

Ziņojums par preventīvo pārbaudi par apsardzes pakalpojumu sniegšanas uzturēšanu sniegtiem pakalpojumiem attiecībā uz videonovērošanu

Datu valsts inspekcija 2025. gada darba plāna ietvaros noteica veikt preventīvu pārbaudi uzturēumos, kuru pamatdarbība ir apsardzes pakalpojumu sniegšana, un kuri pamatdarbības ietvaros piedāvā arī pakalpojumus, kas saistīti ar videonovērošanas uzstādīšanu, veikšanu juridisku personu īpašumos pēc to lūguma.

Šāda preventīvās pārbaudes joma izvēlēta ņemot vērā līdz šim Datu valsts inspekcijā saņemtos jautājumus par apsardzes uzturēšanu uzstādītām videonovērošanas sistēmām, kas saistīti, piemēram, ar nepamatotu videoierakstu vai to attēlu noplūdi un publicēšanu, kā arī tādēļ, ka 2024. gada rudenī tika publicētas Datu valsts inspekcijas sagatavotās vadlīnijas “PRAKTISKĀS VIDEO NOVĒROŠANAS VADLĪNIJAS JURIDISKĀM PERSONĀM UN KOPIĀŠNIEKIEM”. Tāpat Datu valsts inspekcija savā praksē novērojusi neizpratni vai neatbilstošu izpratni par datu aizsardzības lomu sadalījumu (pārzinis - apstrādātājs), kad viena juridiska persona norīko citu uzstādīt videonovērošanas sistēmu dažādiem nolūkiem.

Pārbaude veikta, izvēloties 25 Latvijā reģistrētus komersantus, kuri nodarbojas ar apsardzes pakalpojumu sniegšanu, sākotnēji uzdodot tiem jautājumus par to īstenoto praksi (ja tāda ir) attiecībā par videonovērošanas sistēmu uzstādīšanu juridiskām personām. Pārbaudes mērķis ir uzzināt par situāciju šajā nozarē, datu aizsardzības nosacījumu izpratni attiecībā uz videonovērošanas veikšanu un, jo īpaši, iegūto videoierakstu apstrādi, kā arī, cik vien iespējams, līdz pārbaudes noslēgumam novērst esošās nepilnības.

Šajā ziņojumā tiks aprakstīts pārbaudes nozīmīgums, pārbaudes būtība, gaita un uz šī ziņojuma sastādīšanas brīdi iegūtie secinājumi par komersantu pieļautajām kļūdām un to sniegtās atbildes uz Datu valsts inspekcijas uzdotajiem jautājumiem. Šī ziņojuma galvenā būtība ir nonākt līdz secinājumiem par apsardzes uzturēšanu praksi, analizējot to iesūtītās atbildes uz Datu valsts inspekcijas jautājumiem, ar uzsvaru uz sliktās prakses piemēriem, par kuriem savukārt tālāk būtu nepieciešams informēt visus pārbaudē iesaistītos uzturēumus, kā arī citus šīs jomas uzturēumus, publicējot ziņojumu Datu valsts inspekcijas tīmekļa vietnē www.dvi.gov.lv.

Tekstā lietotie saīsinājumi:

Inspekcija	Datu valsts inspekcija
Datu regula	Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)
VID	Valsts ieņēmumu dienests
Komersants	Uzņēmums, kura pamatdarbība, atbilstoši <i>NACE</i> 2.1 red. 80.09 (Citur neklasificēti drošības nodrošināšanas pakalpojumi) vai <i>NACE</i> 2.1 red. 80.01 (Izmeklēšanas un personiskās drošības nodrošināšanas pakalpojumi) kodam, ir apsardzes pakalpojumu sniegšana
Klients	Uzņēmums, kurš uz līguma vai cita pamata saņem apsardzes un videonovērošanas pakalpojumus no Komersanta
Pārzinis	Juridiska vienība, kas atbildīga par datu apstrādi un kas nosaka tās veikšanas mērķus un līdzekļus
Apstrādātājs	Uzņēmums vai persona, kurai pārzinis uzticējis veikt darbības tā vārdā.

Inspekcijas uzdevumi ir noteikti Datu regulas 57. pantā un Fizisko personu datu apstrādes likuma 4. pantā. Savukārt Inspekcijas, kā galvenās datu aizsardzības uzraudzības iestādes Latvijā, kompetence noteikta Datu regulas 55. un 56. pantā. Viena no Inspekcijas svarīgām pamatfunkcijām ir sabiedrības informēšana par aktuāliem jautājumiem savas kompetences jomās¹, tai skaitā analizējot datu apstrādes procesus pie Latvijā esošiem pārziņiem un meklējot problēmjautājumus, par kuriem nepieciešami detalizētāki skaidrojumi.

Inspekcijā viens no populārākajiem jautājumiem cilvēkiem - fiziskām personām un uzņēmumu pārstāvjiem, kā arī iestādēm, ir par videonovērošanas veikšanu – labo praksi, slikto praksi, par citu personu veiktu videonovērošanu, par to, kurš atbildīgs, kad videonovērošanas sistēma nepieciešama vienai personai, bet to uzstāda un apkalpo cita.

Līdz šim Inspekcija ir izdevusi dažādus rakstus par videonovērošanu, tai skaitā: [Videonovērošana plašā mērogā. Kritēriji un nosacījumi](#); [Vai var veikt videonovērošanu privātās telpās?](#); [Kā nodrošināt likumīgu videonovērošanu uzņēmumā?](#); [Kas jāievēro uzstādot videonovērošanu kopīpašumā?](#); [Kas jāzina par šaura mēroga videonovērošanu privātīpašumā?](#); [Darbinieku videonovērošana veicot darba pienākumus klātienē](#). Tāpat Inspekcija ir izdevusi vadlīnijas privātpersonām: [Videokameru uzstādīšana un videonovērošanas veikšana fiziskas personas privātīpašumā](#), un juridiskām personām: [Praktiskās videonovērošanas vadlīnijas juridiskām personām un kopīpašniekiem](#). Lai gan skaidrojošo materiālu un vadlīniju saturs ir rekomendējošs, tomēr to izveidošanas mērķis ir veicināt izpratni par datu aizsardzības jautājumiem, kad tiek veikta videonovērošana, it īpaši, kad tās veicēju vidū ir personas ar nepietiekamām zināšanām šajos jautājumos.

Ievērojot Inspekcijas 2025. gada darba plānā iekļauto uzdevumu un ievērojot iepriekš minēto, tika lemts par preventīvas pārbaudes veikšanu, par pārbaudes objektu nosakot 25 (divdesmit piecus) datu apstrādes pārziņus – komersantus, kuru pamatdarbība ir saistīta ar

¹ Saskaņā ar Fizisko personu datu apstrādes likuma 4. panta pirmās daļas 11. punktu

apsardzes pakalpojumu sniegšanu², par kuriem tālāk pārbaudes gaitā plānots noskaidrot, vai tie nodarbojas arī ar videonovērošanas kameru un sistēmu uzstādīšanu un uzturēšanu citām juridiskām personām (uzņēmums norīko uzņēmumu uzstādīt kameru). Minētais savukārt tos padarītu par derīgiem pārbaudes turpināšanai.

Pārbaudes saturs pamatā ir orientēts uz tehnisko un organizatorisko prasību ievērošanu videonovērošanas laikā, videomateriālu iegūšanu un nodošanu apstrādātāja un pārziņa starpā, piekļuves nodrošināšanu. Tāpat tiek pievērsta uzmanība arī datu apstrādes principiem, jo īpaši glabāšanas ierobežojumiem un konfidencialitātei.

Tāpat Inspekcija neizslēdza iespēju, ka pārbaudes ietvaros var tikt vērsta uzmanība arī uz citām, ar videonovērošanu nesaistītām, pārbaudes laikā pamanītām nepilnībām, piemēram, kad komersants pārbaudē informējis, ka tam iecelts datu aizsardzības speciālists, bet faktiski Inspekcijas rīcībā šādas informācijas nav.

Pārbaude pamatā organizēta ar mērķi identificēt nepilnības komersantu veiktajā datu apstrādē, kad tie uzglabā vai kā citādi apstrādā savu klientu videoierakstus, par šīm nepilnībām informējot visus pārbaudē iesaistītos komersantus (neatklājot, kurš komersants pieļāvis kļūdu). Tāpat pārbaudes mērķis ir identificētās nepilnības novērst, tādējādi, galvenokārt, aizsargājot personu, kuru dati nonākuši videoierakstos, tiesības uz datu aizsardzību, kā arī veicinot vai nodrošinot komersantu veikto darbību atbilstību Datu regulas un citu saistošo normatīvo aktu prasībām. Vienlaikus pārbaudes mērķis nav pārbaudāmo uzņēmumu sodīšana.

Pārbaudes nozare

Lai uzsāktu pārbaudi, vispirms bija nepieciešams izraudzīt nozari. Ņemot vērā, ka apsardzes uzņēmumi vien atsevišķas reizes pārbaudīti individuālos gadījumos, taču pati tēma ir aktuāla jau vairākus gadus un pat pirms Datu regulas ieviešanas, 2025. gads ir izraudzīts par īsto laiku pārbaudes veikšanai. Tāpat jāņem vērā, ka apsardzes nozare ir pietiekami plaša, kas nozīmē, ka, ja šīs pārbaudes rezultātā taps materiāls, kas var noderēt arī citiem šīs jomas uzņēmumiem, tas palīdzēs sasniegt lielu sabiedrības un uzņēmējdarbības daļu³. Turklāt pārbaude varētu palīdzēt kļiedēt, iespējams, maldīgu priekšstatu, ka šajā nozarē datu aizsardzības prasību neievērošana varētu būt neapzināta vai ierasta norma.

Pretēji citām lielapjoma preventīvām pārbaudēm, tieši šajā bija būtiski pārbaudīt komersantus, kuri no visa saraksta ir reģistrējuši lielāku apgrozījumu, un tādējādi visticamāk darbojas ar lielāku klientu skaitu un saglabāto datu apjomu. Un tā kā videonovērošanas ietvaros ir salīdzinoši grūtāk īstenot tiesības iebilst pret datu apstrādi, un šādi apstrādei netiek prasīta personas piekrišana, ar datu subjektiem, kuru dati apstrādāti, var tikt nodarīts lielāks kaitējums. Šeit arī jāņem vērā, ka, kaut arī pamatā, kad apsardzes uzņēmums klientam ievieš videonovērošanas sistēmu un to uzrauga, atbildību par to (datu apstrādi) jānes klientam, kurš pasūtījis šādu pakalpojumu. Nereti praksē novērots, ka savstarpēji visa atbildība novelta uz apsardzes uzņēmuma *pleciem*, jo pie tiem glabājas ieraksti un tiem pamatā ir pieeja tiem. Tādēļ arī Inspekcijai bija svarīgi vērsties ne tieši pie klientiem, bet pie apsardzes uzņēmumiem, kas šādas sistēmas kā pakalpojumu klientam ievieš. Kaut arī apsardzes uzņēmumi neieņem pārziņa lomu šajā apstrādē, tiem tāpat ir saistošas Datu regulas normas, kā arī savstarpējā, ar klientu noslēgtajā līgumā noteiktais.

Pārbaudāmo komersantu atlase

Lai iegūtu objektīvu un ticamu sarakstu ar komersantiem, kas darbojas apsardzes jomā, šī informācija tika pieprasīta VID⁴, ņemot vērā, ka šajā iestādē uzņēmumiem jāreģistrē sava pamatdarbība, kā arī jāziņo par apgrozījumu un citiem uzņēmuma rādītājiem. No VID tika saņemts

² Atbilstoši NACE 2.1 red. 80.09 (Citur neklasificēti drošības nodrošināšanas pakalpojumi) vai NACE 2.1 red. 80.01 (Izmeklēšanas un personiskās drošības nodrošināšanas pakalpojumi) kodam

³ Ņemot vērā VID 2025. gada 14. aprīļa vēstulē Nr. [...] sniegto informāciju, zem NACE 2.1 red. 80.09 un NACE 2.1 red. 80.01 koda uz to brīdi darbojās 572 komersanti.

⁴ Ar Inspekcijas 2025. gada 1. aprīļa vēstuli Nr. [...]

saraksts ar 572 komersantiem, kuri nodarbojas ar citur neklasificētu drošības nodrošināšanas pakalpojumu sniegšanu vai izmeklēšanas un personiskās drošības nodrošināšanas pakalpojumu sniegšanu. Lai gada ietvaros būtu iespējams pārbaudi arī noslēgt, tika nolemts aptaujāt 25 komersantus un izvērtēt to darbību attiecībā uz datu apstrādi videonovērošanas jomā.

Lai atlasītu pārbaudāmos komersantus, no iegūtā komersantu saraksta vispirms tika dzēsti komersanti, par kuriem uz informācijas sagatavošanas brīdi vēl nebija informācijas par pēdējā apgrozījuma apjomu vai arī apgrozījums bija norādīts "0", kā arī uzņēmumi, pie kuriem bija veikta atzīme, ka "vienīgais īpašnieks miris". No atlikušajiem tie tika sakārtoti pēc apgrozījuma apjoma, no saraksta vispirms ņemot pirmos 25 komersantus ar lielāko apgrozījumu. Tāpat bija būtiski, lai tiktu izraudzīti uzņēmumi, kuri reģistrēti Latvijā. No sakārtotā saraksta nākamais solis bija atlasīt komersantus, kuriem ir funkcionējošas tīmekļa vietnes, kuras manuāli apskatot secināms, ka šie komersanti nodarbojas vai varētu nodarboties ar videonovērošanas sistēmu ierīkošanu, uzstādīšanu vai apkalpošanu.

Pārbaudes gaita un saņemtā informācija

Kad tika sagatavots saraksts ar pārbaudei derīgiem komersantiem, tiem tika izsūtīta vienota vēstule ar 16 jautājumiem⁵, uz kuriem tika lūgts sniegt patiesas atbildes, ņemot vērā, ka šīs pārbaudes mērķis nav sodīt komersantus par pieļautajām kļūdām, bet identificēt tās un vēlāk par tām komersantus informēt. Tāpat vēstulē lūgts atbildēm pievienot klāt dokumentus, kas varētu palīdzēt izprast komersanta praksi.

Atbilžu sagatavošanai komersantiem tika dots aptuveni mēnesis, paturot prātā, ka var būt komersanti, kas lūgtu atbilžu termiņu pagarināt.

Turpmākajā tekstā uzskaitīti Inspekcijas vēstulē uzdotie jautājumi pa vienam un norādītas komersantu sniegtās atbildes, cik iespējams, apkopotā veidā. Jāpiemin, ka pārbaudes gaitā viens no 25 pārziņiem nesniedza atbildes noteiktajā termiņā, savukārt cits uzņēmums, atbildot uz vēstuli, norādīja uz argumentiem, kāpēc tomēr neietilps pārbaudāmo kategorijā. Tādējādi atbildes ir apkopotas par 23 komersantiem, kuri turpināja dalību pārbaudē.

1. Vai Uzņēmums piedāvā jebkāda veida apsardzes pakalpojumus? Kādus?

No 23 komersantiem visi atbildēja, ka piedāvā apsardzes pakalpojumus. Visbiežāk uzņēmumi min fiziskās apsardzes pakalpojumus, kas ietver objektu, pasākumu un teritoriju apsardzi, kā arī patrulēšanu. Tāpat tiek piedāvāti tehniskās apsardzes risinājumi, kuros ietilpst signalizācijas, trauksmes un videonovērošanas sistēmu uzstādīšana, uzturēšana un monitorings. Mazāk kā puse uzņēmumu nodrošina arī apsardzes vadības centru operatoru darbu un centralizētu tehnisko sistēmu uzraudzību. Savukārt seši uzņēmumi specializējas apsardzes sistēmu projektēšanā, konsultācijās un individuālu drošības risinājumu izstrādē. Tikai neliela daļa piedāvā vien fiziskās apsardzes pakalpojumus bez tehniskā nodrošinājuma, savukārt lielākā daļa uzņēmumu izvēlas sniegt kompleksus drošības risinājumus, apvienojot abas pieejas, lai pielāgotos klientu vajadzībām.

2. Līdz ar apsardzes pakalpojumu sniegšanu, kurus ar videonovērošanas sistēmām saistītus pakalpojumus Uzņēmums piedāvā juridiskām personām (Klientiem)? Piemēram, kameru uzstādīšana, uzraudzība, apkalpošana, ierakstu uzglabāšana, dzēšana, piekļuves nodrošināšana.

Lielākā daļa Komersantu piedāvā kameru un videonovērošanas sistēmu uzstādīšanu, kā arī to apkalpošanu un tehnisko uzturēšanu. Gandrīz trešdaļa nodrošina arī attēlu reāllaika monitoringu, trauksmju uzraudzību un klientu informēšanu. Salīdzinoši retāk tiek piedāvāta projektēšana, modernizācija un sistēmu konfigurēšana, kā arī ierakstu arhīva pārbaude vai piekļuves nodrošināšana. Tikai neliela daļa Komersantu sniedz arī konsultācijas vai tirgo iekārtas.

⁵ Inspekcijas 2025. gada 17. aprīļa vēstule Nr. [..]

3. Vai tiek slēgts līgums ar Klientu, kuram Uzņēmums sniedz videonovērošanas sistēmas ierīkošanas pakalpojumu? Kāds ir šī līguma priekšmets? Atbildei pievienojiet līguma paraugu.

Tikai trijos no 23 gadījumiem līgums netiek slēgts, bet, piemēram, sagatavota pasūtījuma tāme. Pārējos gadījumos līgums tiek noslēgts, bet visbiežāk tā priekšmets ir saistīts nevis ar pārziņa-apstrādātāja sadarbību attiecībā uz datu apstrādi, bet gan videonovērošanas kameru uzstādīšanu, ierīkošanu, tai skaitā reāllaika uzraudzību jeb monitoringu. Tikai divos gadījumos uzskatāmi norādīts, ka līguma saturā iekļauts arī apraksts par glabāšanas kārtību un datu apstrādes pilnvarojumu. Vairāk aprakstīta atbildība par tehnisko nodrošinājumu. Svarīgi pieminēt, ka šī līguma iniciators ir “apstrādātājs” jeb Komersants. Vienlaikus atsevišķos līgumos iekļauti tādi vispārīgi noteikumi kā pienākums nodrošināt konfidencialitāti un par to informēt uzņēmuma darbiniekus, kā arī “Puses vienojas ievērot spēkā esošos normatīvos aktus par fizisko personu datu apstrādi.”

4. Vai Uzņēmumā ir iecelts datu aizsardzības speciālists?

Deviņiem no 23 komersantiem datu aizsardzības speciālists nav iecelts, 14 ir iecelts. Deviņi no 14 Komersantiem nav informējuši Inspekciju par speciālista norīkošanu.

5. Kur parasti tiek glabāti Klienta videoieraksti un kas tiem var piekļūt?

Lielākā daļa Komersantu – vairāk nekā puse – norādījuši, ka videoieraksti tiek glabāti pie klienta, un piekļuve ir tikai klienta pilnvarotām personām. Daži Komersantu precizējuši, ka neglabā ierakstus, bet tikai nodrošina reāllaika uzraudzību. Ir arī atbildes, kur minēts, ka piekļuve tiek nodrošināta tikai autorizētiem darbiniekiem, ja tāda ir nepieciešama.

6. Ja Uzņēmums piekļūst videoierakstiem, kādi ir piekļuves kontroles un drošības pasākumi šādas piekļuves gadījumā?

Vairākums Komersantu norādīja, ka Uzņēmums nepiekļūst klientu videoierakstiem vai piekļuve ir tikai tehniska, Klientam klātesot. Apmēram trešdaļā gadījumu Komersants piekļūst videoierakstiem, ievērojot noteiktus piekļuves kontroles un drošības pasākumus (autentifikācija, autorizēti darbinieki, auditācijas pieraksti, žurnāli u.c.). Tāpat atsevišķi pārziņi norādījuši, ka ierakstiem nepiekļūst (vai tie netiek veikti), bet gan kamerās redzamo vēro reāllaikā.

7. Ja Uzņēmums piekļūst klienta videonovērošanas sistēmas ierakstiem, kādu lomu no datu aizsardzības tas ieņem – apstrādātāja, pārziņa vai kopīga pārziņa? Un kāda loma ir klientam, kuram tiek uzstādīta videonovērošana?

Gadījumos, kur Komersants norādīja, ka piekļūst Klienta ierakstiem, vairākums norādīja, ka Komersants ieņem apstrādātāja, bet Klients – pārziņa lomu. Daži Komersanti papildus uzsver, ka uzņēmums nepieņem lēmumus par datu apstrādi, un ir arī atbildes, kur norādīts, ka uzņēmums neieņem nekādu lomu, jo nepiekļūst datiem. Vienā gadījumā Komersants norādījis, ka gadījumos, kad tas *saņem trauksmes signālus videoierakstu vai tiešsaistes veidā, ir uzskatāms par pārziņi, jo tā ir kritiski nepieciešama darbība apsardzes darbības nodrošināšanā. Kā pamatojums šādai lomai ir uzskatāms arī Apsardzes darbības likuma 3.panta ceturrtā daļā noteiktais tehniskās apsardzes apraksts, kas norāda uz signālu saņemšanas nepieciešamību un reaģēšanu.*

Vēl cits Komersants norādījis, ka neieņem nevienu lomu, taču Klienta loma var būt gan “pārzinis” vai “apstrādātājs”.

8. Kas nosaka videonovērošanas ierakstu glabāšanas termiņu un kā datu dzēšana tiek īstenota praksē? Cik ilgi tiek glabāti ieraksti?

Aptuveni 96% komersantu norādīja, ka videonovērošanas ierakstu glabāšanas termiņu nosaka Klients, un ierakstu dzēšana tiek veikta automātiski vai saskaņā ar Klienta noteikumiem. Apsardzes uzņēmumi lielākajā daļā gadījumu nav iesaistīti glabāšanas termiņa noteikšanā vai

dzēšanas procesos, un piekļuve videoierakstiem tiek nodrošināta tikai Klientam vai tā pilnvarotajām personām.

Daži Komersanti min konkrētus termiņus, piemēram, 14 dienas, 30 dienas vai 3 mēneši, bet citi atsaucas uz normatīvajiem aktiem.

9. Ja ieraksti glabājas pie Uzņēmuma, vai Klientam tiek nodrošināta iespēja pārvaldīt vai pieprasīt dzēst konkrētus ierakstus, vai iegūt izgriezumus no ierakstiem? Kurš šādu pieprasījumu apstrādā?

Lielākā daļa komersantu norādīja, ka videoieraksti netiek glabāti uzņēmuma infrastruktūrā, bet paliek Klienta rīcībā, un piekļuves tiesības, dzēšanas iespējas un izgriezumu iegūšana tiek nodrošināta tieši Klientam vai viņa pilnvarotām personām. Apmēram puse no Komersantiem precizēja, ka šādus pieprasījumus apstrādā uzraugošais darbinieks vai tehniskais speciālists, bet uzglabāšana un dzēšana ir Klienta kompetencē. Vairāki komersanti uzsvēra, ka tie tikai veic reāllaika objektu monitoringu un nestandarta situāciju gadījumā reaģē, bet ieraksti netiek saglabāti uzņēmuma serveros. Atsevišķos gadījumos uzņēmums sniedz tehnisku palīdzību piekļuvē vai izgriezumu sagatavošanā, taču glabāšana un galvenā kontrole joprojām ir Klientam. Tikai neliela daļa Komersantu norāda uz īpašiem pakalpojumu blokiem, kur tehniskais speciālists īslaicīgi palīdz ar piekļuvi, bet uzglabāšana un dzēšana ir Klienta atbildībā.

10. Kā tiek nodrošināta ierakstu šifrēšana, aizsardzība pret nesankcionētu piekļuvi un ierakstu izsniegšanas/ apstrādes pieraksti (piemēram, piekļuves žurnāli)?

Aptuveni puse Komersantu norāda, ka Klients veic videoierakstu šifrēšanu, piekļuves kontroli un ierakstu izsniegšanu, tādējādi šie Klienti paši uzrauga datu aizsardzības procesus. Četri Komersanti uzņemas šo atbildību paši, izmantojot TLS šifrēšanu datu pārraidei, regulāri mainot IT drošības iestatījumus un uzturot darbinieku piekļuves žurnālus. Pāris gadījumos atbildība ir sadalīta, kur gan Uzņēmums, gan Klients kopīgi nodrošina datu drošību un ierakstu uzraudzību. Četros gadījumos Komersants neveic videoierakstu glabāšanu, kas var būt saistīts ar pakalpojuma raksturu vai līguma noteikumiem, tādējādi neatbild par piekļuvi.

11. Kādas procedūras ir noteiktas gadījumā, ja notiek datu aizsardzības pārkāpums (piemēram, noplūde vai nesankcionēta piekļuve)?

Aptuveni puse Komersantu (11) ir izstrādājuši iekšējās procedūras, kas ietver incidentu reģistrāciju, izmeklēšanu, darba grupu notikumu smaguma novērtēšanai, kā arī ziņošanu Klientam un Inspekcijai. Tikmēr trešdaļā gadījumu šo atbildību pilnībā uzņemas Klients. Divu Komersantu procedūras vēl tiek plānotas vai kombinētas starp klientu un uzņēmumu. Vēl divos gadījumos norādīts, ka procedūras nav nepieciešamas, jo Komersants neveic datu apstrādi.

12. Vai darbinieki, kas apkalpo videonovērošanas sistēmas un apstrādā ierakstus, ir apmācīti datu aizsardzības jomā? Cik bieži un kādā formātā tas tiek organizēts?

Lielākā daļa komersantu (aptuveni divas trešdaļas) nodrošina regulāras datu aizsardzības apmācības darbiniekiem, kas apkalpo videonovērošanas sistēmas vai veic reāllaika uzraudzību. Apmācības tiek organizētas dažādos formātos – semināros, e-apmācībās vai klātienē. Apmācības ietver testus, instruktāžas vai apliecinājumu iesniegšanu par prasību apgūšanu. Trīs komersanti apmācības organizē tikai pēc nepieciešamības vai plāno ieviest regulāru apmācību sistēmu tuvākajā nākotnē. Savukārt piektā daļa Komersantu norādīja, ka darbinieki neapstrādā videoierakstus, tāpēc specifiskas datu aizsardzības apmācības nav nepieciešamas, un darbs aprobežojas ar videonovērošanas tehnisko apkalpošanu.

13. Vai Uzņēmuma darbiniekiem rodas nepieciešamība dalīties savā starpā ar video ierakstiem vai attēliem no Klientu videonovērošanas sistēmām? Aprakstiet šos gadījumus, ja tādi ir iespējami, arī nodošanas mērķi.

Lielākā daļa – 18 no 23 pārziņiem – norādījuši, ka darbiniekiem nav nepieciešamības dalīties ar šādiem materiāliem, gan tādēļ, ka tas ir aizliegts, gan tādēļ, ka nav piekļuves ierakstiem. Trīs pārziņi tomēr papildus atzīmējuši, ka šāda nepieciešamība var rasties, piemēram, incidentu izmeklēšanas vai apsardzes pakalpojumu sniegšanas laikā, ar Klienta atļauju un norādēm. Viens Komersants norādījis, ka ieraksti var tikt nodoti tikai darba vajadzībām, piemēram, trauksmes izmeklēšanai vai ziņošanai klientam. Viens Komersants norādījis, ka “Uzņēmuma apsardzes darbiniekiem ir nepieciešamība dalīties ar klienta sistēmu ierakstiem, apsardzes pakalpojumu sniegšanas laikā. Piemēram, sastādot iesniegumus valsts policijā, informējot citus darbiniekus par personām kas izdarījušas noziegumus, nododot citu informāciju par notikumiem (autotransporta kustību, ēku bojājumiem, tehnoloģiskiem procesiem utt. Šeit vēršam uzmanību – ne visi video ieraksti un attēli satur personas datus)”.

14. Vai Uzņēmumam var rasties situācija, kad videoieraksti (personas dati) no Klientu videonovērošanas sistēmām jānodod trešajām personām? Aprakstiet šīs situācijas un norādiet tiesisko pamatu, atbilstoši Datu regulas 6. panta 1. punktam, uz kāda šie dati tiek nodoti.

Atbildot uz jautājumu, 14 Komersanti norādījuši, ka tiem nerodas šādas situācijas, vai arī nodošana nav viņu kompetencē, vai nodošanu veic pēc Klienta pieprasījuma. Savukārt 8 pārziņi atzīmējuši, ka šādas situācijas var rasties, kad pieprasījumu izsaka tiesībsargājošās iestādes (var nodot ar Klienta piekrišanu) vai datu subjekti, un nodošana tiek veikta uz tiesiska pamata, piemēram, saskaņā ar Datu regulas 6. panta 1. punkta c), e) vai f) apakšpunktu. Divi Komersanti norāda, ka ierakstu nodošana nenotiek, ja vien ierakstus pieprasa Policija, cits, ka nodošana var notikt, bet to veic Klients. Vēl viens Komersants norādījis, ka ierakstu nodošanu nosaka Klients, uzdodot Komersantam sagatavot ierakstu, piemēram tiesībsargājošajām iestādēm, pamatojoties uz Datu regulas 6. panta 1. punkta f) apakšpunktu.

15. Vai Uzņēmuma darbinieki var piekļūt videoierakstiem arī ārpus darba vietas un ārpus darba laika?

Šajā jautājumā 18 no 23 Komersantiem skaidri norādījuši, ka darbiniekiem nav piekļuves videoierakstiem ārpus darba vietas vai darba laika. Daži uzsvēra, ka piekļuve tiek stingri kontrolēta un dokumentēta. Divi pārziņi atzīmējuši, ka piekļuve var būt iespējama, piemēram, ārkārtas situācijās ar VPN savienojumu un atbildīgās personas (Klienta) apstiprinājumu. Tāpat atsevišķi Komersanti norādījuši, ka “Netiek pieļauta bez pamatotas vajadzības un atļaujas. Visi piekļuves gadījumi tiek dokumentēti”; “Piekļuve iespējama tikai darbiniekiem ar attiecīgām pilnvarām, ārkārtas situācijās, nodrošinot piekļuves izsekojamību.”; “ierobežotam personu lokam, ja ir pamatojums, parasti datus skata klātienē, darba laikā”.

16. Vai Uzņēmumam ir izstrādāti iekšējie noteikumi attiecībā uz šādu datu apstrādi?

Šeit 14 Komersanti apstiprinājuši, ka uzņēmumā ir izstrādāti iekšējie noteikumi, kas regulē videonovērošanas datu apstrādi, tostarp drošības politikas, procedūras un darbinieku pienākumi un noteikumi, kas iekļauti darba līgumos, kā arī informācijas drošības procedūras. Deviņi no 23 Komersantiem norādījuši, ka noteikumi nav izstrādāti, pamatojot to ar faktu, ka uzņēmums neveic šādu datu apstrādi vai nav piekļuves videoierakstiem.

Secinājumi

Pārbaudes laikā vien no komersantu sniegtajām atbildēm, var secināt vai noprast par to praksi, sniedzot videonovērošanas sistēmu uzstādīšanas/ apkalpošanas pakalpojumus. Savukārt tālāk, apkopojot saņemtās atbildes, var izprast vidējo izpratni un praksi aptaujāto komersantu vidū. Pēc atbilžu apkopošanas un analizēšanas, fokuss tika vērsts uz biežāk pieļautajām vai zīmīgākajām kļūdām, kas šajās datu apstrādēs pieļautas, kā arī uz citiem secinājumiem, kas radušies pārbaudes laikā.

Kopumā, tiktāl, cik informācija sniegta, atbildot uz Inspekcijas sūtītajiem jautājumiem, komersanti veic savas darbības attiecībā uz datu apstrādi drīzāk atbilstoši vai atbilstoši. Saņemtajās atbildēs neiezīmējās kāda konkrēta kritiska problēma vai arī Komersants, kura prakse būtu izteikti nekorekta vai pat nelikumīga.

Tomēr pēc atbilžu saņemšanas iezīmējās atsevišķas nepilnības, uz kurām vērts vērst Komersantu uzmanību:

1. Līdzīgi kā citās Inspekcijas pārbaudēs, kur ir runa par pārziņu-apstrādātāju līgumiem, arī šajā ir novērota prakse, ka līgums ir sastādīts par pakalpojumu, neapskatot datu apstrādes jautājumus, vai tiem pieskaroties ļoti vispārīgi. Tā kā visbiežāk Komersanti norādījuši, ka to attiecības ar Klientu definējamās kā pārziņa un apstrādātāja attiecības, kur pārzinis ir Klients, šādos gadījumos nepieciešams slēgt pārziņa-apstrādātāja līgumu, ja apstrādātājam (Komersantam) uzdots apstrādāt datus šī (vai cita) datu apstrādes procesa ietvaros. Tādējādi ir jāievēro Datu regulas 28. pantā iekļautie nosacījumi.

Vienlaikus Inspekcijai rekomendējams izstrādāt un publicēt pārziņa-apstrādātāja līguma paraugu, kas var noderēt ikvienam pārzinim, kas norīko apstrādātāju.

2. Tā kā deviņi no 14 Komersantiem, kuriem ir norīkots datu aizsardzības speciālists, par to nav noziņojuši Inspekcijai, ir jāņem vērā Datu regulas 37. panta 7. punkts, kurā noteikts, ka datu aizsardzības speciālista kontaktinformācija jāpaziņo Inspekcijai (uzraudzības iestādei) un datu subjektiem (personām, kuras var nonākt videonovērošanas zonā).

3. Kopumā tendence rāda, ka procedūru un noteikumu izstrāde un īstenošana tiek nodrošināta tur, kur datu apstrāde notiek, bet incidentu ziņošanas pienākumi bieži tiek "deleģēti" Klientam, ja Komersantam nav tiešas piekļuves datiem. Vienlaikus tikai trešdaļā gadījumu šo atbildību pilnībā uzņemas Klients. Saskaņā ar Datu regulas 33. panta 1. un 2. punktu, par datu aizsardzības pārkāpumu apstrādātājs ziņo pārzinim, bet pārzinis Inspekcijai. Tādējādi Komersantam nav pienākums informēt Inspekciju par datu aizsardzības incidentu, bet gan tas jādara Klientam pēc informācijas saņemšanas no Komersanta.

4. Kopumā tendence rāda, ka apmācības datu aizsardzībā tiek sistemātiski nodrošinātas tur, kur darbinieki strādā ar personas datiem, savukārt uzņēmumos, kas neglabā Klienta videonovērošanas kameru ierakstus, šādas apmācības netiek veiktas. Nav novērota nepareiza tendence šajā jautājumā, taču uzņēmumiem būtu jāpatur prātā, ka pat, ja datu apstrāde netiek veikta Klienta norīkojumā vai videonovērošanas jomā, tā var tikt veikta citos procesos, kas savukārt nozīmē, ka apmācības ir nepieciešamas pie jebkuriem datu apstrādes procesiem.

5. Attiecībā uz videoierakstu glabāšanas termiņiem, ja daži Komersanti nosaka konkrētus termiņus, bet citi atsaucas uz normatīvajiem aktiem, jāuzsver, ka termiņu noteikšana, kad tas nav noteikts normatīvajā aktā, ir pārziņa (Klienta) uzdevums, nevis apstrādātāja. Ieteicams pārziņiem skaidri dokumentēt termiņus, pamatojoties uz nolūku un glabāšanas ierobežojuma principu, lai izvairītos no pārmērīgas datu glabāšanas. Tie jāiekļauj pārziņa-apstrādātāja līgumā.

6. Piekļuves kontroles jautājumos ir būtiski, lai visi gadījumi tiktu dokumentēti un piekļuve būtu iespējama tikai pilnvarotiem darbiniekiem, nepieciešamības gadījumos nodrošinot izsekojamību. Šie nosacījumi jāiekļauj iekšējos noteikumos vai pārziņa-apstrādātāja līgumā, un darbinieki jāinformē par atbildību ievērot noteikumus, lai mazinātu datu drošības riskus. Tāpat jāatrunā, kad apsardzes darbiniekam ir pamatoti nodot ierakstus trešajām personām.

7. Norāde, ka Komersants neieņem nevienu datu apstrādes lomu, bet klienta loma vienlaikus var būt gan pārzinis, gan apstrādātājs, prasa precizējumu. Pat, ja Komersants uzskata,

ka nav iesaistīts apstrādē, tehniskais atbalsts vai piekļuves nodrošināšana var radīt apstrādes elementus, tāpēc ieteicams skaidri definēt lomas līgumā, lai izvairītos no neskaidrībām.

Visbeidzot, statistika, kas apliecina, ka lielākajā daļā gadījumu datu pārzinis ir klients, bet Komersants darbojas kā tehnisks atbalsts vai tiešsaistes uzraugs, norāda uz nepieciešamību skaidri nodalīt atbildības robežas. Pat, ja Komersants neglabā un nedzēš ierakstus, tam jānodrošina, ka līgumiskajos dokumentos ir precīzi aprakstīts tā loma un pienākumi, lai izvairītos no pārpratumiem par datu apstrādes atbildību.

8. Reāllaika vērošana kamerās ir uzskatāma par personas datu apstrādi, jo tiek veikta datu iegūšana un izmantošana konkrētam nolūkam. Lai gan dati netiek glabāti, automatizētas apstrādes fakts pastāv, un tas jāņem vērā, piemēram, informējot datu subjektus par novērošanu (tā ir jāveic).

9. Audio ierakstu veikšana videonovērošanas ietvaros ir atsevišķa apstrāde, kas parasti nav ieteicama, jo tā ievērojami palielina privātuma riskus. Audio ieraksti drīkst tikt veikti tikai izņēmuma gadījumos ar pamatotu nepieciešamību, tāpēc ieteicams tos neizmantot, ja nav skaidra tiesiska pamata. Kaut arī pārbaudes ietvaros netika iegūta informācija par audio ieraksta veikšanu līdz ar video ierakstu, vērst uzmanību uz šo un atgādināt ziņojuma ietvaros, šķiet būtiski.

Nemot vērā iegūtos pārbaudes rezultātus, būtu vērts apsvērt, skaidru vadlīniju izstrādi šajā jautājumā. Vadlīnijas būtu noderīgas ne tikai aptaujātajiem Komersantiem, bet arī citiem apsardzes pakalpojumu sniedzējiem. Tāpat ar šī ziņojuma secinājumiem nepieciešams iepazīstināt pārbaudes dalībniekus – Komersantus.