SIA "ALAAS"

Reģ. nr. 42403013918
Juridiskā adrese: „Križevniki 2", Križevņiki
Ozolaines pagasts, Rēzeknes novads, LV-4633
Tālr./Fakss: 64667440; Mob. tel. 28359080
e-pasts: austrumlatgale2@inbox.lv

Biroja adrese: Zilupes iela 50
Rēzekne, LV-4601; Fakss: 64607645
Tālr.: 64607673; Mob. tel. 20211337
e-pasts: sia.alaas@inbox.lv

Rēzeknē

APSTIPRINU
SIA "ALAAS"
Valdes loceklis
_____ A.Metlāns
2019.gada 30.decembrī

Personas datu un ierobežotas pieejamības informācijas apstrādes aizsardzības noteikumi

I. Vispārīgie jautājumi

1. Iekšējie personas datu un ierobežotas pieejamības informācijas apstrādes aizsardzības noteikumi (turpmāk tekstā – Noteikumi) nosaka personas datu apstrādes drošību SIA „ALAAS" (turpmāk tekstā – Uzņēmums) un ir saistoši visiem Uzņēmuma darbiniekiem, kuru amata pienākumos ietilpst darbs ar personas datiem un/vai ierobežotas pieejamības informāciju.
2. Noteikumi regulē informācijas (datu) apstrādi papīra formātā, jebkādās sistēmās vai jebkādos nesējos, kas iesaistīti datu/informācijas apstrādē Uzņēmumā, neatkarīgi no tā, vai datu/informācijas apstrāde ir saistīta ar Uzņēmuma iekšējām komercdarbības operācijām vai Uzņēmuma ārējām attiecībām ar jebkādām trešajām pusēm.
3. Noteikumi regulē arī to, kā Uzņēmuma Darbinieki lieto viņiem pieejamo aprīkojumu un rīkus savu darba pienākumu veikšanas ietvaros.
4. Noteikumi var būt piemērojami kopā ar jebkādām citām politikām, noteikumiem, procedūrām un/vai vadlīnijām, ko periodiski pieņem un ievieš Uzņēmuma valdes loceklis.
5. Ar visiem informācijas drošības sistēmas jautājumiem un informācijas/datu drošības

jautājumiem, kas nav atrunāti šajos Noteikumos, jāvēršas pie Uzņēmuma Valdes locekļa.

I. Personas datu apstrādes kārtība

6. Darbinieks veic personas datu apstrādi gan manuāli (papīra formā, iekļaujot tos līgumos, vēstulēs, aktos u.c. dokumentos), gan elektroniski, apstrādājot personas datus Uzņēmuma elektroniskajā klientu reģistrācijas programmā un elektroniskajās grāmatvedības uzskaites programmās.
7. Personas datu iegūšana no klientiem tiek veikta, ievērojot šo noteikumu, Vispārīgās datu aizsardzības regulas un citu personas datu apstrādi regulējošo normatīvo aktu prasības.
8. Personas datus Darbinieks iegūst no klientiem tikai Uzņēmuma Privātuma politikā norādītajiem nolūkiem.
9. Darbiniekam pirms pirmreizējās klienta personas datu iegūšanas ir mutiski jāinformē klients par paredzēto personas datu apstrādes mērķi un pamatojumu, sniedzot klientam visu Vispārīgās datu aizsardzības regulas 13. pantā minēto informāciju:

Pārzinis: SIA "ALAAS" reģ. Nr. 42403013918, juridiskā adrese: „Križevniki 2", Križevņiki, Ozolaines pagasts, Rēzeknes novads, LV-4633, biroja adrese: Zilupes ielā 50, Rēzeknē, LV-4601, tālrunis: 64607673, mājaslapa www.alaas.lv, e-pasts sia.alaas@inbox.lv .

Personas datu apstrādes nolūks: Līguma noslēgšanai un izpildei - lai noslēgtu līgumu pēc klienta pieteikuma un nodrošinātu tā izpildi; lai izpildītu uz pārzini attiecināmu juridisku pienākumu.

Personas datu apstrādes juridiskais pamatojums: Vispārīgās datu aizsardzības regulas 6.panta pirmās daļas b) un c) apakšpunkti.

Personas datu glabāšanas ilgums: Kamēr ir spēkā ar Klientu noslēgtais līgums; kamēr ārējos normatīvajos aktos noteiktajā kārtībā SIA "ALAAS" vai Klients var realizēt savas leģitīmās intereses; kamēr pastāv juridisks pienākums datus glabāt.

Personas datu saņēmēji: Datu subjekts par sevi; SIA "ALAAS" darbinieki; Apstrādātājs tikai apjomā, lai apstrādātājs varētu nodrošināt un sniegt pakalpojumu SIA "ALAAS" atbilstoši savstarpēji noslēgtajam līgumam; Valsts kontrolējošās institūcijas (ja tām ir atbilstošs pilnvarojums). Personas dati netiek nosūtīti uz trešajām valstīm vai starptautiskām organizācijām un personas dati netiek izmantoti automatizēto lēmumu pieņemšanā.

Datu subjekta tiesības: Datu subjekta tiesības nosaka un regulē Vispārīgā datu

aizsardzības regula, t.sk., bet ne tikai, pieprasīt pārzinim piekļuvi saviem personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežojumu attiecībā uz sevi, vai tiesības iebilst pret datu apstrādi, kā arī tiesības uz datu pārnesamību; atsaukt piekrišanu (ja tāda ir sniegta), neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana; tiesības kontaktēties ar Datu aizsardzības speciālistu un iesniegt sūdzību, t.sk. uzraudzības iestādei - Datu valsts inspekcijai.

Lēmumu pieņemšana: Personas datu apstrādē netiek automatizēta lēmumu pieņemšana, tostarp profilēšana.

Personas datu sniegšana: ir noteikta saskaņā ar likumu un tā ir priekšnosacījums, lai līgumu noslēgtu. Datu subjektam ir pienākums personas datus sniegt, pretējā gadījumā līguma slēgšana nebūs iespējama.

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

III.Datu/informācijas apstrādē iesaistītās sistēmas

11. Jebkādas informācijas sistēmas, tostarp, bet ne tikai datortehnika, jebkāda veida programmatūra, operētājsistēmas, elektroniskā pasta konti, pārlūku sistēmas un jebkāda cita tehniskā bāze un rīki, ko izmanto Uzņēmuma darbībā, uzskatāmi par Uzņēmuma īpašumu.

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

IV.Informācijas fiziskā aizsardzība

13. Datortehnika un ar to saistīts aprīkojums tiek ekspluatēts telpās, kurām iespēja piekļūt ir Uzņēmuma darbiniekiem un klientiem. Darbiniekam ir pienākums nodrošināt savas datortehnikas aizsardzību pret neautorizētu personu iespēju datortehniku pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju.
14. Biroja un Sadzīves atkritumu apglabāšanas poligonā „Križevņiki” (turpmāk tekstā-

poligonā) telpas ir aprīkotas ar:

14.1. ugunsgrēka signalizācijas iekārtu (dūmu detektoru+signalizāciju);

14.2. nepārtrauktās barošanas avotiem (UPS);

14.3. signalizāciju .

15. Nepiederošas personas/klienti telpās drīkst uzturēties tikai Darbinieka klātbūtnē.
16. Datu nesēju fiziskā aizsardzība:

16.1. Uzņēmums veic nepieciešamos drošības pasākumus datu nesēju fiziskai aizsardzībai neatkarīgi no veida (t. sk. demontētas disku iekārtas, USB zibatmiņas, ārējie cietie diski u. Tml.);

16.2. Uzņēmuma Informācijas sistēmas resursi, kurus nav nepieciešams lietot vai pārvietot, tiek glabāti Uzņēmuma telpās tam paredzētās vietās. Ja ir nepieciešams iznīcināt datu nesējus, to iznīcināšanu uzrauga un nodrošina Uzņēmuma valdes loceklis.

16.3. 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.

V.Rezerves kopiju veidošanas kārtība

17. Rezerves kopiju veidošana notiek saskaņā ar Programmatūras ATAPS uzturēšanas līguma noteikumiem.

VI.Darbinieka tiesības un pienākumi

18. Darbinieks ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.
19. Darbinieks nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Uzņēmuma valdes loceklis vai izpilddirektors.
20. Darbinieka pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu Uzņēmuma datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē Uzņēmuma valdes loceklis.
21. Darbiniekam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.
22. Nelicencētas programmatūras uzstādīšana un lietošana Darbinieka datorā ir aizliegta.

Patvaļīgi uzstādītas programmatūras lietošana, bez Uzņēmuma valdes locekļa atļaujas ir aizliegta.

23. Darbinieks nedrīkst izpaust nepilnvarotām personām ziņas par Uzņēmuma datoru tīkla uzbūvi un konfigurāciju.
24. Darbinieks nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja tas nav nepieciešams tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Uzņēmuma valdes loceklis.
25. Darbiniekam ir aizliegts patvarīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.
26. Darbiniekam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.
27. Visus personas datus un citu informāciju, ar kuras palīdzību var identificēt fizisku personu, Darbinieks 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 amata aprakstā noteiktajās robežās un saskaņā ar likumā paredzētajām datu aizsardzības prasībām, jo īpaši, saskaņā ar Vispārīgā datu aizsardzības regulas un Uzņēmuma apstiprinātās Privātuma politikas noteikumiem, kas atrodami Uzņēmuma tīmekļa vietnē www.alaas.lv.
28. Jebkādus datu pieprasījumus un/vai pieprasījumus par datu apstrādi, ko Darbinieks, veicot savus darba pienākumus, ir saņēmis no datu subjektiem – fiziskām personām, nekavējoties pārsūta turpmākai izskatīšanai Uzņēmuma valdes loceklim un Datu aizsardzības speciālistam.
29. Nekādu šajos Noteikumos minēto informāciju/datus Darbinieks nenosūta un nekādā citā veidā neiesniedz trešajām personām, ja vien tas nav nepieciešams Darbinieka darba pienākumu izpildei, un tikai ciktāl tas ir nepieciešams šādu pienākumu izpildei. Gadījumā, ja datus pārsūta vai iesniedz trešajām personām, ir noteikti jānodrošina datu aizsardzība un jāveic visi atbilstošie drošības pasākumi.
30. Ikvienam Darbiniekam ir pienākums ievērot šos Noteikumus, kā arī pildīt spēkā esošo vietējo, reģionālo vai starptautisko normatīvo aktu prasības, kas paredz informācijas/datu apstrādes un aizsardzības nosacījumus.

31. Darbiniekam ir tiesības vērsties pēc konsultācijas pie Uzņēmuma valdes locekļa vai Datu aizsardzības speciālista.
32. Darbinieki, kam ir piekļuve Uzņēmuma Ierobežotas pieejamības informāciju saturošām ziņām, ir atbildīgi par precīzu prasību izpildi, kas tiem izvirzītas ar mērķi nodrošināt minēto ziņu saglabāšanas nodrošināšanu.
33. Darbiniekam, kura darbs saistīts ar personas datu apstrādi un Ierobežotas pieejamības informāciju, ir pienākums iepazīties ar šiem noteikumiem un iesniegt Uzņēmuma valdes loceklim rakstveida apliecinājumu par šo noteikumu prasību ievērošanu (Pielikums Nr.2).
34. Darbiniekam ir pienākums:

34.1. Stingri glabāt Ierobežotas pieejamības informāciju. Par to, ka tam kļuvuši zināmi Ierobežotas pieejamības informācijas izpaušanas, noplūdes gadījumi vai nesankcionētas piekļuves gadījumi Ierobežotas pieejamības informācijai, kā arī dokumentu ar atzīmi "Ierobežotas pieejamības informācija" vai Ierobežotas pieejamības informāciju saturošu datu nesēju nozaudēšanas gadījumā paziņot Uzņēmuma valdes loceklim;

34.2. Iepazīties vienīgi ar dokumentiem un veikt to apstrādi tikai ar mērķi izpildīt amata aprakstā noteiktos pienākumus;

34.3. Strādāt tikai ar tām Datu bāzēm un informācijas resursiem, darbam ar kuriem tam ir piekļuves tiesības;

34.4. Nepieļaut nepamatotu dokumentu izsūtīšanu ar atzīmi "Ierobežotas pieejamības informācija";

34.5. Nepieļaut nepamatotu informācijas kopēšanu, kas glabājas informācijas nesējos ar Ierobežotas pieejamības informāciju.

34.6. Dokumentu projektus un melnrakstus papīra formātā, kuros ietverti personu dati vai ierobežotas pieejamības informācija, iznīcināt ar papīra smalcināmās mašīnas palīdzību;

34.7. Organizējot lietišķas pārrunas ar nepiederošu organizāciju pārstāvjiem vai privātpersonām, jāaprobežojas ar minimālas informācijas sniegšanu, kas reāli nepieciešama pārrunu veiksmīgai noslēgšanai;

34.8. Neizmantot Uzņēmuma ierobežotas pieejamības informāciju, kas kļuva zināma, savā labā, kā arī neveikt darbības, ar kurām tā var tikt izmantota konkurentu labā, nesot zaudējumus Uzņēmumam.

VII.Informācijas sistēmas lietotāju (darbinieku) piekļuves kontrole

35. Katram informācijas sistēmas lietotājam (darbiniekam) tiek piešķirts lietotājvārds un parole, kā arī noteiktas piekļuves tiesības. Informācijas sistēmas lietotājs ir atbildīgs par piešķirtā lietotājvārda (identifikatora) un paroles lietošanu, saglabāšanu un neizpaušanu.
36. Ja darbinieks pārtrauc darba attiecības Uzņēmumā, Uzņēmuma valdes loceklis nekavējoties anulē visas attiecīgā darbinieka piekļuves tiesības Uzņēmuma informācijas sistēmas resursiem.
37. Informācijas sistēmas lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotājvārdu (identifikatoru). Informācijas sistēmas lietotāja autentiskumu nosaka, lai pārliecinātos, ka lietotājvārda izmantotājs ir sankcionētais tā turētājs. Autentiskuma noteikšanai tiek izmantotas paroles. Pēc lietotājvārda un paroles ievadīšanas lietotājs var izmantot informācijas sistēmas resursu.
38. Paroles garums nav mazāks par deviņiem simboliem un satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu vai speciālu simbolu. Parole nedrīkst saturēt garumzīmes un mīkstinājuma zīmes. Nedrīkst par paroli izmantot personu identificējošos datus (piemēram, personas datus, lietotājvārdu (identifikatoru) vai tā daļu, automašīnas numuru, radu vārdus vai uzvārdus, vārdus, kas saistīti ar darbavietu vai kas bieži tiek tajā lietoti).
39. Informācijas sistēmas lietotājam paroli jāmaina vismaz reizi sešos mēnešos. Uzņēmuma datortehnikas mehāniķim ir jānodrošina:
    a. automātisku paroles maiņas pieprasījumu ik pēc 6 mēnešiem;
    b. sistēmas bloķēšanu uz laiku līdz 5.min., ja lietotājs piecas reizes pēc kārtas ir ievadījis nepareizu paroli vai lietotājvārdu.
40. Ja radušās aizdomas, ka paroli uzzinājusi cita persona, informācijas sistēmas lietotājs to nekavējoties nomaina un par incidentu ziņo Uzņēmuma valdes loceklim.
41. Uz datora ir jābūt uzstādītam ekrāna saudzētājam ar aktivizācijas paroli. Tam ir automātiski jāaktivizējas, ja 15 minūšu laikā lietotājs nav veicis nekādas darbības.
42. Datu apstrāde Uzņēmuma informācijas sistēmā notiek Uzņēmuma biroja telpās – Zilupes ielā 50, Rēzeknē, LV-4601, Sadzīves atkritumu apglabāšanas poligonā „Križevņiki” (“Križevniki 2”, Križevņiki, Ozolaines pagasts, Rēzeknes novads).

VII.Datu apstrādes aizsardzība videonovērošanas jomā

43. Par informācijas resursiem (video ieraksta programmatūru, ierakstu uzglabāšanu, drošību un pieejamību, paroļu veidošanu un lietošanas uzraudzību, datorsistēmām) ir atbildīgs Informācijas resursu turētājs - Uzņēmuma datortehnikas mehāniķis.

    43.1. Informācijas resursu turētājs:

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

44. Par tehniskajiem resursiem (videonovērošanas iekārtu un datortehnikas uzturēšanu un izmantošanu) ir atbildīgs tehnisko resursu turētājs – Uzņēmuma izpilddirektors - birojā, Uzņēmuma valdes loceklis - poligonā .

    44.1. Tehnisko resursu turētājs:

        c) nodrošina fiziskās aizsardzības pasākumus;
        d) nodrošina tehnisko resursu darbspēju;
        e) nodrošina tehnisko resursu atjaunošanu vai nomaiņu, ja tie bojāti.

45. Informācijas resursu turētājs nosaka informācijas resursu klasifikāciju:

    45.1. vispārējas piekļuves – pieejami bez ierobežojuma visiem Uzņēmuma darbiniekiem,

    45.2. ierobežotas piekļuves – informācija, kurai piekļūt var tikai pilnvarots darbinieks un/vai uzraudzības un kontroles iestādes atbilstoši to kompetencei.

46. Videonovērošana Uzņēmuma teritorijā, biroja telpās, pie biroja telpu ieejas (Zilupes ielā 50, Rēzeknē) un Sadzīves atkritumu apglabāšanas poligonā „Križevņiki” (“Križevniki 2”, Križevņiki, Ozolaines pagasts, Rēzeknes novads) tiek veikta reālā laika režīmā un ieraksti tiek uzglabāti ne vairāk kā 60 dienas un automātiski tiek dzēsti. Videonovērošana, izmantojot videoreģistratorus transportlīdzekļos, tiek veikta reālā laika režīmā un ieraksti tiek uzglabāti ne vairāk kā 60 dienas un automātiski tiek dzēsti.
47. Pie ieejas teritorijā, kur notiek videonovērošana, ir izvietota brīdinājuma zīme. Transportlīdzeklī, kurā uzstādīts videoreģistrators, tiek izvietota brīdinājuma zīme.
48. Videonovērošanas dati klasificējami kā ierobežotas piekļuves informācija, kurai drīkst piekļūt tikai pilnvaroti darbinieki.
49. Videonovērošanas datus nedrīkst kopēt ārējos datu nesējos (CD, DVD, USB diskos,

zibatmiņas ierīcēs u.tml.), izņemot gadījumus, kad tas nepieciešams rezerves kopiju nodrošināšanai (pēc nepieciešamības).

50. Tehniskie resursi, ar kuriem tiek nodrošināta personas datu apstrāde birojā:
    50.1. Videonovērošanas iekārta: *BricKcom 5M, DIGIEVER NVR9;*
    50.2. Stacionārais dators *DIGISTOR;*
    50.3. Videoreģistrators *BRIGADE*.
51. Tehniskie resursi, ar kuriem tiek nodrošināta personas datu apstrāde poligonā:
    51.1. Videonovērošanas iekārta: LOKS, *BRICKCOM Corporation;*
    51.2. Stacionārais dators Intel G2030 un Intel i5-4590, portatīvais dators PACKARD BELL;
    51.3. Video digitālais reģistrators VKI 2, ieraksta ierīce *DIGIEVER Corporation.*
52. Lai nodrošinātos pret nesankcionētu piekļuvi videonovērošanas datiem, tehniskie resursi (datori) novietoti atsevišķā slēdzamā telpā, kurai var piekļūt tikai pilnvaroti darbinieki.

IX.Ierobežotas pieejamības informācija

53. Ar Uzņēmuma ierobežotas pieejamības informāciju saprotamas ziņas, kas nav valsts noslēpums un saistītas ar Uzņēmuma vadību, finansēm, personālu, ražošanas un tehnoloģisko darbību, un kuru izpaušana, noplūde un nesankcionēta pieeja tām var radīt zaudējumus Uzņēmuma interesēm. Uzņēmuma valdes loceklis ar rīkojumu nosaka ierobežotas pieejamības informāciju. Uzņēmuma ierobežotas pieejamības informācija ir tā īpašums. Ja tas ir uz līguma ar citiem uzņēmumiem pamatots kopējas darbības rezultāts, ierobežotas pieejamības informācija var būt divu pušu īpašums, kam jābūt atspoguļotam līgumā.
54. Ar ierobežotas pieejamības informācijas izpaušanu jāsaprot tīšas vai neuzmanīgas amatpersonu vai citu fizisku personu darbības, kas novedušas pie dienesta nepieciešamības neizsauktas vai priekšlaicīgu sargājamo ierobežotas pieejamības informāciju izpaušanu, kā arī šāda rakstura ziņu nodošana pa atklātiem publiskiem sakaru kanāliem vai to apstrāde ar neaizsargātas skaitļojamās tehnikas palīdzību.
55. Ar ierobežotas pieejamības informācijas noplūdi jāsaprot nekontrolējamu ziņu izplatību ārpus Uzņēmuma robežām vai personu loka, kurām šīs ziņas tikušas uzticētas.
56. Ar nesankcionētu pieeju pie ierobežotas pieejamības informācijas jāsaprot ļaundaru

tīšas pretlikumīgas darbības ar mērķi iegūt apsargājamās ziņas.

57. Ar ierobežotas pieejamības informāciju saturošu dokumentu vai informācijas nesēju nozaudēšanu jāsaprot dokumentu vai informācijas nesēju nokļūšana (tai skaitā arī uz laiku) ārpus to personu valdījuma, kam šīs ziņas tikušas uzticētas glabāšanai dienestā vai darbā, kas ir rezultāts to lietošanas noteikto noteikumu pārkāpumam, kā rezultātā šie dokumenti vai informācijas nesēji kļuvuši vai varējuši kļūt par nepiederošu personu īpašumu.
58. Ar ierobežotas pieejamības informācijas atklātu publicēšanu jāsaprot publikācija atklātā presē, radio vai televīzijas pārraidēs, izpaušana starptautiskās, pārrobežu un atklātās Latvijas apspriedēs, konferencēs, publiskās uzstāšanās un disertāciju aizstāvēšanā, to nodošana jebkurā formā citiem uzņēmumiem un valsts organizācijām vai privātpersonām.
59. Ierobežotas pieejamības informācijas aizsardzība paredz:

    59.1. Ierobežotas pieejamības informāciju saturošas informācijas noteikšanas kārtību un tās darbības termiņus;

    59.2. Uzņēmuma darbinieku, privātu personu un komandētu personu pieejas sistēmu ierobežotas pieejamības informācijai;

    59.3.Ierobežotas pieejamības informācijai pielaisto personu pienākumi;

    59.4. darba kārtība ar ierobežotas pieejamības informāciju saturošiem dokumentiem;

    59.5. darba kārtība ar ierobežotas pieejamības informāciju saturošām Datu bāzēm;

    59.6. Ierobežotas pieejamības informāciju saturošas informācijas nesēju izmantošanas kārtība;

    59.7. Ierobežotas pieejamības informāciju saturošu dokumentu, lietu un izdevumu saglabāšanas nodrošināšana

    59.8. Ierobežotas pieejamības informāciju saturošu Datu bāžu saglabāšanas nodrošināšana;

    59.9. Ierobežotas pieejamības informāciju saturošu informācijas nesēju saglabāšanas nodrošināšana;

    59.10. Kontroles organizācijas un veikšanas principi noteiktās kārtības nodrošināšanai darbā ar Ierobežotas pieejamības informāciju;

    59.11. Atbildība par Ierobežotas pieejamības informāciju saturošu ziņu izpaušanu un dokumentu un informācijas nesēju nozaudēšanu;

    59.12. Atbildīgo personu rīcība Ierobežotas pieejamības informācijas izpaušanas

gadījumā.

60. Atbildību par darba organizāciju ar Ierobežotas pieejamības informāciju saturošām ziņām, nepieciešamo pasākumu izstrādi un īstenošanu Ierobežotas pieejamības informācijas saglabāšanai veic Uzņēmuma valdes loceklis.
61. Ierobežotas pieejamības informācijas nodošanai tiem uzņēmumiem un organizācijām, ar kuriem Uzņēmumam nav tiešu darba kontaktu, jābūt regulētai ar līgumattiecībām, kuras nosaka lietotāja pienākumus un atbildību.
62. Jebkuras informācijas sniegšana, kas skar Uzņēmumu, valsts orgānu pārstāvjiem, Saeimas un pašvaldības orgānu deputātiem, preses orgāniem, radio, televīzijai, u.t.t., notiek vienīgi pēc Uzņēmuma valdes locekļa norādījumiem.
63. Nepieciešamību atklāti publicēt Ierobežotas pieejamības informāciju, publicēšanas apjomu, formu un laiku nosaka Uzņēmuma valdes loceklis.
64. Uz līguma vai pilnvaras pamata saņemta, vai kopīgas darbības rezultātā radusies Ierobežotas pieejamības informācijas izmantošana atklātai publicēšanai tiek pieļauta vienīgi ar partneru kopējo piekrišanu.
65. Kontrole pār pasākumu īstenošanu, kuri nodrošina Ierobežotas pieejamības informācijas saglabāšanu veic Uzņēmuma valdes loceklis vai tas tiek uzdots kādam darbiniekam.
66. Uzņēmuma Ierobežotas pieejamības informācijas izpaušanas gadījumā obligātā kārtā jāveic apstākļu noskaidrošana un izmeklēšana.

X. Ziņu attiecināšana uz kategoriju “Komercnoslēpums”

67. Ziņu attiecināšanas nepieciešamība uz kategoriju “Ierobežotas pieejamības informācija” tiek noteikta saskaņā ar šo noteikumu 52.punktu.
68. Uzņēmuma valdes loceklis pēc saviem ieskatiem var attiecināt jebkādu informāciju uz Ierobežotas pieejamības informāciju.
69. Datu bāzes attiecināšana uz kategoriju “Ierobežotas pieejamības informācija” tiek noteikta ar Uzņēmuma valdes locekļa rīkojumu.

XI. Komercnoslēpuma darbības termiņš

70. Ierobežotas pieejamības informācijas darbības termiņš, kas ietverts Datu bāzē, tiek noteikts ar Uzņēmuma valdes locekļa rīkojumu.

XII. Kārtība, kas nosaka pieeju uzņēmuma Ierobežotas pieejamības

informāciju saturošām ziņām

71. Darbinieku piekļūšanu ziņām, kas satur Uzņēmuma Ierobežotas pieejamības informāciju, realizē Uzņēmuma valdes loceklis.
72. Izpilddirektoram ir pienākums nodrošināt sistemātisku kontroli pār piekļuvi šīm ziņām tikai personām, kurām tās nepieciešamas darba pienākumu pildīšanai.
73. Pie ziņām, kas satur Ierobežotas pieejamības informāciju, tiek pielaistas personas, kuru personiskās un lietišķās īpašības nodrošina to spēju glabāt Ierobežotas pieejamības informāciju, un tas notiek tikai darba vajadzībām.
74. Personām, kurām ir pieeja Uzņēmuma Ierobežotas pieejamības informācijai, jābūt iepazīstinātām ar visiem normatīvajiem aktiem, kas skar Ierobežotas pieejamības informāciju un datu aizsardzību Uzņēmumā.
75. Nepiederošu organizāciju pārstāvji un privātas personas var tikt pielaistas iepazīstināšanas nolūkiem un darbam ar dokumentiem un izdevumiem ar atzīmi "Ierobežotas pieejamības informācija" ar Uzņēmuma valdes locekļa atļauju.
76. Nepiederošu organizāciju pārstāvji un fiziskas personas var tikt pielaistas darbam ar Datu bāzēm, kas satur Ierobežotas pieejamības informāciju, tikai ar Uzņēmuma valdes locekļa atļauju.
77. Dokumenti ar atzīmi "Ierobežotas pieejamības informācija" ārpus esošu organizāciju pārstāvjiem un fiziskām personām tiešā veidā netiek izsniegti. Nepieciešamības gadījumā šīs personas ar to saturu tiek iepazīstinātas vienīgi ar Uzņēmuma valdes locekļa atļauju.

XIII. Darbinieku atbildība

78. Gadījumā, ja konstatēts personas datu vai Uzņēmuma ierobežotas pieejamības informāciju saturošu ziņu izplatīšanas vai noplūdes fakts, kā arī nesankcionēta pieeja šādām ziņām, Uzņēmuma darbiniekiem nekavējoši jāveic pasākumi, lai pārtrauktu to izplatīšanu, noplūdi vai nesankcionētu pieeju tām un minimizētu zaudējumus.
79. Par personas datu izpaušanas vai noplūdes faktu, par nesankcionētu piekļuvi personas datiem, darbiniekiem nepieciešams ziņot saskaņā ar kārtību, kura noteikta šo noteikumu 1. pielikumā.
80. Par Uzņēmuma Ierobežotas pieejamības informācijas izpaušanas vai noplūdes faktu, par nesankcionētu piekļuvi Ierobežotas pieejamības informācijai, kā arī dokumentu ar atzīmi "Ierobežotas pieejamības informācija" vai Ierobežotas pieejamības informāciju

saturošu datu nesēju nozaudēšanas gadījumā, darbiniekiem nepieciešams iesniegt ziņojumu Uzņēmuma valdes loceklim. Šādi ziņojumi pieskaitāmi Ierobežotas pieejamības informācijai. Gadījumos, kad nav pieļaujama vilcināšanās, darbiniekam jāpaziņo par notikušo mutiskā veidā izpilddirektoram vai Uzņēmuma valdes loceklim.

81. Gadījumā, ja Uzņēmuma darbinieka darbības vai bezdarbības rezultātā notikusi personas datu vai Uzņēmuma ierobežotas pieejamības informāciju saturošu ziņu izpaušana vai noplūde, kā arī radusies iespēja nesankcionētai pieejai šādām ziņām, un tas tiek apstiprināts ar dienesta izmeklēšanas materiāliem, pret darbinieku var tikt vērsti šādi pasākumi:
    81.1. rakstveida piezīme;
    81.2. rājiens;
    81.3. pieejas liegšana Ierobežotas pieejamības informācijas ziņām;
    81.4. pārcelšana citā amatā;
    81.5. atlaišana no darba;
    81.6. pieteikuma iesniegšana tiesā darbinieka saukšanai pie civiltiesiskās atbildības;
    81.7. iesnieguma iesniegšana tiesībsargājošajos orgānos darbinieka saukšanai pie krimināatbildības.
82. Darbinieks, kura darbība vai bezdarbība novedušas pie personas datu vai Uzņēmuma ierobežotas pieejamības informāciju saturošu ziņu izpaušanas, noplūdes, kā arī iespējas nesankcionēti piekļūt šādām ziņām, var labprātīgi pilnīgi vai daļēji dzēst zaudējumus, kas radušies Uzņēmumam šādas darbības vai bezdarbības rezultātā.
83. Ja personas datu vai Uzņēmuma Ierobežotas pieejamības informācija izpaušana vai noplūde notikusi tādas juridiskas vai fiziskas personas darbības vai bezdarbības rezultātā, kam šīs ziņas tikušas uzticētas, pamatojoties uz līgumu, vai ir kopējais īpašums ar tiem, Uzņēmuma darbinieks, fiksē notikušā cēloņus un apstākļus, kā arī Uzņēmumam nodarīto zaudējumu apmērus.

Pielikums Nr.1
"Personas datu un ierobežotas pieejamības
informācijas apstrādes aizsardzības noteikumiem"

Personas datu aizsardzības pārkāpuma ziņošanas kārtība uzraudzības iestādei un datu subjektam

Kas ir datu aizsardzības pārkāpums?

Datu aizsardzības pārkāpums ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

1. Jebkuram darbiniekam ir pienākums nekavējoties ziņot Valdes loceklim par jebkādu situāciju, kad, iespējami, tā rīcībā esošie personas dati varētu tikt kompromitēti, piemēram, bet ne tikai – kļūdainam adresātam nosūtīts e-pasta sūtījums, informācijas izpaušana telefonsarunas laikā personai, kas nav viennozīmīgi identificēta un ir radušās aizdomas, ka informācija ir izpausta personai, kas nebija pilnvarota saņemt to, kompromitētas pieejas tiesības (lietotājvārdi un paroles kļuvušas zināmas nepilnvarotām personām, tajā skaitā, ja ir *"uzlauzti"* personīgie profili un šis fakts var ietekmēt Uzņēmuma informācijas un tehniskos resursus, piemēram, mobilos telefonus un tajos esošo informāciju u tml.).
2. Valdes loceklim, saņemot informāciju par iespējamo personas datu aizsardzības pārkāpumu, ir pienākums, jebkādu šādu faktu izmeklēt un fiksēt personas datu aizsardzības pārkāpumu žurnālā.
3. Ievērojot attiecīgā ziņojuma saturu par iespējamo personas datu aizsardzības pārkāpumu, Valdes loceklis, ja tas uzskata par nepieciešamu, tiklīdz tas iespējams, izveido personas datu aizsardzības pārkāpuma izmeklēšanas komisiju.
4. Valdes loceklis vai personas datu aizsardzības pārkāpuma izmeklēšanas komisija nekavējoties sagatavo ziņojumu, izņemot gadījumus, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām. Paziņojumā iekļauj vismaz sekojošu informāciju:
   4.1. apraksta personas datu aizsardzības pārkāpuma raksturu, tostarp, ja iespējams, attiecīgo datu subjektu kategorijas un aptuveno skaitu un attiecīgo personas datu ierakstu kategorijas un aptuveno skaitu;
   4.2. apraksta personas datu aizsardzības pārkāpuma iespējamās sekas;
   4.3. apraksta pasākumus, ko pārzinis veicis vai ierosinājis veikt, lai novērstu

personas datu aizsardzības pārkāpumu, tostarp attiecīgā gadījumā – pasākumus, lai mazinātu tā iespējamās nelabvēlīgās sekas.

5. Valdes loceklis vai personas datu aizsardzības pārkāpuma izmeklēšanas komisija ne vēlāk kā 72 stundu laikā izvērtē un izlemj vai konstatētais personas datu aizsardzības pārkāpums varētu radīt risku datu subjekta tiesībām un brīvībām un ir nepieciešams :
   5.1. Paziņot par to uzraudzības iestādei (Datu valsts inspekcijai), iesniedzot par to paziņojumu (ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums kļuvis zināms)**;**
   5.2. Paziņot par to datu subjektam, kura tiesības un brīvības ir aizskartas personas datu aizsardzības pārkāpuma rezultātā un attiecīgais pārkāpums var radīt augstu risku tā tiesībām un brīvībām (jāpaziņo bez nepamatotas kavēšanas).
6. Paziņojums datu subjektam nav jāsniedz, ja tiek izpildīts jebkurš no šādiem nosacījumiem:
   6.1. Uzņēmums ir īstenojis atbilstīgus tehniskus un organizatoriskus aizsardzības pasākumus un minētie pasākumi ir piemēroti datiem, ko skāris datu aizsardzības pārkāpums, jo īpaši tādi pasākumi, kas personas datus padara nesaprotamus personām, kurām nav pilnvaru piekļūt datiem, piemēram, šifrēšana;
   6.2. Uzņēmums ir veicis turpmākus pasākumus, ar ko nodrošina, lai, visticamāk, vairs nevarētu materializēties augstais risks attiecībā uz datu subjektu tiesībām un brīvībām;
   6.3. tas prasītu nesamērīgi lielas pūles. Šādā gadījumā tā vietā izmanto publisku saziņu vai līdzīgu pasākumu, ar ko datu subjekti tiek informēti vienlīdz efektīvā veidā.
7. Ja paziņošana uzraudzības iestādei nav notikusi 72 stundu laikā, paziņojumam pievieno kavēšanās iemeslus.
8. Ja gadījumā uz ziņošanas brīdi nav apkopota visa informācija, lai nodrošinātu tās sniegšanu uzraudzības iestādei, būtu sniedzama informācija, kas Uzņēmumam ir zināma, un, tiklīdz tas ir iespējams, nepieciešams papildināt ziņojumu un nosūtīt to atkārtoti uzraudzības iestādei.
9. Ziņošana uzraudzības iestādei jāveic, aizpildot Datu valsts inspekcijas mājaslapā esošo veidlapu, un iesniedzot to elektroniski parakstītu, nosūtot uz Datu valsts inspekcijas oficiālo e-pasta adresi info@dvi.gov.lv ar norādi “Paziņojums par personas datu aizsardzības pārkāpumu”, ierakstītā sūtījumā vai personīgi Datu valsts inspekcijā, kā arī veicot autorizāciju valsts pārvaldes pakalpojumu portālā www.latvija.lv.

Pielikums Nr.2
"Personas datu un ierobežotas pieejamības
informācijas apstrādes aizsardzības noteikumiem"

DARBINIEKA APLIECINĀJUMS
PAR "PERSONAS DATU UN IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJAS APSTRĀDES AIZSARDZĪBAS NOTEIKUMU"
PRASĪBU IEVĒROŠANU

Es,_____
(vārds, uzvārds)

Ar šo, zemāk parakstījies, apliecinu, ka:

1. Esmu iepazinies (-usies), izprotu un apņemos bez ierunām ievērot Personas datu un ierobežotas pieejamības informācijas apstrādes aizsardzības noteikumu un tā pielikuma prasības un citus rīkojumus, instrukcijas utt. par personu datu aizsardzību un ierobežotas pieejamības informācijas aizsardzību, kuras attiecas uz mani un ar kurām esmu iepazīstināts (a).

2. Apņemos neizmantot ierobežotas pieejamības informāciju, kas saņemta no SIA "ALAAS", savu vai trešo personu interesēs, kā arī apņemos ievērot Fizisko personu datu apstrādes likuma un Vispārīgās datu aizsardzības regulas prasības.

3. Es piekrītu, ka pārtraucot darba (līguma) attiecības ar SIA "ALAAS" jebkādu iemeslu dēļ, es nekavējoties nodošu SIA "ALAAS" manā rīcībā esošo programmatūru un tehnisko aprīkojumu, kā arī manā rīcībā esošos informācijas oriģinālus un kopijas, ko esmu saņēmis(usi) darba (līguma izpildes) laikā, un kas ir manā rīcībā vai kas ir citādi tieši vai netieši manā pārvaldībā.

4. Darba līgumattiecību pārtraukšanas gadījumā, neizpaudīšu un neizmantošu savām un citu vajadzībām ziņas, kas satur personas datus vai ierobežotas pieejamības informāciju.

5. Esmu brīdināts, ka dotā apliecinājuma pārkāpšanas gadījumā, man būs jāsedz zaudējumi vai arī es varu tikt saukts pie krimināatbildības saskaņā ar Latvijas Republikas Krimināllikuma 144.panta, 145.panta un 245. panta noteikumiem.

_____	_____	_____	_____
/Vārds, Uzvārds/	/Paraksts/	/Paraksta atšifrējums/	/Datums/