



## LIELVĀRDES NOVADA DOME

PVN.Nr.90000024489, Raiņa iela 11A, Lielvārde, Lielvārdes novads, LV-5070, tel. 65053370, fakss 65053775, e-pasts: [dome@lielvarde.lv](mailto:dome@lielvarde.lv)

### NOTEIKUMI

Lielvārdē

2018.gada 29.augustā

**Nr.18**

(protokols Nr.13, 20.punkts)

APSTIPRINĀTI

ar Lielvārdes novada domes

2018.gada 29.augusta lēmumu Nr.330

### LIELVĀRDES NOVADA TERITORIJAS VIDEONOVĒROŠANAS NOTEIKUMI

*Izdoti saskaņā ar Eiropas Parlamenta un Padomes  
2016. gada 27. aprīļa regulas (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)  
6. panta 1. punkta (c), (d) un (e) apakšpunktu  
un 2. punkta (e) apakšpunktu*

#### I. Vispārīgie noteikumi

1. Šie Lielvārdes novada pašvaldības videonovērošanas noteikumi (turpmāk – noteikumi) nosaka kārtību, kādā Lielvārdes novada pašvaldības (turpmāk – Pārzinis) administratīvajā teritorijā tiek veikta personas datu – personas attēla, apstrāde videonovērošanas sistēmā (turpmāk – Sistēma), tās vispārīgās tehniskās un organizatoriskās prasības atbilstoši normatīvo aktu prasībām, kas regulē fizisko personu datu aizsardzību.
2. Saskaņā ar noteikumos noteikto kārtību un izmantojot tehniskos līdzekļus, videonovērošanas uzdevums ir apstrādāt bezkontakta veidā iegūtos personas datus ar mērķi:
  - 2.1. piedalīties sabiedriskās kārtības nodrošināšanā;
  - 2.2. apkarot žūpību un netiklību;
  - 2.3. aizsargāt personu dzīvību, veselību un īpašumu;
  - 2.4. identificēt, novērst vai atklāt prettiesiskus nodarījumus;
  - 2.5. saglabājot pierādījumus par personu prettiesiskām darbībām.
3. Pārzinis videonovērošanas kameras un iekārtas uzturēšanu uztic trešajai personai (turpmāk – Ārpakalpojuma sniedzējs), kura, pamatojoties uz ar Pārzini noslēgto pakalpojuma sniegšanas līgumu, nodrošina Pārziņa videonovērošanas kameru un iekārtu

pārvaldību, attīstību, drošību un auditu. Ārpakalpojuma sniedzējam jānodrošina tādas pat datu apstrādes aizsardzības prasības kādas nodrošina Pārzinis.

4. Pārziņa atbildīgajai personai par datu apstrādi (turpmāk – atbildīgā persona) un Ārpakalpojuma sniedzējam un Ārpakalpojuma sniedzēja darbiniekiem kā Sistēmas lietotājiem (turpmāk – lietotājs) ir saistoši šie noteikumi un licencēto iekārtu, tās programmas lietošanas instrukcijās norādītās prasības.
5. Ārpakalpojuma sniedzēja pienākums ir lietot nepieciešamos tehniskos un organizatoriskos līdzekļus, lai aizsargātu personas datus un novērstu nelikumīgu to apstrādi.
6. Ja videonovērošanas laikā netiek iegūts attēls, no kura ir iespējams identificēt datu subjektu (piem., zema izšķirtspēja), tad šo noteikumu prasības, kas attiecas uz fizisko personu datu aizsardzību, nav piemērojamas.

## **II. Tehniskie resursi ar kādiem tiek nodrošināta personas datu apstrāde un tās drošība**

7. Personas dati tiek uzglabāti un apstrādāti Sistēmā – licencētajās video iekārtās un to programmās, novērošanai izmantojot videonovērošanas kameras, kas darbojas reaģējot uz kustību vai izmantojot videonovērošanas kameras, kas darbojas nepārtraukti.
8. Sistēmas iekārtām un videokamerām ir jābūt uzstādītām tādām, lai nodrošinātu attēla nolūkam atbilstošu kvalitāti, ņemot vērā tehnisko specifikāciju un vietu vai vidi, kur tās ir novietotas.
9. Ja tiek lietota bezvadu datu pārraide, jānodrošina attiecīgi drošības pasākumi, lai datu pārraidē nebūtu pārrāvumi un personas dati noteiktu laiku tiktu saglabāti, kā arī dati netiktu pārtverti.
10. Sistēmā nepieciešamības gadījumā ir jāizvēlas atbilstošs datu saspiešanas (kompresijas) lielums, lai neietekmētu attēla kvalitāti.
11. Uz video ieraksta attēliem nodrošina precīzu laiku un datumu, kad ieraksts tiek veikts vai ir veikts.
12. Ārpakalpojuma sniedzējs organizē pastāvīgu videokameru tehnisko apkalpošanu, lai nodrošinātu videokameras augstas kvalitātes darbspēju.
13. Vietās, kurās tiek veikta videonovērošana, izvieto informatīvo paziņojuma par videonovērošanas veikšanu (1. pielikums).
14. Sistēmā esošajiem personas datiem Ārpakalpojuma sniedzējs nodrošina piekļuvi Pārziņa atbildīgajai personai ar atsevišķi piešķirtu piekļuves lietotājvārdu un unikālu paroli, kura ir zināma tikai šai personai.
15. Parole sastāv no vismaz deviņiem simboliem un veidojama komplicēti, izmantojot mazo un lielo burtu un ciparu kombināciju (piem., Saule2013s);
16. Paroli aizliegts veidot, izmantojot ar sistēmas lietotāju saistītu informāciju (piemēram, personu vārdus, uzvārdus, dzimšanas dienas, tālruņa numurus, automašīnas numuru, mājdzīvnieku un tuvinieku vārdus u.tml.).
17. Paroli ieteicams mainīt ne retāk kā reizi trijos mēnešos. Izveidojot jaunu paroli, aizliegts lietot iepriekšējās trīs izmantotās paroles.
18. Atbildīgajai personai un Lietotājam parole ir jāiegaumē. Nedrīkst paroli pierakstīt, ja šo informāciju neglabā aizslēgtā seifā vai citā vietā ar ierobežotu piekļuvi citām personām.

19. Parole nedrīkst būt pieejama trešajām personām.
20. Ja Sistēmā tiek uzglabāti īpašo kategoriju personas dati, tad tās piekļuvei ievieš vairāklīmeņu autentifikāciju ar ID kartēm, sertifikātiem, kodu kalkulatoriem vai citiem līdzekļiem.
21. Sistēmas nodrošināšanai izmanto licencētu programmatūru.
22. Telpā, kurā tiek veikta personas datu apstrāde (servera vai datora atrašanās vietā) nepieciešamā temperatūra ir ne mazāk kā + 10 C° un ne vairāk kā + 30 C°. Nepieciešamie fiziskie apstākļi datu nesēja iekārtai tiek uzturēti, nodrošinot telpās apkuri un ventilāciju un telpā ir uzstādīta pārvietojamā ugunsdzēsamā iekārta.
23. Tehnisko resursu darbības nepārtrauktību nodrošina nepārtraukta barošanas iekārta (UPS).
24. Sistēmas ierakstu rezerves kopiju veikšana nav obligāta. Lēmumu par nepieciešamību nodrošināt rezerves kopiju pieņem Pārziņa atbildīgā persona.
25. Sistēmas datu rezerves kopijām jānodrošina tāds pats drošības un aizsardzības līmenis kā pašai Sistēmai atbilstoši šiem noteikumiem.
26. Iespēju robežās ierakstu aplūkošanu un izpaušanu nodrošina tā, lai tiktu identificēta persona, kura aplūkoja vai izpauđa personas datus, kā arī šādu personas datu saņēmēju identitāti (auditācija).

### **III. Videonovērošanas kameru izvietošana un novērošana**

27. Aizliegts izmantot videonovērošanas kameras, lai ierakstītu sarunas starp cilvēkiem. Iekārtas ierīko tādas, kas neveic audio ierakstus vai videonovērošana veic tādā veidā, lai audio ieraksta funkcija tiktu atslēgta.
28. Sistēmai pieslēgtās videonovērošanas kameras novieto tā, lai netiktu apstrādāti tādi īpašo kategoriju personas dati, kuru apstrāde nav nepieciešama un tā, lai videonovērošanas sistēma nodrošinātu personas privātumu.
29. Videonovērošanas kameras jāuzstāda tā, lai to novērošanas laukums būtu tik liels, cik ir nepieciešams konkrētam videonovērošanas mērķim.
30. Sistēmas iekārtām un videokamerām ir jābūt uzstādītām tā, lai nodrošinātu attēla atbilstošu kvalitāti, ņemot vērā to tehnisko specifikāciju un vietu vai vidi, kur tās ir novietotas.
31. Sistēmas videonovērošanas attēlu aplūkošana jāveic atsevišķā telpā vai tādā veidā, lai nepiederošām personām nebūtu iespēja to redzēt.
32. Videonovērošanas attēlus monitorā drīkst vērot tikai tās personas, kuras pienākumos ietilpst minētās darbības veikšana.
33. Videokameras izvieto precīzi un atbilstoši uzstādīšanas nolūkam – iekārta ir jāizvieto tā, lai ar to varētu novērot tikai tās vietas, kas paredzētas videonovērošanai.
34. Videonovērošanas laikā iegūtajiem attēliem jābūt noderīgiem paredzētajam nolūkam.
35. Ja paredzēts padarīt attēlus plašāk pieejamus, tad šādu lēmumu jāpieņem domes priekšsēdētājam, dokumentējot pieņemtā lēmuma pamatojumu.
36. Ja pieņemts lēmums par attēlu izpaušanu plašsaziņas līdzekļiem, tad fizisko personu attēli ir jākodē vai jāpadara neskaidri, lai personas nebūtu identificējamās.

37. Ja videomateriāls vai no tā iegūtie attēli tiek glabāti kā pierādījums, tad tie jāglabā drošā vietā, kurai piekļuve tiek kontrolēta.
38. Piekļuve ierakstītajiem datiem jāierobežo tikai līdz vadītājam (domes priekšsēdētājam) vai nozīmētam darbiniekam, kurš pieņems lēmumu par to, vai pieņemt piekļuves pieprasījumus no datu subjekta un trešajām personām saskaņā ar noteikumos iestrādāto kārtību.

#### **IV. Sistēmā apstrādājamo datu klasifikācija**

39. Pēc vērtības Sistēmā esošā informācija ir uzskatāma par vidēji augstas vērtības informāciju.
40. Pēc konfidencialitātes informācija ir uzskatāma par konfidenciālu un ierobežotas pieejamības informāciju.
41. Videonovērošanas dati klasificējami kā ierobežotas pieejamības informācija, kurai drīkst piekļūt tikai Pārzinis, atbildīgā persona un lietotāji.

#### **V. Drošības pasākumi attiecībā uz piekļuvi Sistēmai**

42. Lai nodrošinātu Sistēmā esošo datu drošību un fiksētu visus personas datu apstrādes gadījumus, ir jāievēro šādas prasības:
  - 42.1. Videonovērošana tiek veikta reālā laika režīmā un ieraksti tiek uzglabāti ne mazāk kā septiņas dienas un ne vairāk kā 30 dienas, ja speciālie normatīvie akti nenosaka citu personas datu glabāšanas termiņu. Ieraksti tiek dzēsti automātiski hronoloģiskā secībā no ieraksta brīža;
  - 42.2. par Sistēmā esošo personas datu dzēšanu, tajā skaitā rezerves kopijas, un par personas datu saglabāšanu ir atbildīgs Pārzinis vai Ārpakalpojuma sniedzējs;
  - 42.3. Ārpakalpojuma sniedzējs ar rīkojumu ieceļ atbildīgo personu piekļuvei Sistēmai un tajā esošo personas datu apstrādei;
  - 42.4. Sistēmā esošo personu datu dzēšanu, kopēšanu, vai nodošanu tiesībaizsardzības iestādēm, citai personai vai datu subjektam veic atbildīgā persona pēc minētās iestādes, datu subjekta vai citas personas tiesiska, rakstiska pamatojuma un ar Pārziņa atļauju;
  - 42.5. sagatavojot personas datus nodošanai tiesībaizsardzības iestādei, citai personai vai datu subjektam, ievēro, ka personas datu nodošana nedrīkst radīt citas videoierakstā redzamas personas tiesību aizskārumu. Šādos gadījumos videoierakstā esošos datus, kas neattiecas uz konkrēto personu, apslēpj (izdzēš, aizklāj vai padara neskaidrus).
43. Personas datu apstrāde Sistēmā tiek ierakstīta reģistrācijas lapā:
  - 43.1. videoieraksta iekārtā esošo datu (ierakstu) apskate (arī trešo personu apskate) un nodošana trešajām personām un tiesībaizsardzības iestādēm vai pārsūtīšana pa elektronisko pastu (2. pielikums);
  - 43.2. videoieraksta iekārtā esošo datu (ierakstu) kopēšana uz citiem datu nesējiem vai pārsūtīšana elektroniski pa elektronisko pastu (3. pielikums);
  - 43.3. videoieraksta iekārtā esošo datu (ierakstu) manuāla dzēšana (4. pielikums).

44. Visas reģistrācijas lapas tiek uzglabātas pie Ārpakalpojuma sniedzēja un ir pieejamas Pārziņa atbildīgajai personai, un pēc pieprasījuma arī kompetentām tiesībsardzības iestādēm un citām personām normatīvajos aktos noteiktajos gadījumos un kārtībā.

## **VI. Ārkārtas apstākļi**

45. Ārkārtas apstākļu gadījumā Sistēmas darbības aizsardzība notiek saskaņā ar telpu ugunsdrošības noteikumiem. Iespēju gadījumā tehniskie resursi, uz kuriem tiek glabāti personas dati jānogādā drošā vietā.
46. Ārpakalpojuma sniedzējs nodrošina pietiekamu dokumentāciju, lai varētu izdarīt izmaiņas Sistēmā vai arī pilnībā atjaunot Sistēmu apdraudējuma iestāšanās gadījumā.
47. Ārkārtas apstākļu gadījumā Sistēmas darbības atjaunošanai izmanto līdzīgus tehniskos resursus un, ja nepieciešams, izmanto arī rezerves kopiju pierakstus.

## **VII. Līdzekļi ar kādiem tiek nodrošināti tehniskie resursi pret tīšu bojāšanu un neatļautu personas datu iegūšanu**

48. Sistēmas tehniskie resursi tiek saglabāti, nodrošinot telpu aizslēgšanu pēc darba laika beigām.
49. Telpā, kurā tiek veikta personas datu apstrāde (atrodas serveris vai dators, kurā glabājas ieraksts) Sistēmai nevar piekļūt nepiederošas personas.

## **VIII. Lietotāja tiesības un pienākumi**

50. Lietotājs ir persona, kurai Ārpakalpojuma sniedzējs ir piešķīris piekļuvi Sistēmas darbam, ņemot vērā šo noteikumu 14. punkta prasības.
51. Lietotājs nav tiesīgs pēc savas iniciatīvas Sistēmas tehniskajos resursos instalēt programmatūru bez licences vai jebkādu citu programmatūru, kas neattiecas uz lietotāja darbu. Lietotājam nav tiesības pieinstalēt tehniskajiem resursiem arī pieslēdzamu ārējo datu nesēju (cietais disks, zibatmiņa un līdzīgas atmiņas iekārtas, lasītājus un jebkuras citas iekārtas) bez atbildīgās personas atļaujas.
52. Lietotājs nav tiesīgs bez Ārpakalpojuma sniedzēja rakstiskas atļaujas ienest un pieslēgt iekārtai savu personīgo datoru vai citu ierīci, kā arī iznest jebkādu informāciju uz jebkādiem datu nesējiem ārpus darba vietas bez Pārziņa vadības vai atbildīgās personas rakstiskas atļaujas.
53. Sistēmas datus lietotājs nedrīkst kopēt ārējos datu nesējos (CD, DVD, USB diskos, zibatmiņas ierīcēs u.tml.), izņemot gadījumus, kad tas nepieciešams rezerves kopiju nodrošināšanai.
54. Paroles nozaudēšanas vai citādas kontroles nozaudēšanas gadījumā, lietotājam ir pienākums par to nekavējoties paziņot Ārpakalpojuma sniedzējam un nekavējoties tiek nomainīta attiecīgā lietotāja piekļuves parole.
55. Lietotājs nav tiesīgs pats iznīcināt datu nesējus, tie jānodod atbildīgajai personai.
56. Lietotājam nav tiesību piekļūt auditācijas pierakstiem bez Ārpakalpojuma sniedzēja atļaujas.

57. Lietotājam nav tiesību izpaust ziņas par Sistēmas uzbūvi un konfigurāciju, kā arī atklāt klasificēto informāciju citām personām.
58. Lietotājiem šo noteikumu prasības tiek izklāstītas klātienē.
59. Par jebkuru personas datu apstrādes incidentu lietotājam, kas to konstatējis, ir nekavējoties jāpaziņo ārpakalpojuma sniedzējam:
  - 59.1. ja konstatēts jebkāda veida apdraudējums tehniskajiem resursiem (elektroenerģijas padeves pārtraukums, šķidrums vai svešķermeņu iekļūšana, bojājumi fiziska trieciena, uguns iedarbības vai plūdu rezultātā u.c.);
  - 59.2. ja konstatēts jebkāda veida apdraudējums informācijas resursiem (trešajām personām kļuvusi zināma pieejas parole, konstatēta nesankcionēta piekļuve, konstatēti darbības pārtraukumi u.c.).
60. Incidentu gadījumā lietotājam savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt tehnisko un informācijas resursu drošību līdz atbildīgās personas ierašanās brīdim.

### **IX. Pārziņa un Ārpakalpojuma sniedzēja pienākumi**

61. Atbildīgo personu ar rīkojumu nosaka Pārziņa vadītājs divu nedēļu laikā no šo noteikumu spēkā stāšanās dienas. Ar rīkojumu Pārzinis iepazīstina Ārpakalpojuma sniedzēju.
62. Ārpakalpojuma sniedzējam ir šādi pienākumi:
  - 62.1. uzraudzīt personas datu apstrādē lietotāju darbības ar tehniskajiem līdzekļiem un informācijas resursiem;
  - 62.2. nodrošināt lietotāju instruēšanu un iepazīšanos ar šiem noteikumiem un apņemšanos saglabāt un nelikumīgi neizpaust personas datus;
  - 62.3. nodrošināt Sistēmas darbību atbilstoši normatīvo aktu prasībām, kas regulē fizisko personu datu aizsardzību;
  - 62.4. veikt personas datu apstrādes fiksāciju šo noteikumu 43. punktā minētajās reģistrācijas lapās;
  - 62.5. šo noteikumu 43. punktā minētās reģistrācijas lapas saglabāt 60 mēnešus no pēdējā ieraksta datuma attiecīgajā lapā;
  - 62.6. nodrošināt, ka uzstādītajām Sistēmas videokamerām, kā arī serverim, datoram un tā cietajam diskam vai citām ar to saistītajām ierīcēm var piekļūt tikai lietotāji;
  - 62.7. regulāri pārbaudīt Sistēmas iekārtu stāvokli un darbību, kā arī pārbaudīt un novērst konstatētās iekārtu darbības problēmas;
  - 62.8. veikt lietotāju darba un pienākumu uzraudzību Sistēmā;
  - 62.9. katru gadu organizēt personas datu apstrādes iekšējo auditu, identificējot informācijas sistēmas apdraudējuma riskus un to iestāšanās varbūtību (organizē riska analīzes veikšanu), un noteikt veicamos pasākumus informācijas sistēmu tehnisko un informācijas resursu aizsardzībai;
  - 62.10. pārbaudīt ugunsdrošības iekārtu derīguma pārbaudes veikšanu un nepieciešamības gadījumā ierosināt darbības, lai novērstu trūkumus;
  - 62.11. noteikt Sistēmā esošās informācijas vērtību un konfidencialitātes pakāpi, nepieciešamības gadījumā sagatavo lēmumu par informācijas vērtību vai konfidencialitātes pakāpes paaugstināšanu vai pazemināšanu;

- 62.12. nodrošināt pastāvīgu kontroles aizsardzību pret datorvīrusiem, ļaunatūru un citiem līdzīgiem draudiem. Regulāri atjaunināt Sistēmas programmatūru;
  - 62.13. sagatavot Sistēmā esošo personas datu nodošanu tiesībaizsardzības iestādei, citai personai vai datu subjektam, ievērojot citu videoieraksta redzamo personu tiesību aizskārumu, dzēšot, aizklājot vai padarot miglainu šo personu;
  - 62.14. ja noticis personas datu aizsardzības pārkāpums, nekavējoties, bet ne vēlāk kā 72 stundu laikā pēc tam, kad pārkāpums tam kļuvis zināms, par to paziņo Pārziņa atbildīgajai personai, uzraudzības iestādei un Informācijas tehnoloģiju drošības incidentu novērošanas institūcijai (turpmāk – CERT.lv);
  - 62.15. pēc Pārziņa vai Ārpakalpojuma sniedzēja lietotāja darba tiesisko attiecību izbeigšanu vai ilgstošu prombūtni, nekavējoties bloķēt tā kontu un citus autentifikācijas līdzekļus;
  - 62.16. reizi gadā veikt Ārpakalpojuma sniedzēja lietotāju apmācības saistībā ar personas datu aizsardzību, akcentējot rīcību, kad iespējams ir notikusi nelikumīga personas datu apstrāde.
63. Ārpakalpojuma sniedzējam ir šādas tiesības:
- 63.1. liegt konkrētam lietotājam tiesības piekļūt Sistēmai, ja lietotājs apdraud Sistēmas darbību vai pārkāpj šos noteikumus;
  - 63.2. veikt lietotāju paroli nomaiņu bez iepriekšēja brīdinājuma. Lietotājs var saņemt paroli pēc tās nomaiņas;
  - 63.3. veikt Sistēmā esošo personu datu dzēšanu, kopēšanu, vai nodošanu tiesībaizsardzības iestādei, citai personai vai datu subjektam pēc minētās iestādes, datu subjekta vai citas personas tiesiska, rakstiska pamatojuma un ar Pārziņa vadības atļauju.

## **X. Datu subjekta tiesības saņemt videonovērošanas datus**

64. Datu subjektam ir tiesības piekļūt informācijai attiecībā uz videonovērošanu, kas ir Ārpakalpojuma sniedzēja rīcībā (tai skaitā, ja tā ir tehniski pieejama), bet to nav iespējams labot vai papildināt, jo pretējā gadījumā tā tiks uzskatīta par informācijas viltošanu vai sagrozīšanu.
65. Ārpakalpojuma sniedzējs nodrošina videomateriāla kopijas rezervēšanu, izrakstot videomateriālu no lokālā video arhīva:
  - 65.1. ja saņemts datu rezervācijas pieprasījums no tiesībaizsardzības iestādes. Šādu pieprasījumu Ārpakalpojuma sniedzējs apstrādā nekavējoties pēc tā saņemšanas un nosūta tiesībaizsardzības iestādei videomateriāla kopiju;
  - 65.2. ja ir saņemta personas sūdzība par jebkuru informācijas kanālu, ko Ārpakalpojuma sniedzējs kontekstā ar videonovērošanas nolūkiem ir novērtējis kā pietiekamu datu rezerves pieprasījuma apstrādei (piem., ja subjekts klātienē nav identificēts, bet viņš pa informatīvo tālruni paziņo, ka viņš ir novērojis ka, Pārziņa vai Ārpakalpojuma sniedzēja darbinieks ir veicis prettiesiska labuma pieņemšanu);
  - 65.3. ja ir iestājies notikums, kas automātiski informē par drošības incidenta pazīmēm, vai ja Ārpakalpojuma sniedzējs ir veicis rezervācijas pieprasījumu saskaņā ar iekšējās kontroles prasībām;

- 65.4. ja ir saņemts rakstveida iesniegums no datu subjekta, kas satur informāciju pieprasīto datu identificēšanai, un datu subjekts klātienē ir identificēts saskaņā ar noteiktajām prasībām atbilstoši 68. punktam.
66. Ārpakalpojuma sniedzējs vai Pārzinis datu subjektam izsniedz foto fiksāciju/-as no videomateriāla, aizzīmējot citu personu foto fiksācijas datus, videomateriāla aprakstu un/vai audioieraksta izklāstu, neatklājot citu personu audioieraksta datus. Datu subjektam izsniedz to foto fiksāciju, kas visvairāk atbilst videonovērošanas datu pieprasījuma pamatojumam.
67. Ja datu subjekts nav identificēts pirms rezervācijas pieprasījuma saņemšanas, tad Pārzinis datu subjektam izsniedz videonovērošanas datus, ja datu subjekts klātienē ir identificēts saskaņā ar noteiktajām prasībām atbilstoši 68. punktam un, datu subjekts ir iesniedzis rakstveida iesniegumu atbilstoši 69. punktam.
68. Noteiktās prasības datu subjekta identificēšanai klātienē:
- 68.1. datu subjekts ierodas Pārziņa mītnes vietā – Raiņa iela 11 A, Lielvārdē, Lielvārdes novadā, LV-5070, klientu apkalpošanas centrā un informē, ka vēlas saņemt videonovērošanas datus un ir ieradies klātienē identifikācijai;
- 68.2. datu subjekts Pārziņa darbiniekam uzrāda personu apliecinošu dokumentu un iesniedz vienu krāsainu fotogrāfiju, kur datu subjekts redzams pilnā augumā un pēc kuras datu subjektu var vizuāli identificēt atbilstoši personu apliecinošajā dokumentā esošajai fotogrāfijai.
69. Noteiktās prasības rakstveida iesnieguma saturam, kas ir iesniedzams pēc datu subjekta identificēšanas klātienē, tam klāt pievienojot vienu krāsainu fotogrāfiju:
- 69.1. videonovērošanas datu pieprasīšanas pamatojums;
- 69.2. datums, laiks un vieta (tai skaitā videokameras atrašanās vieta, ja tā ir zināma), kur videomateriāls tika uzņemts;
- 69.3. situācijas vai notikuma apraksts (kurā fiksēti datu subjekta videonovērošanas dati);
- 69.4. detalizēts datu subjekta vizuālā izskata apraksts, kas ietver informāciju par apģērbu un mantām, kas atradās pie datu subjekta, un konkrētu datu subjekta atrašanās vietu, kurā datu subjekts bija atradies;
- 69.5. cita informācija, kas ir būtiska pieprasīto datu identificēšanai;
- 69.6. vēlamais videonovērošanas datu saņemšanas termiņš.
70. Datu subjektam ir tiesības saņemt tikai tos videonovērošanas datus, kuros ir redzams vai dzirdams konkrētais datu subjekts, kura vizuālais izskats sakrīt ar iesniegto fotogrāfiju un vizuālā izskata aprakstu. Tomēr netiks izsniegti videonovērošanas dati, ja netiks gūta pietiekami pamatota pārliecība par videonovērošanas datu pieprasīšanas pamatotību un datu subjekta atpazīstamību videomateriālā.
71. Datu subjektam nav tiesību saņemt videonovērošanas datus, kuros ir redzami vai dzirdami citi datu subjekti. Tāpēc datu subjektam izsniedz informāciju attiecībā uz videonovērošanu tikai 68. punktā noteiktajā veidā, bet neizsniedz videomateriāla kopijas rediģētā veidā, it īpaši tāpēc, ka atbilstoši Pārziņa veiktās videonovērošanas apjomam, kontekstam un nolūkiem:
- 71.1. videonovērošanas vietā var atrasties citi datu subjekti, kuru dati nav izpaužami (ne identificētā, ne neidentificētā veidā);
- 71.2. rediģētā veidā sagatavotais videomateriāls var radīt maldīgu priekšstatu par patieso notikuma gaitu.



72. Datu subjektam neizsniedz informāciju attiecībā uz videonovērošanu, ja datu subjekta pieprasījums ir acīmredzami nepamatots (tai skaitā nesaistīts ar videonovērošanas nolūkiem vai ar nepietiekamu videonovērošanas datu pieprasīšanas pamatojumu), vai prasa pārmērīgas Pārziņa vai Ārpakalpojuma sniedzēja pūles, jo īpaši regulārās atkārtotās dēļ.
73. Uz ikvienu datu subjekta rakstveida iesniegumu, tai skaitā par savu tiesību īstenošanu, Pārzinis vai Ārpakalpojuma sniedzējs atbild datu subjektam viena mēneša laikā, izņemot normatīvajos aktos noteiktos datu subjektus, kuriem atbilde sniedzama īsākā laika periodā.
74. Ja datu subjekta tiesību īstenošana ir informācijas saņemšana attiecībā uz videonovērošanu, Pārzinis un Ārpakalpojuma sniedzējs pēc iespējas ņems vērā datu subjekta norādīto vēlamo videonovērošanas datu saņemšanas termiņu, ko iespēju robežās centīsies izpildīt ātrāk atbilstoši datu subjekta lūgumam. Taču, ja atbildi nebūs iespējams sniegt viena mēneša laikā vai citā normatīvajā aktā noteiktajā termiņā, datu subjektu informēs par kavēšanās iemesliem.
75. Ja datu subjekts uzskata, ka videonovērošanas zonā ir noticis datu subjekta tiesību aizskārums, un ir nepieciešama steidzama pierādījumu nodrošināšana par noziedzīgu nodarījumu, datu subjektam būtu nekavējoties jāvēršas ar iesniegumu tiesībaizsardzības iestādē, kura Pārzinim vai Ārpakalpojuma sniedzējam iesniedz datu rezervācijas pieprasījumu, pamatojoties uz normatīvajos aktos noteiktajām tiesībām pieprasīt un saņemt informāciju.
76. Pārzinis un Ārpakalpojuma sniedzējs sadarbojas ar tiesībaizsardzības iestādēm, lai optimizētu to kompetences ietvaros pieprasītās informācijas par noziedzīgiem nodarījumiem, citiem likumpārkāpumiem un notikumiem, kuri apdraud personu vai sabiedrības drošību, datu apmaiņas procesu un lai nodrošinātu informācijas pieejamību.

## **XI. Drošības incidentu izmeklēšanas kārtība**

77. Gadījumā, ja Sistēmas iekārta ir bojāta vai ir noticis nesankcionēts mēģinājums piekļūt informācijai, vai informācija, vai iekārtas daļa ir zudusi, tas uzskatāms par drošības incidentu.
78. Konstatējot personas datu aizsardzības pārkāpumu vai Sistēmas drošības incidentu, šo noteikumu pārkāpumu vai tā sekas, atbildīgā persona veic šādas darbības:
  - 78.1. pārbauda manuālos un elektroniskos auditācijas pierakstus un to integritāti piekļuvei Sistēmā un pārtrauc Sistēmas darbību, kamēr nav noskaidroti riski un incidenta cēloņi;
  - 78.2. pieprasa personas datu aizsardzības pārkāpumā vai drošības incidentā iesaistītajai Pārziņa vai Ārpakalpojuma sniedzēja atbildīgajai personai rakstveida paskaidrojumu;
  - 78.3. par notikušo personas datu aizsardzības pārkāpumu vai iespējamo drošības incidenta esamību izdara ierakstu Pārkāpumu reģistrā (5. pielikums);
  - 78.4. noskaidro personas datu aizsardzības pārkāpuma vai drošības incidenta cēloņus un nepieciešamības gadījumā izstrādā grozījumus šajos drošības noteikumos, ieviešot papildu aizsardzības prasības;
  - 78.5. pieņem lēmumu par riska ietekmi uz datu subjekta tiesībām;

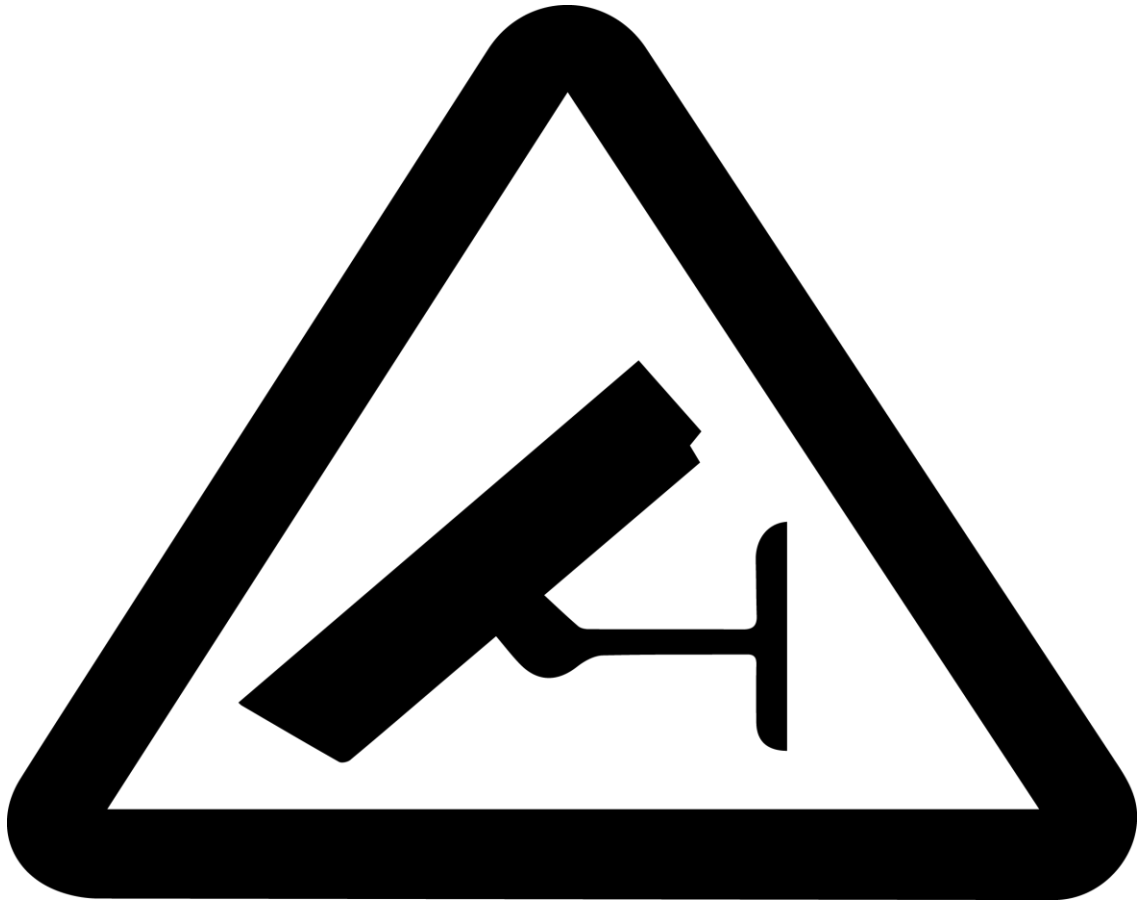
- 78.6. ja personas datu aizsardzības pārkāpums vai drošības incidents var radīt risku datu subjekta tiesībām un brīvībām, tad Ārpakalpojuma sniedzējs par datu aizsardzības pārkāpumu nekavējoties paziņo Datu valsts inspekcijai un CERT.lv, bet ne vēlāk kā 72 stundu laikā no brīža, kad drošības incidents ir kļuvis zināms;
- 78.7. ja konstatē, ka personas datu aizsardzības pārkāpums vai drošības incidents var radīt augstu risku datu subjekta tiesībām un brīvībām Ārpakalpojuma sniedzējs nekavējoties par to paziņo datu subjektam;
- 78.8. nepieciešamības gadījumā virza jautājumu par vainīgās Pārziņa vai Ārpakalpojuma sniedzēja darbinieka saukšanas pie atbildības.
79. Ja rodas aizdomas par noziedzīgu nodarījumu (piem., personas datu zādzību), Pārzinis pēc saskaņošanas ar atbildīgo personu un Ārpakalpojuma sniedzēju pieņem lēmumu par ziņošanu tiesībaizsardzības iestādēm.
80. Sistēmas drošības incidentu gadījumā tiek veikta pārbaude un nepieciešamības gadījumā tiek ieviesti citi drošības pasākumi.
81. Personas datu apstrādes aizsardzības drošības incidenta paziņojuma veidlapa datu valsts inspekcijai ir pieejama: <http://www.dvi.gov.lv/lv/personas-datu-apstrades-aizsardzibas-parkapuma-pazinojuma-iesniegsana/>.

## **XII. Noslēguma jautājumi**

82. Noteikumos paredzētās drošības prasības tiek pārskatītas vienu reizi gadā, kā arī, ja ir notikušas izmaiņas spēkā esošajos ārējos normatīvajos aktos.
83. Šie noteikumi ir uzskatāmi par ierobežotas pieejamības informāciju un izpaužami tikai noteiktos gadījumos, kad to pieprasa valsts pārvaldes vai tiesībaizsardzības iestādes.

Domes priekšsēdētāja

S.Ločmele



### VIDEONOVĒROŠANA

**Mērķis:** aizsargāt personu vitālās intereses, tajā skaitā dzīvības un veselības, aizsardzību, izpildīt uzdevumu, kas tiek veikts sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras.

**Pārzinis:** Lielvārdes novada pašvaldība, adrese: Raiņa iela 11 A, Lielvārde, Lielvārdes novads, LV-5070, tālr. \_\_\_\_\_, e-pasta adrese: \_\_\_\_\_,

**Tiesiskais pamats:** Datu regulas 6. panta 1. punkta (c), (d) un (e) apakšpunkts un 2. punkta (e) apakšpunkts

**Leģitīmās intereses:** noziedzīgu nodarījumu novēršana, sabiedriskās kārtības nodrošināšana

**Datu saņēmēji:** valsts pārvaldes un tiesībaizsardzības iestādes, to likumā noteikto funkciju un uzdevumu izpildei. Datu nodošana uz trešo valsti nav paredzēta

**Glabāšanas termiņš:** ieraksti tiek uzglabāti ne ilgāk kā 30 kalendārās dienas.

**Sūdzības** par datu apstrādes pārkāpumiem jāiesniedz Datu valsts inspekcijai, Blaumaņa ielā 11/13 – 11, Rīga, LV-1011, e-pasta adrese:

**Lielvārdes novada pašvaldības videonovērošanas sistēmas veikto videoierakstu  
(personas datu) apskates/nodošanas trešajām personām reģistrācijas lapa Nr.1**

Nr. p.k.	Datums un laiks	Trešā persona, vārds, uzvārds, amats, kura piedalījās datu apskatē	Trešās personas paraksts vai nosūtīšanas adrese	Atbildīgās personas paraksts	Ieraksta apskates /nodošanas iemesls	Datums un laiks par kādu periodu tika veikta ieraksta apskate/nodošana
1.						
2.						
3.						
4.						
5.						
6.						
7.						

**Lielvārdes novada pašvaldības videonovērošanas sistēmas veikto videoierakstu  
(personas datu) kopēšanas uz citiem datu nesējiem reģistrācijas lapa Nr.1**

Nr. p.k.	Datums un laiks	Vārds, uzvārds, amats, kura piedalījās datu kopēšanā	Atbildīgās personas paraksts	Ieraksta kopēšanas iemesls	Datums un laiks par kādu periodu tika veikt ieraksts kopēšana
1.					
2.					
3.					
4.					
5.					
6.					
7.					

**Lielvārdes novada pašvaldības  
videonovērošanas sistēmas veikto videoierakstu (personas datu)  
dzēšanas reģistrācijas lapa Nr.1**

<b>Nr. p. k.</b>	<b>Datums un laiks</b>	<b>Vārds, uzvārds, amats, kura piedalījās datu dzēšanā</b>	<b>Atbildīgās personas paraksts</b>	<b>Ieraksta dzēšanas iemesls</b>	<b>Datums un laiks par kādu periodu tika veikta ieraksta dzēšana</b>
1.					
2.					
3.					
4.					
5.					
6.					
7.					

**Pārkāpumu reģistrs**

Nr. p.k.	Pārkāpuma veids	Pārkāpumu konstatējošā persona	Pārkāpuma konstatēšanas brīdis	Pārkāpuma rašanās iemesls	Ietekme uz datu subjekta tiesībām	Ziņošana DVI/ datu subjektam/ tiesībaizsardzības iestādēm	Pārkāpuma radīto seku novēršana
1.							
2.							
3.							
4.							
5.							
6.							
7.							