APSTIRINĀTS

ar SIA "Ķekavas nami"

Reģ. Nr. 40003359306

valdes lēmumu Nr.3 (protokols Nr.1-2020)

2020.gada 14.janvārī.

IEKŠĒJIE DATU APSTRĀDES UN INFORMĀCIJAS AIZSARDZĪBAS NOTEIKUMI

Lietotie termini un saīsinājumi

Auditācijas pieraksti – analīzei pieejami pieraksti, kuros reģistrēti dati par noteiktiem notikumiem IS (piekļuve, datu ievade, maiņa, dzēšana, izvade u.c.).

Autorizēts lietotājs – tāds autentificēts lietotājs, kuram ir pieejas tiesības attiecīgai IS.

Ārpakalpojuma sniedzējs IT un IS pārvaldībā - trešā persona, kura pamatojoties uz ar Uzņēmumu noslēgto pakalpojuma sniegšanas līgumu nodrošina Uzņēmuma IT un IS pārvaldību, attīstību, drošību, auditu, kā arī sniedz Uzņēmumam citus līgumā norādītos pakalpojumus saistītus ar IS drošību.

Darbinieks – Uzņēmuma darbinieks, kura amata aprakstā norādītajos amata pienākumos ietilpst fizisko personu datu apstrāde, un kurš atbild par tās nodrošināšanu atbilstoši Latvijas Republikas normatīvo aktu regulējumam fizisko personu datu aizsardzības jomā un Uzņēmuma iekšējiem normatīvajiem aktiem.

Informācijas (datu) nesējs – Informācijas uzglabāšanas vai pārraides kanāls (piem., zibatmiņas, CD/DVD diski, disketes, iekšējie/ārējie cietie diski, magnētiskās lentes, video kartes u.tml.)

Informācija – šo Noteikumu ietvaros jebkāda veida informācija elektroniskā vai papīra formātā, kas satur visa veida Uzņēmuma apstrādāto informāciju, t.sk., fizisko personu datus.

Informācijas resursi – informācijas vienības, kurās ietilpst datu faili, kas satur IS glabājamo, apstrādājamo un IS lietotājiem pieejamo informāciju, kā arī visi IS ievades un izvades dokumenti, neatkarīgi no Informācijas (datu) nesēja veida.

Informācijas tehnoloģijas (IT) – metožu un instrumentu kopums attēlu, teksta, skaņas un cita veida informācijas apstrādei, iegūšanai, uzglabāšanai un izplatīšanai ar mikro elektroniski balstītu skaitļošanas un telekomunikāciju kombināciju. Pamatā tā ir datoru izmantošana informācijas apstrādei jebkurā vietā un laikā.

Informācijas resursu turētājs – Uzņēmuma darbinieks, kurš ir atbildīgs par Informācijas resursiem (to pieejamību, integritāti, konfidencialitāti, lietošanu un lietošanas sekām) un kura pienākumi ir noteikti Uzņēmuma iekšējos normatīvajos aktos, t.sk., šajos Noteikumos.

Informācijas sistēma/-as (IS) – datu ievadīšanas, uzglabāšanas un apstrādes datorizēta sistēma, kas paredz Lietotāju pieeju tajā glabātajiem datiem vai informācijai.

Ierobežotas pieejamības informācija – iekšējās aprites informācija, kurai Informācijas resursu turētājs ir noteicis pieejas pilnvaroto personu loku.

Incidents – gadījums, kurā IS apdraudējumi ir negatīvi ietekmējuši IS darbību, izmantojot tās trūkumus.

Integritāte – raksturo, cik lielā mērā informācija tiek uzglabāta un/vai pārraidīta pilnīga, precīza, patiesa un aktuāla.

Konfidencialitāte – īpašība, ka informācija nav pieejama vai netiek atklāta nepilnvarotām personām.

Komercnoslēpums – visa veida ekonomiska, tehniska, saimnieciska rakstura Uzņēmuma informācija, lietas vai ziņas, kas fiksētas rakstveida vai citādā veidā, izņemot Uzņēmuma gada pārskatā sniegto informāciju.

Lietotājs – persona, kurai piešķirtas IS lietotāja tiesības un kura ir atbildīga par visām darbībām, kuras veiktas IS ar tās lietotāja vārdu.

Noteikumi – Uzņēmuma iekšējie datu apstrādes un informācijas aizsardzības noteikumi.

Tehniskie resursi – programmatūra (izpildāms programmas kods un konfigurācijas faili, kas nodrošina IS funkcionēšanu), datori, datortīklu aparatūra, video sistēmas, komunikāciju līnijas u.c. tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei un glabāšanai.

Tehnisko resursu turētājs – Uzņēmuma darbinieks, kurš ir atbildīgs par Tehnisko resursu uzturēšanu un drošību.

Uzņēmums – Sabiedrības ar ierobežotu atbildību "Ķekavas nami".

I. Vispārīgie jautājumi

1. Šie Noteikumi ir izstrādāti atbilstoši Latvijas Republikas normatīvajos aktos noteiktajām prasībām personas datu aizsardzības jomā un attiecas uz visa veida Informāciju, kas satur Uzņēmuma komercnoslēpumu un Uzņēmumā apstrādātos personas datus, izmantojot Tehniskos un Informācijas resursus, saņemot, filmējot, reģistrējot, ievadot, uzglabājot, sakārtojot, pārveidojot, izmantojot, pārsūtot, kopējot, nododot, izdrukājot, pārraidot, izpaužot, bloķējot, dzēšot iepriekšminēto Informāciju un ne tikai.
2. Noteikumi nosaka:
   2.1. vispārējos principus un regulējumu Uzņēmuma Informācijas komercnoslēpuma un konfidencialitātes, integritātes un pieejamības jomā, kuru piemērošana ierobežo ar Informācijas sistēmu saistītos riskus;
   2.2. par Informācijas resursiem, Tehniskajiem resursiem un personas datu aizsardzību atbildīgās personas, to tiesības un pienākumus;
   2.3. personas datu klasifikāciju atbilstoši to vērtības un konfidencialitātes pakāpei;
   2.4. Tehniskos resursus, ar kādiem tiek nodrošināta personas datu apstrāde;
   2.5. personas datu apstrādes organizatorisko procedūru, nosakot personas datu apstrādes laiku, vietu un kārtību;
   2.6. pasākumus, kas veicami Tehnisko resursu aizsardzībai pret ārkārtas apstākļiem;
   2.7. līdzekļus, ar kādiem nodrošina Tehniskos resursus pret tīšu bojāšanu un neatļautu iegūšanu;
   2.8. Informācijas (datu) nesēju glabāšanas un iznīcināšanas kārtību;
   2.9. paroles garumu un uzbūves nosacījumus;
   2.10. paroles lietošanas kārtību, kā arī laika posmu, pēc kura parole nomaināma;
   2.11. rīcību, ja parole vai kriptoatslēga kļuvusi zināma citai personai;
   2.12. personas datu lietotāju tiesības, pienākumus, ierobežojumus un atbildību;
   2.13. personas datu aizsardzības pārkāpumu procedūru.

3. Noteikumi izstrādāti ar mērķi nodrošināt Uzņēmuma Darbinieku izpratni par Informācijas, kas satur fizisko personu datus, apstrādes, drošības, aizsardzības un komercnoslēpuma jautājumiem.
4. Personu datu apstrāde Uzņēmumā tiek veikta šādiem mērķiem:
   4.1. pakalpojumu sniegšanai, preču ražošanai un tirdzniecībai;
   4.2. noziedzīgu nodarījumu novēršanai vai atklāšanai saistībā ar īpašuma aizsardzību un personu vitāli svarīgu interešu, tajā skaitā dzīvības un veselības, aizsardzību.
5. Noteikumi ir saistoši visiem Uzņēmuma Darbiniekiem, lai aizsargātu Uzņēmuma komercnoslēpumu un nodrošinātu fizisko personu datu apstrādi un aizsardzību.
6. Uzņēmuma darbinieks – valdes loceklis nodrošina, ka Uzņēmuma Darbinieks pēc iepazīšanās ar šiem Noteikumiem paraksta apliecinājumu (šo Noteikumu Pielikums Nr.1) par šajos Noteikumos norādīto prasību ievērošanu un pievieno to katra Uzņēmuma Darbinieka personīgajai lietai.

II. Atbildīgās personas par Informācijas resursiem, Tehniskajiem resursiem un personas datu aizsardzību, to tiesības un pienākumi

7. Par Informācijas resursiem atbildīgā persona Uzņēmumā ir valdes priekšsēdētājs.
8. Uzņēmuma valdes priekšsēdētājs:
   8.1. norīko Uzņēmumā ar rīkojumu darbinieku, kura pārziņā ir IS kā Informācijas resursu turētājam, vai slēdz līgumu ar Ārpakalpojuma sniedzēju;
   8.2. piedalās Uzņēmuma risku analīzes veikšanā, kas attiecas uz konkrētā Informācijas resursu turētāja pārziņā esošo IS.

15. Tehnisko resursu turētājs ir tiesīgs:
   15.1. brīvdienās un ārpus oficiālā darba laika atslēgt Tehniskos resursus, izņemot videonovērošanas sistēmu, lai veiktu uzturēšanas darbus, 3 darba dienas iepriekš par to brīdinot Lietotājus;
   15.2. atslēgt Tehniskos resursus un apturēt Informācijas resursu darbu arī darba laikā, ja noticis incidents (ja iespējams, iepriekš par to brīdinot Lietotājus pa telefonu vai e-pastu).

16. Par personas datu aizsardzību atbildīgā persona Uzņēmumā ir valdes priekšsēdētājs, kurš:
   16.1. atbild par Uzņēmumā veikto personas datu apstrādes atbilstību normatīvo aktu prasībām personu datu aizsardzības jomā;
   16.2. sadarbojas ar Informācijas un Tehnisko resursu turētājiem, lai īstenotu Uzņēmumā datu aizsardzības prasības.

III. Personas datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes līmenim

17. Uzņēmums veic visas Uzņēmumā esošās informācijas klasifikāciju ar mērķi novērtēt šādas informācijas nozīmību pēc konfidencialitātes, vērtības un pieejamības, tādējādi nodrošinot katras informācijas grupas aizsardzību atbilstoši tās klasifikācijas līmenim.
18. Visa informācija, kas attiecas uz personu datu apstrādi Uzņēmumā, tai skaitā, kas attiecas uz visu apstrādāto informāciju Uzņēmumā, tiek klasificēta:
   18.1. publiska informācija (P), kas nav svarīga konfidencialitātes aspektā un ir brīvi pieejama Uzņēmuma darbiniekiem, jebkurai personai vai organizācijai, kas to ir pieprasījusi; šādas informācijas izplatīšana neietekmē Uzņēmumu negatīvā veidā;

18.2. ierobežotas pieejamības informācija (I), kas ir svarīga konfidencialitātes aspektā un šāda informācija ir pieejama tikai Uzņēmuma pilnvarotajiem darbiniekiem;
18.3. komercnoslēpums – visa veida ekonomiska, tehniska, saimnieciska rakstura Uzņēmuma informācija, lietas vai ziņas, kas fiksētas rakstveida vai citādā veidā, izņemot Uzņēmuma gada pārskatā sniegto informāciju;
18.4. Informācijas vērtības (V) līmeni atkarībā no kaitējuma, kas varētu būt nodarīts Uzņēmumam, ja netiktu nodrošināta Informācijas resursu integritāte:

20.4.1. V1 –augstas vērtības informācija;
20.4.2. V2 – vidējas vērtības informācija;
20.4.3. V3 - zemas vērtības informācija.

21. Informācija, kura nav klasificēta atbilstoši konfidencialitātes principiem, automātiski tiek uzskatīta par ierobežotas pieejamības informāciju.
22. Personas datu klasifikāciju atbilstoši tās vērtības un konfidencialitātes līmenim skatīt šo Noteikumu Pielikumā Nr.2, kas ir šo Noteikumu neatņemama sastāvdaļa.

IV. Tehniskie resursi, ar kādiem tiek nodrošināta personas datu apstrāde Uzņēmumā

23. Personas datu apstrāde Uzņēmumā tiek nodrošināta, izmantojot sekojošus Tehniskos resursus:
23.1. serverus;
23.2. tīklu infrastruktūru (datortīkla iekārtas – maršrutētājus u.c.);
23.3. darbstacijas (portatīvos un personālos datorus, printerus, sistēmprogrammas, lietojumprogrammas, palīgprogrammas, sistēmfailus);
23.4. Informācijas (datu) nesējus;

V. Informācijas apstrāde

24. Darbinieki, kuriem darba pienākumu veikšanai iekārtota darba vieta, jānodrošina darba vietas organizācija atbilstoši konfidencialitātes un drošības apsvērumiem.
25. Darbiniekam, kura rīcībā ir konfidenciāla informācija, jāapzinās, ka tā viņam uzticēta tikai tiešo darba pienākumu veikšanai un to nedrīkst izmantot personīgām interesēm, kā arī tīši vai netīši nodot personām, kuras nav tiesīgas to saņemt gan Uzņēmumā, gan ārpus tā.
26. Darbiniekiem, pildot savus tiešos darba pienākumus, ir jānodrošina pareiza rīcība, strādājot ar informāciju – ir jāaizsargā Uzņēmuma konfidenciālā digitālā vai dokumentētā informācija, ko tie lieto vai glabā savās darba vietās.

<u>Dokumentētā informācija</u>

27. Darbinieka darba vietā ārpus darba laika, kā arī laikā, kad Darbinieks atstājis savu darba vietu, nedrīkst atrasties brīvi pieejama Uzņēmuma dokumentēta informācija.
28. Uzņēmuma dokumentiem, kas satur jebkāda veida personas datu informāciju, jāatrodas glabāšanai piemērotos, slēdzamos skapjos, atvilktnēs vai seifos. Ja darba vietā nav piemērotu dokumentu glabāšanas mēbeļu, Darbinieka pienākums par to paziņot savam tiešajam vadītājam.

29. Dokumenti jāizmanto tikai darba vajadzībām un pēc to lietošanas jānovieto atbilstošā dokumentu lietā saskaņā ar lietu nomenklatūru un jāglabā atkarībā no to konfidencialitātes pakāpes.
30. Darbiniekam ir aizliegts iznest ārpus Uzņēmuma ar Uzņēmuma darbību saistītus dokumentus, ja tas nav nepieciešams tiešo darba pienākumu veikšanai un nav saskaņots ar tiešo vadītāju.
31. Laikā, kad Darbinieks pieņem apmeklētāju, darba vietā drīkst atrasties tikai dokumenti, kas attiecas uz izskatāmo jautājumu. Darbiniekam jānodrošina, lai pieņemot apmeklētājus, netiktu pārkāpti konfidencialitātes un drošības noteikumi.
32. Nav pieļaujama dokumentu atstāšana printeros, kopētājos, faksa aparātos. Darbinieks katras darba dienas beigās pārbauda šādas ierīces, vai tajās neatrodas ierobežotas pieejamības dokumenti.
33. Ierobežotas pieejamības informācija, kas atrodas uz tāfelēm vai flipčartiem pēc lietošanas ir jānodzēš;
34. Dokumentētā informācija ir jāiznīcina, izmantojot dokumentu smalcināšanas iekārtas vai jānovieto speciāli šim mērķim paredzētos drošos konteineros, kurus nodrošina Saimniecības daļa.
35. Darbiniekam aizliegts glabāt Uzņēmuma dokumentu oriģinālus vai to kopijas savā dzīvesvietā, automašīnā vai citā dokumentu glabāšanai nepiemērotā vietā ārpus Uzņēmuma telpām. Ja Darbiniekam ir pamatotas aizdomas, ka dokuments ir nokļuvis nepiederošu personu valdījumā, par to jāziņo tiešajam vadītājam.
36. Darbiniekam jāizvairās no nevajadzīgas dokumentu kopiju vai izdruku izgatavošanas. Kopijas jāizgatavo tikai darba vajadzībām un visi liekie vai novecojušie kopiju eksemplāri jāiznīcina speciālās dokumentu smalcināšanas iekārtās. Darbam ar dokumentiem jāizmanto tikai Uzņēmuma telpās esošās kopēšanas un dokumentu smalcināšanas iekārtas.
37. Drošības nolūkos Darbiniekam aizliegts darba vietā atstāt redzamā, pieejamā vietā atslēgas no darba skapjiem un seifiem.

Digitālā informācija

38. Lietojot Tehniskos resursus, Darbiniekam jāseko, lai nenotiktu datu neautorizēta nolasīšana, kopēšana, fotografēšana, filmēšana vai pārnešana.
39. Darbinieka pienākums ir nodrošināt sevis noteikto piekļuves paroļu, ar kurām iespējama piekļuve Uzņēmuma IS, aizsardzību un konfidencialitāti,.
40. Darbiniekam bez saskaņošanas ar IS un IT, aizliegts pievienot Uzņēmuma datortīklam jebkādas iekārtas un izmantot jebkādus Informācijas (datu) nesējus.
41. Darbiniekam aizliegts iepazīstināt trešās personas, izņemot Ārpakalpojuma sniedzējus ar Uzņēmuma IS, lietojamajām datorprogrammām, failu struktūru vai komunikāciju veidiem.
42. Atstājot darba vietu, Darbiniekam obligāti jābloķē pieeja datoram, to aizslēdzot, lai apkārtējie, t.sk., nepiederošas personas nevarētu iepazīties ar dokumentu saturu vai izmantot to.
43. Atstājot Uzņēmuma telpas, dators ir jāizslēdz, vai jāatstāj miega režīmā. Pirms nedēļas nogales vai dodoties ilgstošā prombūtnē dators ir jāizslēdz.
44. Darbiniekiem, kuru rīcībā ir datortehnika, jālieto tikai Uzņēmuma apstiprinātais programmnodrošinājums. Aizliegts instalēt programmas, kuru izcelsme un nozīme nav saskaņota ar Tehnisko resursu turētāju vai tās pilnvarotu personu.
45. Darbiniekiem ir pienākums informēt Tehnisko resursu turētāju par jebkuriem IS drošības incidentiem un apdraudējumiem.
46. Darbiniekiem var tikt piemērots disciplinārsods par ar IS saistīto darbību reglamentējošo pasākumu neievērošanu.
47. Darbinieks ir atbildīgs par visām darbībām, kuras IS ir veiktas ar viņa Lietotāja vārdu.

Darbinieku personīgās sarunas un korespondence

48. Uzņēmuma telpās darba laikā Darbinieki organizē tikšanās tikai darba pienākumu ietvaros un apjomā.
49. Darbinieki apzinās un ir informēti, ka Uzņēmuma telpās tiek veikta telefonsarunu ierakstīšana ar mērķi veikt Uzņēmuma klientu apkalpošanas līmeņa kvalitātes novērtējumu.
50. Darbiniekiem Uzņēmuma telpās stingri aizliegts veikt video filmēšanu vai fotografēšanu bez valdes priekšsēdētāja attiecīgas atļaujas.
51. Lietojot e-pastu Lietotāja elektroniskā sūtījuma apjoms nedrīkst pārsniegt 500 MB. Lietotājam aizliegts atkārtoti sūtīt elektronisko sūtījumu, ja ir saņemts paziņojums, ka adresāts nevar saņemt sūtījumu e-pasta servera limita pārsniegšanas dēļ.
52. Lietotājam ir aizliegts:
    52.1. atvērt neskaidras izcelsmes e-pasta sūtījumus (piemēram, Uzņēmuma darbības specifikai neatbilstoši temati laukā "Temats", pievienota nezināma formāta datne vai izpildāmā datne, interneta saites vēstules saturā), it īpaši, ja par bīstamo datņu veidiem saņemts brīdinājums no Tehnisko resursu turētāja. Lietotājam par šādiem e-pasta sūtījumiem nekavējoties jāinformē Tehnisko resursu turētājs;
    52.2. e-pasta sūtījumam pievienot izpildāmās datnes (piemēram, .shs, *.vbs).
    52.3. e-pasta Lietotājs, regulāri dzēšot nevajadzīgo informāciju, kontrolē, lai tā pastkastes kopapjoms serverī nepārsniegtu 5 Gb, ja IS nav noteikts citādi, pretējā gadījumā, ja pastkastes kopapjoms pārsniedz minēto apjomu, Tehnisko resursu turētājs drīkst bloķēt Lietotāja e-pasta kontu.

VI. Pasākumi, kas veicami Tehnisko resursu aizsardzībai pret ārkārtas apstākļiem

53. Uzņēmums risku pārvaldīšanas ietvaros veic Tehnisko resursu fiziskās aizsardzības pasākumus, kas aizsargā tos pret fiziskas iedarbības radītu apdraudējumu (piemēram, ugunsgrēks, plūdi, elektropadeves traucējumi, Tehnisko resursu tīši vai netīši bojājumi, zādzība, ekspluatācijas noteikumiem neatbilstošs mitrums un gaisa temperatūras svārstības).
54. Tīklu infrastruktūras, t.sk., komunikāciju tīklu aparatūras, kabeļu tīkla aizsardzībai Uzņēmums ir nodrošinājis tās pietiekamu fizisko aizsardzību to izvietojot tā, lai tai nevarētu nesankcionēti un nemanīti piekļūt, pieslēgties vai bojāt ar Uzņēmumu nesaistītas personas un Uzņēmuma nepilnvaroti darbinieki.

VII. Līdzekļi, ar kādiem nodrošina Tehniskos resursus pret tīšu bojāšanu un neatļautu iegūšanu IS

55. Datorvīrusu darbības novēršanai lieto speciāli šim nolūkam paredzētu programmatūru, visiem datoriem uzstādot pastāvīgu antivīrusu programmatūru (piem., McAfee VirusScan).
56. Lietotājam ieslēdzot datoru, notiek automātiska pretvīrusa programmatūras palaišana.

Rezerves kopijas

57. Uzņēmums regulāri veic svarīgāko Informācijas resursu un programmatūru rezerves datu kopēšanu. Rezerves datu kopēšanu nodrošina Tehnisko resursu turētājs, saskaņojot rezerves datu kopēšanas biežumu un apjomu ar Informācijas resursu turētāju.

58. Ne retāk kā reizi gadā, Tehnisko resursu turētājs sadarbībā ar Informācijas resursu turētāju, veic pārbaudes, lai pārliecinātos, ka rezerves datu kopijas tiek sagatavotas kvalitatīvi un no tām ir iespējams atjaunot IS darbību.

VIII. Informācijas (datu) nesēju glabāšanas un iznīcināšanas kārtība

59. Informācijas (datu) nesēju fiziskās aizsardzības nodrošināšanai Uzņēmums nodrošina, ka neatkarīgi no Informācijas (datu) nesēja veida Informācijas (datu) nesējus, kas satur informāciju, lietot drīkst tikai Uzņēmuma pilnvaroti Darbinieki, kuriem ir pieeja Informācijas resursiem.
60. Informācijas (datu) nesēju aizsardzības ietvaros Uzņēmums veic Tehnisko resursu datu ievades un izvades iekārtu fizisko aizsardzību, novēršot nesankcionētu Informācijas (datu) nesēju pieslēgšanu Tehniskajiem resursiem un to lietošanu, ja tā nav nepieciešama Lietotāja pienākumu veikšanai.
61. Lietotājam Informācijas (datu) nesējus ar klasificētiem Informācijas resursiem aizliegts atstāt nedrošās (piemēram, publiski pieejamās) vietās. Informācijas (datu) nesēju glabāšanas vietai ir jānodrošina tāds pats fiziskais aizsardzības līmenis, kāds ir datiem.
62. Visi Informācijas (datu) nesēji, uz kuriem tiek veidotas sistēmas rezerves kopijas, tiek marķēti, nodrošinot, ka katra vienība ir identificējama.
63. Ja paredzēts iznīcināt Informācijas (datu) nesēju, kas satur klasificētus Informācijas resursus, Tehnisko resursu turētājs to izdara veidā, lai nebūtu iespējams veikt uz tā esošo datu atjaunošanu.

IX. Informācijas lietotāji, to tiesības, pienākumi, ierobežojumi un atbildība

64. Darbinieku tiesības, pienākumus, ierobežojumus un atbildību nosaka katra Uzņēmuma Darbinieka amata apraksts, Uzņēmuma iekšējie normatīvie akti, t.sk., šie Noteikumi.
65. Darbinieku, kura amata pienākumos ietilpst Informācijas, kas satur personas datus, apstrāde pienākumos ietilpst:
    65.1. godprātīga un likumīga personas datu apstrādes veikšana;
    65.2. personas datu apstrādes veikšana tikai atbilstoši personas datu apstrādes mērķiem un tam nepieciešamajā apjomā;
    65.3. tādu personas datu glabāšanas veidu, kas ļauj personu identificēt attiecīgajā laikposmā, kas nepārsniedz paredzētajam datu apstrādes mērķim noteikto laikposmu;
    65.4. personas datu pareiza un to savlaicīga atjaunošana, labošana, dzēšana, ja personas dati ir nepilnīgi vai neprecīzi, saskaņā ar personas datu apstrādes mērķi.
66. Normatīvajos aktos paredzētajos gadījumos Darbiniekam ir tiesības izpaust personas datus tikai tām valsts un pašvaldību amatpersonām, kuras pirms datu izpaušanas ir identificētas.
67. Darbinieku pienākumi:
    67.1. rīkoties ar Uzņēmuma dokumentiem ar pienācīgu rūpību, strādājot ar tiem nepieļaut to bojāšanu, nozaudēšanu vai nozagšanu;

67.2. nekavējoši paziņot savam tiešajam vadītājam, kas attiecīgi informē augstāk stāvošās amatpersonas, par konfidenciālas informācijas izpaušanu, Uzņēmuma dokumentu izplatīšanu vai nozaudēšanu;

67.3. nodot Uzņēmumam visus Darbinieka rīcībā esošos Uzņēmumam dokumentu oriģinālus un to kopijas pēc darba tiesisko attiecību izbeigšanās;

67.4. iepazīties ar koplietošanas katalogā ievietotajām instrukcijām un ieteikumiem;

67.5. iepazīties ar Tehnisko resursu turētāja sūtītajiem ziņojumiem un savlaicīgi izpildīt tā norādījumus;

67.6. regulāri izdzēst darbam nevajadzīgos e-pasta sūtījumus;

67.7. nepārtraukt pretvīrusu programmas atjaunināšanas procesu;

67.8. sekot, lai uz datora obligāti būtu aktivizēts ekrāna saudzētājs ar paroles aizsardzību;

67.9. neatvērt nezināmas izcelsmes pievienotos failus; ja rodas šaubas par kāda e-pasta vai pievienota faila atvēršanas drošību, nekavējoties konsultēties ar datortīkla administratoru.

68. Darbiniekam aizliegts:

68.1. darba tiesisko attiecību laikā un pēc darba tiesisko attiecību izbeigšanās izpaust konfidenciālo informāciju, kas kļuvusi zināma, Darbiniekam pildot savus amata pienākumus;

68.2. izmantot savtīgos nolūkos konfidenciālo informāciju, kas kļuvusi zināma, Darbiniekam pildot savus amata pienākumus;

68.3. nesankcionēti nodot programmatūras un Uzņēmuma Informāciju trešajām personām;

68.4. izpaust informāciju par individuālo Lietotāja paroli citiem Uzņēmuma Darbiniekiem vai trešajām personām, izņemot šajos Noteikumos paredzētajos gadījumos;

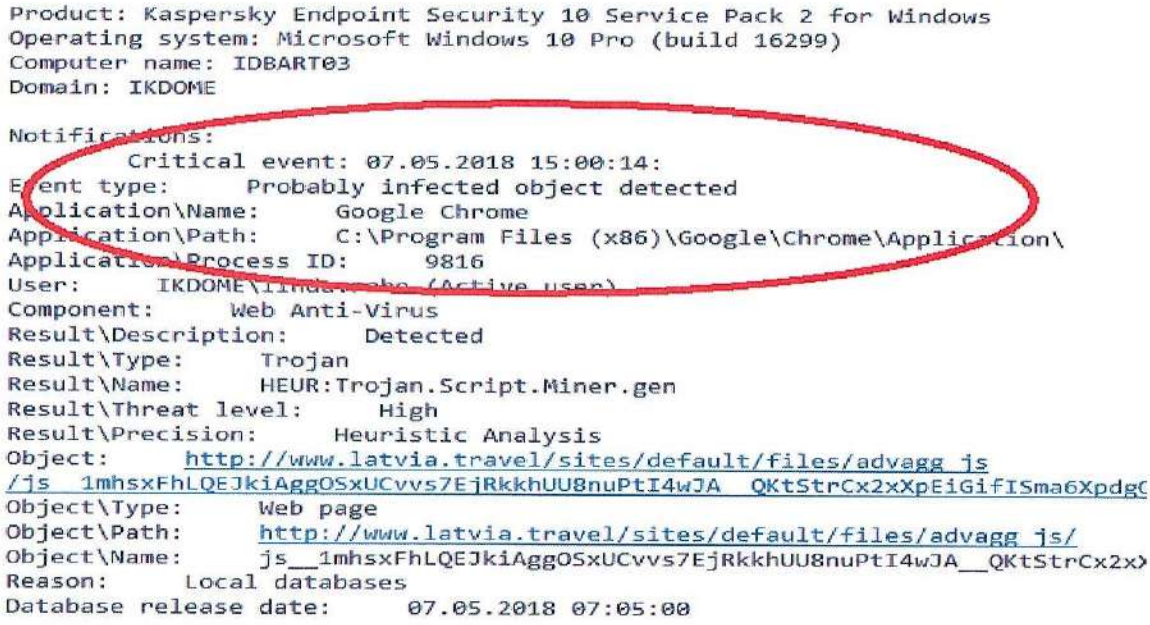
69.

XIII. Personas datu aizsardzības pārkāpumu procedūra

70. Saskaņā ar Eiropas Parlamenta un padomes 2016. gada 27. aprīļa Regulu 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (turpmāk - Regula) 33.un 34. pantu Uzņēmums konstatē, reģistrē izmeklē, izvērtē un pieņem lēmumu par notikušu Personas datu aizsardzības pārkāpuma paziņošanu Datu valsts inspekcijai un/vai Personas datu subjektam.

71. Darbinieks vai Lietotājs, kurš ir konstatējis drošības incidentu nekavējoties ziņo gan Informācijas resursu, gan tehnisko resursu turētājam, par Personas datu aizsardzības Pārkāpumu vai tā pazīmēm:

71.1. antivīrusu programmas paziņojums (piemēram,:



```
Product: Kaspersky Endpoint Security 10 Service Pack 2 for Windows
Operating system: Microsoft Windows 10 Pro (build 16299)
Computer name: IDBART03
Domain: IKDOME

Notifications:
        Critical event: 07.05.2018 15:00:14:
Event type:      Probably infected object detected
Application\Name:      Google Chrome
Application\Path:      C:\Program Files (x86)\Google\Chrome\Application\
Application\Process ID:      9816
User:      IKDOME\[illegible] (Active user)
Component:      Web Anti-Virus
Result\Description:      Detected
Result\Type:      Trojan
Result\Name:      HEUR:Trojan.Script.Miner.gen
Result\Threat level:      High
Result\Precision:      Heuristic Analysis
Object:      http://www.latvia.travel/sites/default/files/advagg_js
/js__1mhsxFhLQEJkiAggOSxUCvvs7EjRkkhUU8nuPtI4wJA__QKtStrCx2xXpEiGifISma6XpdgC
Object\Type:      Web page
Object\Path:      http://www.latvia.travel/sites/default/files/advagg_js/
Object\Name:      js__1mhsxFhLQEJkiAggOSxUCvvs7EjRkkhUU8nuPtI4wJA__QKtStrCx2x>
Reason:      Local databases
Database release date:      07.05.2018 07:05:00
```

71.2. neikdienišķu datora darbību (piemēram, strauji samazinājusies datora ātrdarbība, nav iespējams startēt darba programmas),
71.3. dators nereaģē uz *kursora* pozicionēšanas ierīces (*peles*) vai klaviatūras klikšķiem;
71.4. dokumentu pazušana no darba mapēm;
71.5. dokumentu satura patvaļīga izmainīšanās;
71.6. patvaļīgu datora pārstartēšanās;
71.7. aizdomīgi paziņojumi uz datora ekrāna;
71.8. programmu darbs ir ar pārtraukumiem vai ilgstošu gaidīšanu;
71.9. patvaļīga interneta mājas lapu atvēršanās;
71.10. patvaļīga *kursora* pozicionēšanas ierīces (*peles*) pārvietošanās pa datora ekrānu;
71.11. regulāra aizdomīgu e-pasta saņemšana vai citas aizdomīgas pazīmes.

72. Pārkāpuma gadījumā Darbiniekam vai Lietotājam savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt tehnisko un Informācijas resursu drošību līdz attiecīgo resursu turētāju ierašanās brīdim.

73. Saņemot Darbinieka, Lietotāja, Datu Apstrādāja, sadarbības partnera vai jebkuras Trešās personas informāciju par iespējamo Pārkāpumu, Uzņēmuma valdes priekšsēdētājs (turpmāk- atbildīgā persona) nekavējoties veic pārbaudi par to, vai informācija ir patiesa. Aizdomu gadījumā par Pārkāpumu, tas nekavējoties tiek fiksēts Pārkāpumu reģistrā (pielikums Nr.3).

74. Par Pārkāpumu reģistra vešanu ir atbildīga atbildīgā persona.

75. Pēc Pārkāpuma reģistrēšanas atbildīgā persona uzsāk izmeklēšanu un noskaidro Pārkāpuma veidu, rašanas iemeslus un pieņem lēmumu par riska Ietekmi uz datu subjekta tiesībām.

76. Izšķir šādus Pārkāpumu veidus:

76.1. Pieejamības Pārkāpums – (A)

76.2. Integritātes Pārkāpums – (B)

76.3. Konfidencialitātes Pārkāpums – (C)

77. Vairāku Pārkāpumu veidu gadījumā Pārkāpumu reģistrā norāda visus attiecīgos Pārkāpuma apzīmējumus.

78. Pēc Ietekmes uz datu subjekta tiesībām un brīvībām izšķir šādas Pārkāpuma Ietekmes:

78.1. Pārkāpums nerada risku vai maz ticams, ka tiks radīts risks (mazs kaitējums) – (1)

78.2. Pārkāpums var radīt risku vai rada risku (vidējs kaitējums) – (2)

78.3. Pārkāpums rada augstu risku (liels kaitējums) – (3)

79. Ja tiek konstatēti vairāki Pārkāpumi veidi ar dažādām risku Vērtībām, rīcība attiecībā uz Pārkāpuma paziņošanu tiek veikta, ņemot vērā augstāko riska Ietekmes Vērtību.

80. Pēc Pārkāpuma Ietekmes izvērtēšanas tiek pieņemts lēmums par tā ziņošanu saskaņā ar šiem noteikumiem.

81. Papildus Pārkāpuma Ietekmes izvērtēšanai veic Pārkāpuma radīto seku novēršanu atbilstoši Ietekmei, ko Pārkāpums ir radījis, nepieciešamības gadījumā pārtraucot Informācijas sistēmas darbību.

82. Ja ir maz ticams, ka Pārkāpums var radīt risku datu subjekta tiesībām un brīvībām (Zema riska informācija), paziņošanu Datu valsts inspekcijai neveic.

83. Ja Pārkāpums var radīt risku vai augstu risku datu subjekta tiesībām un brīvībām, Uzņēmums par datu aizsardzības pārkāpumu paziņo Datu Valsts inspekcijai nekavējoties, bet ne vēlāk kā 72 stundu laikā no brīža, kad Pārkāpums ir kļuvis zināms.

84. Paziņojumā Datu Valsts inspekcijai Uzņēmums norāda sekojošo:

84.1. apraksta Pārkāpuma raksturu, tajā skaitā, datu subjekta kategorijas un aptuveno skaitu;

84.2. datu aizsardzības speciālista kontaktinformāciju, vai citu kontaktinformāciju, kur iespējams iegūt papildus informāciju;

84.3. Pārkāpuma iespējamās sekas;

84.4. pasākumus, kurus Uzņēmums ir veicis vai plāno veikt, lai novērstu Pārkāpumu un tā nelabvēlīgas sekas.

85. Ja uzņēmums konstatē, ka Pārkāpums var radīt augstu risku datu subjekta tiesībām un brīvībām, Uzņemums nekavējoties par to paziņo datu subjektam.

86. Paziņojumā datu subjektam norāda 134.punktā noteikto informāciju.

87. Paziņošana datu subjektam neveic, ja:

87.1. Uzņēmums 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;

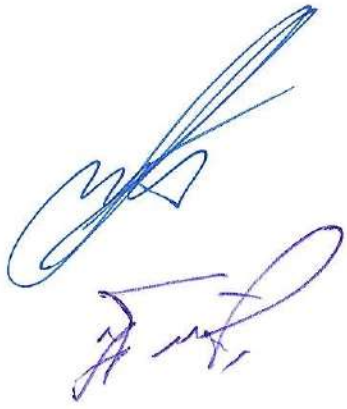
87.2. Uzņēmums pēc Pārkāpuma ir veicis tehniskas un organizatoriskas darbības, lai datu subjektam netiktu radīts augsts risks viņa tiesībām un brīvībām;

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

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

89. Personas datu apstrādes aizsardzības pārkāpuma paziņojuma veidlapa Datu valsts inspekcijai ir pieejama: http://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana/ .

89. Personas datu apstrādes aizsardzības pārkāpuma paziņojuma veidlapa Datu valsts inspekcijai ir pieejama: http://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana/ .



Valdes priekšsēdētājs : Ēriks Linters

Valdes loceklis : Juris Firsts

Pielikums Nr.1

SIA "Ķekavas nami"
Iekšējiem datu apstrādes un informācijas aizsardzības noteikumiem

Apliecinājums

Es,_____,
(vārds, uzvārds, personas kods)

esmu iepazinies (-usies) ar SIA "Ķekavas nami" Iekšējiem datu apstrādes un informācijas aizsardzības noteikumiem un apņemos:

1. apstrādāt fizisko personu datus, t.sk. īpašo kategoriju personu datus, kas man kļūst zināmi pildot Amata aprakstā un Darba līgumā noteiktos darba pienākumus, atbilstoši personas datu aizsardzības jomu regulējošo normatīvo aktu un Iekšējo datu un informācijas apstrādes aizsardzības noteikumu prasībām;
2. nelikumīgi neapstrādāt fizisko personu datus, t.sk. īpašo kategoriju personu datus, kas man kļuvuši zināmi, pildot amata pienākumus SIA "Ķekavas nami";
3. ziņot tiešajam vadītājam par fizisko personu datu aizsardzības jomā konstatētajiem pārkāpumiem un prettiesiskiem mēģinājumiem iegūt no manis informāciju par fizisko personu datiem, t.sk. īpašo kategoriju personu datiem;
4. apņemos neizpaust, arī pēc darba tiesisko attiecību izbeigšanas, uzņēmuma Komercnoslēpumu - ekonomiska, tehniska un saimnieciska rakstura Uzņēmuma informāciju, lietas vai ziņas, kas fiksētas rakstveidā vai citādā veidā, izņemot Uzņēmuma gada pārskatā sniegto informāciju.

Esmu brīdināts (-a), ka par Uzņēmuma komercnoslēpuma, fizisko personu datu, t.sk. īpašo kategoriju personu datu, prettiesisku apstrādi un izpaušanu, par IS un IT resursu drošības noteikumu neievērošanu varu tikt saukts (-a) pie disciplinārās, administratīvās, kriminālās vai civiltiesiskās atbildības.

201__. gada __. _____

_____
Vārds, uzvārds

_____
Amats

Apliecinājumu pieņēma:

_____
Vārds, uzvārds, Amats

Pielikums Nr.2
SIA "Ķekavas nami"
Iekšējiem datu apstrādes un informācijas aizsardzības noteikumiem

Komercnoslēpuma, personas datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes pakāpei

Nr.p.k.	Resurss	Informācijas resurss	Resursu aizbildnis (saturs)	Resursu aizbildnis (personas, kuras ikdienā apstrādā informāciju un personu datus)	Informācijas vērtība	Informācijas konfidencialitāte
1.	Valdes birojs	Personāla dokumenti elektroniskā formā	Valdes priekšsēdētājs	Biroja vadītājs	V1	I, K
2.	Valdes birojs	Personāla dokumenti papīra formā (darba līgumi, amatu apraksti, darbinieku personas lietas, darbinieku atvaļinājumu grafiki, instrukciju žurnāli, darbinieku sanitārās grāmatiņas u.c.)	Valdes priekšsēdētājs	Biroja vadītājs	V1	I, K
3.	Valdes birojs	Uzņēmuma juridiskie dokumenti elektroniskā formā	Valdes priekšsēdētājs	Biroja vadītājs	V1	I, K
4.	Valdes birojs	Uzņēmuma juridiskie dokumenti papīra formātā (līgumi, vienošanās u.tml.)	Valdes priekšsēdētājs	Biroja vadītājs	V1	I, K
5.	Valdes birojs	Uzņēmuma darbības nodrošināšanai nepieciešamie dokumenti elektroniskā formā	Valdes priekšsēdētājs	Biroja vadītājs	V1	I, K
6.	Valdes birojs	Uzņēmuma darbības nodrošināšanai nepieciešamie dokumenti papīra formā (rīkojumi, noteikumi, procedūras, instrukcijas)	Valdes priekšsēdētājs	Biroja vadītājs	V1	I, K
7.	Valdes birojs	Iesniegumi, vēstules	Valdes priekšsēdētājs	Biroja vadītājs	V1	I

8.	Grāmatvedība	Grāmatvedības sistēma	Grāmatvedība	Galvenais grāmatvedis	V1	I, K
9.	Grāmatvedība	Grāmatvedības uzskaites dokumenti	Grāmatvedība	Galvenais grāmatvedis	V1	I, K
10.	Valdes birojs	Videonovērošanas sistēma un videonovērošanas ieraksti	Valdes priekšsēdētājs	Valdes priekšsēdētājs	V1	I
11.	Uzņēmuma interneta tīmekļa vietne	Ievietotā informācija Uzņēmuma interneta tīmekļa vietnē	SIA xx	SIA xxxx	V3	P
12.	Arhīvs	Pastāvīgi glabājamie dokumenti un personāla dokumenti papīra formā	Valdes priekšsēdētājs	Biroja vadītājs	V1	I, K
13.	Statistika	Statistikas atskaites	Grāmatvedība	Galvenais grāmatvedis	V1	I, K
14.	Uzņēmuma pārskats	Informācija, kas saskaņā ar spēkā esošajiem normatīvajiem aktiem iekļaujami uzņēmuma pārskatos	Valdes priekšsēdētājs	Galvenais grāmatvedis	V3	P

P - publiska informācija
K - komercnoslēpums
I - ierobežotas pieejamības informācija
V1 –augstas vērtības informācija
V2 – vidējas vērtības informācija
V3 - zemas vērtības informācija

Pielikums Nr.3
SIA "Ķekavas nami"
Iekšējiem datu apstrādes un informācijas aizsardzības noteikumiem

Pārkāpumu reģistrs

1.	Pārkāpuma veids	
2.	Pārkāpumu konstatējuša persona	
3.	Pārkāpuma konstatēšanas brīdis	
4.	Pārkāpuma rašanās iemesls	
5.	Lēmums par riska ietekmi uz datu subjekta tiesībām	
6.	Lēmums par ziņošanu DVI/ datu subjektam/ tiesībsargājošām iestādēm	
7.	Pārkāpuma radīto seku novēršana	