SIA "CIETKOKS"

Reģistrācijas Nr. *40003789658*

Juridiskā adrese: "Betta", Kandavas pagasts, Kandavas novads, LV-3120

INFORMĀCIJAS DROŠĪBAS POLITIKA

Izstrādāta pamatojoties uz EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti.

Kandavā, 2021

Saturs

1. Vispārīgie jautājumi

1.1. Informācijas drošības politika ir attiecināma uz visiem Pārziņa darbiniekiem, kuri ir iesaistīti personas datu apstrādē, vai veic personas datu apstrādi.

1.2. Pārziņa darbinieku pienākums ir atbildēt par šīs Informācijas drošības politikas prasību ievērošanu.

2. Lietoto terminu definīcijas

Uzņēmums	*Fiziska vai juridiska persona, kas veic saimniecisku darbību, neatkarīgi no tās juridiskā statusa, tostarp partnerības vai apvienības, kas regulāri veic saimniecisku darbību.*
Pārzinis	*Fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus; ja šādas apstrādes nolūkus un līdzekļus nosaka ar Savienības vai dalībvalsts tiesību aktiem, pārzini vai tā iecelšanas konkrētos kritērijus var paredzēt Savienības vai dalībvalsts tiesību aktos.*
Darbinieks	*Uzņēmuma nodarbināta fiziska persona.*
Informācijas drošības politika	*Personas datu aizsardzības vadlīnijas, ko stingri ievēro pārzinis vai apstrādātājs, kas veic uzņēmējdarbību dalībvalsts teritorijā, attiecībā uz personas datu nosūtīšanu vai vairākkārtēju nosūtīšanu pārzinim vai apstrādātājam vienā vai vairākās trešās valstīs uzņēmumu grupā vai uzņēmējsabiedrību grupā, kas iesaistīta kopīgā saimnieciskā darbībā.*
Personas dati	*Jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjekts"); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.*
Apstrāde	*Jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana.*
Datu aizsardzības speciālists	*Pārziņa iecelta fiziska persona vai personas, kas veic datu aizsardzības speciālista pienākumus atbilstoši Vispārīgās datu aizsardzības regulas prasībām.*
Apstrādātājs	*Fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus.*
Trešā persona	*Fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus.*
Piekrišana	*Datu subjekta "piekrišana" ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei.*

Personas datu aizsardzības pārkāpums	*Drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.*

3. Personas datu apstrādes principi

Likumīgums, godprātība un pārredzamība	*Tiek apstrādāti likumīgi, godprātīgi un datu subjektam pārredzamā veidā.*
Nolūka ierobežojumi	*Tiek vākti konkrētos, skaidros un leģitīmos nolūkos, un to turpmāku apstrādi neveic ar minētajiem nolūkiem nesavietojamā veidā; turpmāka apstrāde arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos.*
Datu minimizēšana	*Ir adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos.*
Precizitāte	*Ir precīzi un, ja vajadzīgs, atjaunināti; ir jāveic visi saprātīgi pasākumi, lai nodrošinātu, ka neprecīzi personas dati, ņemot vērā nolūkus, kādos tie tiek apstrādāti, bez kavēšanās tiktu dzēsti vai laboti.*
Glabāšanas ierobežojums	*Tiek glabāti veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā; personas datus var glabāt ilgāk, ciktāl personas datus apstrādās tikai arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos saskaņā ar to, ka tiek īstenoti atbilstoši tehniski un organizatoriski pasākumi, kas šajā regulā paredzēti, lai aizsargātu datu subjekta tiesības un brīvības.*
Integritāte un konfidencialitāte	*Tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus.*
Pārskatatbildība	*Pārzinis ir atbildīgs par atbilstību tam, ka dati tiek apstrādāti likumīgi, godprātīgi un datu subjektam pārredzamā veidā, un var to uzskatāmi parādīt.*

4. Datu apstrādes mērķis un apjoms

4.1. SIA "CIETKOKS" (turpmāk - SIA) informācijas drošības sistēmas mērķis ir pasargāt SIA darbiniekus, partnerus un klientus no nelikumīgām vai kaitējošām personu tiešām vai netiešām, apzinātām vai neapzinātām darbībām, apstrādājot informāciju un datus, kas nonāk attiecīgo personu rīcībā, kā arī lietojot noteiktu aprīkojumu savu darba pienākumu izpildes vajadzībām.

4.2. Informācijas drošības politika (turpmāk - Politika) regulē informācijas apstrādi jebkādās sistēmās vai jebkādos nesējos, kas iesaistīti datu/informācijas apstrādē SIA, neatkarīgi no tā, vai datu/informācijas apstrāde ir saistīta ar SIA iekšējām darbības operācijām vai SIA ārējām attiecībām ar jebkādām trešajām pusēm.

4.3. Šī Politika regulē arī to, kā SIA Darbinieki lieto viņiem pieejamo aprīkojumu un rīkus, savu darba pienākumu veikšanas ietvaros.

4.4. Politika var būt piemērojama kopā ar jebkādām citām politikām, noteikumiem, procedūrām un/vai vadlīnijām, ko periodiski pieņem un ievieš SIA vadība.

4.5. Ar visiem informācijas drošības sistēmas jautājumiem un informācijas/datu drošības jautājumiem, kas nav atrunāti šajā Politikā, jāvēršas pie SIA *valdes priekšsēdētāja Viestura Vārpiņa.*

5. Informācijas klasifikācija

5.1. Jebkādu informāciju/datus, kas kļūst pieejami Darbiniekiem, veicot savus darba pienākumus, ja šāda informācija/dati ir saistīti ar SIA tās darbību un pakalpojumu sniegšanu, klientiem vai sadarbības partneriem, uzskata par SIA piederošu un konfidenciālu informāciju, ko, līdz ar to, aizsargā atbilstoši piemērojamie normatīvie akti par konfidenciālu informāciju un personas datu aizsardzību.

5.2. Lai nodrošinātu pienācīgu informācijas un datu aizsardzību, SIA veic iekšējo informācijas klasifikāciju. Informāciju/datus aizsargā neatkarīgi no tā, vai šāda informācija ir nonākusi Darbinieka rīcībā drukātu materiālu veidā, jebkādās datu uzglabāšanas ierīcēs, audio/video materiālu veidā vai jebkādā citā veidā.

5.3. SIA lieto šādu vispārīgu informācijas klasifikāciju:

Kategorija	***Apraksts***	***Piemērojamības apjoms (tostarp, bet ne tikai)***
Publiska informācija	*Informācija, kuru var apstrādāt un izplatīt SIA iekšienē vai ārpus tā, bez jebkādas negatīvas ietekmes uz SIA, jebkuru no tā partneriem, klientiem un /vai saistītajām pusēm.*	• Publiski finanšu pārskati, kurus sniedz valsts iestādēm; • Informācija, kas pieejama publiskos resursos vai ir kā citādi publiski zināma, ja vien tā nav kļuvusi publiski zināma dēļ tā, ka Darbinieks rīkojies, pārkāpjot informācijas/datu drošības prasības.
Iekšējā informācija	*Jebkāda informācija, kuras jebkāda veida lietošana, ja tas notiek, pārkāpjot piemērojamo normatīvo aktu, šīs Politikas vai jebkura cita SIA pieņemta regulējuma prasības, var kaitēt SIA un jebkura tā Darbinieka, p klientu vai partneru interesēm.*	• Jebkura SIA Darbinieka, struktūrvienības izstrādāti un sagatavoti dokumenti; • Jebkādi SIA darbības mērķiem izveidoti un lietoti katalogi (kontaktu, informācijas, u. tml.); • Jebkādi iekšēji dienesta ziņojumi, paziņojumi, izziņas, slēdzieni, kas izstrādāti SIA darbības vai pakalpojuma nodrošināšanas

		vajadzībām.
Konfidenciāla informācija	*Jebkāda informācija, kas ir tik būtiska SIA, jebkuram no tā klientiem un partneriem vai saistītajām pusēm, kuras neautorizēta izpaušana var negatīvi ietekmēt SIA, tā dalībnieku, klientu un sadarbības partneru darbību, operācijas, reputāciju, statusu kopumā, un šādas izpaušanas rezultātā jebkurai no šīm personām var tikt nodarīts nopietns kaitējums.*	• Informācija par klientiem, kas saņem medicīniskos pakalpojumus; • Politikas, procedūras, iekšējie noteikumi, vadības lēmumi; • Informācija, kas Darbiniekam norādīta kā SIA darbības noslēpums; • Cita finanšu, cilvēkresursu, juridiskas, mārketinga dabas informācija, pārdošanas procedūras, plāni un operācijas; • Biznesa, produkcijas plāni; • Personas identifikācijas dati; • Informācija, ko aizsargā katra Darbinieka parakstīta konfidencialitātes vienošanās; • Informācija, ko aizsargā konfidencialitātes vienošanās vai sadarbības līgumi, ko SIA ir noslēgusi savas darbības gaitā.

6. Datu informācijas apstrādē iesaistītās sistēmas

6.1. Jebkādas informācijas sistēmas, tostarp, bet ne tikai datortehnika, jebkāda veida programmatūra, operētājsistēmas, jebkādas uzglabāšanas vides, tīkla konti, elektroniskā pasta konti, pārlūku sistēmas un jebkāda cita tehniskā bāze un rīki, ko izmanto SIA darbībā vai pakalpojuma nodrošināšana, uzskatāmi par SIA īpašumu.

6.2. Ikvienam Darbiniekam ir pienākums lietot šādu tehnisko aprīkojumu un rīkus ar pienācīgu rūpību un uzmanību, un tikai ar SIA darbību saistītiem mērķiem. Vienīgais izņēmums ir gadījumi, kad SIA ir piešķīris Darbiniekam tehnisko aprīkojumu (piemēram mobilā tālruņa ierīci), sniedzot skaidru piekrišanu to lietot arī personīgām vajadzībām.

7. Datu aizsardzības speciālista pienākumi

7.1. Datu aizsardzības speciālista pienākums ir veikt sekojošus uzdevumus:

7.1.1. uzraudzīt Datu aizsardzības regulas prasību ievērošanu;

7.1.2. pārstāvēt SIA sadarbībā ar Datu valsts inspekciju;

7.1.3. nepieciešamības gadījumā konsultēt SIA vadību un darbiniekus;

7.1.4. ieteikt datu apstrādes aizsardzības sistēmas un kontroles uzlabošanu;

7.1.5. izveidot un uzturēt SIA apstrādes reģistru;

7.1.6. veikt novērtējumu jeb auditu atbilstoši SIA apstrādes prasībām;

7.1.7. veikt SIA darbinieku apmācību atbilstoši Datu aizsardzības prasībām;

7.1.8. veikt Datu apstrādes pārkāpuma identificēšanu un iespējamo seku novēršanu kā arī ziņošanu Datu valsts inspekcijai 72 stundu laikā.

8. Darbinieku pienākumi

8.1. Jebkāda informācija vai dati, kas nonāk Darbinieka rīcībā, pildot savus darba pienākumus, uzskatāmi par konfidenciāliem un lietojami kā konfidenciāli, ievērojot to aizsardzību saskaņā ar šo Politiku, un tos neizpauž nekādām trešajām pusēm, kamēr un ja vien Vadība nepaziņo, ka šāda informācija ir kļuvusi publiska vai ir kā citādi pārklasificēta par informāciju, kas vairs netiek aizsargāta šajā Politikā paredzētajā kārtībā.

8.2. Visus personas datus un citu informāciju, ar kuras palīdzību var identificēt fizisku personu, ievāc un apstrādā tikai, ja tas ir nepieciešams un ciktāl tas ir nepieciešams Darbinieka darba pienākumu veikšanas nolūkā, ar nosacījumu, ka šādas darbības tiek veiktas Darbiniekam piešķirto pilnvaru robežās un saskaņā ar likumā paredzētajām datu aizsardzības prasībām, jo īpaši, saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis, par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti.

8.3. Jebkādus datu pieprasījumus vai pieprasījumus par datu apstrādi, ko Darbinieks, veicot savus darba pienākumus, ir saņēmis no datu īpašniekiem – fiziskām personām, nekavējoties pārsūta turpmākai izskatīšanai Vadībai.

8.4. Ikvienam Darbiniekam ir pienākums ievērot šo Politiku, kā arī pildīt spēkā esošo vietējo, reģionālo vai starptautisko normatīvo aktu prasības, kas paredz datu vai informācijas apstrādes un aizsardzības nosacījumus. Politikas neievērošanu uzskata par būtisku noteiktās darba kārtības pārkāpumu un tā rezultātā, pēc SIA ieskatiem, Darbiniekam var piemērot disciplinārsodu vai atlaist Darbinieku no darba. Tas tāpat var izraisīt pārkāpumu pieļāvušā Darbinieka saukšanu pie administratīvās vai kriminālatbildības.

8.5. Ikvienam Darbiniekam ir pienākums, nosūtot e-pastu darbiniekiem, klientiem, sadarbības partneriem un trešajām personām, ja tas ir likumā noteiktā kārtībā, ar personas datu saturošu informāciju, e-pastam pievienot sekojošu informāciju:

E-pasts aizsargāts un tajā iekļautās informācijas apstrāde, ja tā saistās ar personas datiem, izmantojama un apstrādājama atbilstoši Eiropas Parlamenta un Padomes Regulai (ES) 2016/679 (2016. gada 27. aprīlis).

9. Piekļuves un aizsardzības pārvaldība

9.1. Darbinieki var piekļūt jebkādām Darbiniekiem pieejamām ierīcēm, ja tas nepieciešams attiecīgo Darbinieku darba pienākumu veikšanas vajadzībām, atbildības ietvaros un uz zinātvajadzības pamata. Piekļuves tiesības jebkādai sistēmai nenozīmē, ka Darbinieks ir pilnvarots apskatīt vai lietot visu attiecīgajā sistēmā esošo informāciju.

9.2. Izmantotie lietotāja ID ir unikāli un identificē konkrētu Darbinieku. Ikviens Darbinieks atbild par visām darbībām kas saistītas ar viņa vai viņas personīgo ID kontu, līdz ar to, primārais pienākums ir nodrošināt, lai Darbinieka ID nebūtu pieejams nekādām trešajām pusēm un pat ne citiem Darbiniekiem, ja vien SIA nav noteikusi citu kārtību.

9.3. Sistēmas drošības paroles, 8 (astoņi) simboli, izveido ar pienācīgu rūpību, ar nosacījumu, ka tās nevar viegli atminēt, tās neietver personas datus un tās tiek regulāri mainītas (vismaz reizi 3 (trīs) mēnešos). Ikviens Darbinieks personīgi atbild par savas drošības paroles atbilstību šai Politikai un jebkādiem citiem SIA noteikumiem.

9.4. Darbinieks piekļūst datiem vai konfidenciālai informācijai tikai tad, ja šādas pilnvaras ir paredzētas attiecīgā Darbinieka Darba līgumā, vai ja SIA ir piešķīris Darbiniekam šādas pilnvaras ar pilnvarojumu.

10. Drošības pasākumi

10.1. Visiem jebkādā formā (drukātā, elektroniskā, u.tml.) ievāktiem un apstrādātiem datiem un informācijai piemērojamas šīs Politikas un jebkāda normatīvā regulējuma prasības attiecībā uz datu, informācijas ievākšanu, apstrādi, aizsardzību un uzglabāšanu, un šādus dokumentus uzglabā SIA norādītā, drošā vietā ar tādu uzglabāšanas termiņu, kādu paredz piemērojamie likumi vai norāda SIA.

10.2. Darbiniekiem aizliegts glabāt jebkādu konfidenciālu informāciju savās ierīcēs, izņemot informāciju, kas ir īslaicīgi nepieciešama konkrētai, ar darbu (proti sniedzamo pakalpojumu) saistītai darbībai. Visa nepieciešamā konfidenciālā un personīgi identificējamā informācija jāuzglabā tikai SIA IT personāla vai apkalpojošā uzņēmuma apstiprinātā mākoņa krātuvē un SIA iekštīklā. Ir jāizvairās no jebkādas šādu datu lejupielādēšanas vietējās ierīcēs un tas jādara tikai, ja tas ir pamatoti nepieciešams saistībā ar informācijas apstrādi darba (proti sniedzamo pakalpojumu) vajadzībām.

10.3. Pienācīgi pilnvarots SIA IT personāls ir tiesīgs filtrēt un pārraudzīt Darbinieku interneta piekļuvi un Darbinieku internetā veiktās darbības saskaņā ar piemērojamo normatīvo aktu prasībām.

10.4. Jebkurām mobilajām, portatīvajām ierīcēm (tostarp, klēpjdatoriem, planšetēm, viedtālruņiem un citām plaukstdatoru ierīcēm), kā arī jebkādām mākoņa informācijas uzglabāšanas vietām jābūt apstiprinātām no SIA IT personāla puses un pienācīgi aizsargātām, lai novērstu neautorizētu piekļuvi.

10.5. SIA lietotajā aprīkojumā un rīkos var instalēt un lietot tikai SIA licencētas un autorizētas sistēmas un programmatūru. Pirms jebkādas programmatūras lejupielādēšanas vai instalēšanas Darbiniekiem piederošās un lietotās ierīcēs šajā Politikā aprakstītajiem mērķiem, ir jāsaņem IT personāla atļauja.

10.6. Gadījumos, kad Darbinieki lieto personīgās (mājas) ierīces, lai piekļūtu SIA korporatīvajiem resursiem (piemēram, klientu datiem, elektroniskais pasts, tiešsaistes, mākoņa datubāzes), Darbiniekiem ir pienākums ievērot šīs Politikas prasības tieši tāpat kā ja viņi lietotu SIA nodrošināto aprīkojumu. Līdz ar to, ierīcē ir aizliegts glabāt jebkādus ar SIA saistītus datus un informāciju; jebkāda datu apstrāde ir pieļaujam tikai ar SIA lietoto mākoņa un tiešsaistes glabāšanas vietu starpniecību.

10.7. Jebkurā gadījumā, ir stingri aizliegts izmantot publiskas piekļuves ierīces (piemēram, interneta kafejnīcās, bibliotēkās, u.tml.), ja vien tas nav kritiski un steidzami nepieciešams saistībā ar darbu un Darbinieka Tiešais vadītājs ir sniedzis skaidru rakstveida piekrišanu šādai darbībai.

10.8. Gadījumā, ja Darbiniekam tiek piešķirtas tiesības piekļūt SIA klienta, datņu glabāšanas sistēmai, Darbiniekam ir pienākums lietot klienta piešķirtos piekļuves rīkus un ievērot sniegtos norādījumus par drošas informācijas, datu apstrādes prasībām (tostarp, šifrēšanas sistēmu, paroļu lietošana, datu lietošanas ierobežojumi, īpaši paredzētu atrašanās vietu lietošana, u.tml.).

10.9. Tiklīdz, pēc SIA ieskatiem, aizsargātie dati, informācija vairs nav nepieciešama SIA darbībai, šādus datus vai informāciju dzēš, iznīcina visas to kopijas, un attiecīgās informācijas datu apstrādē iesaistītos Darbiniekus attiecīgi informē par viņu pienākumu dzēst vai iznīcināt un nodot atpakaļ SIA informāciju vai datus, kas viņiem vairs nav nepieciešami savu darba pienākumu veikšanai, un, jo īpaši, atdot atpakaļ SIA, dzēst un iznīcināt kopijas, ja ar attiecīgo Darbinieku tiek izbeigtas darba tiesiskās attiecības.

10.10. Nekādu šajā Politikā minēto informāciju vai datus nenosūta, nepārsūta un nekādā citā veidā neiesniedz Trešajai pusei, ja vien tas nav nepieciešams Darbinieka darba pienākumu (proti sniedzamo pakalpojumu) izpildei, un tikai ciktāl tas ir nepieciešams šādu pienākumu izpildei. Gadījumā, ja datus pārsūta vai iesniedz Trešajām pusēm, ir noteikti jānodrošina datu aizsardzība un jāveic visi atbilstošie drošības pasākumi.

10.11. SIA auditē informācijas un datu apstrādē pielietotās sistēmas, lai kontrolētu nepārtrauktu atbilstību šai Politikai un piemērojamajām normatīvajām prasībām.

11. Informācija, kas jāsniedz datu subjektam, iegūstot personas datus

11.1. Iegūstot personas datus no datu subjekta, datu subjektam pirms personas datu iegūšanas, tiek sniegts sekojoša informācija:

Pārzinis	*Pārziņa nosaukums*
Datu aizsardzības speciālists	*Speciālista vārds, uzvārds*
Personas datu apstrādes nolūks	*Kādam mērķim dati tiek vākti*
Personas datu apstrādes juridisks pamatojums	*Likumiskais, līgumiskais vai cits tiesiskais pamatojums*
Personas datu apstrādes ieguves avoti	*Kas datus nodod, vai no kurienes dati saņemti*
Personas datu kategorijas	*Piemēram, vārd, uzvārds, personas kods u.c.*
Personas datu glabāšanas ilgums	*Norāde par to, cik ilgi dati tiek glabāti*
Personas datu saņēmēji	*Kas būs tās fiziskās vai juridiskās personas, kas datus saņems*
Datu subjekta tiesības	*Subjekta tiesības saņemt izziņu par datu apstrādi, kā arī datus labot, mainīt, dzēst u.c.*

12. Aizliegtās darbības

12.1. Izņemot īpaši paredzētus izņēmumus, nekādu SIA, tā klientiem vai sadarbības partneriem piederošu aprīkojumu, sistēmas vai rīkus nekādā gadījumā un nekādos apstākļos nedrīkst izmantot ar Darbinieka darba pienākumiem vai ar SIA darbību nesaistītiem mērķiem.

12.2. Turpmāk minētās darbības ir stingri aizliegtas, bez izņēmumiem:

12.2.1. Jebkuras personas vai uzņēmuma ar intelektuālā īpašuma tiesībām aizsargātu tiesību pārkāpšana, tostarp, bet ne tikai jebkādas nelegālas programmatūras, tiešsaistes platformu, jebkādu citu elektronisko saturu, kurus SIA nav licencēta lietot, uzstādīšana, kopēšana, izplatīšana vai uzglabāšana jebkādās SIA sistēmās vai aprīkojumā;

12.2.2. Ar autortiesībām aizsargātu materiālu neautorizēta kopēšana;

12.2.3. Jebkuras personas tiesību aizskaršana, pārmērīgi un bez vajadzības ievācot un apstrādājot attiecīgā subjekta personas datus;

12.2.4. Piekļuve datiem, serverim vai kontam tādiem mērķiem, kas nav saistīti ar SIA darbību (proti sniedzamo pakalpojumu) vai attiecīgā Darbinieka darba pienākumu veikšanu;

12.2.5. Programmatūras, tehniskās informācijas, šifrēšanas programmatūras vai tehnoloģijas eksportēšana, pārkāpjot piemērojamos starptautiskos vai nacionālos normatīvos aktus vai SIA norādījumus;

12.2.6. Jebkādu datu vai informācijas, kurai ir īpašuma vai konfidenciāla vērtība SIA, informācijas eksportēšana, ja šāda eksportēšana nav nepieciešama SIA darbības (proti sniedzamo pakalpojumu) vai Darbinieka darba pienākumu veikšanas gaitā, vai, ja tā pārkāpj SIA iekšējos noteikumus, piemērojamos normatīvos aktus;

12.2.7. Darbinieka konta paroles atklāšana citām personām un citu personu pielaišana lietot šādu kontu (tostarp, bet neaprobežojoties ar Darbinieka ģimenes locekļiem);

12.2.8. Krāpniecisku pakalpojumu piedāvājumu izveide, izmantojot SIA kontu;

12.2.9. Tīkla sakaru drošības pārkāpumu vai pārtraukumu īstenošana. Šādi drošības pārkāpumi iekļauj, bet tie neaprobežojas ar piekļuvi datiem, ja Darbinieks nav to paredzētais saņēmējs, vai pierakstīšanos serverī vai kontā, kuram Darbinieks nav skaidri pilnvarots piekļūt, ja vien šādas piekļuves tiesības nav piešķirtas Darbiniekam saistībā ar attiecīgā Darbinieka dalību konkrētā SIA projektā;

12.2.10. Jebkādas programmas, skripta, komandas lietošana vai jebkāda veida ziņojuma nosūtīšana, ar nolūku ar jebkādiem līdzekļiem traucēt vai atspējot lietotāja darba sesiju.

13. Personas datu apstrādes politikas aktualizācija

13.1. Visas SIA izstrādātās procedūras saistībā ar personas datu apstrādi, šīs Politikas pielikumi, papildinājumi vai cita Darbiniekiem pieejamā informācija saistībā ar datu apstrādi, kā arī SIA interneta vietnēs publicētā informācija ir šīs Politikas neatņemama sastāvdaļa.

13.2. Politika tiek aktualizēta un ja nepieciešams, atjaunota vienu reizi gadā. Izstrādāto politiku apstiprina SIA valdes priekšsēdētājs un tajā iekļauto norādījumu izpilde kļūst obligāta visiem SIA darbiniekiem.

13.3. Pēc Politikas aktualizēšanas veikšanas ar aktuālo redakciju iepazīstina visus SIA Darbiniekus.

14. Ziņošana par drošības incidentiem

14.1. Par visiem informācijas un datu apstrādes drošības incidentiem vai iespējamiem incidentiem nekavējoties ir jāziņo Vadībai, kura, attiecīgi, veic visus pasākumus iespējamā kaitējuma novēršanai, radītā kaitējuma seku likvidēšanai un iepriekšējā drošības stāvokļa atjaunošanai.

14.2. Vadībai ir pienākums nodrošināt turpmāku ziņošanu par datu vai informācijas drošības pārkāpumu iestādēm un iesaistītajām fiziskajām personām, kā to paredz piemērojamie normatīvie akti un Eiropas Savienības likumi.

14.3. Datu aizsardzības speciālists dokumentē visus personas datu aizsardzības pārkāpumus, norādot faktus, kas saistīti ar personas datu pārkāpumu, tā sekas un veiktās koriģējošās darbības. Minētā dokumentācija ļauj Datu valsts inspekcijai pārbaudīt šā panta ievērošanu.

14.4. Gadījumā, ja personas datu aizsardzības pārkāpums varētu radīt augstu risku fizisku personu tiesībām un brīvībām, pārzinis bez nepamatotas kavēšanās paziņo datu subjektam par personas datu aizsardzības pārkāpumu.

14.5. Personas datu aizsardzības pārkāpuma gadījumā Pārzinis bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms, paziņo par personas datu aizsardzības pārkāpumu Datu valsts inspekcijai. Ja paziņošana uzraudzības iestādei nav notikusi 72 stundu laikā, paziņojumam pievieno kavēšanās iemeslus.

Valdes priekšsēdētājs Viesturs Vārpiņš */paraksts/*

Datu aizsardzības speciāliste Daiga Reča /paraksts/
(Personas datu aizsardzības speciālista apliecības Nr. 416, derīga līdz 2023.gada 19.aprīlim).

Kandavā, 2021.gada 28.janvārī.