Pamatnostādnes 3/2019 par personas datu apstrādi, izmantojot videoierīces

Versija 2.0

Pieņemtas 2020. gada 29. janvārī

Translations proofread by EDPB Members. This language version has not yet been proofread.

Līdzšinējās versijas

Versija 2.1	2020. gada 2. februāris	Būtiskas kļūdas labojums
Versija 2.0	2020. gada 29. janvāris	Pamatnostādņu pieņemšana pēc sabiedriskās apspriešanas
Versija 1.0	2019. gada 10. jūlijs	Pamatnostādņu pieņemšana sabiedriskajai apspriešanai

Satura rādītājs

Eiropas Datu aizsardzības kolēģija,

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulā (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 (turpmāk "VDAR");

ņemot vērā EEZ līgumu un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas 2018. gada 6. jūlija Lēmumu Nr. 154/2018[1];

ņemot vērā tās Reglamenta 12. un 22. pantu,

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

1 IEVADS

1. Intensīvai videoierīču izmantošanai ir liela ietekme uz iedzīvotāju uzvedību. Šādu ierīču plaša izmantošana daudzās iedzīvotāju dzīves jomās radīs papildu slogu indivīdiem, jo viņi vēlēsies, lai netiek filmēts tas, ko varētu uzskatīt par vispārpieņemtajām normām neatbilstošu. Šīs tehnoloģijas faktiski var ierobežot anonīmas pārvietošanās iespējas un pakalpojumu anonīmu izmantošanu un var kopumā ierobežot iespēju palikt nepamanītam. Tam ietekme uz datu aizsardzību ir ļoti liela.

2. Indivīdiem var neradīt neērtības videonovērošana, kas ierīkota, piemēram, konkrētam drošības nolūkam, tomēr ir jāveic garantijas pasākumi, lai izvairītos no videonovēršanas ļaunprātīgas izmantošanas pilnīgi atšķirīgiem un datu subjektam negaidītiem mērķiem (piemēram, tirgvedības nolūkā, vai, lai novērotu, kā darbinieki strādā, u. tml.). Turklāt tagad ir ieviesti daudzi rīki uzņemto attēlu izmantošanai un tradicionālo kameru pārvēršanai viedajās kamerās. Video radīto datu apjoms apvienojumā ar šiem rīkiem un paņēmieniem palielina sekundārās izmantošanas (neatkarīgi no tā, vai šāda izmantošana ir saistīta ar sistēmai sākotnēji noteikto mērķi) vai pat ļaunprātīgas izmantošanas riskus. Attiecībā uz videonovērošanu vienmēr būtu rūpīgi jāapsver VDAR 5. pantā noteiktie vispārējie principi.

3. Videonovērošanas sistēmas daudzējādā ziņā maina to, kā speciālisti no privātā un publiskā sektora mijiedarbojas privātās un publiskās vietās, lai uzlabotu drošību, iegūtu mērķauditorijas analīzi, piedāvātu personalizētas reklāmas utt. Arvien intensīvāk ieviešot inteliģento video analīzi, videonovērošana ir kļuvusi augstāk attīstītāka. Šīs tehnikas var būt vairāk traucējošas (piemēram, sarežģītas biometriskās tehnoloģijas) vai mazāk traucējošas (piemēram, vienkāršās skaitīšanas algoritmi). Palikt anonīmam un saglabāt privātumu kopumā kļūst arvien grūtāk. Datu aizsardzības jautājumi, kas rodas katrā situācijā, var atšķirties, tāpat kā atšķiries juridiskā analīze izmantojot vienu vai otru šo tehnoloģiju.

4. Papildus privātuma jautājumiem pastāv arī riski, kas saistīti ar iespējamiem šo ierīču darbības traucējumiem un neobjektivitāti, ko tie var izraisīt. Pētnieki norāda, ka programmatūra, ko izmanto sejas identificēšanai, atpazīšanai vai analīzei, darbojas atšķirīgi atkarībā no identificējamās personas

[1] Šajā atzinumā atsauces uz "dalībvalstīm" būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".

vecuma, dzimuma un etniskās izcelsmes. Algoritmi darbojas, pamatojoties uz atšķirīgu demogrāfiju, līdz ar to neobjektivitāte seju atpazīšanā draud pastiprināt aizspriedumus sabiedrībā. Tāpēc datu pārziņiem arī jānodrošina, ka attiecībā uz biometrisko datu apstrādi, kas izriet no videonovērošanas, tiek regulāri novērtēta tās atbilstība un sniegto garantiju pietiekamība.

5. Videonovērošana nav uztverama kā pašsaprotama nepieciešamība, ja ir citi līdzekļi, ar kuriem var sasniegt pamatmērķi. Pretējā gadījumā mēs riskējam mainīt esošos uzskatus, kā rezultātā privātuma trūkums var tikt atzīts par vispārēju normu.

6. Šo pamatnostādņu mērķis ir sniegt norādījumus par to, kā piemērot VDAR attiecībā uz personas datu apstrādi, ko veic, izmantojot videoierīces. Sniegtie piemēri nav izsmeļoši un vispārējo argumentāciju var attiecināt uz visām potenciālajām izmantošanas jomām.

2 PIEMĒROŠANAS JOMA[2]

2.1 Personas dati

7. Konkrētas vietas sistematizēta automātiska novērošana, izmantojot optiskus vai audiovizuālus līdzekļus, lielākoties īpašuma aizsardzības nolūkos vai lai aizsargātu indivīdu dzīvību un veselību, ir kļuvusi par mūsdienām raksturīgu parādību. Šī darbība ietver attēlu vai audiovizuālas informācijas vākšanu un glabāšanu par visām personām, kuras ienāk novērotajā zonā un kuras ir identificējamas pēc viņu izskata vai citām specifiskām pazīmēm. Pamatojoties uz šīm pazīmēm, ir iespējams noteikt personu identitāti. Šī darbība arī ļauj tālāk apstrādāt personas datus par personu klātbūtni un uzvedību konkrētā vietā. Jo lielāka novērotās zonas platība un jo vairāk cilvēku to apmeklē, jo lielāks ir iespējamais šādu datu ļaunprātīgas izmantošanas risks. Šis fakts ir atspoguļots Vispārējās datu aizsardzības regulas 35. panta 3. punkta c) apakšpunktā, kurā noteikts, ka gadījumā, ja notiek publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā, ir jāveic novērtējums par ietekmi uz datu aizsardzību, kā arī 37. panta 1. punkta b) apakšpunktā, kurā noteikts, ka datu apstrādātājiem ir jāieceļ datu aizsardzības speciālists, ja apstrādes darbības pēc būtības ietver datu subjektu regulāru un sistemātisku novērošanu.

8. Tomēr regula nav piemērojama attiecībā uz tādu datu apstrādi, kuros nav atsauces uz personu, piemēram, ja indivīdu nevar identificēt ne tieši, ne netieši.

> Piemērs. VDAR nav piemērojama attiecībā uz kameru butaforijām (t. i., kamerām, kas nefunkcionē kā kameras un tādējādi neapstrādā personas datus). *Tomēr dažās dalībvalstīs uz šādām kamerām var attiekties citi tiesību akti.*
>
> Piemērs. Uz ierakstiem, kas veikti no liela augstuma, VDAR darbības joma attiecas tikai tad, ja konkrētajos apstākļos apstrādātos datus var sasaistīt ar konkrētu personu.
>
> Piemērs. Automobilī ir iebūvēta videokamera, lai atvieglotu automobiļa novietošanu stāvvietā. Ja kamera ir konstruēta vai noregulēta tā, ka tā nereģistrē nekādu informāciju par fizisku personu (piemēram, automobiļu reģistrācijas numura zīmes vai informāciju, pēc kuras varētu identificēt garāmgājējus), VDAR nav piemērojama.

9.

2.2 Tiesībaizsardzības direktīvas (TAD) ((ES) 2016/680) piemērošana

10. Konkrēti uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu, attiecas Direktīva (ES) 2016/680.

2.3 Izņēmums attiecībā uz mājsaimniecībām

11. Atbilstoši 2. panta 2. punkta c) apakšpunktam VDAR darbības joma neattiecas uz personas datu apstrādi, ko veic fiziska persona tikai personiska vai mājsaimnieciska pasākuma gaitā un kas var ietvert arī darbību tiešsaistē[3].

[2] EDAK norāda, ka gadījumos, kad VDAR to atļauj, var būt piemērojamas īpašas prasības, kas noteiktas valsts tiesību aktos.

[3] Sk. arī 18. apsvērumu.

12. Šis noteikums — tā dēvētais izņēmums attiecībā uz mājsaimniecībām — videonovērošanas kontekstā ir jāinterpretē šaurā nozīmē. Tādējādi, kā atzinusi Eiropas Savienības Tiesa, tā dēvētais "izņēmums attiecībā uz mājsaimniecībām" "jāinterpretē tādējādi, ka tas attiecas vienīgi uz darbībām, kas ietilpst personu privātajā vai ģimenes dzīvē, kā tas acīmredzami nav gadījumā, kad personas dati tiek apstrādāti, tos publicējot internetā, un tādējādi šie dati tiek padarīti pieejami nenoteiktam personu skaitam"[4]. Turklāt, ja videonovērošanas sistēma ietver personas datu pastāvīgu ierakstīšanu un glabāšanu un "pat daļēji aptver publisko telpu un tādēļ ir vērsta uz personas, kura ar šo līdzekli veic datu apstrādi, privātās sfēras ārpusi, to nevar uzskatīt par darbību tikai un vienīgi personiskām vai sadzīviskām vajadzībām" [personiska vai mājsaimnieciska pasākuma gaitā] Direktīvas 95/46 3. panta 2. punkta otrā ievilkuma izpratnē"[5].

13. Uz videoierīcēm, ko izmanto privātpersonas telpās, var tikt attiecināts izņēmums, kas paredzēts attiecībā uz mājsaimniecībām. Tas ir atkarīgs no vairākiem faktoriem, kas ir jāņem vērā, lai nonāktu pie secinājuma. Papildus iepriekš minētajiem elementiem, kas norādīti EST nolēmumos, personai, kura izmanto videonovērošanu mājās, ir jāizvērtē, vai viņai ir jebkāda veida personīgas attiecības ar datu subjektu, vai novērošanas apmērs vai biežums norāda uz kādu viņa profesionālo darbību un kāda varētu būt novērošanas iespējamā nelabvēlīgā ietekme uz datu subjektiem. Ja pastāv kāds no iepriekš minētajiem elementiem, tas vēl nenozīmē, ka uz apstrādi neattiecas izņēmums, kas paredzēts attiecībā uz mājsaimniecībām, un lai to noteiktu, ir jāveic vispārējs novērtējums.

> Piemērs. Tūrists ieraksta video gan savā mobilajā tālrunī, gan videokamerā, lai dokumentētu savas brīvdienas. Uzfilmēto videomateriālu viņš rāda draugiem un ģimenei, taču nedara to pieejamu nenoteiktam cilvēku skaitam. Šajā gadījumā ir piemērojams izņēmums attiecībā uz mājsaimniecībām.
>
> Piemērs. Kalnu riteņbraucēja vēlas ierakstīt savu nobraucienu no kalna, izmantojot sporta kameru. Viņa brauc nomaļā apgabalā un plāno ierakstus izmantot tikai savām izklaides vajadzībām mājās. Šajā gadījumā ir piemērojams izņēmums attiecībā uz mājsaimniecībām, pat ja noteiktā apmērā tiek veikta personas datu apstrāde.
>
> Piemērs. Persona novēro savu dārzu un ieraksta tajā notiekošo. Īpašums ir nožogots, un dārzā regulāri ienāk tikai pats datu pārzinis un viņa ģimene. Šajā gadījumā ir piemērojams izņēmums attiecībā uz mājsaimniecībām, ar nosacījumu, ka videonovērošana, pat ne daļēji,— neietver sabiedriskas vietas vai kaimiņu īpašuma novērošanu.

14.

[4] Eiropas Savienības Tiesa, spriedums lietā C-101/01, *Bodil Lindqvist lieta*, 2003. gada 6. novembris, 47. punkts.

[5] Eiropas Savienības Tiesa, spriedums lietā C-212/13, *František Ryneš / Úřad pro ochranu osobních údajů*, 2014. gada 11. decembris, 33. punkts.

3 APSTRĀDES LIKUMĪGUMS

15. Pirms datu apstrādes ir sīki jānorāda tās nolūki (5. panta 1. punkta b) apakšpunkts). Videonovērošanai var būt vairāki nolūki, piemēram, veicināt īpašuma un citas mantas aizsardzību, veicināt personu dzīvības un fiziskās integritātes aizsardzību, savākt pierādījumus civilprasībām[6]. Šie novērošanas nolūki būtu jādokumentē rakstveidā (5. panta 2. punkts), un tie ir jānorāda par katru izmantoto novērošanas kameru. Kameras, ko viens datu pārzinis izmanto vienam un tam pašam nolūkam, var dokumentēt kopā. Turklāt datu subjekti ir jāinformē par apstrādes nolūku(-iem) saskaņā ar 13. pantu (*sk. 7. iedaļu "Pārredzamība un informēšanas pienākumi"*). Ja videonovērošanas vienīgais nolūks ir "drošībai" vai "jūsu drošībai", šāds nolūks nav pietiekami konkrēts (5. panta 1. punkta b) apakšpunkts). Turklāt tas ir pretrunā principam, ka personas datus apstrādā likumīgi, godprātīgi un datu subjektam pārredzamā veidā (sk. 5. panta 1. punkta a) apakšpunktu).

16. Principā katrs juridiskais pamatojums, kas norādīts 6. panta 1. punktā, ir juridisks pamats videonovērošanas datu apstrādei. Piemēram, 6. panta 1. punkta c) apakšpunkts ir piemērojams, ja valsts tiesību aktos ir paredzēts pienākums veikt videonovērošanu[7]. Tomēr praksē visbiežāk izmantotie pamati, visticamāk, būs šādi:

- 6. panta 1. punkta f) apakšpunkts (leģitīmas intereses);
- 6. panta 1. punkta e) apakšpunkts (nepieciešamība izpildīt uzdevumu, ko veic sabiedrības interesēs vai īstenojot oficiālās pilnvaras).

Izņēmuma gadījumos pārzinis kā likumīgo pamatu var izmantot 6. panta 1. punkta a) apakšpunktu (piekrišana).

3.1 Leģitīmas intereses (6. panta 1. punkta f) apakšpunkts)

17. VDAR 6. panta 1. punkta f) apakšpunkta juridiskais novērtējums būtu jāveic saskaņā ar VDAR 47. apsvērumu un pamatojoties uz turpmāk izklāstītajiem kritērijiem.

3.1.1 Leģitīmu interešu esamība

18. Videonovērošana ir likumīga, ja tā ir nepieciešama pārziņa vai trešās personas leģitīmo interešu ievērošanai, izņemot gadījumus, kad datu subjekta intereses vai pamattiesības un pamatbrīvības ir svarīgākas par šādām interesēm (6. panta 1. punkta f) apakšpunkts). Datu pārziņa vai trešās personas leģitīmās intereses var būt juridiskas[8], ekonomiskas vai nemateriālas intereses[9]. Tomēr pārzinim būtu jāņem vērā, ka tad, ja datu subjekts iebilst pret novērošanu saskaņā ar 21. pantu, pārzinis var veikt attiecīgā datu subjekta videonovērošanu tikai tad, ja tas tiek veikts *pārliecinošās* leģitīmās interesēs, kas ir svarīgākas par datu subjekta interesēm, tiesībām un brīvībām, vai lai celtu, īstenotu vai aizstāvētu likumīgas prasības.

19. Ņemot vērā reālu un bīstamu situāciju, mērķis aizsargāt īpašumu no ielaušanās, zādzības vai vandālisma var būt leģitīmas intereses, lai veiktu videonovērošanu.

---

[6] Noteikumi par pierādījumu vākšanu civilprasībām katrā dalībvalstī atšķiras.

[7] Šajās pamatnostādnēs nav analizēti vai sīki aprakstīti tiesību akti, kas var atšķirties starp dalībvalstīm.

[8] Eiropas Savienības Tiesa, spriedums lietā C-13/16, *"Rīgas satiksmes" lieta*, 2017. gada 4. maijs.

[9] Sk. WP217, 29. panta darba grupa.

20. Leģitīmajām interesēm ir jāpastāv realitātē un jābūt aktuālām (t. i., tās nedrīkst būt fiktīvas vai spekulatīvas)[10]. Pirms uzsākt videonovērošanu, iepriekš ir jābūt bijušai briesmu situācijai reālajā dzīvē, piemēram, bojājumu nodarīšanai vai nopietniem incidentiem. Ņemot vērā pārskatatbildības principu, pārziņiem būtu ļoti ieteicams dokumentēt attiecīgos incidentus (datumu, veidu, finansiālos zaudējumus) un saistītās krimināllapsūdzības. Šādi dokumentēti incidenti var būt pārliecinoši pierādījumi leģitīmu interešu esībai. Leģitīmu interešu esība, kā arī novērošanas nepieciešamība būtu jānovērtē atkārtoti ar periodiskiem intervāliem (piemēram, reizi gadā, atkarībā no apstākļiem).

> Piemērs. Veikala īpašnieks vēlas atvērt jaunu veikalu un uzstādīt videonovērošanas sistēmu, lai novērstu vandālismu. Atsaucoties uz statistiku, viņš var pierādīt, ka tuvējā apkaimē pastāv liela vandālisma varbūtība. Noderīga ir arī blakus esošo veikalu pieredze. Nav vajadzīgs, lai kaitējums attiecīgajam pārzinim jau būtu bijis nodarīts. Kamēr vien apkaimē nodarītie bojājumi liecina par bīstamību vai tamlīdzīgiem apstākļiem, tā var būt norāde, ka pastāv leģitīmas intereses. Tomēr nepietiek tikai ar atsaukšanos uz valsts vai vispārējo noziedzības statistiku, neanalizējot situāciju attiecīgajā apgabalā vai bīstamību konkrētajam veikalam.

21.

22. Draudošu bīstamu situāciju gadījumā var uzskatīt, ka pastāv leģitīmas intereses, piemēram, attiecībā uz bankām vai veikaliem (juvelierizstrādājumu veikaliem), kas pārdod vērtīgas preces vai teritorijām, par kurām ir zināms, ka tajās bieži mēdz notikt pret īpašumu vērsti noziegumi (degvielas uzpildes stacijās).

23. VDAR ir arī skaidri noteikts, ka publiskas iestādes nevar datu apstrādē atsaukties uz leģitīmām interesēm, ja tās apstrādi veic, pildot savus uzdevumus (6. panta 1. punkta otrais teikums).

3.1.2 Apstrādes nepieciešamība

24. Personas datiem būtu jābūt adekvātiem, atbilstīgiem un vajadzētu ietvert tikai to, kas nepieciešams to apstrādes nolūkos (“datu minimizēšana”) (sk. 5. panta 1. punkta c) apakšpunktu). Pirms videonovērošanas sistēmas uzstādīšanas pārzinim vienmēr būtu kritiski jāizvērtē, vai šis pasākums, pirmkārt, ir piemērots vēlamā mērķa sasniegšanai un, otrkārt, ir atbilstošs un nepieciešams tā nolūkiem. Videonovērošanas pasākumi būtu jāizvēlas tikai tad, ja apstrādes nolūku nevar sasniegt ar citiem līdzekļiem, kas ir mazāk traucējoši datu subjekta pamattiesībām un pamatbrīvībām.

25. Ņemot vērā to, ka pārzinis vēlas novērst ar īpašumu saistītus noziegumus, tā vietā, lai uzstādītu videonovērošanas sistēmu, pārzinis varētu veikt arī alternatīvus drošības pasākumus, piemēram, nožogot īpašumu, ieviest apsardzes darbinieku regulāru patrulēšanu, izmantot vārtziņus, ierīkot labāku apgaismojumu, uzstādīt drošības slēdzenes, izturīgus logus un durvis vai sienas nokrāsot ar pretgrafiti krāsu vai apšūt ar foliju. Šie pasākumi var būt tikpat efektīvi pret ielaušanos, zādzību un vandālismu kā videonovērošanas sistēmas. Pārzinim katrā individuālā gadījumā ir jānovērtē, vai šādi pasākumi var būt saprātīgs risinājums.

26. Pirms sākt izmantot videonovērošanas sistēmu, pārzinim ir pienākums novērtēt, kur un kad videonovērošanas pasākumi ir stingri nepieciešami. Parasti videonovērošanas sistēmas lietošana, kas tiek veikta nakts laikā, kā arī ārpus parastā darba laika, būs atbilstoša pārziņa vajadzībai novērst jebkādu apdraudējumu viņa īpašumam.

[10] Sk. WP217, 29. panta darba grupa, 24. lpp. un turpmākās lpp. Sk. arī EST spriedumu lietā C-708/18, 44. punktu.

27. Parasti vajadzība izmantot videonovērošanu pārziņa telpu aizsardzībai beidzas līdz ar īpašuma robežām.[11] Tomēr ir gadījumi, kad ar īpašuma novērošanu nepietiek, lai nodrošinātu efektīvu aizsardzību. Atsevišķos gadījumos var būt nepieciešams videonovērošanu paplašināt, ietverot arī tuvāko apkaimi. Šajā gadījumā pārzinim būtu jāapsver fizisku un tehnisku līdzekļu izmantošana, piemēram, nebūtisko zonu attēlu aizkrāsošana vai pikselēšana.

> Piemērs. Grāmatnīcas īpašnieki vēlas aizsargāt savas telpas no vandālisma. Parasti šādos gadījumos kamerām būtu jāfilmē tikai pašas telpas, jo nav nepieciešamības šajā nolūkā novērot blakus esošās telpas vai sabiedriskas vietas grāmatnīcas telpu apkaimē.

28.

29. Jautājumi apstrādes nepieciešamības sakarā rodas arī attiecībā uz to, kā notiek pierādījumu saglabāšana. Dažos gadījumos var būt nepieciešams izmantot melnās kastes risinājumus, kur uzfilmētais materiāls tiek automātiski dzēsts pēc noteikta glabāšanas laikposma un tam var piekļūt tikai incidenta gadījumā. Citās situācijās var vispār nebūt vajadzības ierakstīt videomateriālu, bet tā vietā kā atbilstošāks risinājums var būt novērošana reāllaikā. Lēmums par to, vai izvēlēties melnās kastes risinājumus vai novērošanu reāllaikā, būtu jāpieņem, ņemot vērā arī novērošanas nolūku. Piemēram, ja videonovērošanas nolūks ir pierādījumu saglabāšana, tad reāllaika novērošanas metodes parasti nav piemērotas. Dažreiz reāllaika novērošanas metodes var būt vairāk apgrūtinošas nekā materiāla saglabāšana un automātiska dzēšana pēc noteikta laikposma (piemēram, ja kādam ir pastāvīgi jāskatās monitorā, tas var būt vairāk apgrūtinoši nekā gadījumā, ja monitora nav un viss materiāls tiek tieši saglabāts melnajā kastē). Šajā saistībā ir jāievēro datu minimizācijas princips (5. panta 1. punkta c) apakšpunkts). Būtu arī jāpatur prātā, ka pārzinim var būt iespēja videonovērošanas vietā izmantot apsardzes darbiniekus, kuri spēj nekavējoties reaģēt un iejaukties.

3.1.3 Interešu līdzsvarošana

30. Pieņemot, ka videonovērošana ir nepieciešama, lai aizsargātu pārziņa likumīgās intereses, ir jāņem vērā tas, ka videonovērošanas sistēmu var izmantot tikai tad, ja par pārziņa vai trešo personu leģitīmajām interesēm (piemēram, īpašuma vai fiziskās integritātes aizsardzība) pārākas nav datu subjekta intereses vai pamattiesības un pamatbrīvības. Pārzinim ir jāapsver, 1) ciktāl novērošana skar indivīdu intereses, pamattiesības un pamatbrīvības un 2) vai tā izraisa pārkāpumus vai negatīvas sekas attiecībā uz datu subjekta tiesībām. Faktiski šāda interešu līdzsvarošana ir obligāta. No vienas puses ir rūpīgi jāizvērtē un jālīdzsvaro pamattiesības un pamatbrīvības un, no otras puses, pārziņa leģitīmās intereses.

[11] Dažās dalībvalstīs uz to var attiekties arī vietējie tiesību akti.

Piemērs. Privātas automobiļu stāvvietas uzņēmums ir dokumentējis atkārtotas problēmas saistītas ar zādzībām no stāvēšanai novietotajiem automobiļiem. Stāvvieta ir atklāta teritorija, kurai var viegli piekļūt ikviens, tomēr tā ir skaidri nodalīta ar zīmēm un apkārt tās teritorijai izvietotiem ceļa bloķētājiem. Stāvvietas uzņēmumam ir leģitīmas intereses (novērst zādzības no klientu automobiļiem) novērot teritoriju diennakts laikā, kad tiek konstatētas problēmas. Datu subjekti tiek novēroti ierobežotā laikposmā, viņi šajā teritorijā neatrodas atpūtas nolūkos un arī viņu pašu interesēs ir šādu zādzību novēršana. Šajā gadījumā pārziņa leģitīmās intereses ir svarīgākas par datu subjektu interesēm netikt novērotiem.

Piemērs. Restorāns nolemj uzstādīt videokameras tualetes telpās, lai kontrolētu sanitāro telpu tīrību. Šajā gadījumā datu subjektu tiesības acīmredzami ir svarīgākas par pārziņa interesēm, tāpēc kameras šajās telpās uzstādīt nedrīkst .

31.

3.1.3.1 Lēmuma pieņemšana katrā individuālā gadījumā

32. Tā kā saskaņā ar regulu interešu līdzsvarošana ir obligāta, lēmums ir jāpieņem katrā gadījumā atsevišķi (sk. 6. panta 1. punkta f) apakšpunktu). Nepietiek atsaukties uz abstraktām situācijām vai savstarpēji salīdzināt līdzīgus gadījumus. Pārzinim ir jāizvērtē riski, kad var tikt traucētas datu subjekta tiesības. Izvērtēšanai izšķirošais kritērijs ir tas, cik intensīvi notiek iejaukšanās indivīda tiesībās un brīvībās.

33. Intensitāti var noteikt apkopotās informācijas veids (informācijas saturs), apjoms (informācijas blīvums, telpiskais un ģeogrāfiskais tvērums), attiecīgo datu subjektu skaits, konkrēts skaitlis vai izteikts procentos no attiecīgās iedzīvotāju grupas, konkrētā situācija, datu subjektu grupas faktiskās intereses, alternatīvi līdzekļi, kā arī datu novērtējuma veids un apjoms.

34. Svarīgi līdzsvarošanas faktori var būt novērotās zonas lielums un novēroto datu subjektu daudzums. Videonovērošanas izmantošana nomaļā vietā (piemēram, lai novērotu savvaļas dzīvniekus vai aizsargātu kritisku infrastruktūru, privātīpašumā esošu radioantenu) ir jāvērtē citādi nekā videonovērošana gājēju zonā vai lielveikalā.

Piemērs. Ja ir uzstādīts videoreģistrators (piemēram, lai iegūtu pierādījumus, gadījumā, ja notiek negadījums), ir svarīgi nodrošināt, lai tas pastāvīgi neierakstītu satiksmi, kā arī ceļa malā esošās personas. Ja tas netiek nodrošināts, šo būtisko iejaukšanos datu subjektu tiesībās nevar pamatot ar interesi izmantot videoierakstus kā pierādījumus teorētiskā gadījumā, kad notiek ceļu satiksmes negadījums[11].

35.

3.1.3.2 Saprātīgas datu subjektu gaidas

36. Saskaņā ar 47. apsvērumu leģitīmu interešu esība ir rūpīgi jāizvērtē. Šajā ziņā ir jāņem vērā saprātīgas datu subjekta gaidas tā personas datu apstrādes laikā un kontekstā. Attiecībā uz sistemātisku novērošanu attiecības starp datu subjektu un pārzini var būt ļoti atšķirīgas un var ietekmēt to, kādas saprātīgas gaidas var būt datu subjektam. Jēdziena "saprātīgas gaidas" interpretācija nebūtu jābalsta tikai uz attiecīgajām subjektīvajām gaidām. Izšķirošajam kritērijam drīzāk jābūt tam, vai objektīva trešā persona var saprātīgi gaidīt un secināt, ka viņa tiks novērota konkrētajā situācijā.

37. Piemēram, vairumā gadījumu darbinieks savā darbavietā negaidīs, ka viņa darba devējs viņu novēros[12]. Tāpat netiek gaidīts, ka novērošana tiks veikta kāda privātajā dārzā, dzīvojamās telpās vai medicīnisko izmeklējumu un ārstniecības telpās. Kā arī, nav saprātīgi gaidīt, ka novērotas tiks sanitārās vai saunas telpas, jo šādu telpu novērošana ir intensīva iejaukšanās datu subjekta tiesībās. Datu subjektu saprātīgas gaidas ir tādas, ka šādās vietās videonovērošana netiks veikta. Turpretī bankas klients var sagaidīt, ka viņš(-a) tiks novērots(-a) bankas telpās vai pie bankomāta.

38. Datu subjekti arī var sagaidīt, ka viņi netiks novēroti sabiedriskās vietās, jo īpaši vietās, ko parasti izmanto atveseļošanās, spēku atgūšanas un brīvā laika pavadīšanas vajadzībām, kā arī vietās, kur indivīdi uzturas un/vai komunicē, piemēram, uzgaidāmajās telpās, pie galdiņiem restorānos, parkos, kinoteātros un fitnesa iestādēs. Šajos gadījumos datu subjekta intereses vai tiesības bieži vien būs svarīgākas par pārziņa leģitīmajām interesēm.

> Piemērs. Tualetēs datu subjekti sagaida, ka viņi netiks novēroti. Videonovērošana, ko veiktu, piemēram, lai novērstu negadījumus, nebūtu samērīga.

39.

40. Zīmēm, ar kurām datu subjekts tiek informēts par videonovērošanu, nav nozīmes, ja tās tiek lietotas situācijās, kad datu subjekts objektīvu iemeslu dēļ nesagaida, ka tiek veikta videonovērošana. Tas nozīmē, ka, piemēram, veikala īpašnieks nevar paļauties uz to, ka klienti sagaidīs, ka viņi tiek novēroti, tikai tāpēc vien, ka pie ieejas ir izvietota zīme, kas informē par novērošanu.

3.2 Nepieciešamība izpildīt uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras (6. panta 1. punkta e) apakšpunkts)

41. Personas datus var apstrādāt, izmantojot videonovērošanu, saskaņā ar 6. panta 1. punkta e) apakšpunktu, ja ir nepieciešamība izpildīt uzdevumu, ko veic sabiedrības interesēs vai īstenojot oficiālās pilnvaras[13]. Ir iespējams, ka oficiālo pilnvaru īstenošana nepieļauj šādu apstrādi, bet citi juridiskie pamati, piemēram, "veselība un drošība", lai aizsargātu apmeklētājus un darbiniekus, var paredzēt ierobežotu apstrādi, vienlaikus ņemot vērā VDAR noteiktos pienākumus un datu subjektu tiesības.

42. Dalībvalstis var paturēt spēkā vai ieviest īpašus valsts tiesību aktus par videonovērošanu, lai pielāgotu VDAR noteikumu piemērošanu, precīzāk nosakot konkrētas prasības attiecībā uz apstrādi, kamēr vien tas ir saskaņā ar VDAR noteiktajiem principiem (piemēram, par glabāšanas ierobežojumu, samērīgumu).

[12] Sk. arī: 29. panta darba grupa, Atzinums 2/2017 par datu apstrādi darba vietā, WP249, pieņemts 2017. gada 8. jūnijā.

[13] Minētās apstrādes pamats ir noteikts Savienības tiesību vai dalībvalsts tiesību aktos, un tas ir vajadzīgs, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras (6. panta 3. punkts).

3.3 Piekrišana (6. panta 1. punkta a) apakšpunkts)

43. Piekrišanai ir jābūt sniegtai brīvi, ar konkrētu, apzinātu un viennozīmīgu norādi, kā tas ir aprakstīts Pamatnostādnēs par piekrišanu[14].

44. Attiecībā uz sistemātisku novērošanu, saskaņā ar 7. pantu (sk. 43. apsvērumu) datu subjekta piekrišana var būt juridisks pamats tikai izņēmuma gadījumos. Novērošana pēc būtības nozīmē to, ka ar šo tehnoloģiju tiek vienlaikus novērots nezināms cilvēku skaits. Pārzinis diezin vai spēs pierādīt, ka datu subjekts ir sniedzis piekrišanu pirms tā personas datu apstrādes (7. panta 1. punkts). Pieņemot, ka datu subjekts nesniedz piekrišanu, pārzinim būs grūti pierādīt, ka personas datu apstrāde netiek turpināta (7. panta 3. punkts).

> Piemērs. Daži atlēti var pieprasīt novērošanu individuālo treniņu laikā, lai viņi varētu analizēt savas treniņu metodes un rezultātus. Turpretī, ja sporta klubs ar tādu pašu nolūku uzņemas iniciatīvu novērot visu komandu, tad datu subjekta piekrišana bieži vien nebūs derīga, jo dažiem atlētiem var šķist, ka viņi ir spiesti sniegt piekrišanu, lai viņu atteikums to sniegt nekaitētu citiem komandas dalībniekiem.

45.

46. Ja pārzinis vēlas paļauties uz piekrišanu, viņam ir pienākums nodrošināt, ka ikviens datu subjekts, kurš ienāk zonā, kas tiek novērota, ir sniedzis piekrišanu. Šādai piekrišanai ir jāatbilst 7. panta nosacījumiem. Ienākšana marķētā novērotā zonā (piemēram, personas tiek aicinātas iziet caur noteiktu gaiteni vai vārtiem, lai ienāktu novērotajā zonā) nav uzskatāma par paziņojumu vai skaidru apstiprinošu darbību, kas vajadzīga piekrišanai, izņemot, ja tā atbilst 4. un 7. panta kritērijiem, kā aprakstīts Pamatnostādnēs par piekrišanu[15].

47. Ņemot vērā varas nelīdzsvarotību starp darba devējiem un darba ņēmējiem, vairumā gadījumu darba devējiem, apstrādājot personas datus, nebūtu jāpamatojas uz darba ņēmēja piekrišanu, jo ir maz ticams, ka tā ir tikusi sniegta brīvi. Šajā gadījumā būtu jāņem vērā Pamatnostādnes par piekrišanu.

48. Dalībvalstu tiesību aktos vai koplīgumos, tostarp "darba līgumos", var būt paredzēti konkrēti noteikumi par darbinieku personas datu apstrādi nodarbinātības kontekstā (sk. 88. pantu).

[14] 29. panta darba grupa (29. panta DG), Pamatnostādnes par piekrišanu saskaņā ar Regulu 2016/679 (WP 259 rev. 01) — apstiprinājusi EDAK.

[15] 29. panta darba grupa (29. panta DB), Pamatnostādnes par piekrišanu saskaņā ar Regulu 2016/679 (WP259) — apstiprinājusi EDAK —, kas būtu jāņem vērā.

4 UZFILMĒTĀ VIDEOMATERIĀLA IZPAUŠANA TREŠĀM PERSONĀM

49. Pamatā uz videoierakstu izpaušanu trešām personām attiecas VDAR vispārējie noteikumi.

4.1 Vispārīgi par uzfilmētā videomateriāla izpaušanu

50. Izpaušana ir definēta 4. panta 2. punktā kā nosūtīšana (piemēram, individuāla paziņošana), izplatīšana (piemēram, publicēšana tiešsaistē) vai cita veida darbība, lai materiālu darītu pieejamu. Trešās personas ir definētas 4. panta 10. punktā. Ja izpaušana notiek trešām valstīm vai starptautiskām organizācijām, piemēro arī īpašos 44. panta un turpmāko pantu noteikumus.

51. Jebkura personas datu izpaušana ir atsevišķa veida personas datu apstrāde, kuras veikšanai pārzinim ir nepieciešams juridisks pamats, kā tas noteikts 6. pantā.

> Piemērs. Pārzinim, kurš vēlas internetā augšupielādēt ierakstu, ir jāpaļaujas uz juridisku pamatu šādai apstrādei, piemēram, iegūstot piekrišanu no datu subjekta atbilstoši 6. panta 1. punkta a) apakšpunktam.

52.

53. Videomateriāla nosūtīšana trešām personām citiem nolūkiem, kas nav nolūki, kādiem dati savākti, ir iespējama atbilstoši 6. panta 4. punktam.

> Piemērs. Lai risinātu strīdus bojājumu gadījumos, ir uzstādīta barjeras videonovērošana (automobiļu stāvvietā). Tiek izdarīts bojājums, un ieraksts tiek nosūtīts juristam lietas ierosināšanai. Šādā gadījumā ierakstīšanas nolūks ir tāds pats kā nosūtīšanas gadījumā.
>
> Piemērs. Lai risinātu strīdus bojājumu gadījumos, ir uzstādīta barjeras videonovērošana (automobiļu stāvvietā). Šāds ieraksts tiek publicēts tiešsaistē vienkārši izklaides nolūkos. Šajā gadījumā nolūks ir mainījies un vairs nav saderīgs ar sākotnējo nolūku. Tāpēc būtu problemātiski argumentēt juridisko pamatu šādai apstrādei (publicēšanai).

54.

55. Datu saņēmējam, kas ir trešā persona, arī ir jāveic juridiskā analīze, jo īpaši nosakot savu apstrādes veikšanas juridisko pamatu atbilstoši 6. pantam (piemēram, saņemot materiālu).

4.2 Uzfilmētā videomateriāla izpaušana tiesībaizsardzības iestādēm

56. Arī videoierakstu izpaušana tiesībaizsardzības iestādēm ir neatkarīgs process, kas pārzinim ir jāpamato atsevišķi.

57. Saskaņā ar 6. panta 1. punkta c) apakšpunktu apstrāde ir likumīga, ja tā ir nepieciešama, lai izpildītu uz pārzini attiecināmu juridisku pienākumu. Lai gan piemērojamie policijas darbu regulējošie tiesību akti ir jautājums, kas ir ekskluzīvā dalībvalstu kontrolē, visticamāk, katrā dalībvalstī pastāv vispārēji noteikumi, kas reglamentē pierādījumu nosūtīšanu tiesībaizsardzības iestādēm. Apstrādi, ko veic pārzinis, kurš nodod datus, reglamentē VDAR. Ja valsts tiesību akti nosaka, ka pārzinim ir jāsadarbojas ar tiesībaizsardzības iestādēm (piemēram, izmeklēšanā), juridiskais pamats datu nodošanai ir juridiskais pienākums, kas noteikts 6. panta 1. punkta c) apakšpunktā.

58. Nolūka ierobežojums, kas noteikts 6. panta 4. punktā, bieži nesagādā problēmas, jo izpaušana ir skaidri noteikta dalībvalsts tiesību aktos. Tādēļ nav nepieciešams īpaši apsvērt speciālās prasības par nolūka maiņu a)–e) apakšpunkta nozīmē.

59. Piemērs. Veikala īpašnieks ieraksta pie veikala ieejas notiekošo. Ierakstā redzams, kā persona nozog citai personai naudas maku. Policija pieprasa, lai pārzinis nodod materiālu izmeklēšanas vajadzībām. Šādā gadījumā veikala īpašnieks ,lai veiktu nodoto datu apstrādi, izmantotu juridisko pamatu, kas ir noteikts 6. panta 1. punkta c) apakšpunktā (juridisks pienākums), to lasot kopsakarā ar attiecīgajiem dalībvalsts tiesību aktiem..

60. Piemērs. Veikalā drošības apsvērumu dēļ ir uzstādīta kamera. Veikala īpašniekam šķiet, ka ierakstā ir redzams kaut kas aizdomīgs, un viņš nolemj nosūtīt materiālu policijai (bez iepriekš saņemtām indikācijām, ka notiek jebkāda veida izmeklēšana). Šādā gadījumā veikala īpašniekam ir jāizvērtē, vai nosacījumi, kas paredzēti, lielākoties, 6. panta 1. punkta f) apakšpunktā, ir izpildīti. Parasti tie ir izpildīti, ja veikala īpašniekam ir pamatotas aizdomas, ka ir izdarīts noziegums.

61. Uz personas datu apstrādi, ko veic pašas tiesībaizsardzības iestādes, VDAR neattiecas (sk. 2. panta 2. punkta d) apakšpunktu), taču uz to attiecas Tiesībaizsardzības direktīva ((ES) 2016/680).

5 ĪPAŠU KATEGORIJU DATU APSTRĀDE

62. Videonovērošanas sistēmas parasti apkopo ievērojamu apjomu personas datu, starp kuriem var būt ļoti personiski dati un pat īpašu kategoriju dati. Patiešām, sākotnēji šķietami nebūtiskus datus, kas savākti ar video starpniecību, var izmantot citas informācijas izsecināšanai, lai sasniegtu pavisam citu mērķi (piemēram, lai noskaidrotu indivīda paradumus). Tomēr ne vienmēr ir jāuzskata, ka videonovērošanā tiek apstrādāti īpašu kategoriju personas dati.

63. Piemērs. Videoierakstus, kuros redzams datu subjekts ar brillēm vai ratiņkrēslā, pašu par sevi neuzskata par īpašām personas datu kategorijām.

64. Tomēr, ja videoierakstus apstrādā, lai iegūtu īpašu kategoriju datus, piemēro 9. pantu.

65. Piemērs. Politiskus uzskatus var izsecināt no attēliem, kuros redzami datu subjekti, kas piedalās pasākumā, iesaistās streikā u. tml. Uz šo gadījumu attiecas 9. pants.

Piemērs. Ja slimnīcā uzstāda videokameru, lai novērotu pacienta veselības stāvokli, to uzskata par īpašu kategoriju personas datu apstrādi (9. pants).

66. Saskaņā ar vispārējo principu vienmēr, kad uzstāda videonovērošanas sistēmu, būtu rūpīgi jāapsver datu minimizācijas princips. Tādējādi pat gadījumos, kad 9. panta 1. punkts nav piemērojams, datu pārzinim būtu vienmēr jācenšas mazināt risku, ka uzfilmētais materiāls atklāj citus sensitīvus datus (pārsniedzot 9. pantu), neatkarīgi no nolūka.

67. Piemērs. Uz baznīcas videonovērošanu kā tādu neattiecas 9. pants. Tomēr pārzinim, novērtējot datu subjekta intereses, ir jāveic īpaši rūpīgs novērtējums saskaņā ar 6. panta 1. punkta f) apakšpunktu, ņemot vērā datu veidu, kā arī risku, ka novērošanā varētu tikt iegūt citi sensitīvi dati (9. pants).

68. Ja videonovērošanas sistēmu izmanto, lai apstrādātu īpašu kategoriju datus, pārzinim ir jāidentificē gan izņēmums īpašu kategoriju datu apstrādei saskaņā ar 9. pantu (t. i., izņēmums attiecībā uz vispārējo noteikumu, ka nevajadzētu apstrādāt īpašu kategoriju datus), gan juridiskais pamats saskaņā ar 6. pantu.

69. Piemēram, teorētiski un izņēmuma gadījumos var izmantot 9. panta 2. punkta c) apakšpunktu (“(..), ja apstrāde ir vajadzīga, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses (..)”), tomēr datu pārzinim tas ir jāpamato kā absolūta nepieciešamība aizsargāt personas vitālas intereses un jāpierāda, ka konkrētais “(..) datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu”. Turklāt datu pārzinim nav atļauts izmantot videonovērošanas sistēmu jebkādam citam mērķim.

70. Šajā ziņā ir svarīgi norādīt, ka ne katrs 9. pantā uzskaitītais izņēmums var būt izmantojams, lai pamatotu īpašu kategoriju datu apstrādi, veicot videonovērošanu. Konkrētāk, datu pārziņi, kas apstrādā šādus datus videonovērošanas kontekstā, nevar atsaukties uz 9. panta 2. punkta e) apakšpunktu, ar kuru ir atļauta apstrāde, kas attiecas uz personas datiem, kurus datu subjekts apzināti ir publiskojis. Tikai tas vien, ka persona ienāk kameras uztveršanas zonā, nenozīmē, ka datu subjekts ir iecerējis, ka tiks publiskoti īpašu kategoriju dati, kas attiecas uz viņu.

71. Turklāt īpašu kategoriju datu apstrādei ir vajadzīga paaugstināta un nepārtraukta modrība, lai tiktu izpildīti konkrēti pienākumi, piemēram, vajadzības gadījumā ir jāveic augsta līmeņa drošības un ietekmes uz datu aizsardzību novērtējums.

> Piemērs. Darba devējs nedrīkst izmantot videonovērošanas ierakstus, kuros redzama demonstrācija, lai identificētu streikotājus.

72.

5.1 Vispārēji apsvērumi biometrisko datu apstrādē

73. Biometrisko datu un jo īpaši sejas atpazīšanas izmantošana ir saistīta ar paaugstinātiem riskiem datu subjektu tiesībām. Ir svarīgi, lai šādu tehnoloģiju izmantošanā tiktu ievēroti VDAR noteiktie likumīguma, nepieciešamības, samērīguma un datu minimizācijas principi. Lai gan šo tehnoloģiju izmantošana var tikt uzskatīta par īpaši efektīvu, pārziņiem vispirms būtu jānovērtē ietekme uz pamattiesībām un pamatbrīvībām un jāapsver mazāk traucējoši veidi, kā sasniegt to likumīgo apstrādes mērķi.

74. Lai datus kvalificētu par biometriskajiem datiem, kā tie definēti VDAR, izejas datu, piemēram, fiziskas personas fizisko, fizioloģisko vai uzvedības pazīmju, apstrādei jābūt saistītai ar šo iezīmju mērījumiem. Tā kā biometriskie dati ir šādu mērījumu rezultāts, VDAR 4. panta 14. punktā ir noteikts, ka tie ir personas dati "(..) pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju (..)". Tomēr nofilmēto materiālu, kurā redzams indivīds, pašu par sevi nevar uzskatīt par biometriskajiem datiem saskaņā ar 9. pantu, ja tas nav ticis īpaši tehniski apstrādāts, lai atvieglotu indivīda identificēšanu[16].

75. Lai to uzskatītu par īpašu kategoriju personas datu apstrādi (9. pants), biometriskajiem datiem jābūt apstrādātiem "nolūkā veikt fiziskas personas unikālu identifikāciju".

76. Rezumējot, ņemot vērā 4. panta 14. punktu un 9. pantu, ir jāņem vērā šādi trīs kritēriji:

- **datu veids** —dati, kas attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm;
- **apstrādes līdzekļi un veids** — dati "pēc specifiskas tehniskas apstrādes";
- **apstrādes nolūks** — datiem jābūt izmantotiem nolūkā veikt fiziskas personas unikālu identifikāciju.

77. Lai izmantotu videonovērošanu, tostarp biometriskās atpazīšanas funkciju, ko uzstādījušas privātas struktūras savām vajadzībām (piemēram, tirgdarbībai, statistikai vai pat drošībai), lielākajā daļā gadījumu būs vajadzīga skaidra piekrišana no visiem datu subjektiem (9. panta 2. punkta a) apakšpunkts), tomēr var būt arī gadījumi, kad ir piemērojams arī cits atbilstošs izņēmums, kas noteikts 9. pantā.

[16] VDAR 51. apsvērumā ir apstiprināta šī analīze, nosakot: "Fotogrāfiju apstrāde nebūtu sistemātiski jāuzskata par īpašu kategoriju personas datu apstrādi, jo uz tām biometrisko datu definīcija attiecas tikai tad, kad tās apstrādās ar konkrētiem tehniskiem līdzekļiem, kas ļauj veikt fiziskas personas unikālu identifikāciju vai autentifikāciju. (..)".

Piemērs. Lai uzlabotu savu pakalpojumu sniegšanu, privātuzņēmums pasažieru identifikācijas pārbaudes punktus lidostā (bagāžas nodošana, iekāpšana) aizstāj ar videonovērošanas sistēmām, kas izmanto sejas atpazīšanas metodes, lai pārbaudītu to pasažieru identitāti, kuri izvēlējušies piekrist šādai procedūrai. Tā kā uz šo apstrādi attiecas 9. pants, pasažieriem, kuri iepriekš būs snieguši skaidru piekrišanu, būs jāpiesakās, piemēram, automātiskā terminālī, lai izveidotu un reģistrētu savu sejas veidni, kas piesaistīta viņu iekāpšanas kartei un identitātei. Pārbaudes punktiem ar sejas atpazīšanu jābūt skaidri nošķirtiem, piemēram, sistēmai jābūt uzstādītai kontroles statīvā tā, lai nevarētu tikt izveidotas biometriskās veidnes personām, kuras nav tam piekritušas. Ar biometrisko sistēmu aprīkotus statīvus izmantos tikai tie pasažieri, kuri iepriekš būs snieguši piekrišanu un veikuši iepriekšēju reģistrāciju.

Piemērs. Pārzinis pārvalda piekļuvi savai ēkai, izmantojot sejas atpazīšanas metodi. Personas var izmantot šo piekļuves veidu, ja viņas iepriekš ir sniegušas skaidri apzinātu piekrišanu (saskaņā ar 9. panta 2. punkta a) apakšpunktu). Tomēr, lai nodrošinātu, ka netiek reģistrēta neviena persona, kura nav sniegusi savu piekrišanu, sejas atpazīšanas metode ir jāaktivizē pašam datu subjektam, piemēram, nospiežot pogu. Lai nodrošinātu apstrādes likumīgumu, pārzinim vienmēr ir jāpiedāvā alternatīvs veids, kā piekļūt ēkai bez biometriskās apstrādes, piemēram, izmantojot žetonus vai atslēgas.

78.

79. Šādos gadījumos, kad tiek izveidotas biometriskās veidnes, pārziņiem ir jānodrošina, ka, tiklīdz ir iegūts atbilsmes vai neatbilsmes rezultāts, visas starpposma veidnes, kas radītas procesā (ar datu subjekta skaidru un apzinātu piekrišanu), lai tās salīdzinātu ar veidnēm, ko datu subjekti izveidojuši pieteikšanās laikā, tiek nekavējoties un drošā veidā izdzēstas. Pieteikšanās vajadzībām izveidotās veidnes būtu jāpatur tikai apstrādes nolūka īstenošanai un nebūtu jāglabā vai jāarhivē.

80. Tomēr, ja apstrādes nolūks ir, piemēram, nošķirt vienu personu kategoriju no citas, bet ne unikāli identificēt kādu personu, uz šādu apstrādi 9. pants neattiecas.

Piemērs. Veikala īpašnieks vēlas pielāgot savas reklāmas, pamatojoties uz videonovērošanas sistēmas nofilmēto personu dzimuma un vecuma pazīmēm. Ja šāda sistēma neizveido biometriskās veidnes personu unikālai identificēšanai, bet tikai fiksē minētās fiziskās pazīmes, lai klasificētu personu, tad uz šādu apstrādi 9. pants neattiecas (kamēr vien netiek apstrādāti citi īpašu kategoriju datu veidi).

81.

82. Tomēr 9. pants ir piemērojams, ja pārzinis glabā biometriskus datus (visbiežāk tas tiek darīts, izmantojot veidnes, ko izveido, izgūstot būtiskākās iezīmes no biometriskajiem izejas datiem (piemēram, sejas mērījumus no attēla)), lai unikāli identificētu personu. Ja pārzinis vēlas noteikt datu subjektu, kurš atkārtoti ienāk telpā vai ieiet citā telpā (piemēram, lai ieplānotu pielāgotu reklāmu pastāvīgu izvietošanu), tad nolūks ir unikāli identificēt fizisku personu, kas nozīmē, ka uz šo darbību jau 9. pants attiecas. Tā var būt gadījumā, kad pārzinis saglabā izveidotās veidnes, lai izvietotu vēl vairāk pielāgotas reklāmas vairākos stendos dažādās vietās visā veikalā. Tā kā sistēma izmanto fiziskas pazīmes, lai noteiktu konkrētus indivīdus, kuri atgriežas atpakaļ kameras uztveršanas zonā (piemēram, lielveikala apmeklētājus), un izsekotu viņu pārvietošanos, tā ir uzskatāma par biometriskās identifikācijas metodi, jo tās mērķis ir atpazīšana, izmantojot specifisku tehnisku apstrādi.

Piemērs. Veikala īpašnieks savā veikalā ir uzstādījis sejas atpazīšanas sistēmu, lai pielāgotu savas reklāmas konkrētiem indivīdiem. Pirms šādas biometriskās sistēmas izmantošanas un pielāgotu reklāmu izvietošanas datu pārzinim ir jāsaņem skaidra un apzināta visu datu subjektu piekrišana. Šādas sistēmas lietošana būtu nelikumīga, ja tā filmētu apmeklētājus vai garāmgājējus, kuri nav piekrituši viņu biometriskās veidnes izveidei, pat ja viņu veidne tiktu izdzēsta iespējami īsā laikā. Šādas pagaidu veidnes patiesi ir biometriskie dati, ko apstrādā, lai unikāli identificētu personu, kura, iespējams, nevēlas saņemt pielāgotas reklāmas.

83.

84. EDAK norāda, ka dažas biometriskās sistēmas ir uzstādītas nekontrolētās vidēs[17], kas nozīmē, ka sistēma darbojoties nofilmē jebkuru kameras uztveršanas zonā ienākušu indivīdu sejas, tostarp tādu personu sejas, kuras nav sniegušas piekrišanu biometriskās ierīces izmantošanai, un tādējādi izveido biometriskās veidnes. Šīs veidnes tiek salīdzinātas ar izveidotajām to datu subjektu veidnēm, kuri ir snieguši iepriekšēju piekrišanu pieteikšanās procesā (t. i., biometriskās ierīces lietotāju veidnēm), lai datu pārzinis atpazītu, vai persona ir biometriskās ierīces lietotājs vai nav. Šajā gadījumā sistēma bieži ir veidota tā, lai indivīdus, kurus tā vēlas atpazīt datubāzē, nošķirtu no indivīdiem, kuri nav pieteikušies. Tā kā mērķis ir unikāli identificēt fiziskas personas, tad joprojām ir vajadzīgs VDAR 9. panta 2. punktā noteiktais izņēmums attiecībā uz ikvienu personu, kuru kamera nofilmē.

Piemērs. Viesnīcā tiek izmantota videonovērošana, lai automātiski brīdinātu viesnīcas pārvaldnieku, ka ir ieradusies ļoti svarīga persona, kad tiek atpazīta viesa seja. Šīs ļoti svarīgās personas ir iepriekš devušas skaidru piekrišanu sejas atpazīšanas sistēmas izmantošanai, pirms tam reģistrējoties šim nolūkam izveidotā datubāzē. Šādas biometrisko datu apstrādes sistēmas būtu nelikumīgas, ja vien visi pārējie viesi, kurus novēro (lai identificētu ļoti svarīgas personas), nav piekrituši datu apstrādei saskaņā ar VDAR 9. panta 2. punkta a) apakšpunktu.

Piemērs. Pārzinis uzstāda videonovērošanas sistēmu ar sejas atpazīšanas funkciju pie viņa pārvaldītās koncertzāles ieejas. Pārzinim ir jāierīko skaidri nošķirtas ieejas — viena aprīkota ar biometrisko sistēmu, bet otra neaprīkota ar šādu sistēmu (kur var, piemēram, noskenēt biļeti). Ieejām, kas ir aprīkotas ar biometriskajām ierīcēm, jābūt iekārtotām un pieejamām tā, lai nepieļautu, ka sistēma izveido biometriskās veidnes koncertzāles apmeklētājiem, kuri nav snieguši piekrišanu.

85.

86. Visbeidzot, ja ir nepieciešama piekrišana saskaņā ar VDAR 9. pantu, datu pārzinim nevajadzētu piemērot nosacījumu, ka tā pakalpojumi ir pieejami tikai tādā gadījumā, ja ir sniegta piekrišana biometriskajai apstrādei. Proti, jo īpaši tad, kad biometrisko apstrādi izmanto autentifikācijas nolūkā, datu pārzinim ir jāpiedāvā alternatīvs risinājums, kas neietver biometrisko apstrādi, neradot ierobežojumus vai papildu izmaksas datu subjektam. Šāds alternatīvs risinājums ir vajadzīgs arī personām, kuras neatbilst biometriskās ierīces iespējām (pieteikšanās vai biometrisko datu nolasīšana ir neiespējama, invaliditāte, kas apgrūtina ierīces izmantošanu, u. tml.), un gadījumos, kad ir paredzams, ka biometriskā ierīce nebūs pieejama (piemēram, ierīces darbības traucējumu gadījumā), ir jābūt ieviestam rezerves risinājumam, lai nodrošinātu piedāvātā pakalpojuma nepārtrauktību, bet tam ir jābūt izmantotam tikai izņēmuma gadījumos. Dažos gadījumos var būt situācija, kad biometrisko datu apstrāde ir atbilstoši līgumam sniegta pakalpojuma pamatā, piemēram,

[17] Tas nozīmē, ka biometriskā ierīce atrodas publiski pieejamā vietā, un to var aktivizēt ikviens garāmgājējs, atšķirībā no biometriskajām sistēmām kontrolētās vidēs, ko var izmantot tikai ar personas piekrišanu.

muzejs rīko izstādi, lai demonstrētu sejas atpazīšanas ierīces izmantošanu, šādā gadījumā datu subjekts nevarēs noraidīt biometrisko datu apstrādi, ja viņš vēlēsies piedalīties izstādē. Šādā gadījumā piekrišana, kas nepieciešama saskaņā ar 9. pantu, ir spēkā, ja ir izpildītas 7. panta prasības.

5.2 Ieteicamie pasākumi risku mazināšanai biometrisko datu apstrādē

87. Saskaņā ar datu minimizācijas principu datu pārziņiem jānodrošina, ka dati, ko iegūst no digitāla attēla, lai izveidotu veidni, nav pārmērīgi un satur tikai informāciju, kas vajadzīga norādītajam nolūkam, tādējādi izvairoties no iespējamas turpmākas to apstrādes. Tāpat arī būtu jāievieš pasākumi, kas garantētu, ka veidnes nevar tikt nodotas un izmantotas citās biometriskajās sistēmās.

88. Identifikācijas un autentifikācijas/verifikācijas gadījumā var būt nepieciešamība saglabāt veidni, lai to vēlāk izmantotu salīdzināšanā. Šajā gadījumā datu pārzinim ir jāapsver, kāda būtu visatbilstošākā vieta šādu datu glabāšanai. Kontrolētā vidē (norobežotos gaiteņos vai kontrolpunktos) veidnes glabā individuālā ierīcē, kas atrodas pie lietotāja un ir tikai viņa kontrolē (viedtālrunī vai personas apliecībā), vai, ja veidnes ir vajadzīgas īpašiem nolūkiem un ja pastāv objektīvas vajadzības, veidnes glabā centralizētā datubāzē un šifrētas, atslēgu/ slepeno paroli darot zināmu tikai attiecīgajai personai, lai novērstu neatļautu piekļuvi veidnei vai tās glabāšanas vietai. Ja datu pārzinis nevar izvairīties no vajadzības piekļūt šīm veidnēm, viņam ir jāveic attiecīgi pasākumi, kas nodrošinātu glabāto datu drošību. Tā var būt, piemēram, veidnes šifrēšana, izmantojot kriptogrāfisku algoritmu.

89. Jebkurā gadījumā pārzinim ir jāveic visi nepieciešamie piesardzības pasākumi, lai saglabātu apstrādāto datu pieejamību, integritāti un konfidencialitāti. Šajā nolūkā pārzinis veic jo īpaši šādus pasākumus: sadala datus pa daļām to nosūtīšanas un glabāšanas laikā, glabā biometriskās veidnes un izejas datus vai identitātes datus atsevišķās datubāzēs, šifrē biometriskos datus, it īpaši biometriskās veidnes, un nosaka šifrēšanas un atslēgu pārvaldības politiku, integrē organizatoriskus un tehniskus pasākumus krāpšanas konstatēšanai, piesaista datiem integritātes kodu (piemēram, parakstu vai jaucējkodu) un aizliedz jebkādu ārēju piekļuvi biometriskajiem datiem. Šie pasākumi būtu jāpielāgo tehnoloģiju attīstībai.

90. Turklāt datu pārziņiem jāveic izejas datu (sejas attēlu, runas signālu, gaitas utt.) dzēšana un jānodrošina dzēšanas efektivitāte. Ja apstrādes juridiskais pamats vairs nepastāv, izejas dati ir jādzēš. Tā kā biometriskās veidnes tiek iegūtas no izejas datiem, tad pamatoti var uzskatīt, ka to datu bāzu veidošana var radīt tādu pašu, ja ne vēl lielāku, datu drošības apdraudējumu (jo ne vienmēr var būt viegli nolasīt biometrisko veidni, ja nav zināms, kā tā programmēta, savukārt izejas dati ir jebkuras veidnes veidošanas bloki). Ja datu pārzinim ir vajadzība glabāt šādus datus, ir jāapsver traucējumu pievienošanas metožu (piemēram, ūdenszīmju uz attēla) izmantošana, kas veidnes izveidi padarītu neefektīvu. Pārzinim biometriskie dati un veidnes ir jādzēš arī tad, ja ir notikusi neatļauta piekļuve nolasīšanas un salīdzināšanas terminālim vai glabāšanas serverim, un biometriskās ierīces kalpošanas laika beigās, ja dati nav noderīgi turpmākai apstrādei.

6 DATU SUBJEKTA TIESĪBAS

91. Ņemot vērā datu apstrādes specifiku, izmantojot videonovērošanu, dažas datu subjektu tiesības, kas noteiktas VDAR, būtu jāpaskaidro sīkāk. Tomēr šī nodaļa nav izsmeļoša, un personas datu apstrādē, izmantojot videonovērošanu, ir piemērojamas visas VDAR noteiktās tiesības.

6.1 Tiesības piekļūt datiem

92. Datu subjektam ir tiesības saņemt no pārziņa apstiprinājumu par to, vai viņa personas dati tiek apstrādāti. Attiecībā uz videonovērošanu tas nozīmē, ka gadījumā, ja dati nekādā veidā netiek saglabāti vai nosūtīti, tikai tad, kad ir beidzies reāllaika novērošanas brīdis, pārzinis var sniegt informāciju, ka personas dati vairs netiek apstrādāti (papildus vispārējam informēšanas pienākumam, kas noteikts13. pantā, sk. *7. iedaļu "Pārredzamības un informēšanas pienākumi"*). Tomēr, ja pieprasījuma brīdī dati vēl joprojām tiek apstrādāti (t. i., ja dati tiek glabāti vai jebkādā veidā pastāvīgi apstrādāti), datu subjektam būtu jāsaņem piekļuve tiem un informācija saskaņā ar 15. pantu.

93. Tomēr pastāv vairāki ierobežojumi, kas dažos gadījumos var būt piemērojami attiecībā uz tiesībām piekļūt datiem.

> VDAR 15. panta 4. punkts — nelabvēlīga ietekme uz citu personu tiesībām

94. Ņemot vērā, ka vienā un tajā pašā videonovērošanas sekvencē var tikt ierakstīts jebkāds datu subjektu skaits, uzfilmētā materiāla caurskatīšana izraisītu citu datu subjektu personas datu papildu apstrādi. Ja datu subjekts vēlas saņemt materiāla kopiju (15. panta 3. punkts), tas var nelabvēlīgi ietekmēt citu materiāla aptverto datu subjektu tiesības un brīvības. Lai novērstu šo ietekmi, pārzinim būtu jāņem vērā, ka video ierakstīšana pēc būtības ir traucējoša, tāpēc pārzinim dažos gadījumos nebūtu jāizsniedz uzfilmētais videomateriāls, ja tajā var identificēt citus datu subjektus. Tomēr trešo personu tiesību aizsardzība nebūtu jāizmanto kā attaisnojums, lai izvairītos no likumīgiem indivīdu piekļuves pieprasījumiem, šādos gadījumos pārzinim būtu jāīsteno tehniski pasākumi, lai izpildītu piekļuves pieprasījumu (piemēram, attēla rediģēšana ar aizkrāsošanu vai sadrumstalošanu). Taču tas nenozīmē, ka pārziņiem ir pienākums īstenot šādus pasākumus, ja viņi var citādi nodrošināt to, ka viņi spēj reaģēt uz pieprasījumu saskaņā ar 15. pantu 12. panta 3. punktā noteiktajā termiņā.

> VDAR 11. panta 2. punkts — pārzinis nespēj identificēt datu subjektu

95. Ja uzfilmētais videomateriāls nav piemērots, lai tajā meklētu personas datus (t. i., pārzinim būtu jācaurskata liels saglabātā materiāla apjoms, lai atrastu attiecīgo datu subjektu), iespējams, ka pārzinis nevarēs identificēt datu subjektu.

96. Šo iemeslu dēļ datu subjektam (papildus sevis identificēšanai, tostarp ar identifikācijas dokumentu vai personīgi) savā pieprasījumā pārzinim būtu jānorāda, kad (samērīgā laikposmā attiecībā pret reģistrēto datu subjektu skaitu) viņš(-a) ienāca novērotajā zonā. Pārzinim iepriekš būtu jāinformē datu subjekts par to, kāda informācija ir vajadzīga, lai pārzinis varētu izpildīt pieprasījumu. Ja pārzinis spēj pierādīt, ka viņš nevar identificēt datu subjektu, pārzinim, ja iespējams, attiecīgi par to jāinformē datu subjekts. Šādā situācijā pārzinim savā atbildē datu subjektu būtu jāinformē par precīzu novērošanas zonu, izmantoto kameru pārbaudi utt., lai datu subjektam būtu pilnīga izpratne par to, kādi viņa(-as) personas dati var būt apstrādāti.

Piemērs. Ja datu subjekts pieprasa kopiju ar saviem personas datiem, kas apstrādāti, izmantojot videonovērošanu pie ieejas lielveikalā, kuru apmeklē 30 000 cilvēku dienā, datu subjektam būtu jāprecizē laiks, kad viņš(-a) ir šķērsojis novēroto zonu, aptuveni vienas stundas ietvaros. Ja pārzinis joprojām apstrādā materiālu, datu subjektam būtu jāiesniedz nofilmētā videomateriāla kopija. Ja tajā pašā materiālā vēl var identificēt citus datu subjektus, materiāla attiecīgā daļa būtu jāanonimizē (piemēram, sapludinot kopiju vai tās daļas) pirms kopijas nodošanas datu subjektam, kurš iesniedzis pieprasījumu.

Piemērs. Ja pārzinis automātiski dzēš visu ierakstīto materiālu, piemēram, pēc divām dienām, viņš vairs nevar izsniegt uzfilmēto materiālu datu subjektam pēc šīm divām dienām. Jā pārzinis saņem pieprasījumu pēc šīm divām dienām, datu subjekts ir attiecīgi jāinformē.

97.

) VDAR 12. pants — pārmērīgi pieprasījumi

98. Ja no datu subjekta saņemtais pieprasījums ir pārmērīgs vai acīmredzami nepamatots, pārzinis var pieprasīt saprātīgu maksu saskaņā ar VDAR 12. panta 5. punkta a) apakšpunktu vai atteikties izpildīt pieprasījumu (VDAR 12. panta 5. punkta b) apakšpunkts). Pārzinim jāspēj pierādīt, ka pieprasījums ir acīmredzami nepamatots vai pārmērīgs.

6.2 Tiesības uz dzēšanu un tiesības iebilst

6.2.1 Tiesības uz dzēšanu (tiesības tikt aizmirstam)

99. Ja pārzinis turpina apstrādāt personas datus pēc novērošanas reāllaikā (piemēram, tos uzglabā), datu subjekts var pieprasīt, lai personas dati tiek dzēsti saskaņā ar VDAR 17. pantu.

100. Saņemot pieprasījumu, datu pārzinim ir pienākums dzēst personas datus bez liekas kavēšanās, ja ir piemērojams kāds no VDAR 17. panta 1. punktā uzskaitītajiem apstākļiem (un nav piemērojams neviens no VDAR 17. panta 3. punktā uzskaitītajiem izņēmumiem). Minētais ietver pienākumu dzēst personas datus, kad tie vairs nav vajadzīgi nolūkam, kādam tiem sākotnēji saglabāti, vai ja apstrāde ir nelikumīga (sk. arī *8. iedaļu "Glabāšanas laikposmi un dzēšanas pienākums"*). Turklāt atkarībā no apstrādes juridiskā pamata personas dati būtu jādzēš:

- *attiecībā uz piekrišanu* — ikreiz, kad piekrišana netiek sniegta (un nav cita juridiskā pamata apstrādes veikšanai);
- *attiecībā uz leģitīmajām interesēm* —
    - ikreiz, kad datu subjekts īsteno tiesības iebilst pret apstrādi (sk. *6.2.2. iedaļu*) un apstrādei nav svarīgāku pārliecinošu leģitīmu iemeslu, vai
    - attiecībā uz tiešo tirgvedību (tostarp profilēšanu) — ikreiz, kad datu subjekts iebilst pret apstrādi.

101. Ja pārzinis ir publiskojis videoierakstu (piemēram, to pārraidījis vai straumējis tiešsaistē), ir jāveic saprātīgi pasākumi, lai informētu citus pārziņus (kas apstrādā attiecīgos personas datus) par pieprasījumu atbilstoši VDAR 17. panta 2. punktam. Šajos saprātīgajos pasākumos ir jāiekļauj tehniski pasākumi, kuros ņemtas vērā pieejamo tehnoloģiju un īstenošanas izmaksas. Ciktāl iespējams, pārzinim, dzēšot personas datus, saskaņā ar VDAR 19. pantu, būtu jāinformē par to ikviena persona, kurai personas dati iepriekš bijuši izpausti.

102. Papildus pārziņa pienākumam dzēst personas datus pēc datu subjekta pieprasījuma, pārzinim ir pienākums saskaņā ar VDAR vispārējiem principiem ierobežot laikposmus personas datu glabāšanai (sk. *8. iedaļu*).

103. Attiecībā uz videonovērošanu ir lietderīgi ņemt vērā, ka, piemēram, sapludinot attēlu bez iespējas atgūt personas datus, ko attēls iepriekš ietvēra, personas datus var uzskatīt par dzēstiem saskaņā ar VDAR.

> Piemērs. Ikdienas preču veikalam ir problēmas ar vandālismu, jo īpaši tā ārpusē, tāpēc pie ieejas ārpusē tiek izmantota videonovērošana, kura nostiprināta uz ārsienas. Garāmgājējs pieprasa, lai viņa personas dati tiek nekavējoties dzēsti. Pārzinim ir pienākums atbildēt uz šādu pieprasījumu bez nepamatotas kavēšanās, vēlākais, viena mēneša laikā. Tā kā uzfilmētais materiāls vairs neatbilst nolūkam, kādam tas sākotnēji iegūts (jo brīdī, kad datu subjekts gāja garām, vandālisms nenotika), pieprasījuma brīdī nav leģitīmu interešu saglabāt datus, kas būtu svarīgākas par datu subjektu interesēm. Šajā situācijā pārzinim ir jādzēš personas dati.

104.

6.2.2 Tiesības iebilst

105. Attiecībā uz videonovērošanu, pamatojoties uz*leģitīmām interesēm* (VDAR 6. panta 1. punkta f) apakšpunkts), vai nepieciešamību, kad tiek pildīts uzdevums *sabiedrības interesēs* (VDAR 6. panta 1. punkta e) apakšpunkts), datu subjektam ir tiesības jebkurā laikā, pamatojoties uz viņa(-as) konkrēto situāciju, saskaņā ar VDAR 21. pantu iebilst pret apstrādi. Tad iebildušā indivīda datu apstrāde ir jāizbeidz, ja vien pārzinis nepierāda, ka ir pārliecinoši leģitīmi iemesli, kas ir svarīgāki par datu subjekta tiesībām un interesēm. Pārzinim ir pienākums atbildēt uz datu subjekta pieprasījumu bez nepamatotas kavēšanās, vēlākais, viena mēneša laikā.

106. Šādu iebildumu videonovērošanas kontekstā var izteikt tad, kad datu subjekts ienāk novērotajā zonā, uzturas tajā vai pēc iziešanas no tās. Praksē tas nozīmē, ka, ja vien pārzinim nav pārliecinošu leģitīmu iemeslu, tādas zonas novērošana, kurā varētu identificēt fiziskas personas, ir likumīga tikai tad, ja:

    (1) pārzinis spēj nekavējoties apturēt personas datu apstrādi ar kameru, kad tas tiek pieprasīts, vai

    (2) novērotā zona ir tik stingri norobežota, ka pārzinis var nodrošināt apstiprinājuma saņemšanu no datu subjekta pirms ienākšanas zonā, un šī zona nav teritorija, kurai datu subjekts kā pilsonis ir tiesīgs piekļūt.

107. Šo pamatnostādņu mērķis nav noteikt, kas ir uzskatāms par *pārliecinošām* leģitīmām interesēm (VDAR 21. pants).

108. Izmantojot videonovērošanu tiešās tirgdarbības nolūkos, datu subjektam ir tiesības iebilst pret apstrādi pamatojoties uz tā individuālu lēmumu , jo šajā kontekstā tiesības iebilst ir absolūtas (VDAR 21. panta 2. un 3. punkts).

Piemērs. Uzņēmumam ir problēmas saistītas ar drošības pārkāpumiem pie tā publiskās ieejas, tāpēc tiek veikta videonovērošana pamatojoties uz tā leģitīmām interesēm, lai aizturētu nelikumīgi ienākošās personas. Apmeklētājs iebilst pret viņa(-as) datu apstrādi ar videonovērošanas sistēmas starpniecību, pamatojoties uz iemesliem, kas saistīti ar viņa(-as) konkrēto situāciju. Tomēr uzņēmums šajā gadījumā atsakās izpildīt šo prasību, paskaidrojot, ka saglabātais uzfilmētais materiāls ir vajadzīgs notiekošas iekšējas izmeklēšanas dēļ, tāpēc tam ir pārliecinoši leģitīmi iemesli turpināt personas datu apstrādi.

109.

7 PĀRREDZAMĪBAS UN INFORMĒŠANAS PIENĀKUMI[18]

110. Eiropas datu aizsardzības tiesību aktos jau sen pastāv prasība, ka datu subjektiem ir jābūt informētiem par faktu, ka notiek videonovērošana. Viņi būtu sīki jāinformē par novērotajām vietām[19]. Vispārējie pārredzamības un informēšanas pienākumi ir noteikti VDAR 12. pantā un tās turpmākajos pantos. Sīkāka informācija ir sniegta 29. panta darba grupas Pārredzamības pamatnostādnēs saskaņā ar Regulu 2016/679 (WP260), ko EDAK apstiprināja 2018. gada 25. maijā. Saskaņā ar WP260 26. punktu, ja personas datus iegūst "(..) no datu subjekta ar novērojumiem (piemēram, izmantojot automātiskās datu uztveršanas ierīces vai datu uztveršanas programmatūru, piemēram, kameras (..)", ir piemērojams VDAR 13. pants.

111. Ņemot vērā informācijas apjomu, kas jāsniedz datu subjektam, ja datu pārziņi pārredzamības nodrošināšanai izvēlas izmantot vairāku metožu apvienojumu, tad datu pārzinim ir jāīsteno vairāku līmeņu pieeju (WP260, 35. punkts; WP89, 22. punkts). Attiecībā uz videonovērošanu vissvarīgākā informācija būtu jānorāda uz pašas brīdinājuma zīmes (pirmais līmenis), savukārt obligāto papildu informāciju datu pārzinis var sniegt ar citiem līdzekļiem (otrais līmenis).

7.1 Pirmā līmeņa informācija (brīdinājuma zīme)

112. Pirmais līmenis attiecas uz primāro veidu, kā notiek pārziņa pirmreizējā mijiedarbība ar datu subjektu. Šajā līmenī pārziņi var izmantot brīdinājuma zīmi, kurā ir norādīta nepieciešamā informācija. Norādīto informāciju var kombinēt ar ikonu, lai viegli uztveramā, saprotamā un skaidri salasāmā veidā sniegtu jēgpilnu pārskatu par paredzēto datu apstrādi (VDAR 12. panta 7. punkts). Informācijas formāts būtu jāpielāgo individuālajai vietai (WP89, 22. punkts).

7.1.1 Brīdinājuma zīmes izvietošana

113. Informācija būtu jāizvieto tā, lai datu subjekts pirms ienākšanas novērotajā zonā varētu viegli atpazīt novērošanas apstākļus (aptuveni acu līmenī). Nav nepieciešams atklāt kameru atrašanās vietu, ja vien nav šaubu par to, kuras zonas tiek novērotas, un ja ir nepārprotami precizēts novērošanas konteksts (WP89, 22. punkts). Datu subjektam ir jāspēj noteikt, kuru zonu kamera filmē, lai vajadzības gadījumā varētu izvairīties no novērošanas vai pielāgot savu izturēšanos.

7.1.2 Pirmā līmeņa saturs

114. Pirmā līmeņa informācijai (brīdinājuma zīme) parasti ir jābūt vissvarīgākajai informācijai, piemēram, informācijai par apstrādes nolūkiem, pārziņa identitāti un datu subjekta tiesību esamību, kā arī informācijai par apstrādes lielāko ietekmi[20]. Tā var ietvert, piemēram, pārziņa (vai trešās personas) leģitīmās intereses un datu aizsardzības speciālista (ja piemērojams) kontaktinformāciju. Jābūt arī atsaucei uz detalizētāko otrā līmeņa informāciju un to, kur un kā to atrast.

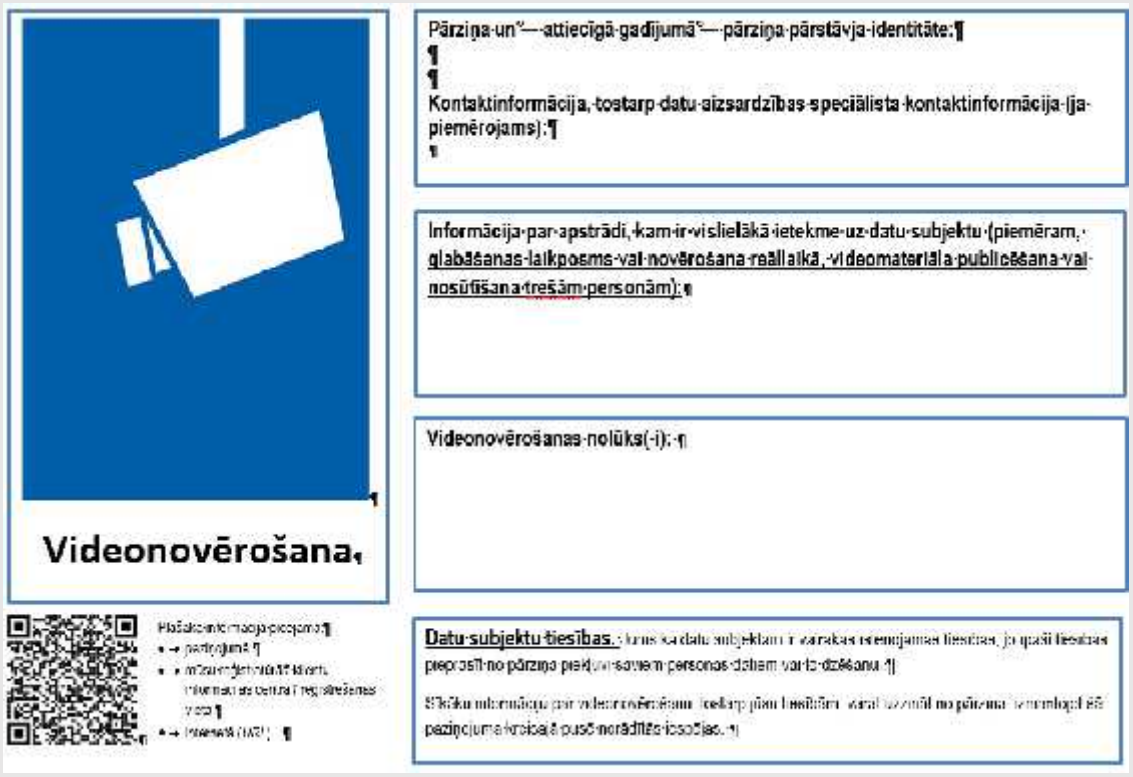
115. Turklāt zīmē arī jābūt norādītai jebkādai informācijai, kas varētu būt svarīga datu subjektu (WP260, 38. punkts). Tā var būt, piemēram, nosūtīšana trešām personām, it īpaši ja tās atrodas ārpus ES, un glabāšanas laikposmu. Ja šī informācija nav norādīta, datu subjektam jābūt pārliecinātam, ka notiek tikai novērošana reāllaikā (bez datu ierakstīšanas vai nosūtīšanas trešām personām).

[18] Var būt piemērojamas īpašas prasības, kas noteiktas dalībvalsts tiesību aktos.

[19] Sk. WP89, 29. panta darba grupas Atzinums 4/2004 par personas datu apstrādi, izmantojot videonovērošanu.

[20] Sk. WP260, 38. punkts.

Piemērs (ar ieteikuma raksturu).



116.

7.2 Otrā līmeņa informācija

117. Arī otrā līmeņa informācija datu subjektam ir jādara pieejama viegli pieejamā vietā, piemēram, kā aizpildīta informācijas lapa, kas pieejama kādā no centrālajām vietām (informācijas centrā, reģistratūrā vai pie kasiera) vai izvietota uz viegli pieejama plakāta. Kā jau minēts iepriekš, pirmā līmeņa brīdinājuma zīmē ir jābūt skaidrai norādei uz otrā līmeņa informāciju. Turklāt ir ļoti ieteicams, lai pirmā līmeņa informācijā būtu norāde uz otrā līmeņa digitālu avotu (piemēram, *QR* kodu vai tīmekļa vietnes adresi). Tomēr informācijai arī jābūt viegli pieejamai nedigitālā formātā. Jābūt arī iespējai piekļūt otrā līmeņa informācijai, neienākot novērotajā zonā, it īpaši, ja informācija ir sniegta digitāli (to var panākt, piemēram, izmantojot saiti). Cits atbilstošs līdzeklis var būt tālruņa numurs, uz kuru var zvanīt. Neatkarīgi no tā, kādā veidā informācija tiek sniegta, tajā jābūt ietvertai visai informācijai, kas noteikta VDAR 13. pantā.

118. Papildus šiem pasākumiem, arī lai tie būtu efektīvāki, EDAK iesaka informācijas sniegšanai datu subjektiem izmantot tehnoloģiskus līdzekļus. Tie var būt, piemēram, ģeolokācijas kameras un informācijas iekļaušana karšu lietotnēs vai tīmekļa vietnēs, lai indivīdi varētu viegli identificēt un noteikt video avotus, kas saistīti ar viņu tiesību īstenošanu, no vienas puses, un iegūt sīkāku informāciju par apstrādes darbību, no otras puses.

Piemērs. Veikala īpašnieks veic videonovērošanu savā veikalā. Lai izpildītu 13. panta prasības, ir pietiekami pie veikala ieejas viegli pieejamā vietā izvietot brīdinājuma zīmi, kurā ir norādīta pirmā līmeņa informācija. Turklāt īpašniekam pie kasiera vai kādā citā centrālā un viegli pieejamā vietā savā veikalā ir jāizvieto informācijas lapa, kurā ir otrā līmeņa informācija.

119.

8 GLABĀŠANAS LAIKPOSMI UN DZĒŠANAS PIENĀKUMS

120. Personas datus nedrīkst glabāt ilgāk, nekā tas ir nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā (VDAR 5. panta 1. punkta c) un e) apakšpunkts). Dažās dalībvalstīs attiecībā uz videonovērošanu var būt pieņemti īpaši noteikumi par glabāšanas laikposmiem saskaņā ar VDAR 6. panta 2. punktu.

121. Tas, vai personas datus ir vai nav nepieciešams glabāt, būtu jācaurskata īsā laikposmā. Pamatā videonovērošanas leģitīmie nolūki bieži vien ir īpašuma aizsardzība vai pierādījumu saglabāšana. Radītos bojājumus parasti var konstatēt vienas vai divu dienu laikā. Lai būtu vieglāk pierādīt atbilstību datu aizsardzības regulējumam, pārziņa interesēs ir jau iepriekš veikt organizatoriskos pasākumus (piemēram, vajadzības gadījumā iecelt pārstāvi videomateriāla caurskatīšanai un aizsargāšanai). Ņemot vērā VDAR 5. panta 1. punkta c) un e) apakšpunktā noteiktos principus, proti, datu minimizāciju un glabāšanas laikposma ierobežošanu, būtu vēlams lielākajā daļā gadījumu (piemēram, ja novērošanu veic vandālisma atklāšanai) personas datus dzēst, ideālā gadījumā, automātiski jau pēc dažām dienām. Jo ilgāks ir glabāšanas laikposms (sevišķi, ja tas pārsniedz 72 stundas), jo vairāk argumentu ir jāsniedz nolūka leģitimitātes un glabāšanas vajadzības pamatošanai. Ja pārzinis ne tikai izmanto videonovērošanu savu telpu novērošanai, bet arī plāno saglabāt datus, viņam ir jāpierāda, ka glabāšana ir faktiski nepieciešama nolūka sasniegšanai. Tādā gadījumā glabāšanas laikposms ir skaidri jādefinē un jānosaka atsevišķi katram konkrētajam nolūkam. Pārzinim ir pienākums noteikt glabāšanas laikposmu saskaņā ar nepieciešamības un samērīguma principiem un pierādīt atbilstību VDAR noteikumiem.

> Piemērs. Maza veikala īpašnieks notikušu vandālismu visdrīzāk pamanītu jau tajā pašā dienā. Parasti pietiekamais glabāšanas laikposms būtu 24 stundas. Tomēr nedēļas nogales vai ilgākas brīvdienas, kad veikals ir slēgts, var būt iemesls ilgākam glabāšanas laikposmam. Ja tiek konstatēts vandālisms, arī tad var būt nepieciešams uzfilmēto materiālu uzglabāt ilgāk, lai izmantotu kā pierādījumu lietā pret likumpārkāpēju.

122.

9 TEHNISKIE UN ORGANIZATORISKIE PASĀKUMI

123. Kā noteikts VDAR 32. panta 1. punktā, personas datu apstrādei videonovērošanas laikā ne tikai jābūt likumīgi pieļaujamai, bet pārziņiem un apstrādātājiem tā ir arī pienācīgi jāaizsargā. Īstenotajiem **organizatoriskajiem un tehniskajiem pasākumiem** jābūt **samērīgiem attiecībā pret riskiem fizisku personu tiesībām un brīvībām**, kuri izriet no videonovērošanas datu nejaušas vai nelikumīgas iznīcināšanas, nozaudēšanas, pārveidošanas, neatļautas izpaušanas vai piekļuves tiem. Saskaņā ar VDAR 24. un 25. pantu pārziņiem jāīsteno tehniski un organizatoriski pasākumi arī tāpēc, lai apstrādes laikā nodrošinātu visu datu aizsardzības principu ievērošanu un lai noteiktu veidus, kā datu subjekti var īstenot savas tiesības, kā tas definēts VDAR 15.–22. pantā. Datu pārziņiem būtu jāpieņem iekšējais regulējums un politikas nostādnes, kas nodrošina šo pasākumu īstenošanu gan tad, kad tiek noteikti apstrādes līdzekļi, gan tad, kad notiek apstrāde, tostarp vajadzības gadījumā veicot novērtējumus par ietekmi uz datu aizsardzību.

9.1 Pārskats par videonovērošanas sistēmu

124. Videonovērošanas sistēma (*VSS*)[21] sastāv no analogām un digitālām ierīcēm, kā arī programmatūrām, kas paredzētas noteiktas vietas attēlu uzņemšanai, to apstrādei un uzrādīšanai operatoram. Tās komponenti ir sagrupēti šādās kategorijās:

- video vide — attēlu uzņemšana, starpsavienojumi un attēlu apstrāde:
  - attēlu uzņemšanas mērķis ir ģenerēt attēlu no reālās pasaules tādā formātā, lai to varētu izmantot pārējā sistēma;
  - starpsavienojumi raksturo visu datu pārraidi video vidē, t. i., savienojumus un sakarus. Savienojumu piemēri ir kabeļi, digitālie tīkli un bezvadu pārraide. Sakari raksturo visus video un kontrolē datu signālus, kas var būt digitāli vai analogi;
  - attēlu apstrāde ietver attēla vai attēlu sekvences analīzi, glabāšanu un noformēšanu.
- No sistēmas pārvaldības viedokļa *VSS* ir šādas loģiskās funkcijas:
  - datu un darbību pārvaldība, kas ietver operatora komandu un sistēmas ģenerēto darbību (trauksmes procedūru, operatoru brīdināšanas) pārvaldību;
  - saskarnes ar citām sistēmām var ietvert savienojumu ar citām drošības (piekļuves kontroles, ugunsgrēka trauksmes) sistēmām un ar drošību nesaistītām sistēmām (ēkas pārvaldības sistēmām, automobiļu reģistrācijas numura zīmju automātisko atpazīšanu).
- *VSS* drošība sastāv no sistēmas un datu konfidencialitātes, integritātes un pieejamības:
  - sistēmas drošība ietver visu sistēmas komponentu fizisko drošību un piekļuves *VSS* kontroli;
  - datu drošība ietver datu nozaudēšanas vai manipulāciju ar tiem novēršanu.

[21] VDAR nav sniegta tās definīcija. Tehnisks apraksts ir atrodams, piemēram, standartā EN 62676-1-1:2014 Videonovērošanas sistēmas izmantošanai drošības lietojumos — 1-1. daļa: Prasības videosistēmai.

125.

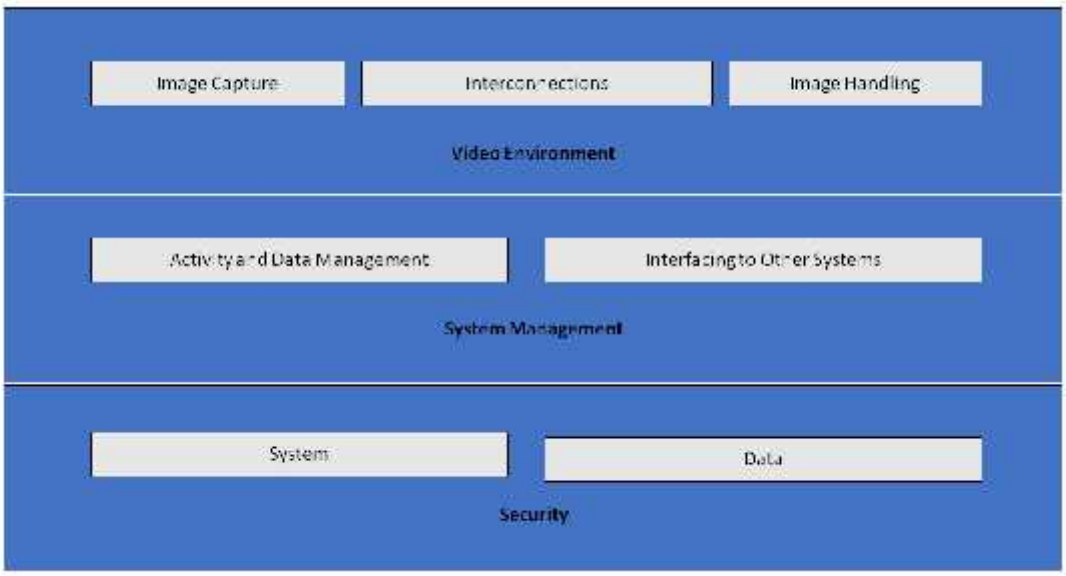


Image Capture	Attēlu uzņemšana
Interconnections	Starpsavienojumi
Image Handling	Attēlu apstrāde
Video Environment	Video vide
Activity and Data Management	Darbību un datu pārvaldība
Interfacing to Other Systems	Saskarnes ar citām sistēmām
System Management	Sistēmas pārvaldība
System	Sistēma
Data	Dati
Security	Drošība

1. attēls. Videonovērošanas sistēma

9.2 Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma

126. Kā noteikts VDAR 25. pantā, pārziņiem jāīsteno atbilstoši datu aizsardzības tehniskie un organizatoriskie pasākumi, tiklīdz viņi ieplāno veikt videonovērošanu — pirms viņi sāk videomateriāla apkopošanu un apstrādi. Šie principi uzsver vajadzību pēc integrētām privātuma uzlabošanas tehnoloģijām, noklusējuma iestatījumiem, kas minimizē datu apstrādi, un tādu nepieciešamo rīku nodrošināšanas, kuri ļauj sasniegt visaugstāko iespējamo personas datu aizsardzības līmeni[22].

127. Pārziņiem datu un privātuma aizsardzības pasākumi būtu jāintegrē ne tikai tehnoloģiju specifikāciju izstrādē, bet arī organizatoriskajā praksē. Attiecībā uz organizatorisko praksi, pārzinim būtu jāpieņem atbilstošs pārvaldības regulējums, jānosaka un jāievieš politikas nostādnes un procedūras, kas saistītas ar videonovērošanu. Tehniskā ziņā sistēmas specifikācijā un izstrādē būtu jāiekļauj prasības attiecībā uz personas datu apstrādi saskaņā ar principiem, kas noteikti VDAR 5. pantā (apstrādes likumīgums, nolūks un datu ierobežojums, datu minimizācija pēc noklusējuma VDAR 25. panta 2. punkta nozīmē, integritāte un konfidencialitāte, pārskatatbildība u. c.). Ja pārzinis plāno iegādāties komerciālu videonovērošanas sistēmu, viņam šīs prasības jāiekļauj iepirkuma specifikācijā. Pārzinim jānodrošina

[22] WP168, atzinums "Privātuma nākotne", 29. panta datu aizsardzības darba grupas un policijas un tiesiskuma jautājumu darba grupas kopīgi sagatavotais dokuments apspriedēm ar Eiropas Komisiju par tiesisko regulējumu attiecībā uz pamattiesībām uz personas datu aizsardzību (pieņemts 2009. gada 1. decembrī).

atbilstība šīm prasībām, tās piemērojot attiecībā uz visiem sistēmas komponentiem un visiem tās apstrādātajiem datiem visā to dzīves ciklā.

9.3 Konkrēti attiecīgu pasākumu piemēri

128. Lielākā daļa pasākumu, ko var izmantot videonovērošanas aizsardzībai, jo īpaši tad, kad izmanto digitālo aprīkojumu un programmatūru, neatšķirsies no pasākumiem, ko izmanto citās IT sistēmās. Tomēr neatkarīgi no izvēlētā risinājuma pārzinim ir pienācīgi jāaizsargā visi videonovērošanas sistēmas komponenti un dati visos posmos, t. i., datu glabāšanas (kad dati netiek izmantoti), nosūtīšanas (kad dati tiek pārraidīti) un apstrādes (kad dati tiek izmantoti) laikā. Šajā nolūkā ir nepieciešams, lai pārziņi un apstrādātāji apvienotu organizatoriskos un tehniskos pasākumus.

129. Izvēloties tehniskos risinājumus, pārzinim būtu jāapsver arī privātumam draudzīgas tehnoloģijas, jo tās uzlabo drošību. Šādu tehnoloģiju piemēri ir sistēmas, kas ļauj aizkrāsot vai sadrumstalot zonas, kuras nav būtiski svarīgas novērošanai, vai izrediģēt trešo personu attēlus, kad videomateriāls tiek nodots datu subjektiem.[23] Tomēr izvēlētajiem drošības risinājumiem nebūtu jāpilda funkcijas, kas nav nepieciešamas (piemēram, neierobežota kameru kustība, tālummaiņas opcija, radiopārraide, analīze un audioieraksti). Funkcijas, kas ir nodrošinātas, bet nav nepieciešamas, būtu jādeaktivizē.

130. Ir pieejams daudz literatūras par šo tematu, tostarp starptautiski standarti un tehniskas specifikācijas par multivides sistēmu fizisko drošību[24] un vispārējo IT sistēmu drošību[25]. Tāpēc šajā iedaļā ir sniegts tikai augsta līmeņa pārskats par šo tematu.

9.3.1 Organizatoriskie pasākumi

131. Papildus novērtējumam par ietekmi uz datu aizsardzību (NIDA), ja tas ir nepieciešams (sk. *10. iedaļu*), pārziņiem, izstrādājot savas videonovērošanas politikas nostādnes un procedūras, būtu jāapsver šādi jautājumi:

- kurš ir atbildīgs par videonovērošanas sistēmas pārvaldību un darbību;
- videonovērošanas projekta mērķis un tvērums;
- atbilstīga un aizliegta izmantošana (kur un kad videonovērošana ir atļauta un kur un kad tā nav atļauta, piemēram, slēpto kameru un noklausīšanās ierīču izmantošana papildus video ierakstīšanai)[26];
- pārredzamības pasākumi, kas minēti *7. iedaļā (Pārredzamības un informēšanas pienākumi)*;
- kā un uz cik ilgu laiku notiek video ierakstīšana, tostarp ar drošības incidentiem saistītu videoierakstu glabāšana arhīvā;
- kurām personām nepieciešama attiecīga apmācība un kad;
- kurām personām ir piekļuve video ierakstiem un kādiem nolūkiem;
- darbības procedūras (piemēram, kurš un kur uzrauga videonovērošanu, kā rīkoties datu pārkāpuma incidenta gadījumā);

[23] Šādu tehnoloģiju izmantošana dažos gadījumos var būt pat obligāta, lai izpildītu 5. panta 1. punkta c) apakšpunktu. Jebkurā gadījumā tās var kalpot kā paraugprakses piemēri.

[24] IEC TS 62045 — Multivides drošība — Pamatnostādne par aprīkojuma un sistēmu privātuma aizsardzību to izmantošanas laikā un ārpus izmantošanas laika.

[25] ISO/IEC 27000 — Informācijas drošības pārvaldības sistēmu sērijas.

[26] Tas var būt atkarīgs no dalībvalsts tiesību aktiem un nozares noteikumiem.

- kādas procedūras citām personām ir jāievēro, lai pieprasītu videoierakstus, un procedūras šādu pieprasījumu izpildei vai noraidīšanai;
- *VSS* iepirkuma, uzstādīšanas un apkopes procedūras;
- incidentu pārvaldības un atgūšanas procedūras.

9.3.2 Tehniskie pasākumi

132. **Sistēmas drošība** nozīmē visu sistēmas komponentu **fizisko drošību** un sistēmas integritāti, t. i., **aizsardzību un noturību pret tīšiem, un netīšiem traucējumiem tās normālajā darbībā** un **piekļuves kontroli**. Datu drošība nozīmē **konfidencialitāti** (dati ir pieejami tikai personām, kurām ir piešķirta piekļuve), **integritāti** (nozaudēšanas vai manipulāciju ar tiem novēršana) un **pieejamību** (datiem var piekļūt, kad tas ir vajadzīgs).

133. **Fiziskā drošība** ir būtiska datu aizsardzības un pirmā aizsardzības līmeņa daļa, jo tā pasargā *VSS* aprīkojumu no zādzības, vandālisma, dabas katastrofām, cilvēka izraisītām katastrofām un nejaušiem bojājumiem (piemēram, pārsprieguma, galējām temperatūrām un kafijas izšļakstīšanās). Analogo sistēmu gadījumā fiziskajai drošībai ir galvenā loma to aizsardzībā.

134. **Sistēmas un datu drošība**, t. i., aizsardzība pret plānotiem un neplānotiem traucējumiem tās normālajā darbībā, var ietvert:

- visas *VSS* infrastruktūras (tostarp tālvadības kameru, vadojuma un energopadeves) aizsardzību pret fizisku iejaukšanos un zādzību;
- aizsardzību videomateriāla nosūtīšanā, izmantojot sakaru kanālus, kas ir droši pret pārtveršanu;
- datu kodēšanu;
- uz aparatūru un programmatūru balstītu risinājumu, piemēram, ugunsmūru, antivīrusu programmu vai ielaušanās konstatēšanas sistēmu, izmantošanu aizsardzībai pret kiberuzbrukumiem;
- komponentu, programmatūras un starpsavienojumu atteiču konstatēšanu;
- līdzekļus sistēmas pieejamības atjaunošanai gadījumā, ja ir noticis fizisks vai tehnisks negadījums.

135. **Piekļuves kontrole** nodrošina, ka tikai pilnvarotas personas var piekļūt sistēmai un datiem, bet citām personām šāda iespēja ir liegta. Fiziskās un loģiskās piekļuves kontroles atbalsta pasākumi ir šādi:

- pasākumi, lai nodrošinātu, ka visas telpas, kurās notiek videonovērošana un kurās tiek glabāts filmētais videomateriāls, ir aizsargātas pret trešo personu patvaļīgu piekļuvi;
- monitoru izvietošana (it īpaši ja tie atrodas atklātās vietās, piemēram, reģistratūrā) tā, lai tajos parādīto varētu redzēt tikai pilnvaroti operatori;
- noteiktas un ieviestas procedūras fiziskās un loģiskās piekļuves piešķiršanai, maiņai un atsaukšanai;
- ieviestas metodes un līdzekļi lietotāju autentifikācijai un autorizācijai, tostarp, piemēram, paroļu garums un maiņas biežums;
- lietotāju veikto darbību (gan sistēmā, gan ar datiem) reģistrēšana un regulāra pārskatīšana;
- pastāvīga neizdevušos piekļuves gadījumu uzraudzība un atklāšana, un konstatēto trūkumu pēc iespējas drīzāka novēršana.

10 NOVĒRTĒJUMS PAR IETEKMI UZ DATU AIZSARDZĪBU

136. Saskaņā ar VDAR 35. panta 1. punktu pārziņiem ir jāveic novērtējums par ietekmi uz datu aizsardzību (NIDA), ja, ņemot vērā apstrādes veidu, varētu tikt radīts augsts risks fizisku personu tiesībām un brīvībām. VDAR 35. panta 3. punkta c) apakšpunktā ir noteikts, ka novērtējums par ietekmi uz datu aizsardzību pārziņiem ir jāveic jo īpaši tad, ja apstrāde ietver publiski pieejamas zonas sistemātisku uzraudzību plašā mērogā. Turklāt saskaņā ar VDAR 35. panta 3. punkta b) apakšpunktu novērtējums par ietekmi uz datu aizsardzību jāveic arī tad, ja pārzinis plāno apstrādāt īpašu kategoriju datus lielā mērogā.

137. Pamatnostādnēs par novērtējuma ietekmi uz datu aizsardzību[27] ir sniegti plašāki norādījumi un ir sīkāk aprakstīti piemēri saistībā ar videonovērošanu (piemēram, attiecībā uz "ierakstīšanas sistēmas izmantošanu, lai uzraudzītu braukšanas kultūru uz autoceļiem"). VDAR 35. panta 4. punktā ir noteikts, ka katrai uzraudzības iestādei ir jāpublisko saraksts ar tiem apstrādes darbību veidiem, attiecībā uz kuriem to valstī ir obligāti jāveic novērtējums par ietekmi uz datu aizsardzību (NIDA). Šie saraksti parasti ir atrodami iestāžu tīmekļu vietnēs. Ņemot vērā biežākos videonovērošanas nolūkus (cilvēku un īpašuma aizsardzība, noziedzīgu nodarījumu atklāšana, novēršana, pierādījumu un aizdomās turamo personu biometriskās identifikācijas iegūšana), ir saprātīgi secināt, ka daudzos videonovērošanas gadījumos būs vajadzīgs NIDA. Tāpēc datu pārziņiem būtu rūpīgi jāizskata šie dokumenti, lai noteiktu, vai ir vajadzīgs šāds novērtējums, un lai to vajadzības gadījumā varētu veikt. Pārzinim īstenojamie datu aizsardzības pasākumi būtu jāizvēlas vadoties no veiktā NIDA rezultāta.

138. Svarīgi ir arī ņemt vērā, ka tad, ja NIDA rezultāti liecina, ka apstrāde radītu augstu risku, neraugoties uz pārziņa plānotajiem drošības pasākumiem, pirms apstrādes būs nepieciešams apspriesties ar attiecīgo uzraudzības iestādi. Sīkāka informācija par šādu apspriešanos ar uzraudzības iestādi ir atrodama 36. pantā.

Eiropas Datu aizsardzības kolēģijas vārdā —

priekšsēdētāja

(Andrea Jelinek)

[27] WP248 vers. 01, Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē — apstiprinājusi EDAK.