakalpojumu lietošanas pieredzi, piemēram, pielāgojot pakalpojumu attēlošanu izmantotajā ierīcē un, lai sagatavotu Klientam piemērotus piedāvājumus. Ja vien Klients nav ierobežojis tiešo mārketingu attiecībā uz sevi, DLV var veikt Personas datu apstrādi DLV pakalpojumu vispārīgu un personalizētu piedāvājumu sagatavošanai. Šāds mārketings var būt pamatots uz Klienta izmantotajiem pakalpojumiem un to, kā Klients izmanto pakalpojumus un to, kā Klients darbojas DLV digitālajos kanālos. Uz personalizētajiem piedāvājumiem un mārketingu balstītajai profilēšanai, kas tiek veikta saskaņā ar DLV leģitīmajām interesēm, DLV nodrošina, ka Klienti var izdarīt izvēli un izmantot ērtu rīku

			savu privātuma iestatījumu pārvaldīšanai. DLV var arī vākt statistikas datus par Klientu, t.sk. par raksturīgo uzvedību un dzīvesveida paradumiem, pamatojoties uz demogrāfiskajiem mājsaimniecības datiem. Statistikas dati segmentu/profilu izveidei var tikt iegūti arī no ārējiem avotiem un var tikt apvienoti ar DLV iekšējiem datiem.
Personas datu izpaušana	Darbinieka Personas dati tiek izpausti: - serveru nodrošinātājiem; - jebkuram auditoram, finanšu konsultantam, parādu piedzinējam, juriskonsultam, zvērinātam advokātam, zvērinātam notāram un/vai zvērinātam tiesu izpildītājam vai citam DLV apstiprinātam Personas datu apstrādātājam pēc DLV izvēles; - Darba vides risku novērtēšanai kompetentam speciālistam, jo jāizvērtē katra Darbinieka darba vieta; - pakalpojumu sniedzējiem par Darbinieku apmācībām (ugunsdrošības jomā u.tml.); - Izložu un azartspēļu uzraudzības inspekcijai, Valsts ieņēmumu dienestam un citām institūcijām (piemēram, tiesībsargājošajās iestādes un finanšu izmeklēšanas iestādes,	Līgumslēdzēja Personas dati tiek izpausti: - serveru nodrošinātājiem un citām trešajām personām, kas ir iesaistītas DLV sniegto pakalpojumu sniegšanā; - jebkuram auditoram, finanšu konsultantam, parādu piedzinējam, juriskonsultam, zvērinātam advokātam, zvērinātam notāram un/vai zvērinātam tiesu izpildītājam vai citam DLV apstiprinātam Personas datu apstrādātājam pēc DLV izvēles; - Izložu un azartspēļu uzraudzības inspekcijai, Valsts ieņēmumu dienestam un citām institūcijām (piemēram, tiesībsargājošajās iestādes un finanšu izmeklēšanas iestādes, tiesas, ārpustiesas strīdu risināšanas iestādes, bankrota vai maksātnespējas procesa administratori); - citām personām, kuras ir	Klienta Personas dati tiek izpausti: - serveru nodrošinātājiem un citām trešajām personām, kas ir iesaistītas DLV sniegto pakalpojumu sniegšanā**;** - jebkuram auditoram, finanšu konsultantam, parādu piedzinējam, juriskonsultam, zvērinātam advokātam, zvērinātam notāram un/vai zvērinātam tiesu izpildītājam vai citam DLV apstiprinātam Personas datu apstrādātājam pēc DLV izvēles; - Izložu un azartspēļu uzraudzības inspekcijai, Valsts ieņēmumu dienestam un citām institūcijām (piemēram, tiesībsargājošajās iestādes un finanšu izmeklēšanas iestādes, tiesas, ārpustiesas strīdu risināšanas iestādes, bankrota vai maksātnespējas procesa administratori); - atzītām tirgus un sabiedriskās domas

	tiesas, ārpustiesas strīdu risināšanas iestādes, bankrota vai maksātnespējas procesa administratori)' - citām personām, kuras ir saistītas ar DLV pakalpojumu sniegšanu, t.sk. arhivēšanas, pasta pakalpojumu sniedzēji u.tml.	saistītas ar DLV pakalpojumu sniegšanu, t.sk. arhivēšanas, pasta pakalpojumu sniedzēji u.tml.	izpētes kompānijām (ES robežās) - aptauju un pētījumu veikšanai saistībā ar DLV piedāvātajiem pakalpojumiem; - citām personām, kuras ir saistītas ar DLV pakalpojumu sniegšanu, t.sk. arhivēšanas, pasta pakalpojumu sniedzēji u.tml.
Personas datu glabāšana	Darba līgumi, darba apraksti, darba kārtības noteikumi, instrukcijas, citi dokumenti (valsts valodas prasmes apliecinājums, uzturēšanās atļaujas) glabājas papīra formātā birojā, mapēs, slēgtā skapī. Elektroniski noformētie darba līgumi glabājas datorā un uz servera atsevišķā mapē "Juridiskā nodaļa". Darba līgumu uzskaites žurnāli ir pieejami gan elektroniski (datorā un uz servera), gan papīra formātā (birojā, mapēs, slēgtā skapī) par iepriekšējiem gadiem. Darbinieku Obligātās veselības pārbaudes kartes tiek glabātas birojā – mapē, slēgtā skapī. Darba līgumu kopijas tiek glabātas objektos (mapēs, slēgtā skapī) – tūlītējai uzrādīšanai Valsts darba inspekcijai, to veikto pārbaužu laikā (pārbaudes, kas attiecas uz nelegālo nodarbinātību). Rīkojumi par Darbinieku apriti – gan elektroniski (datorā un uz servera), gan papīra formā (birojā, slēgtā skapī), izveido personāla nodaļa, tiek nodoti apstrādei grāmatvedībā.	Līgumslēdzēju līgumi glabājas papīra formātā birojā slēgtā skapī	Klienta līgumu, aizpildītās anketas (pieteikums Lojalitātes programmai) fiziskā formātā glabājas mapēs (struktūrvienībās), atrodas skapjos. Klienta informācija glabājas Klientu vadības sistēmā.

	Grāmatvedībā papīra formātā tiek iesniegti Darbinieku norēķinu konti algas izmaksai. Grāmatvedības rīkojumi glabājas grāmatvedībā (mapēs, slēgtā skapī). Ar Darbinieku (darba pretendentu) Personu datiem var iepazīties DLV valde vai tās pilnvarotais Darbinieks (t.sk. grāmatvedības ārpakalpojumu sniedzējs u.tml.) nepieciešamajiem mērķiem. Darbinieku vārdi un uzvārdi var tikt izpausti citiem DLV Darbiniekiem un Klientiem, bet pārējos personu datus DLV var izpaust tikai, ja ir saņemta attiecīgā Darbinieka vai pretendenta piekrišana.		
Apstrādes ģeogrāfiskā teritorija	Personas dati tiek apstrādāti Eiropas Savienībā/Eiropas Ekonomiskajā zonā (ES/EEZ).		
Glabāšanas periods	Apstrādāto Personas datu uzglabāšanas periods var būt pamatots ar līgumu, DLV Leģitīmajām interesēm vai piemērojamajiem normatīvajiem aktiem (piemēram: likumiem par grāmatvedību, arhīviem, noziedzīgi iegūto līdzekļu legalizēšanu, noilgumu, civiltiesībām u.tml.). DLV glabā Personas datus atbilstoši Personas datu mērķiem un nolūkiem, kā arī atbilstoši Regulas un normatīvo aktu prasībām, t.sk., DLV Leģitīmo interešu ievērošanai (pierādījumu nodrošināšanai pret prasījumiem par pakalpojuma neatbilstību un/vai līgumsaistību izpildi, kā arī pierādījumu nodrošināšanai pret iespējamo prasījumu, kas izriet no delikta), DLV glabā Personas datus desmit gadus no pakalpojuma jeb līguma izpildes dienas. Pēc glabāšanas perioda beigām DLV dzēš failus, kas satur Personas datus.		

3. INFORMĀCIJAS RESURSI, TEHNISKIE RESURSI UN PAR PERSONAS DATU AIZSARDZĪBU ATBILDĪGĀS PERSONAS, TO TIESĪBAS UN PIENĀKUMI

Informācijas resursu un tehnisko resursu pārvalde:

Par personu datu aizsardzību, informācijas drošības un pilnveidošanas procesu kopumā atbild DLV valde, kura pati vai ar norīkoto personu starpniecību kontrolē Personu datu apstrādes sistēmu drošību.

Valde norīko Personas datu apstrādes speciālistu/-us un/vai Informācijas resursu un tehnisko resursu turētāju/-us, vai arī pati uzņemas veikt attiecīgos uzdevumus.

Valde vai Personas datu apstrādes speciālists vai Informācijas resursu un tehnisko resursu turētājs norīko personas, kuras atrodas Personas datu apstrādes speciālista vai Informācijas resursu un tehnisko resursu turētāja pakļautībā, un kas atbild par Informācijas sistēmu drošību.

Valde budžeta ietvaros nodrošina Informācijas resursu un tehnisko resursu turētāju ar līdzekļiem, kas nepieciešami Informācijas sistēmas drošības pasākumiem.

Informācijas resursu turētājs:

- kopīgi ar tehnisko resursu turētāju un (ja iespējams) ar informācijas devēju veic ar Informācijas resursiem saistītā riska analīzi;
- nodrošina Loģiskās aizsardzības pasākumus;
- nodrošina Informācijas sistēmas Auditācijas pierakstus, kā arī to saglabāšanu un Pieejamību pārbaudei saskaņā ar Informācijas sistēmas drošības noteikumiem;
- nosaka kārtību, kādā Informācijas sistēmas Lietotājiem piešķir tiesības piekļūt Informācijas resursiem un rīkoties ar tiem, un organizē šo resursu izmantošanas kontroli;
- nodrošina Informācijas resursu rezerves kopiju izgatavošanu un glabāšanu, kā arī Informācijas resursu atjaunošanu, ja Informācijas sistēmas funkcionēšana tehnisko resursu bojājumu vai citu iemeslu dēļ bijusi traucēta vai neiespējama.

Tehnisko resursu turētājs:

- nodrošina fiziskās aizsardzības pasākumus;
- piedalās riska analīzē, nosaka ar tehniskajiem resursiem saistītus Informācijas sistēmas Apdraudējumus un novērtē šo Apdraudējumu īstenošanās varbūtību;
- nodrošina tehnisko resursu atjaunošanu, ja tie ir bojāti;
- nodrošina tehnisko resursu atjaunošanu;

Informācijas resursu un tehnisko resursu turētājs nosaka Darbinieku pienākumus Informācijas sistēmas drošības jomā un nodrošina Darbinieku apmācību un zināšanu pārbaudi Informācijas resursu un tehnisko resursu aizsardzības jomā.

4. PERSONAS DATU AIZSARDZĪBAS KLASIFIKĀCIJA ATBILSTOŠI TO VĒRTĪBAS UN KONFIDENCIALITĀTES PAKĀPEI

Informācijas klasifikācijas mērķis ir apzināt visas DLV rīcībā esošās informācijas nozīmību un nodrošināt katras informācijas grupas aizsardzību atbilstoši tās klasifikācijas līmenim.

Informācijas resursu turētāji veic Informācijas resursu Klasificēšanu pēc to Vērtības, Konfidencialitātes un Pieejamības. Informācijas Klasificēšanu veic saskaņā ar Informācijas resursu turētāja prasībām, ja tas tādas ir noteicis.

Informācijas klasifikācija attiecas uz visu informāciju neatkarīgi no informācijas nesēja (papīrs, mikrofilmas, videokasetes, magnētiskās lentes, kasetes, kompaktdiski, datoru cietie diski, disketes vai citi informācijas nesēji).

Informāciju klasificē pēc Konfidencialitātes pakāpes, kad tiek vērtēti Draudi tās nesakcionētai noplūdei, sekojoši:

- Vispārpieejamā informācija;
- Ierobežotas pieejamības informācija.

Informāciju klasificē pēc Vērtības līmeņa, kad tiek vērtēti Draudi informācijas Integritātei, sekojoši:

- Augsti vērtīga informācija;
- Vidēji vērtīga informācija.

Informāciju pēc Pieejamības līmeņa, kad tiek vērtēti Draudi tās Pieejamībai. Klasificējot nosaka arī pieļaujamo laiku, kurā Informācijas resursi var nebūt pieejami. Klasificē sekojoši:

- informācija ir pieejama nepārtraukti;
- informācija pieejama tikai darba laikā.

Informācija, kura nav klasificēta atbilstoši Konfidencialitātes principiem, automātiski tiek uzskatīta par Ierobežotas pieejamības informāciju.

Ja informācijas nesējā glabājas dažādu līmeņu klasificētā informācija, kā kopīgo informācijas nesēja klasifikācijas līmeni norāda augstāko šajā nesējā esošās informācijas līmeni.

Visiem Ierobežotas pieejamības informācijas nesējiem jābūt attiecīgai atzīmei par informācijas klasifikāciju.

5. TEHNISKIE RESURSI, AR KĀDIEM TIEK NODROŠINĀTA PERSONAS DATU APSTRĀDE

Personas datu apstrāde tiek nodrošināta ar šādiem tehniskajiem resursiem:

- stacionārajām darbstacijām, portatīvo vai personālo datoru;
- serveriem;
- videonovērošanas sistēmām;
- citām iekārtām un programmatūrām pēc vajadzības.

6. PERSONAS DATU APSTRĀDES ORGANIZATORISKĀ PROCEDŪRA

Personas datu apstrāde notiek DLV telpās, telpās, kur ir izvietoti DLV serveri, un jebkurā vietā, no kuras ir nodrošināta attālināta piekļuve Informācijas resursiem. Personas dati tiek apstrādāti nepārtraukti vai pēc vajadzības, atbilstoši to apstrādes mērķiem.

DLV apstrādā Personas datus atbilstoši normatīvajos aktos noteiktajam un tikai tad, ja ir vismaz viens no šādiem nosacījumiem:

- saņemta Personas datu subjekta piekrišana;
- Personas datu apstrāde izriet no datu subjekta līgumsaistībām vai, ievērojot datu subjekta lūgumu, Personas datu apstrāde nepieciešama, lai noslēgtu attiecīgu līgumu;

- Personas datu apstrāde nepieciešama DLV likumā noteikto pienākumu veikšanai;

- Personas datu apstrāde nepieciešama, lai aizsargātu datu subjekta vitāli svarīgas intereses, tajā skaitā dzīvību un veselību;

- Personas datu apstrāde nepieciešama, lai nodrošinātu DLV interešu ievērošanu vai realizētu publiskās varas uzdevumus, kuru veikšanai Personas dati ir nodoti DLV;

- Personas datu apstrāde ir nepieciešama, lai, ievērojot datu subjekta pamattiesības un brīvības, realizētu DLV vai tās Trešās personas likumiskās intereses, kurai Personas dati atklāti.

7. VIDEONOVĒROŠANA

DLV veic videonovērošanu noziedzīgu nodarījumu novēršanai vai atklāšanai saistībā ar īpašuma aizsardzību un personu vitāli svarīgu interešu, tajā skaitā dzīvības un veselības, aizsardzību, kā arī izložu un azartspēļu normatīvajos aktos noteikto pienākumu veikšanai.

Videonovērošana tiek veikta DLV spēļu zālēs iekštelpās un ārā nepārtraukti.

Video tiek ierakstīts uz datoru datu nesējiem, kas atrodas katrā spēļu zālē.

Piekļuve videoierakstiem ir tikai no DLV biroja centralizēti, attālināti pieslēdzoties katras spēļu zāles datoram.

Videoieraksti tiek glabāti ne mazāk kā 7 dienas no ieraksta izdarīšanas brīža un tik ilgi kamēr to atļauj katras konkrētās videonovērošanas sistēmas datu nesēja kapacitāte. Beidzoties videonovērošanas sistēmas datu nesēja kapacitātei nākamie videonovērošanas dati tiek rakstīti pāri iepriekšējiem tajā pašā datu nesējā.

Disciplinārlietu, administratīvo vai krimināllietu ietvaros DLV saglabā attiecīgo videoierakstu tik ilgi, kamēr tiek izbeigta attiecīgā lieta.

Nav pieļaujama videonovērošana tualetēs un Darbinieku atpūtas telpās/zonās.

Pie katras spēļu zāles jebkuram redzamā vietā ir jāizvieto rakstisks paziņojums/uzlīme, kas informē, ka tiek veikta videonovērošana, norādot tajā videonovērošanas mērķi, DLV firmu un kontaktinformāciju.

8. DATU SUBJEKTA (DARBINIEKA, LĪGUMSLĒDZĒJA, KLIENTA) TIESĪBAS

Pirms Personas datu apstrādes, DLV sniedz informāciju par Personas datu apstrādi:

- Darbiniekam, parakstot attiecīgu pielikumu pie darba līguma par Personas datu apstrādi;

- Līgumslēdzējam, iekļaujot līgumā noteikumus par Personas datu apstrādi;

- Klientam, iepazīstinot Klientu ar Paziņojumu par privātumu un Privātuma politiku.

Datu subjektam ir šādas tiesības:

1.1. pieprasīt savu Personas datu labošanu, ja tie ir neatbilstoši, nepilnīgi vai nepareizi;

1.2. iebilst savu Personas datu apstrādei, ja Personas datu izmantošana ir balstīta uz leģitīmajām interesēm, tai skaitā profilēšanu tiešā mārketinga nolūkiem (piemēram, mārketinga piedāvājumu saņemšanai vai dalībai aptaujās);

1.3. prasīt savu Personas datu dzēšanu, piemēram, ja Personas dati tiek apstrādāti, pamatojoties uz piekrišanu, ja datu subjekts ir atsaucis savu piekrišanu. Šīs tiesības nav spēkā, ja Personas dati, kuru dzēšana tiek pieprasīta, tiek apstrādāti, arī pamatojoties uz citu tiesisku pamatu, piemēram, līgumu vai no attiecīgiem normatīvajiem aktiem izrietošajiem pienākumiem aktiem (piemēram, Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likumu) vai citos Regulā noteiktajos gadījumos;

1.4. ierobežot savu Personas datu apstrādi saskaņā ar piemērojamajiem normatīvajiem aktiem, piemēram, laikā, kad DLV izvērtē, vai datu subjektam ir tiesības uz savu datu dzēšanu;

1.5. saņemt informāciju, vai DLV apstrādā tā Personas datus un, ja apstrādā, tad arī piekļūt tiem un iegūt informāciju, kā tie tiek apstrādāti un kam nodoti;

1.6. saņemt savus Personas datus, ko tas ir sniedzis un kas tiek apstrādāti uz piekrišanas un līguma izpildes pamata rakstiskā formā vai kādā no biežāk izmantotajiem elektroniskajiem formātiem un, ja iespējams, nodot šādus datus citam pakalpojumu sniedzējam (datu pārnesamība).;

1.7. atsaukt savu piekrišanu savu Personas datu apstrādei, ja Personas dati tiek iesniegti DLV uz datu subjekta piekrišanas pamata;

1.8. netikt pakļautam pilnībā automatizētai lēmumu pieņemšanai, tai skaitā profilēšanai, ja šādai lēmumu pieņemšanai ir tiesiskās sekas vai, kas līdzīgā veidā ievērojami ietekmē datu subjektu. Šīs tiesības nav spēkā, ja lēmuma pieņemšana ir nepieciešama, lai noslēgtu vai izpildītu līgumu ar datu subjektu, ja lēmuma pieņemšana ir atļauta saskaņā ar piemērojamajiem normatīvajiem aktiem vai, ja datu subjekts ir devis savu nepārprotamu piekrišanu;

1.9. iesniegt sūdzības par Personas datu izmantošanu Datu valsts inspekcijai (www.dvi.gov.lv), ja datu subjekts uzskata, ka tā Personas datu apstrāde pārkāpj tā tiesības un intereses saskaņā ar piemērojamajiem normatīvajiem aktiem.

Tiesības, kuras persona <u>NEVAR</u> izmantot (ar "X" atzīmētās tiesības, kuras fiziska persona (datu subjekts) NEVAR izmantot. Ailes BEZ "X" ir tiesības, kuras fiziska persona (datu subjekts) VAR izmantot):

Pamats Personas datu apstrādei:	Tiesības uz datu dzēšanu	Tiesības uz datu pārnesamību	Tiesības iebilst
Piekrišana			X bet tiesības atsaukt piekrišanu
Līgums			X
Likumiskais pienākums	X	X	X
Būtiskas intereses		X	X
Valsts iestāžu uzdevumā	X	X	
Leģitīmas intereses		X	

9. Kārtība, kādā DLV nodrošina Datu subjektam garantētās tiesības un Personas datu drošības pasākumi

<u>Datu subjektu tiesību nodrošināšana.</u>

Datu subjektu pieprasījumi:

Ja no datu subjekta saņemts pieprasījums izsniegt vai izpaust DLV rīcībā esošos datu subjekta Personu datus, šādus pieprasījumus izskata DLV valdes loceklis vai viņa norīkota persona, un attiecīgos Personu datus var izsniegt un izpaust tikai DLV valdes loceklis vai viņa norīkota persona, ja šāda izpaušana vai nodošana ir pamatota.

Lai aizsargātu Personas datus no nelikumīgas atklāšanas, DLV, saņemot datu subjekta lūgumu par datu sniegšanu vai citu datu subjekta tiesību īstenošanu, pārliecinās par datu subjekta identitāti. Šim nolūkam DLV ir tiesīga lūgt datu subjektam norādīt Personas datus, salīdzinot, vai datu subjekta norādītie dati sakrīt ar attiecīgajiem DLV rīcībā esošajiem Personas datiem. Veicot šo pārbaudi, DLV tāpat var izsūtīt kontroles paziņojumu uz datu subjekta norādīto telefonu vai e-pastu (īsziņas vai e-pastas veidā), lūdzot veikt autorizāciju. Ja pārbaudes procedūra nav veiksmīga (piem.,

datu subjekta norādītie dati nesakrīt ar DLV rīcībā esošajiem Personas datiem vai datu subjekts nav veicis autorizāciju pēc nosūtītās īsziņas vai e-pasta paziņojuma), DLV būs spiesta konstatēt, ka datu subjekts nav pieprasīto Personas datu subjekts, un būs spiesta noraidīt attiecīgo iesniegto lūgumu.

Saņemot datu subjekta lūgumu par jebkuru datu subjekta tiesību īstenošanu un veiksmīgi veicot iepriekš norādīto pārbaudes procedūru, DLV apņemamas bez kavēšanās, taču jebkurā gadījumā ne vēlāk kā viena mēneša laikā no datu subjekta lūguma saņemšanas un pārbaudes procedūras beigām, sniegt datu subjektam informāciju par darbībām, ko DLV ir veikusi saskaņā ar datu subjekta iesniegto lūgumu. Ņemot vērā lūgumu sarežģītību un skaitu, DLV ir tiesības viena mēneša periodu pagarināt vēl uz diviem mēnešiem, par to informējot datu subjektu līdz pirmā mēneša beigām un norādot šāda pagarinājuma iemeslus. Ja datu subjekta lūgums ir iesniegts ar elektroniskajiem līdzekļiem, DLV atbildi sniegs arī ar elektroniskajiem līdzekļiem, izņemot gadījumus, kad tas nebūs iespējams (piem., lielā informācijas apjoma dēļ) vai tad, ja datu subjekts būs lūdzis atbildēt citā veidā.

DLV ir tiesīga attiekties apmierināt datu subjekta lūgumu ar motivētu atbildi, ja tiks konstatēti tiesību aktos norādītie apstākļi vai nav iespējams pārliecināties par datu subjekta identitāti, par to rakstiski informējot datu subjektu. Ja datu subjekta pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi, jo īpaši to regulāras atkārtošanās dēļ, DLV kā Datu Pārzinis var vai nu: a) pieprasīt saprātīgu maksu, ņemot vērā administratīvās izmaksas, kas saistītas ar informācijas vai saziņas nodrošināšanu vai pieprasītās darbības veikšanu; vai arī b) atteikties izpildīt pieprasījumu.

Trešo personu pieprasījumi:

Ja no valsts vai pašvaldību iestādēm vai Trešajām personām, kas nav Darbinieki, Līgumslēdzēji vai Klienti, ir saņemts pieprasījums izsniegt vai izpaust DLV rīcībā esošos Personu datus, šādus pieprasījumus izskata DLV valdes loceklis vai viņa norīkota persona, un attiecīgos personu datus var izsniegt un izpaust tikai DLV valdes loceklis vai viņa norīkota persona, ja šāda izpaušana vai nodošana ir pamatota.

Jebkurā gadījumā, ja DLV Darbinieks nezin kā rīkoties – drīkst vai nedrīkst izpaust kādu informāciju – Darbiniekam ir jākonsultējas ar DLV valdes locekli vai viņa norīkotu personu, un Darbinieks drīkst rīkoties attiecīgajā gadījumā tikai tā, kā ir norādījis DLV valdes loceklis vai viņa norīkota persona.

DLV, nododot Personas datus, nodrošina informācijas saglabāšanu par:

- Personas datu nodošanas laiku;
- Personu, kas nodevusi Personas datus;
- Personu, kas saņēmusi Personas datus;
- Personas datiem, kas tikuši nodoti.

<u>Personas datu drošības pasākumi.</u>

Lai aizsargātu Personas datus pret nesankcionētu piekļuvi, nejaušu pazušanu, iznīcināšanu vai bojāšanu, DLV izmanto fiziskās drošības pasākumus: slēgtas kartotēkas, kas satur Personas datus; slēgti biroji / telpas ar Personīgajiem datiem.

DLV izmanto drošības līdzekļus, lai nodrošinātu ierīču un / vai failu aizsardzību pret neautorizētu piekļuvi, nejaušu pazušanu, iznīcināšanu vai bojāšanu: autorizācija, arhivēšana, šifrēšana, Lietotāja piekļuves, rīcības reglamentēšana, SSL sertifikāti, ugunsmūris.

DLV izmanto vēl citus drošības pasākumus, lai aizsargātu Personas datus pret nesankcionētu piekļuvi, nejaušu pazaudēšanu, iznīcināšanu vai bojāšanu: ierobežotas piekļuves tiesības Personas datiem (pamatojoties uz nepieciešamību zināt); droša konfidenciālas informācijas dokumentācijas atkritumu iznīcināšana (gan papīra, gan elektroniskā veidā), darbinieku apmācības.

Apstrādājot Personas datus Informācijas sistēmā, tiek nodrošināta tikai pilnvarotu personu piekļūšana pie Personas datiem, tehniskajiem līdzekļiem un dokumentiem.

Informācijas sistēmu administratoram sadarbībā ar Tehnoloģisko resursu turētāju ir tiesības

veikt Lietotāju darbības auditus. Šādi auditi var ietvert Lietotāja darbību auditācijas veikšanu (tai skaitā apmeklētos interneta resursus), analizēšanu un papildus informācijas pieprasīšanu par veiktajām darbībā.

Informācijas sistēmu lietošanas pārraudzības ietvaros:

- Tehnoloģisko resursu turētājs nodrošina, ka Auditācijas pieraksti tiek veidoti par Informācijas sistēmām, kas satur klasificētus Informācijas resursus, un darbībām datortīklā, kurā ir pieeja Informācijas sistēmām, kas satur klasificētus Informācijas resursus. Auditācijas pierakstos iekļauj visu veiksmīgas un neveiksmīgas pieslēgšanās gadījumu datumu un laiku, kā arī Lietotāja (t.sk. Tehnoloģisko resursu turētāja) kodu vai citu autentifikācijas līdzekli;
- Tehnoloģisko resursu turētājs nodrošina Auditācijas pierakstu Integritāti un regulāri veido Auditācijas pierakstu datu rezerves kopijas saskaņā ar šīs kārtības noteikumiem;
- Tehnoloģisko resursu turētājs regulāri pārrauga visu Informācijas sistēmu darbību, taču īpašu uzmanību pievērsto Informācijas sistēmu darbības pārraudzībai, kas satur klasificētus Informācijas resursus. Šim nolūkam Tehnoloģisko resursu turētājs pēc izvēles lieto speciālas pārraudzības programmas vai datoru iebrukumu noteikšanas sistēmas.

Tehnoloģisko resursu turētājs pārrauga vismaz šādus gadījumus:

- atkārtota neveiksmīga pieslēgšanās Informācijas sistēmai;
- mēģinājumi piekļūt Informācijas resursiem, kuriem Lietotājs nav pilnvarots piekļūt;
- Informācijas sistēmas lietošana neparastā laikā, piemēram, ārpus darba laika;
- atkārtoti mēģinājumi lietot Lietotāja kodus, kuri jau ir atcelti;
- privileģēto Lietotāja kodu piešķiršana un lietošana;
- nesankcionētas programmatūras konfigurācijas maiņas un neatļautas programmatūras uzstādīšana.

Vīrusu kontrole Informācijas sistēmas resursos:

- Tehnoloģisko turētājs nosaka kārtību un veic pasākumus datoru vīrusu darbības novēršanai Informācijas sistēmās;
- vīrusu darbības novēršanai lieto speciāli šim nolūkam paredzētu programmatūru. Vīrusu definīciju failus nekavējoties atjauno, tiklīdz izstrādātājs piedāvā atjaunojuma failus;
- Tehnoloģisko resursu turētājs regulāri veic antivīrusu programmas pārraudzību, lai pārliecinātos par tās darbību un jaunāko vīrusu definīciju failu esamību.

Personālo un portatīvo datoru aizsardzība:

- informācijas turētājs nosaka, kādu informāciju drīkst glabāt uz personālā un portatīvā datora (tālāk tekstā - **personālie datori**). Portatīvajos datoros, kuri tiek lietoti ārpus DLV darba telpām, glabā tikai to informāciju, kas nepieciešami noteiktajā laikā noteiktajam datora Lietotājam;
- personālajā datorā uzstāda un lieto tikai to programmatūru un tādā konfigurācijā, ko ir noteicis Tehnoloģisko resursu turētājs. Personālā datora funkcionalitāti ierobežo līdz darba vajadzībām nepieciešamo funkciju līmenim;
- personālo datoru, atstājot bez Lietotāja uzraudzības, slēdz, lietojot ekrānsaudzētāju ar paroli, speciālu slēgšanas funkciju vai citu metodi, kas ļauj turpināt darbu ar personālo datoru vienīgi tad, ja ir veikta Lietotāja autentifikācija;
- Informācijas resursu turētājs nosaka kārtību, kādā darba vajadzībām Darbinieki lieto viņiem piederošus datorus un kādā lieto DLV datorus ārpus darba telpām. Šī kārtība nedrīkst samazināt noteikto Informācijas resursu aizsardzības līmeni.

Datortīklu aizsardzība:

- Tehnoloģisko resursu turētājs izstrādā un uztur datortīkla shēmu, kurā parādīta datortīklā savienotā aparatūra un nodrošinātie pakalpojumi;
- datu plūsmā starp lokālo datortīklu un ārējo datortīklu atjauj tikai tos pakalpojumus, kas ir nepieciešami DLV funkciju izpildei, šim nolūkam lieto ugunsmūra sistēmas;

- Tehnoloģisko resursu turētājs regulāri pārbauda visu ārējo savienojumu eksistenci un pārliecinās, ka pastāv tikai tie savienojumi, kuri atbilst DLV darbības vajadzībām un ka darbojas rezerves savienojumi;

- pieslēgšanos Informācijas sistēmām no loģiski attālas vietas aizsargā, lietojot kriptogrāfijas līdzekļus kopā ar Lietotāja paroli tā, lai droši noteiktu Lietotāja Autentiskumu.

DLV pēc nepieciešamības veic papildu Loģiskās aizsardzības pasākumus atkarībā no Informācijas sistēmas resursu klasifikācijas līmeņa.

DLV veic līdzvērtīgus Loģiskās aizsardzības pasākumus klasificētiem Informācijas resursiem neatkarīgi no datu glabāšanas veida (t.sk. disketes, papīra dokumenti, audio kasetes u.tml.).

DLV sadarbībā ar ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem:

- nosaka prasības iesaistīto personu atbildībai, pagaidu Lietotāju kontu piešķiršanai, pārmaiņu pārvaldīšanai un citas Informācijas sistēmas drošības prasības;
- saskaņojot ar informācijas turētājiem, piešķir pieejas tiesības Informācijas sistēmas resursiem ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem tikai to pienākumu veikšanai nepieciešamajā apjomā;
- nosaka informācijas izpaušanas ierobežojumus.

Ja DLV izvēlas Informācijas sistēmas uzturēšanu uzticēt ārējam pakalpojumu sniedzējam, tam jānodrošina Informācijas sistēmas drošības līmenis, kas nav zemāks par šajā kārtībā noteikto. DLV iepazīstina ārējo pakalpojumu sniedzēju ar šajā kārtībā noteiktajām Informācijas sistēmas drošības prasībām. Personas datu apstrādes kārtību un piekļuves līmeņus nosaka Informācijas sistēmu Lietotāju lomu sadalījums.

10. PAROLES UZBŪVE, TĀS LIETOŠANAS KĀRTĪBA UN PIEKĻUVE

Katram Informācijas resursu Lietotājam tiek piešķirts Informācijas sistēmas lietotājvārds(i) (identifikators(i)) un parole, kā arī noteiktas piekļuves tiesības. Informācijas sistēmas Lietotājs ir atbildīgs par piešķirtā lietotājvārda (identifikatora) un paroles lietošanu, saglabāšanu un neizpaušanu.

Piekļuves tiesības apstiprina attiecīgo Informācijas resursu turētājs. Balstoties uz Informācijas resursu turētāja pieprasījumu, Informācijas sistēmu administrators izveido Lietotājam piekļuvi visās apstiprinājumā norādītajās Informācijas sistēmās.

Informācijas resursu turētājam ir jāinformē Informācijas sistēmu administrators par tiem Darbiniekiem, kuri pārtrauc darba attiecības ar DLV. Tehnoloģisko resursu turētājs pēc šīs informācijas saņemšanas nekavējoties anulē visas attiecīgā Darbinieka piekļuves tiesības DLV Informācijas sistēmas resursiem.

Informācijas sistēmu Lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotājvārdu (identifikatoru). Informācijas sistēmu Lietotāja Autentiskumu nosaka, lai pārliecinātos, ka lietotājvārda (identifikatora) izmantotājs ir sankcionētais tā turētājs. Autentiskuma noteikšanai tiek izmantotas paroles. Pēc lietotājvārda (identifikatora) un paroles ievadīšanas Informācijas sistēmu Lietotājs var izmantot Informācijas sistēmas resursu atbilstoši noteiktajām piekļuves tiesībām.

Parole sastāv no burtu, ciparu un zīmju kombinācijas un tās garums nedrīkst būt īsāks par astoņiem simboliem. Nedrīkst par paroli izmantot personu identificējošus datus (piemēram, Personas datus, automašīnas numuru, radu vārdus vai uzvārdus, vārdus, kas saistīti ar darbavietu vai kas bieži tiek tajā lietoti).

Informācijas sistēmas Lietotājam, ievadot paroli, tā nedrīkst būt salasāma uz datora ekrāna.

Informācijas sistēmu Lietotājam paroli jāmaina vismaz reizi trijos mēnešos. Informācijas sistēmu administratoram ir jānodrošina:

automātisku paroles maiņas pieprasījumu, Lietotājam pirmo reizi reģistrējoties tīklā;

automātisku paroles maiņas pieprasījumu ik pēc trim mēnešiem;

sistēmas bloķēšanu uz laiku līdz 1 stundai, ja Lietotājs piecas reizes pēc kārtas ir ievadījis nepareizu paroli vai lietotājvārdu.

Informācijas sistēmu Lietotājam parole ir jāiegaumē. Rakstiskā veidā paroles atļauts glabāt

tikai aizslēgtā seifā.

Ja radušās aizdomas, ka paroli uzzinājusi cita persona, Informācijas sistēmu Lietotājs nekavējoties ziņo par Incidentu Informācijas resursu turētājam, tehnisko resursu turētājam un Informācijas sistēmu administratoram.

Aizliegts mēģināt uzzināt citu Lietotāju paroles, izņemot gadījumus, kad tas ir nepieciešams Informācijas sistēmu administratoram viņa tiešo pienākumu veikšanai. Pēc minēto darbu pabeigšanas Informācijas sistēmu Lietotājs paroli nomaina.

Uz datora ir jābūt uzstādītam ekrāna saudzētājam ar aktivizācijas paroli. Tam ir automātiski jāaktivizējas, ja piecu minūšu laikā Lietotājs nav veicis nekādas darbības.

11. PASĀKUMI, KAS VEICAMI TEHNISKO RESURSU AIZSARDZĪBAI PRET ĀRKĀRTAS APSTĀKĻIEM UN LĪDZEKĻI, AR KĀDIEM NODROŠINA TEHNISKOS RESURSUS PRET TĪŠU BOJĀŠANU UN NEATĻAUTU IEGŪŠANU

DLV veic Informācijas sistēmu fiziskās aizsardzības pasākumus, kas aizsargā tās no nevēlamiem apkārtējās vides (ugunsgrēks, plūdi, temperatūras svārstības u.c.), tehniskajiem (neatbilstoša elektroenerģijas padeve u.c.) un cilvēkfaktoriem (tīši vai netīši bojājumi, zādzība u.c.).

Serveru Fiziskā aizsardzība:

- DLV nodrošina, ka visas Informācijas sistēmas tiek ekspluatētas ierobežotas pieejamības, slēdzamās telpās, kuru Fiziskā aizsardzība nodrošina tikai pilnvarotu personu piekļuvi, vai arī nodrošina serveru fizisko aizsardzību, lai tos nevarētu izslēgt, pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju. Serveru telpas izvieto ēkas vietās, kurās ir mazāka Apdraudējumu īstenošanās iespējamība;

- nepiederošas personas, t.sk. ārējie pakalpojumu sniedzēji serveru telpās drīkst uzturēties tikai pilnvarotu personu pavadībā;

- atkarībā no iespējamo zaudējumu apmēra DLV nodrošina pietiekamu serveru un serveru telpu aizsardzību pret fiziskiem Apdraudējumiem (t.sk. neatbilstošiem klimatiskajiem apstākļiem, ugunsgrēku, plūdiem, elektroenerģijas padeves pārtraukumiem, tīšiem bojājumiem), nepieciešamības gadījumā ierīkojot apsardzes un ugunsdzēsības signalizāciju, automātiskās ugunsdzēšanas sistēmu, uzstādot alternatīvās strāvas padeves iekārtas un gaisa dzesēšanas iekārtas.

Tīklu infrastruktūrai (t.sk. komunikāciju tīklu aparatūrai, kabeļu tīklam) DLV nodrošina pietiekamu fizisko aizsardzību, to izvietojot tādējādi, lai tai nevarētu nesankcionēti un iemānīti piekļūt, pieslēgties vai bojāt ar DLV nesaistītas personas, kā arī, lai tai nevarētu nesankcionēti piekļūt, pieslēgties un bojāt, vai nejauši aiz neuzmanības bojāt DLV Darbinieki vai apmeklētāji.

Darbstaciju Fiziskā aizsardzība:

- Tehnoloģisko resursu turētāja darba vietu nodala ierobežotas pieejamības telpās;

- darbstacijas lieto atbilstoši ražotāja noteiktām prasībām un lieto elektroenerģijas nepārtrauktas padeves iekārtas, ja atklājas, ka elektroenerģijas padeves traucējumu risks ir nepieņemami liels.

Portatīvo iekārtu Fiziskā aizsardzība:

portatīvos datorus lieto atbilstoši ražotāja noteiktajām prasībām;

DLV veic portatīvo iekārtu aprites reģistrēšanu, lai noteiktu, kura persona lieto attiecīgo iekārtu.

Datu nesēju Fiziskā aizsardzība:

- DLV veic nepieciešamos drošības pasākumus visu datu nesēju fiziskai aizsardzībai neatkarīgi no veida (t.sk. demontētas disku iekārtas, papīra izdrukas, faksa izdrukas, disketes, optiskie diski u.tml.);

- datu nesējus, kas satur Informācijas sistēmas resursus lietot un pārvietot bez īpaša laika ierobežojuma drīkst tikai DLV pilnvaroti Darbinieki, kuriem ir pieeja Informācijas sistēmas resursiem. Informācijas sistēmas resursi, kurus nav nepieciešams lietot vai pārvietot, tiek glabāti DLV telpās, tam paredzētās vietās. Ja ir nepieciešams iznīcināt datu nesējus, to iznīcināšanu uzrauga vai nodrošina Tehnoloģisko resursu turētājs;

- datu nesēju aizsardzības ietvaros DLV veic datu ievada un izvada iekārtu fizisko aizsardzību, novēršot nesankcionētu lietošanu - printeru iekārtas neizvieto publiski pieejamās telpās, nepieļauj ārējo datu nesēju darbību, ja tas nav nepieciešama Darbinieku pienākumu veikšanai;
- datu nesējus ar klasificētiem Informācijas resursiem aizliegts atstāt nedrošās (piemēram, publiski pieejamās) vietās;
- ja datu nesēju, kas satur klasificētus Informācijas resursus, ir paredzēts iznīcināt, tad to izdara tādā veidā, lai nebūtu iespējams veikt uz tā esošo datu atjaunošanu.

Nepieciešamības gadījumā DLV veic papildu fiziskās aizsardzības pasākumus atkarībā no Informācijas sistēmas resursu klasifikācijas līmeņa. Informācijas sistēmas fiziskās aizsardzības pasākumus veic sistemātiski, nepieļaujot situāciju, ka Informācijas sistēmas resursi atrastos ārpus ierobežotas pieejamības telpām bez DLV pilnvarotu Darbinieku uzraudzības. DLV regulāri veic fiziskās aizsardzības pasākumu pārbaudi.

Datu rezerves kopijas tiek gatavotas atbilstoši DLV valdes locekļa noteiktai procedūrai.

Jebkuru Incidentu gadījumā, piem., datu nesēju zādzības, pazušanas gadījumā, attiecīgais Darbinieks nekavējoties informē Tehnoloģisko un Informācijas resursu turētāju, kas veic visus nepieciešamos pasākumus datu aizsardzībai.

12. INFORMĀCIJAS NESĒJU GLABĀŠANAS UN IZNĪCINĀŠANAS KĀRTĪBA

Informācijas sistēmas slēgšanas gadījumā vai pirms informācijas nesēju iznīcināšanas atbildīgā persona dzēš informācijas saturu, datubāzu saturu, kā arī visas citas saistītās datnes.

Ja nepieciešams dzēst datus no Informācijas sistēmas, DLV nodrošina pilnīgu datu dzēšanu no Informācijas sistēmas, lai tos nebūtu iespējams atjaunot.

13. PERSONAS DATU LIETOTĀJU TIESĪBAS, PIENĀKUMI, IEROBEŽOJUMI UN ATBILDĪBA

Informācijas sistēmu Lietotāji drīkst izmantot piešķirtos Informācijas sistēmas resursus tikai darba pienākumu veikšanai un apstrādāt Personas datus tikai atbilstoši to apstrādes mērķim un darba pienākumu veikšanai.

Informācijas sistēmu Lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotājvārdu (identifikatoru). Informācijas sistēmu Lietotāja Autentiskumu nosaka, lai pārliecinātos, ka lietotājvārda (identifikatora) izmantotājs ir sankcionētais tā turētājs. Autentiskuma noteikšanai tiek izmantotas paroles. Pēc lietotājvārda (identifikatora) un paroles ievadīšanas Informācijas sistēmu Lietotājs var izmantot Informācijas sistēmas resursu atbilstoši noteiktajām piekļuves tiesībām.

Informācijas sistēmu Lietotājam parole ir jāiegaumē. Rakstiskā veidā paroles atļauts glabāt tikai aizslēgtā seifā.

Aizliegts mēģināt un uzzināt citu Lietotāju paroles, izņemot gadījumus, kad tas ir nepieciešams Informācijas sistēmu administratoram viņa tiešo pienākumu veikšanai. Pēc minēto darbu pabeigšanas Informācijas sistēmu Lietotājs paroli nomaina.

Informācijas sistēmu Lietotājam izbeidzot darba attiecības ar DLV, visas piekļuves tiesības Informācijas sistēmas resursiem Informācijas sistēmu administrators anulē.

Izmantojot Informācijas sistēmas resursus, Informācijas sistēmu Lietotāju pienākums ir nekavējoties ziņot Informācijas sistēmu administratoram šādos gadījumos:

- ja radušās aizdomas, ka Lietotāja paroli uzzinājusi cita persona;
- saņemot neskaidras izcelsmes e-pasta sūtījumus (piemēram, nepazīstami korespondenti, īpatnēji norādīti vēstuļu temati);
- ja radušās aizdomas, ka dators inficēts ar vīrusu, kā arī izslēgt datoru;
- ja radušās aizdomas par datortehnikas bojājumu, kā arī nekavējoties izslēgt bojāto tehniku;

- pamanot novirzes datora vai Informācijas sistēmas darbībā;
- ja nepieciešams mainīt datortehnikas izvietojumu;
- izlasīt Informācijas sistēmu administratora sūtītos ziņojumus un laikus izpildīt norādītās darbības;
- iepazīties ar koplietošanas katalogā ievietotajām instrukcijām un ieteikumiem;
- regulāri izdzēst darbam nevajadzīgos e-pasta sūtījumus;
- nepārtraukt pretvīrusu programmas atjaunināšanas procesu;
- sekot, lai uz datora obligāti būtu aktivizēts ekrāna saudzētājs ar paroles aizsardzību. Ekrāna saudzētājam automātiski jāaktivizējas, ja piecu minūšu laikā Lietotājs nav veicis nekādas darbības.

Informācijas sistēmu Lietotājiem aizliegts:

- izmantot Informācijas sistēmu resursus, lai izplatītu vai uzglabātu ar darbu nesaistītu informāciju (piemēram, komerciāla vai personīga rakstura sludinājumus, uzsaukumus, reklāmas, destruktīvas programmas, spēles);

- veikt darbības, kas nevajadzīgi noslogo Informācijas sistēmas resursus, neņemot vērā citu Informācijas sistēmas Lietotāju vajadzības (piemēram, pārmērīgi izmantot internetu, drukāt nevajadzīgi daudz dokumentu kopiju, atstāt atvērtas uz failu servera esošās datnes, kuras nav nepieciešamas darbam);

- veikt internetā pieejamo programmu lejupielādi;

- patstāvīgi instalēt datoros programmatūru;

- nesankcionēti nodot programmatūras un darba datu kopijas trešajai personai;

- bez saskaņošanas ar DLV valdes locekli veidot sev vai piešķirt citiem Lietotājiem attālinātu pieeju savas darba stacijas, portatīvā datora vai servera resursiem;

- patstāvīgi mainīt datora konfigurāciju, pārvietot stacionāro biroja tehniku un novērst jebkurus datortehnikas bojājumus;

- datoru nepārtrauktās energoapgādes sistēmai pieslēgt jebkuras elektroierīces, izņemot datorus, monitorus un drukas ierīces.

Informācijas sistēmu Lietotājs ir atbildīgs par zaudējumiem, kas radušies šajos noteikumos noteikto prasību neievērošanas dēļ.

Informācijas sistēmu administrators:

- izveido, modificē un likvidē Informācijas sistēmu Lietotāju identifikatorus (kontus) un piešķir attiecīgās tiesības;
- ja nepieciešams, ierobežo failu servera diska vai kāda tā kataloga apjomu, par to informējot visus šī diska vai kataloga Lietotājus ar e-pastu;
- kontrolē, lai Informācijas sistēmas resursu Lietotāji ievērotu šajos noteikumos noteiktos paroļu maiņas nosacījumus.

Informācijas sistēmu administrators ir tiesīgs:

- brīvdienās un ārpus oficiālā darba laika atslēgt Informācijas sistēmas resursus, lai veiktu uzturēšanas darbus, 3 darba dienas iepriekš par to brīdinot Informācijas sistēmu Lietotājus;
- atslēgt Informācijas sistēmas resursus un apturēt sistēmu darbu arī darba laikā, ja notikusi avārija (ja iespējams, iepriekš par to brīdinot Lietotājus pa telefonu un e-pastu).

14. PERSONAS DATU AIZSARDZĪBAS PĀRKĀPUMU PROCEDŪRA

Saskaņā ar Regulas 33.un 34. pantu DLV kā Datu Pārzinis konstatē, reģistrē izmeklē, izvērtē un pieņem lēmumu par notikušu Personas datu aizsardzības pārkāpuma paziņošanu Datu valsts inspekcijai un/vai Personas datu subjektam.

1. Vispārīgi noteikumi.

1.1. Par jebkuru Personas datu aizsardzības Pārkāpumu vai tā pazīmēm Darbinieks, kurš to ir konstatējis, nekavējoties ziņo gan Informācijas resursu, gan tehnisko resursu turētājam.
1.2. Pārkāpuma gadījumā Darbiniekam savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt tehnisko un Informācijas resursu drošību līdz attiecīgo resursu turētāju ierašanās brīdim.

2. Pārkāpumu reģistrēšana, izmeklēšana un izvērtēšana

2.1. Saņemot Darbinieka, Datu Apstrādāja, sadarbības partnera vai jebkuras Trešās personas informāciju par iespējamo Pārkāpumu, atbildīgā persona (datu aizsardzības speciālists) (turpmāk – **Atbildīgā persona**) nekavējoties veic pārbaudi par to, vai informācija ir patiesa. Aizdomu gadījumā par Pārkāpumu, tas nekavējoties tiek fiksēts Pārkāpumu reģistrā (pielikums Nr.1).
2.2. Par Pārkāpumu reģistra vešanu ir atbildīga Atbildīgā persona.
2.3. Pēc Pārkāpuma reģistrēšanas Atbildīgā persona uzsāk izmeklēšanu un noskaidro Pārkāpuma veidu, rašanas iemeslus un pieņem lēmumu par riska Ietekmi uz datu subjekta tiesībām.
2.4. Izšķir šādus Pārkāpumu veidus:
  2.4.1. Pieejamības Pārkāpums – (A)
  2.4.2. Integritātes Pārkāpums – (B)
  2.4.3. Konfidencialitātes Pārkāpums – (C)
2.5. Vairāku Pārkāpumu veidu gadījumā Pārkāpumu reģistrā norāda visus attiecīgos Pārkāpuma apzīmējumus.
2.6. Pēc Ietekmes uz datu subjekta tiesībām un brīvībām izšķir šādas Pārkāpuma Ietekmes:
  2.6.1. Pārkāpums nerada risku vai maz ticams, ka tiks radīts risks – (1)
  2.6.2. Pārkāpums var radīt risku vai rada risku – (2)
  2.6.3. Pārkāpums rada augstu risku – (3)
2.7. Ja tiek konstatēti vairāki Pārkāpumi veidi ar dažādām risku Vērtībām, rīcība attiecībā uz Pārkāpuma paziņošanu tiek veikta, ņemot vērā augstāko riska Ietekmes Vērtību.
2.8. Pēc Pārkāpuma Ietekmes izvērtēšanas tiek pieņemts lēmums par tā ziņošanu saskaņā ar šiem noteikumiem.
2.9. Papildus Pārkāpuma Ietekmes izvērtēšanai veic Pārkāpuma radīto seku novēršanu atbilstoši Ietekmei, ko Pārkāpums ir radījis, nepieciešamības gadījumā pārtraucot Informācijas sistēmas darbību.

3. Paziņošana Datu valsts inspekcijai

3.1. Ja ir maz ticams, ka Pārkāpums var radīt risku datu subjekta tiesībām un brīvībām (Zema riska informācija), paziņošanu Datu valsts inspekcijai neveic.
3.2. Ja Pārkāpums var radīt risku vai augstu risku datu subjekta tiesībām un brīvībām, Datu Pārzinis par datu aizsardzības pārkāpumu paziņo Datu Valsts inspekcijai nekavējoties, bet ne vēlāk kā 72 stundu laikā no brīža, kad Pārkāpums ir kļuvis zināms.
3.3. Paziņojumā Datu Valsts inspekcijai Datu Pārzinis norāda sekojošo:
  3.3.1. apraksta Pārkāpuma raksturu, tajā skaitā, datu subjekta kategorijas un aptuveno skaitu;
  3.3.2. datu aizsardzības speciālista kontaktinformāciju, vai citu kontaktinformāciju, kur iespējams iegūt papildus informāciju;
  3.3.3. Pārkāpuma iespējamās sekas;
  3.3.4. pasākumus, kurus Datu Pārzinis ir veicis vai plāno veikt, lai novērstu Pārkāpumu un tā nelabvēlīgas sekas.

4. Datu subjekta informēšana par datu aizsardzības Pārkāpumu

4.1. Ja Datu Pārzinis konstatē, ka Pārkāpums var radīt augstu risku datu subjekta tiesībām un brīvībām, Datu Pārzinis nekavējoties par to paziņo datu subjektam.

4.2. Paziņojumā datu subjektam norāda 3.3.punktā noteikto informāciju.

4.3. Paziņošana datu subjektam neveic, ja:

4.3.1. Datu Pārzinis ir īstenojis atbilstīgus tehniskus un organizatoriskus aizsardzības pasākumus, un minētie pasākumi ir piemēroti Personas datiem, ko skāris Pārkāpums, jo īpaši tādi pasākumi, kas Personas datus padara nesaprotamus personām, kurām nav pilnvaru piekļūt datiem;

4.3.2. Datu Pārzinis pēc Pārkāpuma ir veicis tehniskas un organizatoriskas darbības, lai datu subjektam netiktu radīts augsts risks viņa tiesībām un brīvībām;

4.3.3. ja paziņošana prasa nesamērīgas pūles. Šajā gadījumā var tikt izmantota publiska paziņošana vai līdzīga saziņa, kas vienlīdz efektīvi informē datu subjektus.

4.4. Ja rodas aizdomas par noziedzīgu nodarījumu (datu zādzību veikušas Trešās personas u.c.), Atbildīgā persona pēc konsultēšanas ar Pārzini pieņem lēmumu par ziņošanu Valsts policijai un Datu valsts inspekcijai.