Gairės 3/2019 dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus

Versija 2.0

Priimta 2020 m. sausio 29 d.

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

Ankstesnės versijos

Versija 2.1	2020 m. vasario 26 d.	Reikšmingos klaidos taisymas
Versija 2.0	2020 m. sausio 29 d.	Gairių priėmimas po viešų konsultacijų
Versija 1.0	2019 m. liepos 10 d.	Gairių priėmimas viešoms konsultacijoms

Turinys

Europos duomenų apsaugos valdyba,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – BDAR) 70 straipsnio 1 dalies e punktą,

atsižvelgdama į EEE susitarimą, ypač į jo XI priedą ir 37 protokolą su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018[1],

atsižvelgdama į Darbo tvarkos taisyklių 12 ir 22 straipsnius,

PRIĖMĖ ŠIAS GAIRES

1 ĮŽANGA

1. Intensyvus vaizdo prietaisų naudojimas turi įtakos piliečių elgesiui. Dėl aktyvaus tokių priemonių diegimo įvairiose asmenų gyvenimo srityse asmuo patiria papildomą spaudimą užkirsti kelią atvejams, kurie gali būti laikomi neįprastais reiškiniais. Šiomis technologijomis faktiškai gali būti apribotos galimybės anonimiškai judėti ir naudotis paslaugomis, taip pat apskritai ribojama galimybė išlikti nepastebėtiems. Poveikis duomenų apsaugai yra didžiulis.

2. Asmenys gali nepatirti nepatogumų, jeigu jie stebimi vaizdo kameromis, pavyzdžiui, siekiant tam tikro su saugumu susijusio tikslo, tačiau būtina imtis garantijų, kad būtų išvengta bet kokio netinkamo naudojimo visiškai kitais ir nenumatytais tikslais, kurių duomenų subjektas, be kita ko, gali nenumatyti (pvz., rinkodaros tikslai, darbuotojų veiklos stebėjimas ir pan.). Be to, dabar įgyvendinta daugybė priemonių, kurios naudoja užfiksuotus vaizdus ir padeda įprastas kameras paversti išmaniosiomis kameromis. Vaizdo kamerose įrašytas duomenų kiekis, įskaitant šių priemonių ir metodų naudojimą, lemia didesnę antrinio (nepaisant to, ar toks panaudojimas yra susijęs su numatyta pradine sistemos paskirtimi) arba net netinkamo panaudojimo riziką. Kalbant apie stebėjimą vaizdo kameromis, pažymėtina, kad visada reikėtų atidžiai atsižvelgti į BDAR (5 straipsnis) nustatytus bendruosius principus.

3. Stebėjimo vaizdo kameromis sistemos daro įvairų poveikį tam, kaip privačiose ir viešose vietose sąveikauja privačiojo ir viešojo sektorių specialistai, siekdami užtikrinti didesnį saugumą, gauti auditorijos analizės duomenis, rodyti suasmenintą reklamą ir pan. Stebėjimas vaizdo kameromis tapo labai veiksmingas dėl vis dažniau naudojamos pažangiosios vaizdo analizės. Šie metodai gali būti daugiau (pvz., sudėtingos biometrinės technologijos) arba mažiau ribojantys (pvz., paprasti skaičiavimo algoritmai). Apskritai galimybė išlikti anonimiškam ir išsaugoti savo privatumą tampa vis sudėtingesnė. Kiekvienoje situacijoje, susijusioje su vienos ar kitos iš šių technologijų naudojimu, kylantys duomenų apsaugos klausimai gali būti skirtingi ir tą patį galima pasakyti apie teisinę analizę.

[1] Šioje nuomonėje vartojamos nuorodos į valstybes nares turėtų būti suprantamos kaip nuorodos į EEE valstybes nares.

4. Be privatumo klausimų, taip pat kyla rizika, susijusi su galimais šių prietaisų veikimo sutrikimais, kurie taip pat gali turėti įtakos išvadų šališkumui. Mokslininkai nurodo, kad veido tapatybės nustatymui, atpažinimui ar analizei naudojama programinė įranga veikia skirtingai, priklausomai nuo asmens, kurio tapatybę ji nustato, amžiaus, lyties ir etninės kilmės. Algoritmų veikimas turėtų būti pagrįstas įvairiais demografiniais duomenimis, todėl šališkas veido atpažinimas kelia pavojų, kad visuomenėje dar labiau įsitvirtins išankstinės nuostatos. Būtent todėl duomenų valdytojai taip pat privalo užtikrinti, kad būtų reguliariai vertinamas biometrinių duomenų, gautų vykdant stebėjimą vaizdo kameromis, tvarkymo aktualumas ir suteikiamų garantijų pakankamumas.

5. Stebėjimas vaizdo kameromis savaime nėra būtinas tais atvejais, kai yra kitų priemonių pagrindiniam tikslui pasiekti. Priešingu atveju gali atsirasti pavojingi kultūrinių normų pokyčiai, kurie lems tai, kad privatumo atsisakymas bus pripažintas bendra išeities pozicija.

6. Šių gairių paskirtis – pateikti rekomendacijas, kaip taikyti BDAR atsižvelgiant į asmens duomenų tvarkymą naudojant vaizdo prietaisus. Pateikti pavyzdžiai nėra išsamūs, o bendrą argumentavimą galima taikyti visoms galimoms naudojimo sritims.

2 TAIKYMO SRITIS[2]

2.1 Asmens duomenys

7. Sisteminis ir automatizuotas konkrečios erdvės stebėjimas naudojant optines arba audiovizualines priemones, daugiausia turto apsaugos tikslais arba siekiant apsaugoti asmens gyvybę ir sveikatą, tapo svarbiu šių laikų reiškiniu. Vykdant šią veiklą renkama ir saugoma vaizdinė arba audiovizualinė informacija apie visus į stebimą erdvę patenkančius asmenis, kuriuos galima atpažinti pagal jų išvaizdą arba kitas konkrečias savybes. Šių asmenų tapatybę galima nustatyti remiantis būtent šiais duomenimis. Tai taip pat sudaro sąlygas toliau tvarkyti asmens duomenis, susijusius su asmenų buvimu ir elgesiu atitinkamoje erdvėje. Potenciali netinkamo šių duomenų naudojimo rizika didėja atsižvelgiant į stebimos erdvės matmenis ir joje besilankančių asmenų skaičių. Į šį faktą atsižvelgiama Bendrojo duomenų apsaugos reglamento 35 straipsnio 3 dalies c punkte, kuriame reikalaujama atlikti poveikio duomenų apsaugai vertinimą, jei vykdoma sisteminga plataus masto viešai prieinamos teritorijos stebėsena, taip pat 37 straipsnio 1 dalies b punkte, kuriame reikalaujama, kad duomenų tvarkytojai paskirtų duomenų apsaugos pareigūną, jei duomenų tvarkymo operacija, atsižvelgiant į jos pobūdį, apima reguliarią ir sistemingą duomenų subjektų stebėseną.

8. Vis dėlto reglamentas duomenų tvarkymui netaikomas, kai nėra nuorodos į asmenį, pavyzdžiui, jeigu tiesiogiai ar netiesiogiai negalima nustatyti asmens tapatybės.

> Pavyzdys. BDAR netaikomas kamerų muliažų naudojimui (t. y. bet kokia kamera, kuri neveikia kaip kamera ir todėl joje netvarkomi jokie asmens duomenys). *Tačiau kai kuriose valstybėse narėse joms gali būti taikomi kiti teisės aktai.*
>
> Pavyzdys. Iš didelio aukščio padarytiems įrašams BDAR taikomas tik tuo atveju, jeigu tokiomis aplinkybėmis tvarkomi duomenys gali būti susiję su konkrečiu asmeniu.
>
> Pavyzdys. Automobilyje įmontuota vaizdo kamera, padedanti statyti automobilį. Jeigu kamera sukonstruota arba sureguliuota taip, kad joje nerenkama jokia su fiziniu asmeniu susijusi informacija (pvz., valstybiniai numeriai ar informacija, kuria remiantis būtų galima nustatyti pro šalį einančių asmenų tapatybę), BDAR netaikomas.

9.

2.2 Teisėsaugos direktyvos (ES) 2016/680 taikymas

10. Į Direktyvos (ES) 2016/680 taikymo sritį visų pirma patenka asmens duomenų tvarkymas, kurį teisėsaugos institucijos vykdo nusikalstamų veikų prevencijos, tyrimo, nustatymo ar traukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo, be kita ko, apsaugos nuo grėsmių visuomenės saugumui ir jų prevencijos, tikslais.

2.3 Namų ūkiams taikoma išimtis

11. Pagal 2 straipsnio 2 dalies c punktą atvejai, kai fizinis asmuo asmens duomenis tvarko vykdydamas tik asmeninę arba namų ūkio veiklą, kuri taip pat gali apimti veiklą internete, nepatenka į BDAR taikymo sritį[3].

---

[2] Europos duomenų apsaugos valdyba pažymi, kad tais atvejais, kai tai leidžiama pagal BDAR, gali būti taikomi konkretūs nacionaliniuose teisės aktuose taikomi reikalavimai.

[3] Taip pat žr. 18 konstatuojamąją dalį.

12. Ši nuostata – vadinamoji namų ūkio išimtis – stebėjimo vaizdo kameromis srityje turi būti aiškinama siaurai. Todėl, kaip nusprendė Europos Sąjungos Teisingumo Teismas, vadinamoji namų ūkio išimtis turi būti „aiškin[ama] kaip numatan[ti] tik tokią veiklą, kuria privatūs asmenys užsiima neperžengdami privataus ar šeimos gyvenimo ribų, o taip akivaizdžiai nėra tvarkant asmens duomenis, kai jie paskelbiami internete ir tampa prieinami neapibrėžtam asmenų skaičiui“[4]. Be to, jeigu stebėjimo vaizdo kameromis sistema, atsižvelgiant į tai, kiek ji yra susijusi su nuolatiniu asmens duomenų įrašymu ir saugojimu, ir apima, „net jei tik iš dalies, viešąją erdvę ir todėl yra nukreipta į tokiu būdu duomenis tvarkančio asmens privačios sferos išorę, ji negali būti laikoma išimtinai „asmenine ar namų ūkio veikla“, kaip tai suprantama pagal Direktyvos 95/46 3 straipsnio 2 dalies antrą punktą“[5].

13. Privataus asmens patalpose naudojamiems vaizdo prietaisams gali būti taikoma namų ūkio išimtis. Tai priklauso nuo kelių veiksnių, į kuriuos visus reikia atsižvelgti norint prieiti prie tam tikros išvados. Be pirmiau minėtų ESTT sprendimuose nustatytų aspektų, stebėjimo vaizdo kameromis namuose naudotojas turi išsiaiškinti, ar jis turi kokių nors asmeninių ryšių su duomenų subjektu, ar stebėjimo mastas arba dažnumas leidžia manyti, kad jis vykdo kokią nors profesinę veiklą, ir ar stebėjimas gali daryti kokį nors neigiamą poveikį duomenų subjektams. Jei nustatoma bet kuri iš pirmiau minėtų aplinkybių, tai nebūtinai reiškia, kad duomenų tvarkymas nepatenka į namų ūkio išimties taikymo sritį – tam reikia atlikti bendrą vertinimą.

> Pavyzdys. Turistas įrašo vaizdo siužetus tiek savo mobiliuoju telefonu, tiek per vaizdo kamerą, kad išsaugotų atsiminimus apie savo atostogas. Jis rodo įrašus draugams ir šeimai, tačiau neleidžia su jais susipažinti neribotam žmonių skaičiui. Šiuo atveju būtų taikoma namų ūkio išimtis.
>
> Pavyzdys. Kalnų dviračių greitojo leidimosi dviratininkė nori įrašyti savo nusileidimą naudodama veiksmo kamerą. Ji dviračiu važiuoja atokioje vietovėje ir įrašus ketina naudoti savo asmeninėms pramogoms namuose. Šiuo atveju būtų taikoma namų ūkio išimtis net jeigu tam tikru mastu būtų tvarkomi asmens duomenys.
>
> Pavyzdys. Asmuo stebi savo sodą ir daro įrašus. Sodo sklypas aptvertas tvora ir jame reguliariai lankosi tik pats duomenų valdytojas ir jo šeima. Šiuo atveju namų ūkio išimtis būtų taikoma, jeigu ta stebėjimo vaizdo kameromis veikla net iš dalies neapima viešosios erdvės ar kaimynystėje esančio turto.

14.

[4] 2003 m. lapkričio 6 d. Europos Sąjungos Teisingumo Teismo sprendimo, *Bodil Lindqvist case*, C-101/01, 47 punktas.

[5] 2014 m. gruodžio 11 d. Europos Sąjungos Teisingumo Teismo sprendimo *František Ryneš prieš Úřad pro ochranu osobních údajů*, C-212/13, 33 punktas.

3 DUOMENŲ TVARKYMO TEISĖTUMAS

15. Prieš pradedant naudoti duomenis, reikia išsamiai nurodyti konkretų duomenų tvarkymo tikslą (5 straipsnio 1 dalies b punktas). Stebėjimas vaizdo kameromis gali būti naudojamas įvairiais tikslais, pavyzdžiui, padedant užtikrinti nuosavybės ir kito turto, gyvybės ir asmenų fizinės neliečiamybės apsaugą, renkant įrodymus civiliniams ieškiniams[6]. Šie stebėsenos tikslai turėtų būti nurodyti rašytiniuose dokumentuose (5 straipsnio 2 dalis), be to, reikia nurodyti konkrečius tikslus, susijusius su kiekviena naudojama stebėjimo vaizdo kamera. Jei kameras tuo pačiu tikslu naudoja vienas duomenų valdytojas, tikslus galima nurodyti viename dokumente. Be to, duomenų subjektus privaloma informuoti apie duomenų tvarkymo tikslą (-us) pagal 13 straipsnį (*žr. 7 skirsnį „Skaidrumo ir informavimo prievolės“*). Stebėjimas vaizdo kameromis, kuris grindžiamas vien „saugumo“ arba „jūsų saugumo“ tikslu, nėra pakankamai pagrįstas (5 straipsnio 1 dalies b punktas). Be to, tai prieštarauja principui, kad duomenų subjekto asmens duomenys turi būti tvarkomi teisėtai, sąžiningai ir skaidriai (žr. 5 straipsnio 1 dalies a punktą).

16. Iš esmės kiekvienas teisinis pagrindas pagal 6 straipsnio 1 dalį gali būti naudojamas tvarkant stebėjimo vaizdo kameromis metu gautus duomenis. Pavyzdžiui, 6 straipsnio 1 dalies a punktas taikomas tais atvejais, kai nacionaliniame įstatyme nustatyta prievolė vykdyti stebėjimą vaizdo kameromis[7]. Tačiau praktikoje labiausiai tikėtina, kad bus taikomos šios nuostatos:

- 6 straipsnio 1 dalies f punktas (teisėti interesai),
- 6 straipsnio 1 dalies e punktas (būtinybė atlikti užduotį, vykdomą viešojo intereso labui arba vykdant viešosios valdžios funkcijas).

Gana išimtiniais atvejais duomenų valdytojas kaip teisinį pagrindą gali naudoti 6 straipsnio 1 dalies a punktą (sutikimas).

3.1 Teisėti interesai (6 straipsnio 1 dalies f punktas)

17. 6 straipsnio 1 dalies f punkto teisinis vertinimas turėtų būti grindžiamas toliau išvardytais kriterijais pagal 47 konstatuojamąją dalį.

3.1.1 Teisėtų interesų buvimas

18. Stebėjimas vaizdo kameromis yra teisėtas, jeigu jis būtinas siekiant su duomenų valdytojo arba trečiosios šalies teisėtais interesais susijusio tikslo, išskyrus atvejus, kai už tokius interesus yra viršesni duomenų subjekto interesai arba pagrindinės teisės ir laisvės (6 straipsnio 1 dalies f punktas). Duomenų valdytojo arba trečiosios šalies teisėti interesai gali būti teisinio[8], ekonominio arba nematerialaus pobūdžio[9]. Tačiau duomenų valdytojas turėtų atsižvelgti į tai, kad jeigu duomenų subjektas nesutinka būti stebimas pagal 21 straipsnį, duomenų valdytojas gali toliau vykdyti to duomenų subjekto stebėjimą vaizdo kameromis, jeigu yra *įtikinamas* teisėtas interesas, kuris yra

[6] Civilinius ieškinius pagrindžiančių įrodymų rinkimo taisyklės valstybėse narėse yra skirtingos.

[7] Šiose gairėse neanalizuojama ir nepateikiama išsami informacija apie nacionalinę teisę, kuri įvairiose valstybėse narėse gali būti skirtinga.

[8] 2017 m. gegužės 4 d. Europos Sąjungos Teisingumo Teismo sprendimas *Rīgas satiksme case*, C-13/16.

[9] žr. 29 straipsnio darbo grupės nuomonę WP 217.

viršesnis už duomenų subjekto interesus, teises ir laisves, arba siekiant pareikšti, vykdyti ar apginti teisinius reikalavimus.

19. Atsižvelgiant į realią ir pavojingą padėtį, tikslas apsaugoti turtą nuo plėšimo įsilaužiant, vagystės arba vandalizmo gali reikšti teisėtą interesą, kuriam apsaugoti reikalingas stebėjimas vaizdo kameromis.

20. Teisėtas interesas turi būti realus ir aktualus (t. y. tai negali būti fiktyvus arba hipotetinis interesas)[10]. Stebėjimo galima imtis tuomet, kai iš tikrųjų įvyksta nelaimė, pavyzdžiui, anksčiau buvo padaryta žala arba įvyko rimti incidentai. Atsižvelgiant į atskaitomybės principą, duomenų valdytojams būtų patartina dokumentuose aprašyti atitinkamus incidentus (data, pobūdis, finansiniai nuostoliai) ir susijusius baudžiamuosius kaltinimus. Šie dokumentais patvirtinti interesai gali būti patikimas teisėto intereso buvimo įrodymas. Reikėtų periodiškai iš naujo įvertinti teisėto intereso buvimą, taip pat būtinybę vykdyti stebėseną (pvz., kartą per metus, priklausomai nuo aplinkybių).

> Pavyzdys. Parduotuvės savininkas nori atidaryti naują parduotuvę ir sumontuoti stebėjimo vaizdo kameromis sistemą, kad išvengtų vandalizmo. Pateikdamas statistinius duomenis jis gali įrodyti, kad artimoje kaimynystėje yra didelė vandalizmo tikimybė. Be to, naudinga yra greta veikiančių parduotuvių patirtis. Nebūtina, kad atitinkamam duomenų valdytojui būtų buvusi padaryta žala. Jeigu atsižvelgiant į kaimynystėje padarytą žalą, galima daryti išvadą dėl pavojaus ar pan., tai gali būti teisėto intereso įrodymas. Tačiau nepakanka pateikti nacionalinio ar bendro nusikalstamumo statistinių duomenų neatlikus atitinkamos teritorijos analizės arba šiai konkrečiai parduotuvei kylančių pavojų.

21.

22. Neišvengiamos pavojingos situacijos gali reikšti teisėtą interesą, pavyzdžiui, bankuose ar parduotuvėse, kuriose parduodamos vertingos prekės (pvz., juvelyriniai dirbiniai), arba teritorijose, kuriose, kaip žinoma, paprastai padaromos su turtu susijusios nusikalstamos veikos (pvz., degalinės).

23. BDAR taip pat aiškiai nustatyta, kad valdžios institucijos negali savo duomenų tvarkymo grįsti su teisėtu interesu susijusiais pagrindais, jeigu jos vykdo savo užduotis (6 straipsnio 1 dalies antras sakinys).

3.1.2 Būtinybė tvarkyti duomenis

24. Asmens duomenys turėtų būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie yra tvarkomi (duomenų kiekio mažinimo principas) (žr. 5 straipsnio 1 dalies c punktą). Prieš sumontuodamas stebėjimo vaizdo kameromis sistemą duomenų valdytojas visada turėtų kritiškai įvertinti, ar ši priemonė, pirma, yra tinkama norint pasiekti norimą tikslą, ir, antra, ar ji yra būtina nustatytiems tikslams pasiekti. Stebėjimo vaizdo kameromis priemonės turėtų būti pasirenkamos tik tuo atveju, jeigu duomenų tvarkymo tikslo pagrįstai nebūtų galima pasiekti kitomis priemonėmis, kuriomis mažiau apribojamos duomenų subjekto pagrindinės teisės ir laisvės.

25. Atsižvelgiant į tai, kad duomenų valdytojas nori užkirsti kelią nusikaltimams nuosavybei, užuot sumontavęs stebėjimo vaizdo kameromis sistemą, jis taip pat galėtų imtis alternatyvių saugumo priemonių, pavyzdžiui, aptverti turtą tvora, pasirūpinti reguliariu apsaugos darbuotojų patruliavimu, naudotis sargo paslaugomis, įrengti geresnį apšvietimą, uždėti apsaugines spynas, įdėti smūgiams atsparius langus ir duris arba naudoti grafičiams atsparią dangą arba foliją. Šios priemonės gali būti lygiai taip pat veiksmingos kaip ir stebėjimo vaizdo kameromis sistemos ir padėti apsisaugoti nuo

[10] Žr. 29 straipsnio darbo grupės nuomonę WP 217, p. 24 ir toliau. Taip pat žr. ESTT bylą C-708/18, p. 44.

plėšimo įsilaužiant, vagystės ir vandalizmo. Duomenų valdytojas kiekvienu konkrečiu atveju turi įvertinti, ar tokios priemonės gali būti pagrįstas sprendimo būdas.

26. Prieš naudodamas kamerų sistemą, duomenų valdytojas privalo įvertinti vietą ir laiką, kada griežtai būtina naudoti stebėjimo vaizdo kameromis priemones. Paprastai stebėjimo sistema, kuri veikia naktį ir po įprastų darbo valandų, atitinka duomenų valdytojo poreikius, susijusius su bet kokio pavojaus jo nuosavybei prevencija.

27. Apskritai būtinybė naudoti stebėjimą vaizdo kameromis, siekiant apsaugoti duomenų valdytojo patalpas, nebėra aktuali už nuosavybės ribų.[11] Tačiau pasitaiko atvejų, kai turto stebėjimo nepakanka veiksmingai apsaugai užtikrinti. Tam tikrais pavieniais atvejais stebėjimą vaizdo kameromis gali prireikti vykdyti arčiausiai patalpų esančioje aplinkoje. Šiomis aplinkybėmis duomenų valdytojas turėtų apsvarstyti fizines ir technines priemones, pavyzdžiui, blokuoti arba pikseliuoti nesvarbias vietas.

> Pavyzdys. Knygynas nori apsaugoti savo patalpas nuo vandalizmo. Apskritai kameros turėtų filmuoti tik pačias patalpas, nes tuo tikslu nebūtina stebėti šalia knygyno patalpų esančių patalpų ar viešųjų erdvių.

28.

29. Kalbant apie įrodymų išsaugojimo būdą, pažymėtina, kad kyla ir su tuo susijusių klausimų dėl būtinybės tvarkyti duomenis. Tam tikrais atvejais gali būti būtina naudoti „juodosios dėžės“ sprendimo būdus, jeigu filmuota vaizdo medžiaga po tam tikro saugojimo laikotarpio ištrinama ir su ja galima susipažinti tik įvykus incidentui. Tam tikrais atvejais vaizdo medžiagos apskritai gali nereikėti įrašyti ir labiau tiktų naudoti stebėjimą tikruoju laiku. Sprendimas naudoti „juodąja dėže“ grindžiamus sprendimo būdus ir stebėjimą tikruoju laiku taip pat turėtų būti pagrįstas siekiamu tikslu. Jeigu, pavyzdžiui, stebėjimo vaizdo kameromis tikslas yra išsaugoti įrodymus, su stebėjimu tikruoju laiku susiję metodai paprastai netinkami. Kartais stebėjimas tikruoju laiku taip pat gali būti laikomas labiau ribojančiu, palyginti su vaizdo medžiagos saugojimu ir ištrynimu po tam tikro laikotarpio (pvz., jeigu kas nors nuolat stebi vaizdą monitoriuje, tai gali būti laikoma labiau ribojančia veikla, palyginti su tuo atveju, kai monitorius nenaudojamas, o visa vaizdo medžiaga tiesiogiai saugoma „juodojoje dėžėje“). Šiomis aplinkybėmis būtina atsižvelgti į duomenų kiekio mažinimo principą (5 straipsnio 1 dalies c punktas). Taip pat reikėtų nepamiršti, kad visai įmanoma, jog duomenų valdytojas, siekdamas greitai reaguoti ir įsikišti, vietoj stebėjimo vaizdo kameromis gali naudotis apsaugos darbuotojų paslaugomis.

3.1.3 Interesų suderinimas

30. Darant prielaidą, kad stebėjimas vaizdo kameromis yra būtinas teisėtiems duomenų valdytojo interesams apsaugoti, stebėjimo vaizdo kameromis sistema gali būti pradedama naudoti tik jeigu nėra už teisėtus duomenų valdytojo arba trečiosios šalies interesus (pvz., turto arba fizinės neliečiamybės apsauga) viršesnių duomenų subjekto interesų arba pagrindinių teisių ir laisvių. Duomenų valdytojas turi įvertinti: 1) kokiu mastu stebėsena daro poveikį asmenų interesams, pagrindinėms teisėms ir laisvėms, ir 2) ar dėl to pažeidžiamos duomenų subjekto teisės arba atsiranda neigiamų su jomis susijusių pasekmių. Iš tiesų, interesus suderinti privaloma. Reikia atidžiai įvertinti ir suderinti, viena vertus, pagrindines teises ir laisves ir, antra vertus, duomenų valdytojo teisėtus interesus.

[11] Šiuo atveju tam tikrose valstybėse narėse taip pat gali būti taikomi nacionaliniai teisės aktai.

Pavyzdys. Privačią automobilių stovėjimo aikštelę valdančios įmonės dokumentacijoje yra duomenų, kad pastatyti automobiliai buvo ne kartą apvogti. Stovėjimo aikštelė yra atvira erdvė, į kurią gali lengvai patekti bet kas, tačiau ji yra aiškiai pažymėta ją supančiais ženklais ir įleistiniais užtvarais. Automobilių stovėjimo paslaugų įmonė turi teisėtą interesą (užkirsti kelią vagystėms klientų automobiliuose) stebėti teritoriją tuo dienos metu, kuriuo susiduriama su problemomis. Duomenų subjektai stebimi ribotą laiką, jie į teritoriją patenka ne rekreaciniais tikslais, be to, jie yra patys suinteresuoti tuo, kad būtų užkirstas kelias vagystėms. Šiuo atveju duomenų valdytojo teisėtas interesas yra viršesnis už duomenų subjektų interesą, susijusį su tuo, kad jis nebūtų stebimas.

Pavyzdys. Restoranas nusprendžia įrengti vaizdo kameras restoranuose, kad būtų galima kontroliuoti sanitarinės įrangos sandarumą. Šiuo atveju duomenų subjektų teisės akivaizdžiai yra viršesnės už duomenų valdytojo interesą, todėl restorane kamerų negalima įrengti.

31.

3.1.3.1 Sprendimų priėmimas kiekvienu konkrečiu atveju

32. Kadangi pagal reglamentą interesus suderinti privaloma, sprendimą reikia priimti kiekvienu konkrečiu atveju (žr. 6 straipsnio 1 dalies f punktą). Nepakanka nurodyti abstrakčias situacijas arba palyginti tarpusavyje panašius atvejus. Duomenų valdytojas turi įvertinti duomenų subjekto teisių apribojimo riziką; šiuo atveju lemiamas kriterijus yra susijęs su tuo, kaip intensyviai apribojamos asmens teisės ir laisvės.

33. Intensyvumą, be kita ko, galima apibūdinti remiantis surinktos informacijos rūšimi (informacijos turinys), taikymo sritimi (informacijos tankis, erdvinis ir geografinis mastas), atitinkamų duomenų subjektų skaičiumi, t. y. konkretus skaičius arba atitinkama gyventojų dalis, aptariama situacija, faktiniais duomenų subjektų grupės interesais, alternatyviomis priemonėmis, taip pat duomenų vertinimo pobūdžiu ir mastu.

34. Svarbūs derinimo veiksniai gali būti stebimos teritorijos dydis ir stebimų duomenų subjektų kiekis. Stebėjimo vaizdo kameromis naudojimas atokioje teritorijoje (pvz., laukinei gyvūnijai stebėti arba ypatingos svarbos infrastruktūrai, pvz., privačiai valdomai radijo antenai, apsaugoti) turi būti vertinamas kitaip, negu stebėjimo vaizdo kameromis naudojimas pėsčiųjų zonoje arba prekybos centre.

Pavyzdys. Jeigu sumontuojamas vaizdo registratorius (pvz., siekiant surinkti įrodymus nelaimingo atsitikimo metu), svarbu užtikrinti, kad šis vaizdo registratorius nuolat nejrašinėtų eismo srauto, taip pat šalia kelio esančių asmenų. Kitu atveju interesas, susijęs su vaizdo įrašų, kaip įrodymų, turėjimu atsižvelgiant į teorinį eismo įvykį, negali būti naudojamas siekiant pateisinti šį rimtą duomenų subjektų teisių apribojimą.

35.

3.1.3.2 Pagrįsti duomenų subjektų lūkesčiai

36. Pagal 47 konstatuojamąją dalį teisėto intereso buvimą reikia atidžiai įvertinti. Šiuo atveju reikia atsižvelgti į pagrįstus duomenų subjekto lūkesčius tuo metu, kai tvarkomi jo asmens duomenys. Kalbant apie sisteminę stebėseną, pažymėtina, kad duomenų subjekto ir duomenų valdytojo santykiai gali iš esmės skirtis ir turėti įtakos pagrįstiems duomenų subjekto lūkesčiams, kuriuos jis gali turėti. Pagrįstų lūkesčių sąvoka turėtų būti aiškinama remiantis atitinkamais subjektyviais lūkesčiais. Iš tiesų, lemiamas kriterijus turi būti susijęs su tuo, ar objektyvi trečioji šalis galėtų pagrįstai tikėtis ir daryti išvadą, kad ji bus stebima šioje konkrečioje situacijoje.

37. Pavyzdžiui, darbuotojas dažniausiai nesitiki, kad darbdavys jį stebės darbo vietoje[12]. Be to, negalima tikėtis, kad asmuo bus stebimas privačiame sode, gyvenamosiose vietose arba apžiūros ir gydymo kabinetuose. Lygiai taip pat negalima pagrįstai tikėtis, kad stebėsena bus vykdoma sanitarinėse arba pirties patalpose, nes tokių vietų stebėsena reiškia rimtą duomenų subjekto teisių apribojimą. Duomenų subjektai pagrįstai tikisi, kad tokiose vietose stebėjimas vaizdo kameromis nebus vykdomas. Kita vertus, banko klientas gali tikėtis, kad jis bus stebimas banke arba prie bankomato.

38. Duomenų subjektai taip pat gali tikėtis, kad jie nebus stebimi viešai prieinamose vietose, ypač jei tos vietos paprastai naudojamos gydymo, reabilitacijos ir laisvalaikio veiklai, taip pat vietose, kuriose asmenys apsistoja ir (arba) bendrauja, pavyzdžiui, sėdimosios vietos, staleliai restoranuose, parkai, kinas ir kūno rengybos salės. Šiuo atveju duomenų subjekto interesai arba teisės ir laisvės dažnai bus viršesni už duomenų valdytojo teisėtus interesus.

> Pavyzdys. Duomenų subjektai tikisi, kad tualetuose jie nebus stebimi. Stebėjimas vaizdo kameromis, pavyzdžiui, siekiant užkirsti kelią nelaimingiems atsitikimams, nėra proporcingas.

39.

40. Ženklai, kuriais duomenų subjektas informuojamas apie stebėjimą vaizdo kameromis, nėra svarbūs nustatant, ko duomenų subjektas objektyviai gali tikėtis. Tai reiškia, kad, pavyzdžiui, parduotuvės savininkas negali pasikliauti klientais, kurie *objektyviai* tikisi būti stebimi vien dėl to, kad prie įėjimo naudojamu ženklu asmuo informuojamas apie stebėjimą.

3.2 Būtinybė vykdyti užduotį viešojo intereso labui arba įgyvendinant oficialius įgaliojimus, suteiktus duomenų valdytojui (6 straipsnio 1 dalies e punktas)

41. Asmens duomenys galėtų būti tvarkomi naudojant stebėjimą vaizdo kameromis pagal 6 straipsnio 1 dalies e punktą, jeigu tai būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant viešosios valdžios funkcijas[13]. Gali būti, kad vykdant viešosios valdžios funkcijas toks duomenų tvarkymas neleidžiamas, tačiau kiti teisiniai pagrindai, pavyzdžiui, „sveikata ir sauga“, kuriais siekiama apsaugoti lankytojus ir darbuotojus, gali suteikti ribotas duomenų tvarkymo galimybes, kartu atsižvelgiant į BDAR prievoles ir duomenų subjektų teises.

42. Valstybės narės gali palikti galioti arba priimti konkrečius stebėjimą vaizdo kameromis reglamentuojančius nacionalinės teisės aktus, kad prisitaikytų prie BDAR taisyklių taikymo šiuo atveju tiksliau nustatydamos konkretesnius duomenų tvarkymo reikalavimus, jeigu jie atitinka BDAR nustatytus principus (pvz., saugojimo trukmės apribojimo principas, proporcingumo principas).

[12] Taip pat žr. 29 straipsnio darbo grupės Nuomonę 2/2017 dėl duomenų tvarkymo darbe, WP 249, priimta 2017 m. birželio 8 d.

[13] Nurodytas duomenų tvarkymo pagrindas nustatomas Sąjungos arba valstybės narės teisėje ir yra būtinas siekiant atlikti užduotį, vykdomą dėl viešojo intereso arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas (6 straipsnio 1 dalis).

3.3 Sutikimas (6 straipsnio 1 dalies a punktas)

43. Sutikimas turi būti duotas laisva valia, konkretus, pagrįstas informacija ir nedviprasmiškas, kaip aprašyta gairėse dėl sutikimo[14].

44. Kalbant apie sisteminę stebėseną, pažymėtina, kad duomenų subjekto sutikimas pagal 7 straipsnį kaip teisinis pagrindas (žr. 43 konstatuojamąją dalį) gali būti naudojamas tik išimtiniais atvejais. Būtent stebėjimo srityje naudojant šią technologiją vienu metu stebimas nežinomas žmonių skaičius. Vargu, ar duomenų valdytojas galės įrodyti, kad duomenų subjektas davė sutikimą prieš pradedant tvarkyti jo asmens duomenis (7 straipsnio 1 dalis). Darant prielaidą, kad duomenų subjektas atšaukia savo sutikimą, duomenų valdytojui bus sudėtinga įrodyti, kad asmens duomenys nebetvarkomi (7 straipsnio 3 dalis).

> Pavyzdys. Sportininkai gali prašyti vykdyti stebėseną per individualias treniruotes, kad galėtų išanalizuoti savo techniką ir veiklos rezultatus. Kita vertus, jeigu sporto klubas imasi iniciatyvos tuo pačiu tikslu stebėti visą komandą, sutikimas dažnai negalios, nes pavieniai sportininkai gali jausti spaudimą duoti sutikimą, kad jų atsisakymas duoti sutikimą nedarytų neigiamo poveikio komandos nariams.

45.

46. Jeigu duomenų valdytojas nori remtis sutikimu, jam tenka pareiga užtikrinti, kad kiekvienas į teritoriją, kuri stebima vaizdo kameromis, įeinantis duomenų subjektas būtų davęs savo sutikimą. Šis sutikimas turi atitikti 7 straipsnyje nustatytas sąlygas. Patekimas į stebimą teritoriją (pvz., žmonių prašoma eiti per specialų koridorių arba pro vartus, kad patektų į stebimą teritoriją) nereiškia pareiškimo arba aiškaus patvirtinamojo veiksmo, kuris yra reikalingas sutikimui duoti, išskyrus atvejus, kai jis atitinka 4 ir 7 straipsnių reikalavimus, kaip aprašyta gairėse dėl sutikimo[15].

47. Atsižvelgiant į darbdavių ir darbuotojų galios pusiausvyros nebuvimą, darbdaviai, tvarkydami asmens duomenis, dažniausiai neturėtų remtis sutikimu, nes mažai tikėtina, kad jis bus duotas laisvai. Šiomis aplinkybėmis reikėtų atsižvelgti į gaires dėl sutikimo.

48. Valstybės narės teisėje arba kolektyviniuose susitarimuose, įskaitant darbo sutartis, gali būti numatytos konkrečios taisyklės dėl darbuotojų asmens duomenų tvarkymo darbo santykių srityje (žr. 88 straipsnį).

[14] 29 straipsnio darbo grupė „Gairės dėl sutikimo pagal Reglamentą Nr. 2016/679“ (WP 259, 01 red.), patvirtino EDAV.

[15] 29 straipsnio darbo grupės „Gairės dėl sutikimo pagal Reglamentą Nr. 2016/679“ (WP 259), kurioms pritarė EDAV ir į kurias reikėtų atsižvelgti.

4 FILMUOTOS VAIZDO MEDŽIAGOS ATSKLEIDIMAS TREČIOSIOMS ŠALIMS

49. Iš esmės vaizdo įrašai trečiosioms šalims atskleidžiami taikant BDAR nustatytas bendrąsias taisykles.

4.1 Filmuotos vaizdo medžiagos atskleidimas trečiosioms šalims apskritai

50. 4 straipsnio 2 punkte informacijos atskleidimas apibrėžiamas kaip perdavimas (pvz., individualus pranešimas), platinimas (pvz., paskelbimas internete) arba kitoks pateikimas. Trečiųjų šalių apibrėžtis pateikta 4 straipsnio 10 punkte. Jeigu informacija atskleidžiama trečiosioms šalims arba tarptautinėms organizacijoms, taip pat taikomos 44 ir kitų straipsnių specialiosios nuostatos.

51. Bet koks asmens duomenų atskleidimas laikomas atskiros rūšies asmens duomenų tvarkymo veikla, kurią duomenų valdytojas turi pagrįsti 6 straipsnyje nustatytu teisiniu pagrindu.

> Pavyzdys. Duomenų valdytojas, kuris nori įkelti įrašą į internetą, turi remtis tuo duomenų tvarkymo teisiniu pagrindu, pavyzdžiui, gaudamas duomenų subjekto sutikimą pagal 6 straipsnio 1 dalies a punktą.

52.

53. Trečiosioms šalims filmuotą vaizdo medžiagą kitu tikslu nei tas, kuriuo duomenys buvo surinkti, perduoti galima pagal 6 straipsnio 4 dalies taisykles.

> Pavyzdys. Užkardo (automobilių stovėjimo aikštelėje) stebėjimo vaizdo kameromis įranga sumontuojama siekiant išspręsti su žala susijusius klausimus. Žala padaroma ir įrašas perduodamas advokatui, kad jis galėtų iškelti bylą. Šiuo atveju įrašymo tikslas yra toks pat kaip ir perdavimo.
>
> Pavyzdys. Užkardo (automobilių stovėjimo aikštelėje) stebėjimo vaizdo kameromis įranga sumontuojama siekiant išspręsti su žala susijusius klausimus. Įrašas internete skelbiamas tik pramoginiais sumetimais. Šiuo atveju tikslas pasikeitė ir yra nesuderinamas su pradiniu tikslu. Be to, būtų sudėtinga nustatyti tokio duomenų tvarkymo (paskelbimo) teisinį pagrindą.

54.

55. Trečioji šalis duomenų gavėja turės pati atlikti teisinę analizę, visų pirma nustatydama, kokį teisinį pagrindą pagal 6 straipsnį ji taikys tvarkydama šiuos duomenis (pvz., gaudama medžiagą).

4.2 Filmuotos vaizdo medžiagos atskleidimas teisėsaugos institucijoms

56. Vaizdo įrašų atskleidimas teisėsaugos institucijoms taip pat yra nepriklausomas procesas, kuriam duomenų valdytojas turi rasti atskirą pagrindimą.

57. Pagal 6 straipsnio 1 dalies c punktą duomenų tvarkymas yra teisėtas, jeigu jis yra būtinas norint laikytis duomenų valdytojui taikomos teisinės prievolės. Nors taikytina policijos teisė yra išimtinė valstybių narių kompetencija, labai tikėtina, kad kiekvienoje valstybėje narėje galioja bendrosios taisyklės, kuriomis reglamentuojamas įrodymų perdavimas teisėsaugos institucijoms. Duomenis perduodančio duomenų valdytojo vykdomas duomenų tvarkymas reglamentuojamas pagal BDAR. Jeigu pagal nacionalinės teisės aktus reikalaujama, kad duomenų valdytojas bendradarbiautų su teisėsauga (pvz., atliekant tyrimą), duomenų perdavimo teisinis pagrindas pagal 6 straipsnio 1 dalies c punktą yra teisinė prievolė.

58. 6 straipsnio 4 dalyje nustatytas tikslo apribojimo principas dažnai nekelia problemų, nes informacijos atskleidimas yra aiškiai susijęs su valstybės narės teise. Todėl nebūtina atsižvelgti į specialius reikalavimus, susijusius su tikslo pakeitimu, kaip apibrėžta a–e punktuose.

59. Pavyzdys. Parduotuvės savininkas prie įėjimo įrašo filmuotą vaizdo medžiagą. Filmuotoje vaizdo medžiagoje matoma, kaip asmuo pavagia kito asmens piniginę. Policija prašo duomenų valdytojo perduoti medžiagą, kuri padėtų atlikti tyrimą. Tokiu atveju parduotuvės savininkas remtųsi teisiniu pagrindu pagal 6 straipsnio 1 dalies c punktą (teisinė prievolė), siejant jį su atitinkamu nacionaliniu įstatymu dėl perduotų duomenų tvarkymo.

60. Pavyzdys. Saugumo sumetimais parduotuvėje įrengiama kamera. Parduotuvės savininkas mano, kad savo filmuotoje vaizdo medžiagoje užfiksavo kažką įtartino ir nusprendžia ją nusiųsti policijai (nenurodydamas, kad atliekamas kokios nors rūšies tyrimas). Šiuo atveju parduotuvės savininkas dažniausiai turi įvertinti, ar tenkinamos būtent 6 straipsnio 1 dalies f punkto sąlygos. Taip paprastai būna tuo atveju, jeigu parduotuvės savininkas pagrįstai įtaria, kad buvo padarytas nusikaltimas.

61. Pačios teisėsaugos institucijos asmens duomenis tvarko ne pagal BDAR (žr. 2 straipsnio 2 dalies d punktą), o pagal Teisėsaugos direktyvą ((ES) 2016/680).

5 SPECIALIŲ KATEGORIJŲ DUOMENŲ TVARKYMAS

62. Naudojant stebėjimo vaizdo kameromis sistemas paprastai renkamas labai didelis asmens duomenų kiekis, be to, tokie duomenys gali būti susiję su ypač asmeninio pobūdžio informacija ir net specialių kategorijų duomenimis. Iš tiesų, akivaizdžiai nereikšmingi duomenys, kurie buvo surinkti naudojant vaizdo kameras, gali būti naudojami kitai informacijai gauti, kad būtų galima pasiekti kitą tikslą (pvz., nustatyti asmens įpročius). Tačiau stebėjimas vaizdo kameromis ne visada laikomas specialių kategorijų asmens duomenų tvarkymu.

> Pavyzdys. Filmuota vaizdo medžiaga, kurioje rodomas duomenų subjektas, nešiojantis akinius arba naudojantis neįgaliojo vežimėlį, pati savaime nelaikoma specialiomis asmens duomenų kategorijomis.

63.

64. Tačiau jeigu filmuota vaizdo medžiaga tvarkoma siekiant gauti specialių kategorijų duomenis, taikomas 9 straipsnis.

> Pavyzdys. Politines pažiūras būtų galima nustatyti, pavyzdžiui, iš nuotraukų, rodančių renginyje dalyvaujančius, streikuojančius duomenų subjektus, kurių tapatybė gali būti nustatyta, ir pan. Šiuo atveju būtų taikomas 9 straipsnis.
>
> Pavyzdys. Ligoninė, kurioje įrengta vaizdo kamera paciento sveikatos būklei stebėti, būtų laikoma tvarkančia specialių kategorijų asmens duomenis (9 straipsnis).

65.

66. Apskritai bendroji taisyklė, kuri taikoma sumontavus stebėjimo vaizdo kameromis sistemą, yra ta, kad reikėtų atidžiai įvertinti duomenų kiekio mažinimo principą. Taigi, net ir tais atvejais, kai 9 straipsnio 1 dalis netaikoma, duomenų valdytojas visada turėtų pabandyti sumažinti riziką, kad bus įrašyta filmuota medžiaga, kurioje, nepaisant tikslo, atsispindės neskelbtini duomenys (nesusiję su 9 straipsniu).

> Pavyzdys. Stebėjimas vaizdo kameromis, kurių stebėjimo lauke matoma bažnyčia, pats savaime nepateks į 9 straipsnio taikymo sritį. Tačiau duomenų valdytojas, vertindamas duomenų subjekto interesus, pagal 6 straipsnio 1 dalies f punktą turi atlikti ypač kruopštų vertinimą ir atsižvelgti į duomenų pobūdį, taip pat į kitų neskelbtinų duomenų (nesusijusių su 9 straipsniu) filmavimo riziką.

67.

68. Jeigu stebėjimo vaizdo kameromis sistema naudojama specialių kategorijų duomenims tvarkyti, duomenų valdytojas privalo nustatyti specialių kategorijų duomenų tvarkymo išimtį pagal 9 straipsnį (t. y. bendrosios taisyklės išimtis, pagal kurią specialių kategorijų duomenys neturėtų būti tvarkomi) ir teisinį pagrindą pagal 6 straipsnį.

69. Pavyzdžiui, 9 straipsnio 2 dalies c punktas („<...> tvarkyti duomenis būtina, kad būtų apsaugoti gyvybiniai duomenų subjekto arba kito fizinio asmens interesai <...>“) teoriškai ir išimtiniais atvejais galėtų būti taikomas, tačiau duomenų valdytojas turėtų tai pagrįsti kaip absoliučią būtinybę apsaugoti gyvybinius asmens interesus ir įrodyti, kad šis „<...> duomenų subjektas *dėl fizinių ar teisinių priežasčių negali duoti sutikimo*“. Be to, duomenų valdytojui nebus leidžiama naudotis sistema dėl kurios nors kitos priežasties.

70. Šiuo atveju svarbu pažymėti, kad mažai tikėtina, jog kiekviena 9 straipsnyje nurodyta išimtis galėtų būti taikoma siekiant pateisinti specialių kategorijų duomenų tvarkymą naudojant stebėjimą vaizdo kameromis. Konkrečiau, duomenų valdytojai, kurie šiuos duomenis tvarko vykdydami stebėjimą vaizdo kameromis, negali remtis 9 straipsnio 2 dalies e punktu, pagal kurį leidžiama imtis tvarkyti asmens duomenis, kuriuos duomenų subjektas akivaizdžiai paskelbė viešai. Vien tai, kad duomenų subjektas patenka į kameros filmavimo lauką, nereiškia, jog duomenų subjektas ketina viešai paskelbti su juo susijusius specialių kategorijų duomenis.

71. Be to, specialių kategorijų duomenų tvarkymas reikalauja didesnio ir nuolatinio budrumo vykdant tam tikras prievoles; pavyzdžiui, prireikus atliekamas aukšto lygio poveikio saugumui ir duomenų apsaugai vertinimas.

> Pavyzdys. Darbdavys negali naudoti demonstracijų įrašų, gautų stebėjimo vaizdo kameromis, kad nustatytų streikuotojų tapatybę.

72.

5.1 Bendros biometrinių duomenų tvarkymo aplinkybės

73. Dėl biometrinių duomenų, ypač veido atpažinimo, naudojimo kyla didesnė rizika duomenų subjektų teisėms. Labai svarbu, kad tokios technologijos būtų naudojamos tinkamai laikantis teisėtumo, būtinumo, proporcingumo ir duomenų kiekio mažinimo principų, kaip nustatyta BDAR. Kadangi šių technologijų naudojimas gali būti suprantamas kaip ypač veiksmingas, duomenų valdytojai pirmiausia turėtų įvertinti poveikį pagrindinėms teisėms ir laisvėms ir apsvarstyti galimybę naudoti mažiau ribojančias priemones, kurios padėtų jiems pasiekti teisėtą duomenų tvarkymo tikslą.

74. Pagal BDAR pateiktą apibrėžtį biometriniai duomenys atsiranda tuomet, kai tvarkant pirminius duomenis, pavyzdžiui, fizinio asmens fizinės, fiziologinės arba elgesio savybės, yra vertinamos šios savybės. Kadangi biometriniai duomenys yra tokio vertinimo rezultatas, BDAR 4 straipsnio 14 punkte nustatyta, kad tai yra „<...> po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę“. Tačiau filmuota vaizdo medžiaga, kurioje matomas asmuo, pati savaime negali būti laikoma biometriniais duomenimis pagal 9 straipsnį, jeigu ji nebuvo techniškai apdorota, kad padėtų nustatyti asmens tapatybę[16].

75. Tam, kad biometriniai duomenys būtų laikomi specialių kategorijų asmens duomenų tvarkymu (9 straipsnis), jie turi būti tvarkomi „siekiant konkrečiai nustatyti fizinio asmens tapatybę“.

76. Atsižvelgiant į 4 straipsnio 14 punktą ir 9 straipsnį, apibendrintai galima teigti, kad būtina paisyti trijų kriterijų:

- **Duomenų pobūdis**: duomenys yra susiję su fizinio asmens fizinėmis, fiziologinėmis ar elgesio savybėmis;
- **Duomenų tvarkymo priemonės ir būdas**: „po specialaus techninio apdorojimo gauti <...> duomenys“;

[16] BDAR 51 konstatuojamojoje dalyje pritariama šiai analizei nurodant, kad „<...> [n]uotraukų tvarkymas neturėtų būti laikomas sisteminiu specialių kategorijų asmens duomenų tvarkymu, nes nuotraukoms biometrinių duomenų apibrėžtis taikoma tik tuo atveju, kai jos tvarkomos taikant specialias technines priemones, leidžiančias konkrečiai nustatyti fizinio asmens tapatybę ar tapatumą. <...>“.

- **Duomenų tvarkymo tikslas**: duomenys turi būti naudojami siekiant konkrečiai nustatyti fizinio asmens tapatybę.

77. Stebėjimo vaizdo kameromis, įskaitant biometrinių duomenų atpažinimo funkciją, kurią įdiegė privatūs subjektai savo reikmėms (pvz., rinkodaros, statistikos arba net saugumo tikslais), naudojimui dažniausiai reikės visų duomenų subjektų sutikimo (9 straipsnio 2 dalies a punktas), tačiau taip pat galėtų būti taikoma kita 9 straipsnyje numatyta tinkama išimtis.

Pavyzdys. Siekdama pagerinti savo paslaugas, privati bendrovė pakeičia oro uoste esančias keleivių tapatybės tikrinimo vietas (bagažo išėmimas, įlipimas į orlaivį) stebėjimo vaizdo kameromis sistemomis, kurios naudoja veido atpažinimo metodus, kad patikrintų keleivių, nusprendusių sutikti su tokia procedūra, tapatybę. Kadangi duomenų tvarkymui taikomas 9 straipsnis, keleiviai, kurie anksčiau bus davę aiškų ir informacija pagrįstą sutikimą, turės patys įsiregistruoti, pavyzdžiui, automatiniame terminale, kad sukurtų ir įregistruotų savo veido atvaizdo šabloną, susietą su įlaipinimo bilietu ir tapatybe. Patikrinimo vietos, kuriose naudojama veido atpažinimo funkcija, turi būti aiškiai atskirtos, pavyzdžiui, sistema sumontuota patikrinimo vartuose, kad nebūtų fiksuojami sutikimo nedavusių asmenų biometriniai šablonai. Tik tie keleiviai, kurie anksčiau bus davę sutikimą ir toliau registruosis, naudosis patikrinimo vartuose sumontuota biometrine sistema.

Pavyzdys. Duomenų valdytojas prieigą prie savo pastato valdo naudodamas veido atpažinimo metodą. Šia prieiga žmonės gali naudotis tik iš anksto davę aiškiai informuoto asmens sutikimą (pagal 9 straipsnio 2 dalies a punktą). Tačiau siekiant užtikrinti, kad nebūtų užfiksuotas nė vienas asmuo, kuris anksčiau nedavė sutikimo, veido atpažinimo metodą turėtų naudoti pats duomenų subjektas, pavyzdžiui, spustelėdamas mygtuką. Siekdamas užtikrinti duomenų tvarkymo teisėtumą, duomenų valdytojas visada privalo pasiūlyti alternatyvų būdą patekti į pastatą nenaudojant biometrinių duomenų tvarkymo, pavyzdžiui, ženklelius arba raktus.

78.

79. Tokiais atvejais, kai sukuriami biometriniai šablonai, duomenų valdytojai užtikrina, kad, gavus teigiamą arba neigiamą rezultatą, visi tikruoju laiku (gavus aiškų ir informacija pagrįstą duomenų subjekto sutikimą) sukurti tarpiniai šablonai, kurie palyginami su pradiniais į sąrašą įtrauktų duomenų subjektų sukurtais šablonais, būtų nedelsiant ir saugiai ištrinti. Šablonai, kurie sukurti siekiant įtraukti asmenį į sąrašą, turi būti saugomi tik tam, kad būtų pasiektas duomenų tvarkymo tikslas, ir jie neturėtų būti saugomi ar archyvuojami.

80. Tačiau tais atvejais, kai duomenų tvarkymo tikslas yra, pavyzdžiui, atskirti vieną asmenų kategoriją nuo kitos, bet ne vienareikšmiškai nustatyti asmens tapatybę, duomenų tvarkymui 9 straipsnis netaikomas.

Pavyzdys. Parduotuvės savininkas norėtų pritaikyti savo reklamą prie kliento lyties ir amžiaus ypatybių, užfiksuotų stebėjimo vaizdo kameromis sistemoje. Jeigu ta sistema nesukuria biometrinių šablonų, kad būtų galima tiksliai nustatyti asmenų tapatybę, o tik nustato tas fizines savybes siekiant klasifikuoti asmenis, tuomet duomenų tvarkymui 9 straipsnis nebūtų taikomas (jeigu netvarkomi jokie kitų rūšių specialių kategorijų duomenys).

81.

82. Tačiau 9 straipsnis taikomas, jeigu duomenų valdytojas saugo biometrinius duomenis (dažniausiai naudodamas šablonus, kurie sukuriami nustatant pagrindines savybes iš pirminių biometrinių duomenų formos (pvz., veido matmenys iš atvaizdo), kad būtų galima vienareikšmiškai nustatyti asmens tapatybę. Jeigu duomenų valdytojas nori nustatyti duomenų subjektą, kuris pakartotinai atvyksta į vietovę arba atvyksta į kitą vietovę (pvz., siekdamas toliau planuoti pritaikytąją reklamą),

tuomet bus siekiama konkrečiai nustatyti fizinio asmens tapatybę, o tai reiškia, kad operacijai nuo pat pradžių būtų taikomas 9 straipsnis. Taip galėtų būti tuo atveju, jeigu duomenų valdytojas saugotų sukurtus šablonus, kad galėtų teikti papildomą pritaikytąją reklamą keliose skelbimų lentose skirtingose parduotuvės vietose. Kadangi sistemoje, siekiant nustatyti konkrečius asmenis, grįžtančius į kameros filmavimo lauką (pvz., prekybos salės lankytojai), ir juos sekti, naudojamos fizinės savybės, tai reikštų biometrinį tapatybės nustatymo metodą, nes juo siekiama atpažinti asmenį atliekant specialų techninį duomenų tvarkymą.

Pavyzdys. Parduotuvės savininkas savo parduotuvėje sumontavo veido atpažinimo sistemą, kad pritaikytų savo reklamą asmenims. Duomenų valdytojas, prieš naudodamasis šia biometrine sistema ir pateikdamas pritaikytąją reklamą, turi gauti aiškų ir informacija pagrįstą visų duomenų subjektų sutikimą. Sistema būtų neteisėta, jeigu joje būtų fiksuojami lankytojai arba praeiviai, kurie nesutiko, kad būtų kuriamas jų biometrinis šablonas, net jeigu jų šablonas ištrinamas per kuo trumpesnį laiką. Iš tiesų šie laikini šablonai yra biometriniai duomenys, tvarkomi siekiant konkrečiai nustatyti asmens, kuris gali nenorėti gauti tikslinės reklamos, tapatybę.

83.

84. EDAV pažymi, kad tam tikros biometrinės sistemos įrengiamos nekontroliuojamoje aplinkoje[17], o tai reiškia, kad sistemoje tikruoju laiku fiksuojamas bet kurio asmens, patenkančio į kameros filmavimo lauką, veidas, įskaitant asmenis, kurie nesutiko su biometrinio prietaiso naudojimu, taigi ir biometrinių šablonų kūrimu. Siekiant, kad duomenų valdytojas atpažintų, ar asmuo yra biometrinio prietaiso naudotojas, šie šablonai yra lyginami su šablonais, sukurtais duomenų subjektų, kurie davė savo išankstinį sutikimą įtraukimo į sąrašą metu (t. y. biometrinio prietaiso naudotojas). Šiuo atveju sistema dažnai būna sukurta taip, kad atskirtų į duomenų bazę įtrauktus asmenis, kuriuos ji nori atpažinti, nuo asmenų, kurių duomenų bazėje nėra. Kadangi taip siekiama konkrečiai nustatyti fizinių asmenų tapatybę, BDAR 9 straipsnio 2 dalyje numatytą išimtį vis tiek reikia taikyti kiekvienam kameros užfiksuotam asmeniui.

Pavyzdys. Viešbutyje naudojama stebėjimo vaizdo kameromis sistema, kuri, atpažinusi svečio veidą, automatiškai perspėja viešbučio vadovą apie tai, kad atvyko labai svarbus asmuo. Šie labai svarbūs asmenys, prieš įrašant jų duomenis į tuo tikslu sukurtą duomenų bazę, davė aiškų sutikimą naudoti veido atpažinimo metodą. Šios biometrinių duomenų tvarkymo sistemos būtų neteisėtos, išskyrus atvejus, kai visi kiti stebimi svečiai (siekiant nustatyti labai svarbius asmenis) būtų sutikę su duomenų tvarkymu pagal BDAR 9 straipsnio 2 dalies a punktą.

Pavyzdys. Duomenų valdytojas prie savo valdomos koncertų salės įėjimo įrengia stebėjimo vaizdo kameromis sistemą su veido atpažinimo funkcija. Duomenų valdytojas turi įrengti du aiškiai atskirtus įėjimus; vieną su biometrine sistema ir vieną be jos (kurioje, pvz., nuskenuojate bilietą). Įėjimai su biometriniais prietaisais turi būti įrengti ir prieinami taip, kad sistema negalėtų užfiksuoti nedavusių sutikimo žiūrovų biometrinių šablonų.

85.

86. Galiausiai, kai pagal BDAR 9 straipsnį reikalaujama gauti sutikimą, duomenų valdytojas savo paslaugomis leidžia naudotis nepriklausomai nuo to, ar buvo duotas sutikimas tvarkyti biometrinius

[17] Tai reiškia, kad biometrinis prietaisas yra visuomenei atviroje erdvėje ir gali stebėti kiekvieną praeivį, palyginti su kontroliuojamoje aplinkoje veikiančiomis biometrinėmis sistemomis, kurios gali būti naudojamos tik dalyvaujant sutikimą davusiam asmeniui.

duomenis. Kitaip tariant, visų pirma tais atvejais, kai biometrinių duomenų tvarkymas naudojamas tapatumo nustatymo tikslu, duomenų valdytojas privalo pasiūlyti alternatyvų sprendimo būdą, kuris nėra susijęs su biometrinių duomenų tvarkymu, netaikydamas duomenų subjektui jokių apribojimų arba nesukurdamas papildomų išlaidų. Šis alternatyvus sprendimo būdas taip pat yra reikalingas asmenims, kurie neatitinka biometrinio prietaiso apribojimų (biometrinių duomenų įrašymas ar nuskaitymas neįmanomas, naudojimą apsunkina negalia ir pan.), ir numatant, kad biometrinio prietaiso nebus galima naudoti (pvz., prietaiso gedimas), todėl, siekiant užtikrinti siūlomos paslaugos tęstinumą, būtina įgyvendinti atsarginį sprendimo variantą, kuris naudojamas tik išimtiniais atvejais. Išimtiniais atvejais gali susidaryti situacija, kai biometrinių duomenų tvarkymas yra pagrindinė pagal sutartį teikiamos paslaugos veikla, pavyzdžiui, muziejus, kuriame rengiama paroda veido atpažinimo prietaiso naudojimui pademonstruoti; tokiu atveju parodoje norintis dalyvauti duomenų subjektas negalės nesutikti, kad būtų tvarkomi asmens duomenys. Tokiu atveju pagal 9 straipsnį reikalaujamas sutikimas tebegalioja, jeigu įvykdomi 7 straipsnyje nustatyti reikalavimai.

5.2 Siūlomos priemonės biometrinių duomenų tvarkymo rizikai sumažinti

87. Laikydamiesi duomenų kiekio mažinimo principo, duomenų valdytojai privalo užtikrinti, kad duomenys, gauti iš skaitmeninio atvaizdo šablonui sukurti, nebūtų pertekliniai ir juose būtų tik konkrečiam tikslui pasiekti reikalinga informacija, taip išvengiant bet kokio galimo tolesnio tvarkymo. Reikėtų nustatyti priemones, kuriomis būtų garantuojama, kad šablonų nebūtų galima perkelti iš vienos biometrinės sistemos į kitą.

88. Atpažinimo, tapatumo nustatymo ir (arba) tikrinimo tikslais šabloną greičiausiai reikės saugoti, kad jį būtų galima naudoti atliekant vėlesnį palyginimą. Duomenų valdytojas privalo apsvarstyti tinkamiausią duomenų saugojimo vietą. Kontroliuojamoje aplinkoje (aptverti koridoriai arba patikrinimo vietos) šablonai saugomi atskirame naudotojo laikomame ir jo vienintelio valdomame prietaise (išmaniajame telefone arba tapatybės kortelėje) arba, – prireikus konkrečiais tikslais ir esant objektyviems poreikiams, – saugomi centralizuotoje duomenų bazėje šifruota forma tik asmeniui suteikiant raktą (slaptažodį), kad būtų užkirstas kelias neteisėtai prieigai prie šablono arba saugojimo vietos. Jeigu duomenų valdytojui būtinai reikalinga prieiga prie šablonų, jis privalo imtis tinkamų veiksmų, kad užtikrintų saugomų duomenų saugumą. Tai gali apimti šablono šifravimą naudojant kriptografinį algoritmą.

89. Bet kuriuo atveju duomenų valdytojas imasi visų būtinų atsargumo priemonių, kad išsaugotų tvarkomų duomenų prieinamumą, vientisumą ir konfidencialumą. Šiuo tikslu duomenų valdytojas visų pirma imasi šių priemonių: perduoda ir saugo duomenis dalimis, saugo biometrinius šablonus ir pirminius duomenis arba tapatybės duomenis atskirose duomenų bazėse, užšifruoja biometrinius duomenis, visų pirma biometrinius šablonus, ir nustato šifravimo ir raktų valdymo politiką, integruoja organizacinę ir techninę sukčiavimo nustatymo priemonę, susieja vientisumo kodą su duomenimis (pvz., parašas ar maiša) ir uždraudžia bet kokią išorinę prieigą prie biometrinių duomenų. Tokias priemones reikia plėtoti atsižvelgiant į technologijų pažangą.

90. Be to, duomenų valdytojai turėtų toliau trinti pirminius duomenis (veido atvaizdus, kalbos signalus, eiseną ir pan.) ir užtikrinti, kad tai būtų daroma veiksmingai. Jeigu teisėtas duomenų tvarkymo pagrindas nebegalioja, pirminius duomenis reikia ištrinti. Iš tiesų, jeigu biometriniai šablonai gaunami iš tokių duomenų, galima manyti, kad duomenų bazių sukūrimas galėtų kelti vienodą ar net didesnę grėsmę (nes ne visada gali būti lengva skaityti biometrinį šabloną nežinant, kaip jis buvo programuojamas, o pirminiai duomenys bus bet kurio šablono pagrindas). Jei duomenų valdytojui reikėtų saugoti tokius duomenis, turi būti išnagrinėti triukšmo metodai (pvz., vandenženklių naudojimas), dėl kurio šablonų sukūrimas taptų neveiksmingas. Duomenų valdytojas taip pat privalo ištrinti biometrinius duomenis ir šablonus, jei suteikiama neteisėta prieiga prie duomenų palyginimo

terminalo arba serverio, ir ištrinti visus duomenis, kurie nėra naudingi tolesniam duomenų tvarkymui pasibaigus biometrinio prietaiso naudojimo laikui.

6 DUOMENŲ SUBJEKTO TEISĖS

91. Atsižvelgiant į duomenų tvarkymo naudojant stebėjimą vaizdo kameromis pobūdį, tam tikras duomenų subjekto teises pagal BDAR reikia paaiškinti išsamiau. Tačiau šis skyrius nėra išsamus, visos BDAR nustatytos teisės taikomos asmens duomenų tvarkymui naudojant stebėjimą vaizdo kameromis.

6.1 Teisė susipažinti su duomenimis

92. Duomenų subjektas turi teisę iš duomenų valdytojo gauti patvirtinimą, ar jo asmens duomenys yra tvarkomi. Stebėjimo vaizdo kameromis atveju tai reiškia, kad jeigu duomenys nesaugomi arba neperduodami kokiu nors būdu, tuomet, pasibaigus stebėjimo tikruoju laiku momentui, duomenų valdytojas galėtų pateikti tik informaciją, kad nebetvarkomi jokie asmens duomenys (be bendrųjų prievolių informuoti pagal 13 straipsnį, žr. *7 skirsnį „Skaidrumo ir informavimo prievolės“*). Tačiau jeigu duomenys prašymo pateikimo metu vis tiek tvarkomi (t. y. jeigu duomenys saugomi arba nuolat tvarkomi bet kuriuo kitu būdu), duomenų subjektui turėtų būti suteikta prieiga ir informacija pagal 15 straipsnį.

93. Tačiau galioja įvairūs apribojimai, kurie tam tikrais atvejais gali būti taikomi teisei susipažinti su duomenimis.

- BDAR 15 straipsnio 4 dalis daro neigiamą poveikį kitų asmenų teisėms

94. Atsižvelgiant į tai, kad stebėjimo vaizdo kameromis sistemoje gali būti įrašoma bet kokio duomenų subjektų skaičiaus seka, tai reikštų, kad atliekant tikrinimą būtų tvarkomi papildomi kitų duomenų subjektų asmens duomenys. Jeigu duomenų subjektas nori gauti įrašo kopiją (15 straipsnio 3 dalis), tai turėtų neigiamą poveikį kito toje įraše esančio duomenų subjekto teisėms ir laisvėms. Todėl, siekdamas užkirsti kelią tokiam poveikiui, duomenų valdytojas turėtų atsižvelgti į tai, kad dėl invazinio filmuotos vaizdo medžiagos pobūdžio duomenų valdytojas tam tikrais atvejais neturėtų skelbti vaizdo medžiagos, kurioje galima nustatyti kitų duomenų subjektų tapatybę. Vis dėlto trečiųjų šalių teisių apsauga neturėtų būti naudojama kaip pasiteisinimas siekiant užkirsti kelią teisėtiems asmenų reikalavimams susipažinti su duomenimis. Tokiais atvejais duomenų valdytojas turėtų įgyvendinti technines priemones, kad patenkintų prašymą susipažinti su duomenimis (pvz., vaizdo redagavimas naudojant maskavimą arba šifravimą). Tačiau duomenų valdytojai neprivalo įgyvendinti tokių techninių priemonių, jeigu jie kitaip gali užtikrinti gebėjimą atsakyti į pagal 15 straipsnį pateiktą prašymą ir laikytis 12 straipsnio 3 dalyje nustatyto termino.

- BDAR 11 straipsnio 2 dalis, duomenų valdytojas negali nustatyti duomenų subjekto tapatybės

95. Jeigu filmuotoje vaizdo medžiagoje negalima atlikti asmens duomenų paieškos (t. y. duomenų valdytojui tikriausiai reikėtų susipažinti su dideliu saugomos medžiagos kiekiu, kad rastų atitinkamą duomenų subjektą), duomenų valdytojas gali nesugebėti nustatyti duomenų subjekto tapatybės.

96. Dėl šių priežasčių duomenų subjektas savo prašyme, kurį pateikia duomenų valdytojui, turėtų nurodyti (be to, kad nurodo savo tapatybę, įskaitant tapatybės nustatymo dokumento pateikimą arba asmens įvardijimą), kada – per pagrįstą laikotarpį, kuris yra proporcingas įrašytų duomenų subjektų skaičiui, – jis pateko į stebimą teritoriją. Duomenų valdytojas turėtų iš anksto pranešti duomenų subjektui, kokios informacijos reikia, kad duomenų valdytojas galėtų patenkinti

prašymą. Jeigu duomenų valdytojas gali įrodyti, kad negali nustatyti duomenų subjekto tapatybės, jei įmanoma, jis privalo apie tai atitinkamai informuoti duomenų subjektą. Tokioje situacijoje duomenų valdytojas, atsakydamas duomenų subjektui, turėtų informuoti apie tikslią stebėsenos teritoriją, naudotų kamerų patikrinimą ir pan., kad duomenų subjektas galėtų visiškai suprasti, kokie jo asmens duomenys galėjo būti tvarkomi.

Pavyzdys. Jeigu duomenų subjektas prašo savo asmens duomenų, kurie buvo tvarkomi prie prekybos centro, kuriame per dieną apsilanko 30 000 lankytojų, įėjimo naudojant stebėjimo vaizdo kameromis sistemą, kopijos, duomenų subjektas turėtų tiksliai (vienos valandos tikslumu) nurodyti, kada jis praėjo pro stebimą vietą. Jeigu duomenų valdytojas vis dar tvarko įrašą, reikėtų pateikti filmuotos vaizdo medžiagos kopiją. Jeigu tame pačiame įraše galima nustatyti kitų duomenų subjektų tapatybę, tuomet dalį įrašo kopijos, prieš ją perduodant jos prašiusiam duomenų subjektui, reikėtų anoniminti (pvz., užtušuojant įrašo kopiją arba jos dalis).

Pavyzdys. Jeigu duomenų valdytojas automatiškai ištrina visą filmuotą vaizdo medžiagą per, pavyzdžiui, 2 dienas, duomenų valdytojas negali pateikti filmuotos vaizdo medžiagos duomenų subjektui praėjus šioms 2 dienom. Jeigu duomenų valdytojas gauna prašymą po tų 2 dienų, apie tai atitinkamai reikėtų informuoti duomenų subjektą.

97.

) BDAR 12 straipsnis, pertekliniai prašymai

98. Jeigu duomenų subjektas pateikia perteklinius arba akivaizdžiai nepagrįstus prašymus, duomenų valdytojas gali pagal BDAR 12 straipsnio 5 dalies a punktą nustatyti pagrįstą mokestį arba atsisakyti patenkinti prašymą (BDAR 12 straipsnio 5 dalies b punktas). Duomenų valdytojas turi sugebėti įrodyti, kad prašymas yra akivaizdžiai nepagrįstas arba perteklinis.

6.2 Teisė reikalauti ištrinti duomenis ir teisė nesutikti

6.2.1 Teisė reikalauti ištrinti duomenis (teisė būti pamirštam)

99. Jeigu duomenų valdytojas toliau tvarko asmens duomenis po stebėjimo tikruoju laiku (pvz., saugo duomenis), duomenų subjektas gali prašyti, kad asmens duomenys būtų ištrinti pagal BDAR 17 straipsnį.

100. Gavęs prašymą duomenų valdytojas privalo nepagrįstai nedelsdamas ištrinti asmens duomenis, jeigu taikoma viena iš BDAR 17 straipsnio 1 dalyje išvardytų aplinkybių (ir negalioja nė viena iš BDAR 17 straipsnio 3 dalyje išvardytų išimčių). Tai apima prievolę ištrinti asmens duomenis, kai jų nebereikia tuo tikslu, kuriuo jie iš pradžių buvo saugomi, arba kai duomenų tvarkymas yra neteisėtas (taip pat žr. *8 skirsnį „Saugojimo laikotarpiai ir prievolė ištrinti“*). Be to, priklausomai nuo duomenų tvarkymo teisinio pagrindo, asmens duomenys turėtų būti ištrinti:

- *sutikimo atveju*, kai sutikimas atšaukiamas (ir nėra jokio kito duomenų tvarkymo teisinio pagrindo);
- dėl *teisėto intereso*:
    - kai duomenų subjektas pasinaudoja teise nesutikti (žr. *6.2.2 skirsnį*) ir nėra viršesnių įtikinamų teisėtų priežasčių tvarkyti duomenis, arba
    - tiesioginės rinkodaros (įskaitant profiliavimą) atveju, kai duomenų subjektas prieštarauja duomenų tvarkymui.

101. Jeigu duomenų valdytojas viešai paskelbė filmuotą vaizdo medžiagą (pvz., transliavo televizijoje arba internete), reikia imtis pagrįstų veiksmų, siekiant informuoti kitus duomenų valdytojus (kurie dabar tvarko atitinkamus asmens duomenis) apie prašymą pagal BDAR 17 straipsnio 2 dalį. Pagrįstos priemonės turėtų apimti technines priemones, atsižvelgiant į turimas technologijas ir įgyvendinimo išlaidas. Ištrynęs asmens duomenis, duomenų valdytojas, kiek tai įmanoma, pagal BDAR 19 straipsnį turėtų informuoti visus asmenis, kuriems anksčiau buvo atskleisti asmens duomenys.

102. Be duomenų valdytojo prievolės ištrinti asmens duomenis duomenų subjekto prašymu, taip pat galioja duomenų valdytojo prievolė pagal BDAR bendruosius principus apriboti saugomus asmens duomenis (žr. *8 skirsnį*).

103. Kalbant apie stebėjimą vaizdo kameromis, verta pažymėti, kad, užtušavus nuotrauką taip, kad iš jos nebūtų galima atgaminti anksčiau joje buvusių asmens duomenų, laikoma, kad asmens duomenys buvo ištrinti pagal BDAR.

> Pavyzdys. Būtiniausių prekių parduotuvei kyla problemų dėl vandalizmo, ypač ant išorinių pastato sienų, todėl šalia įėjimo, kuris tiesiogiai ribojasi su sienomis, naudojama stebėjimo vaizdo kameromis sistema. Praeivis prašo, kad būtų ištrinti iš pat pradžių nufilmuoti jo asmens duomenys. Duomenų valdytojas privalo į prašymą atsakyti nepagrįstai nedelsdamas ir ne vėliau kaip per vieną mėnesį. Kadangi aptariama filmuota medžiaga nebeatitinka tikslo, dėl kurio ji iš pradžių buvo saugoma (duomenų subjektui einant pro šalį nebuvo jokio vandalizmo), prašymo pateikimo metu nėra jokio teisėto intereso saugoti duomenis, kuris būtų viršesnis už duomenų subjektų interesus. Duomenų valdytojas turi ištrinti asmens duomenis.

104.

6.2.2 Teisė nesutikti

105. Jeigu stebėjimas vaizdo kameromis grindžiamas *teisėtu interesu* (BDAR 6 straipsnio 1 dalies f punktas) arba būtinybe atlikti užduotį *viešojo intereso* labui (BDAR 6 straipsnio 1 dalies e punktas), duomenų subjektas turi teisę bet kuriuo metu, remdamasis su jo konkrečia padėtimi susijusiais pagrindais, nesutikti su duomenų tvarkymu pagal BDAR 21 straipsnį. Išskyrus atvejus, kai duomenų valdytojas įrodo įtikinamus teisėtus pagrindus, kurie yra viršesni už duomenų subjekto teises ir interesus, nesutikimą pareiškusio asmens duomenų tvarkymas turi būti sustabdytas. Duomenų valdytojas turėtų būti įpareigojamas nepagrįstai nedelsdamas ir ne vėliau kaip per vieną mėnesį atsakyti į duomenų subjekto prašymus.

106. Stebėjimo vaizdo kameromis atveju šis nesutikimas galėtų būti pareikštas patenkant į stebimą teritoriją, būnant joje arba iš jos išėjus. Praktiškai tai reiškia, kad tol, kol duomenų valdytojas nėra nustatęs įtikinamų teisėtų priežasčių, teritorijos, kurioje galima nustatyti fizinius asmenis, stebėjimas yra teisėtas tik tuo atveju, jei:

    (1) duomenų valdytojas paprašius gali nedelsdamas sustabdyti asmens duomenų tvarkymą arba

    (2) stebima teritorija yra taip tiksliai aptverta, kad duomenų valdytojas gali užtikrintai gauti duomenų subjekto patvirtinimą prieš jam patenkant į teritoriją, be to, tai nėra teritorija, į kurią duomenų subjektas turi teisę patekti kaip pilietis.

107. Šiose gairėse nesiekiama nustatyti, kas laikytina *įtikinamu* teisėtu interesu (BDAR 21 straipsnis).

108. Jeigu stebėjimas vaizdo kameromis naudojamas tiesioginės rinkodaros tikslais, duomenų subjektas turi teisę nesutikti su duomenų tvarkymu savo nuožiūra, nes tomis aplinkybėmis teisė nesutikti yra absoliuti (BDAR 21 straipsnio 2 ir 3 dalys).

Pavyzdys. Įmonė, kuri susiduria su sunkumais dėl saugumo incidentų, įvykstančių prie jos viešo įėjimo, naudoja stebėjimo vaizdo kameromis sistemą remdamasi teisėto intereso pagrindu, kad sugautų neteisėtai įeinančius asmenis. Lankytojas nesutinka, kad jo duomenys būtų tvarkomi naudojant stebėjimo vaizdo kameromis sistemą remdamasis pagrindais, susijusiais su jo konkrečia padėtimi. Tačiau įmonė šiuo atveju atmeta prašymą paaiškindama, kad filmuotos medžiagos saugojimas yra reikalingas dėl vykdomo vidaus tyrimo, todėl ji turi įtikinamų teisėtų priežasčių toliau tvarkyti asmens duomenis.

109.

7 SKAIDRUMO IR INFORMAVIMO PRIEVOLĖS[18]

110. Europos duomenų apsaugos teisei jau seniai būdinga tai, kad duomenų subjektai turėtų žinoti apie tai, kad vykdomas stebėjimas vaizdo kameromis. Juos reikėtų išsamiai informuoti apie stebimas vietas[19]. Pagal BDAR bendrosios skaidrumo ir informavimo prievolės yra nustatytos BDAR 12 ir kituose straipsniuose. Daugiau informacijos pateikiama 29 straipsnio darbo grupės „Skaidrumo pagal Reglamentą 2016/679 gairėse (WP 260)“, kurias 2018 m. gegužės 25 d. patvirtino EDAV. Pagal WP 260 26 dalį taikomas BDAR 13 straipsnis, jeigu asmens duomenys renkami „<...> iš duomenų subjekto stebėjimo būdu (pvz., naudojant automatinius duomenų rinkimo prietaisus arba programinę įrangą, pavyzdžiui, kameras <...>“.

111. Atsižvelgiant į informacijos kiekį, kurį reikalaujama pateikti duomenų subjektui, duomenų valdytojai gali taikyti kelių lygmenų metodą, jeigu jie, siekdami užtikrini skaidrumą, nusprendžia naudoti metodų derinį (WP 260, 35 dalis; WP 89, 22 dalis). Kalbant apie stebėjimą vaizdo kameromis, pažymėtina, kad svarbiausia informacija turėtų būti pateikiama pačiame įspėjamajame ženkle (pirmasis lygmuo), o kita privaloma informacija gali būti pateikiama naudojant kitas priemones (antrasis lygmuo).

7.1 Pirmojo lygmens informacija (įspėjamasis ženklas)

112. Pirmasis lygmuo yra susijęs su pirminiu būdu, kurį duomenų valdytojas taiko pirmą kartą duomenų subjektui. Šiame etape duomenų valdytojai gali naudoti įspėjamąjį ženklą, kuriame rodoma atitinkama informacija. Rodoma informacija gali būti pateikiama kartu su piktograma, siekiant lengvai matomu, suprantamu ir aiškiai įskaitomu būdu pateikti prasmingą numatomo duomenų naudojimo apžvalgą (BDAR 12 straipsnio 7 dalis). Informacijos formatas turėtų būti pritaikytas prie konkrečios vietos (WP 89, 22 dalis).

7.1.1 Įspėjamojo ženklo vieta

113. Informacija turėtų būti išdėstyta taip, kad duomenų subjektas, prieš patekdamas į stebimą teritoriją, galėtų lengvai atpažinti stebėjimo aplinkybes (maždaug akių lygyje). Nebūtina atskleisti informacijos apie kameros buvimo vietą, jeigu nėra jokių abejonių dėl stebimų vietų ir nedviprasmiškai paaiškinamos stebėjimo aplinkybės (WP 89, 22 dalis). Duomenų subjektas turi sugebėti įvertinti kameros filmuojamą plotą, kad galėtų išvengti stebėjimo arba prireikus pakeisti savo elgesį.

[18] Gali būti taikomi konkretūs nacionalinės teisės aktuose nustatyti reikalavimai.

[19] Žr. 29 straipsnio darbo grupės Nuomonę 4/2004 dėl asmens duomenų tvarkymo naudojant stebėjimą vaizdo kameromis.

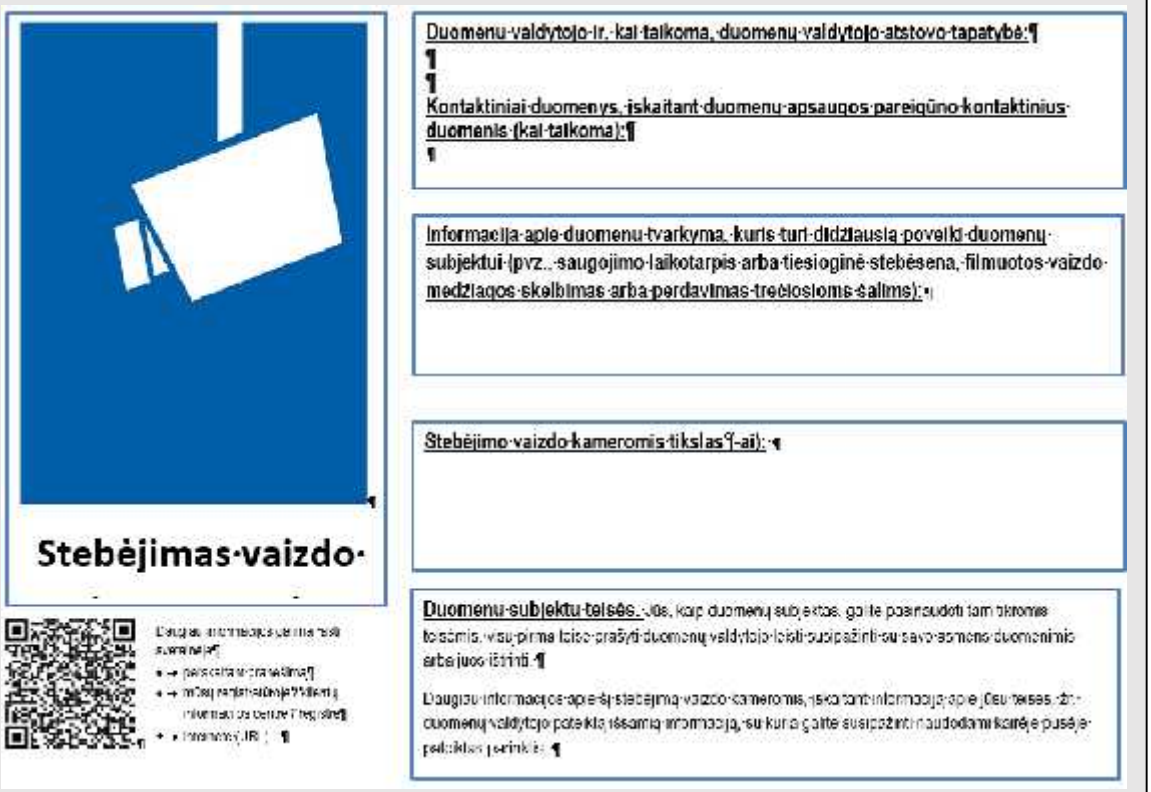
7.1.2 Pirmojo lygmens turinys

114. Pirmojo lygmens informacija (įspėjamasis ženklas) paprastai turėtų apimti svarbiausią informaciją, pavyzdžiui, informacija apie duomenų tvarkymo tikslus, duomenų valdytojo tapatybę ir duomenų subjekto teisių buvimą, įskaitant informaciją apie svarbiausias duomenų tvarkymo pasekmes[20]. Tai, pavyzdžiui, gali reikšti teisėtus interesus, kurių siekia duomenų valdytojas (arba trečioji šalis) ir duomenų apsaugos pareigūno kontaktinius duomenis (jei taikoma). Pirmojo lygmens informacija taip pat turi apimti nuorodą į išsamesnę antrojo lygmens informaciją ir nurodymus, kur ir kaip ją rasti.

115. Be to, ženkle taip pat turėtų būti pateikta visa informacija, kuri duomenų subjektui galėtų būti netikėta (WP 260, 38 dalis). Tai, pavyzdžiui, galėtų būti informacija apie perdavimą trečiosioms šalims, ypač jeigu jos yra už ES ribų, ir saugojimo laikotarpį. Jeigu ši informacija nenurodoma, duomenų subjektui turėtų būti sudaryta galimybė įsitikinti, kad vykdoma tik tiesioginė stebėsena (neregistruojant jokių duomenų ir neperduodant jų trečiosioms šalims).

116.

Pavyzdys (neprivalomas pasiūlymas).



7.2 Antro lygmens informacija

117. Su antrojo lygmens informacija duomenų subjektas taip pat turėtų turėti galimybę susipažinti lengvai prieinamoje vietoje, pavyzdžiui, išsamus informacinis lapas pagrindinėje vietoje (pvz., informacinis stendas, registratūra arba kasa) arba naudojant lengvai matomą plakatą. Kaip minėta, pirmojo lygmens įspėjamajame ženkle turi būti aiškiai rodoma antrojo lygmens informacija. Be to, geriausia, jei kartu su pirmojo lygmens informacija pateikiama nuoroda į antrojo lygmens skaitmeninį šaltinį (pvz., QR kodas arba svetainės adresas). Tačiau taip pat turėtų būti lengvai prieinama ir neskaitmeninė informacija. Su antro lygmens informacija turėtų būti įmanoma susipažinti nepatekus į stebimą teritoriją, ypač jeigu

[20] Žr. WP 260, 38 dalį.

informacija pateikiama skaitmeniniu būdu (tai galima padaryti, pvz., pateikiant hipersaitą). Kitos tinkamos priemonės galėtų būti telefono numeris, kuriuo galima paskambinti. Nepaisant informacijos pateikimo formos, joje turi būti visas BDAR 13 straipsnyje nurodytas privalomas turinys.

118. EDAV ragina naudotis ne tik šiomis priemonėmis, bet ir, siekdama didesnio jų veiksmingumo, skatina naudoti technologines priemones informacijai pateikti, kad duomenų subjektai būtų informuojami. Tai, pavyzdžiui, gali būti geografinės buvimo vietos nustatymo kameros ir informacijos įtraukimas į kartografavimo programėles arba svetaines, kad asmenys, viena vertus, galėtų lengvai nustatyti ir nurodyti vaizdo šaltinius, susijusius su jų teisių įgyvendinimu, ir, antra vertus, gauti išsamesnę informaciją apie duomenų tvarkymo operaciją.

> Pavyzdys. Parduotuvės savininkas stebi savo parduotuvę. Kad būtų laikomasi 13 straipsnio, pakanka lengvai matomoje vietoje prie parduotuvės įėjimo uždėti įspėjamąjį ženklą, kuriame būtų pateikta pirmojo lygmens informacija. Be to, kasoje arba bet kurioje kitoje pagrindinėje ir lengvai prieinamoje savo parduotuvės vietoje jis turi pateikti informacinį lapą su antrojo lygmens informacija.

119.

8 SAUGOJIMO LAIKOTARPIAI IR PRIEVOLĖ IŠTRINTI DUOMENIS

120. Asmens duomenys negali būti saugomi ilgiau, neg būtina siekiant tikslų, kuriais asmens duomenys tvarkomi (BDAR 5 straipsnio 1 dalies c ir e punktai). Tam tikrose valstybėse narėse gali galioti specialios nuostatos dėl saugojimo laikotarpių, taikomų stebėjimui vaizdo kameromis, pagal BDAR 6 straipsnio 2 dalį.

121. Tai, ar asmens duomenis būtina saugoti, ar ne, reikėtų nustatyti per trumpą laiką. Apskritai teisėti stebėjimo vaizdo kameromis interesai dažnai yra susiję su nuosavybės apsauga arba įrodymų išsaugojimu. Paprastai patirta žala gali būti pripažinta per vieną arba dvi dienas. Kad būtų lengviau įrodyti atitiktį duomenų apsaugos sistemai, duomenų valdytojas yra suinteresuotas iš anksto imtis organizacinių priemonių (pvz., prireikus paskirti atstovą vaizdo medžiagai tikrinti ir apsaugoti). Atsižvelgiant į BDAR 5 straipsnio 1 dalies c ir e punktuose nustatytus principus, būtent duomenų kiekio mažinimo ir saugojimo trukmės apribojimo principus, asmens duomenis dažniausiai (pvz., siekiant nustatyti vandalizmo atvejį) ir idealiausiu atveju reikėtų ištrinti po kelių dienų. Kuo ilgesnis saugojimo laikotarpis nustatomas (ypač kai jis ilgesnis negu 72 valandos), tuo daugiau reikia pateikti argumentų, susijusių su tikslo teisėtumu ir saugojimo būtinumu. Jeigu duomenų valdytojas stebėjimą vaizdo kameromis naudoja ne tik savo patalpoms stebėti, bet ir ketina saugoti duomenis, jis privalo patikinti, kad duomenų saugojimas faktiškai yra būtinas norint pasiekti tikslą. Jei taip, saugojimo laikotarpis turi būti aiškiai apibrėžtas ir nustatytas atskirai dėl kiekvieno konkretaus tikslo. Būtent duomenų valdytojas, atsižvelgdamas į būtinumo ir proporcingumo principus, privalo apibrėžti saugojimo laikotarpį ir įrodyti atitiktį BDAR nuostatoms.

> Pavyzdys. Mažos parduotuvės savininkas paprastai tą pačią dieną pastebi bet kokį vandalizmą. Todėl įprastas 24 valandų saugojimo laikotarpis yra pakankamas. Tačiau savaitgaliai, kai parduotuvė nedirba, arba daugiau švenčių dienų gali būti priežastis nustatyti ilgesnį saugojimo laikotarpį. Jeigu nustatoma žala, savininkui taip pat gali reikėti ilgiau saugoti filmuotą vaizdo medžiagą, kad galėtų imtis teisinių veiksmų prieš nusikaltėlį.

122.

9 TECHNINĖS IR ORGANIZACINĖS PRIEMONĖS

123. Kaip nurodyta BDAR 32 straipsnio 1 dalyje, asmens duomenų tvarkymas vykdant stebėjimą vaizdo kameromis turi būti teisiškai leidžiamas, o duomenų valdytojai ir duomenų tvarkytojai taip pat privalo jį užtikrinti. Įgyvendintos **organizacinės ir techninės priemonės** turi būti **proporcingos rizikai, kuri fizinių asmenų teisėms ir laisvėms kyla** dėl atsitiktinio arba neteisėto stebėjimo vaizdo kameromis duomenų sunaikinimo, praradimo, pakeitimo, neleistino atskleidimo arba prieigos prie jų. Pagal BDAR 24 ir 25 straipsnius duomenų valdytojai technines ir organizacines priemones turi įgyvendinti taip pat tam, kad garantuotų visų duomenų apsaugos principų laikymąsi duomenų tvarkymo metu ir nustatytų priemones, kuriomis naudodamiesi duomenų subjektai gali įgyvendinti savo teises, kaip apibrėžta BDAR 15–22 straipsniuose. Duomenų valdytojai turėtų patvirtinti vidaus sistemą ir politiką, kuri padėtų užtikrinti, kad šios priemonės būtų įgyvendintos tiek tuo metu, kai nustatomos duomenų tvarkymo priemonės, tiek pačių duomenų tvarkymo metu, įskaitant poveikio duomenų apsaugai vertinimo atlikimą, kai to reikia.

9.1 Stebėjimo vaizdo kameromis apžvalga

124. Stebėjimo vaizdo kameromis sistemą (angl. *video surveillance system*, VSS)[21] sudaro analoginiai ir skaitmeniniai prietaisai, taip pat programinė įranga, kurios paskirtis – fiksuoti scenos vaizdus, tvarkyti atvaizdus ir rodyti juos operatoriui. Šios sistemos sudedamosios dalys skirstomos į šias kategorijas:

- Filmavimo aplinka: vaizdo fiksavimas, jungtys ir vaizdo tvarkymas:
  - vaizdo fiksavimo tikslas – sukurti tikrovės vaizdą tokiu formatu, kad jį būtų galima naudoti likusioje sistemos dalyje,
  - jungtys reikalingos norint perduoti visus duomenis filmavimo aplinkoje, t. y. sujungimai ir ryšiai. Jungčių pavyzdžiai – kabeliai, skaitmeniniai tinklai ir bevielis transliavimas. Ryšiai – tai visi skaitmeniniai arba analoginiai vaizdo ir valdymo duomenų signalai,
  - vaizdo tvarkymas apima vaizdo arba vaizdų sekos analizę, saugojimą ir pateikimą.
- Žvelgiant iš sistemos valdymo perspektyvos, stebėjimo vaizdo kameromis sistema atlieka šias logines funkcijas:
  - duomenų valdymas ir veiklos valdymas, kuris apima valdymo operatoriaus komandas ir sistemos vykdomą veiklą (pavojaus signalizavimo procedūros, įspėjimus siunčiantys operatoriai),
  - sąsajos su kitomis sistemomis gali apimti prisijungimą prie kitų saugumo sistemų (patekimo kontrolė, priešgaisrinė signalizacija) ir su saugumu nesusijusių sistemų (pastatų valdymo sistemos, automatinis registracijos numerio atpažinimas).
- Stebėjimo vaizdo kameromis sistemos saugumo aspektai apima sistemos ir duomenų konfidencialumą, vientisumą ir prieinamumą:

[21] BDAR šios sistemos apibrėžtis nepateikta, jos techninį aprašymą galima, pavyzdžiui, rasti EN 62676-1-1:2014 „Saugumo prietaikoms skirtos vaizdo stebėjimo sistemos. 1-1 dalis. Reikalavimai vaizdo sistemai“.

- sistemos saugumas apima fizinį visų sistemos komponentų fizinį saugumą ir prieigos prie stebėjimo vaizdo kameromis sistemos kontrolę,
- duomenų saugumas apima duomenų praradimo arba manipuliavimo jais prevenciją.

125.

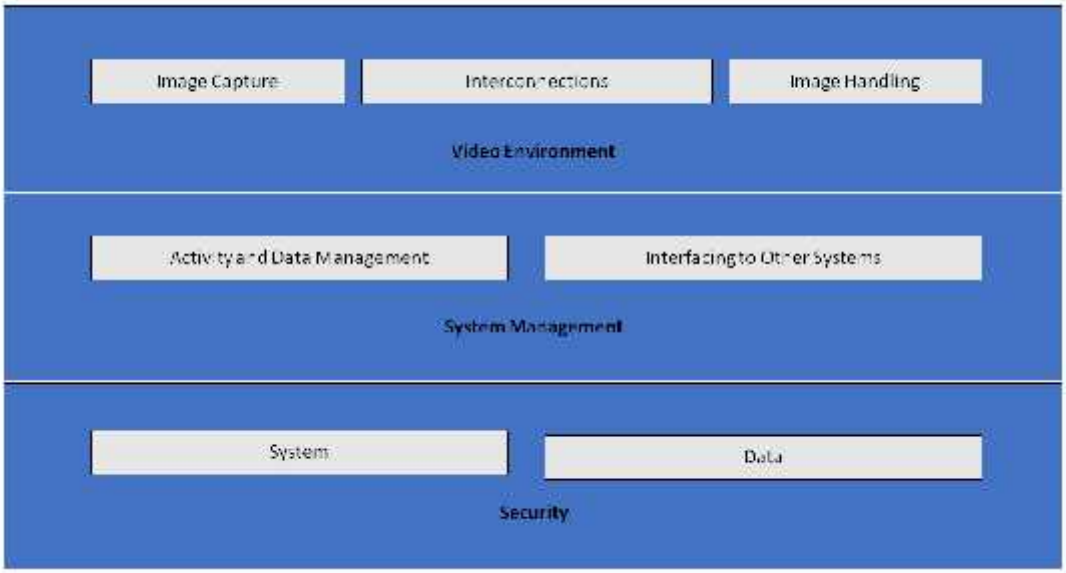


Image Capture	Vaizdo fiksavimas
Interconnections	Jungtys
Image Handling	Vaizdų tvarkymas
Video Environment	Filmavimo aplinka
Activity and Data Management	Veikla ir duomenų valdymas
Interfacing to Other Systems	Sąsajos su kitomis sistemomis
System Management	Sistemos valdymas
System	Sistema
Data	Duomenys
Security	Saugumas

1 pav. Vaizdo stebėjimo sistema

9.2 Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga

126. Kaip nurodyta BDAR 25 straipsnyje, duomenų valdytojai, kuo greičiau, kai planuoja vykdyti stebėjimą vaizdo kameromis ir prieš pradėdami rinkti ir tvarkyti filmuotą vaizdo medžiagą, turi įgyvendinti tinkamas technines ir organizacines duomenų apsaugos priemones. Šiais principais pabrėžiamas įdiegtų privatumo stiprinimo technologijų, numatytųjų nuostatų, kurios padeda kuo labiau sumažinti duomenų tvarkymą, ir būtinų priemonių, kurios sudaro sąlygas užtikrinti kuo didesnę asmens duomenų apsaugą, užtikrinimo poreikis[22].

127. Duomenų valdytojai duomenų apsaugos ir privatumo apsaugos priemonių taikymą turėtų numatyti ne tik technologijos projektavimo specifikacijose, bet ir organizacinėje praktikoje. Kalbant apie organizacinę praktiką, pažymėtina, kad duomenų valdytojas turėtų patvirtinti tinkamą valdymo

[22] WP 168, Nuomonė „Privatumo ateitis“, 29 straipsnio duomenų apsaugos darbo grupės ir Policijos ir teisingumo darbo grupės bendras indėlis į konsultacijas su Europos Komisija dėl pagrindinės teisės į asmens duomenų apsaugą teisinės sistemos (priimta 2009 m. gruodžio 1 d.).

sistemą, nustatyti ir įgyvendinti su stebėjimu vaizdo kameromis susijusią politiką ir procedūras. Techniniu požiūriu sistemos specifikacijose ir projekte turėtų būti numatyti asmens duomenų tvarkymo pagal BDAR 5 straipsnyje nustatytus reikalavimus principai (duomenų tvarkymo teisėtumas, tikslo apribojimo principas, standartizuotas duomenų kiekio mažinimas, kaip apibrėžta BDAR 25 straipsnio 2 dalyje, vientisumas ir konfidencialumas, atskaitomybė ir pan.). Jeigu duomenų valdytojas planuoja įsigyti komercinę stebėjimo vaizdo kameromis sistemą, jis šiuos reikalavimus turi įtraukti į pirkimo specifikaciją. Duomenų valdytojas turi užtikrinti šių reikalavimų laikymąsi taikydamas juos visiems sistemos komponentams ir visiems šioje sistemoje tvarkomiems duomenims, įskaitant jų visą gyvavimo ciklą.

9.3 Konkretūs atitinkamų priemonių pavyzdžiai

128. Dauguma priemonių, kurios gali būti naudojamos stebėjimui vaizdo kameromis užtikrinti, ypač tais atvejais, kai naudojama skaitmeninė įranga ir programinė įranga, nesiskirs nuo kitose IT sistemose naudojamų priemonių. Tačiau, nepaisant pasirinkto sprendimo būdo, duomenų valdytojas privalo tinkamai apsaugoti visus stebėjimo vaizdo kameromis komponentus ir duomenis visais etapais, t. y. saugojimo metu (nenaudojami duomenys), perduodant (perduodami duomenys) ir tvarkant (naudojami duomenys). Šiuo tikslu būtina, kad duomenų valdytojai ir duomenų tvarkytojai derintų organizacines ir technines priemones.

129. Pasirinkdamas techninius sprendimo būdus, duomenų valdytojas, be kita ko, turėtų atsižvelgti į privatumą užtikrinančias technologijas, nes jos padeda užtikrinti didesnį saugumą. Tokių technologijų pavyzdžiai yra sistemos, kurios sudaro sąlygas užmaskuoti arba užšifruoti vietas, kurios nėra svarbios stebėjimui, arba pašalinti trečiųjų asmenų atvaizdus duomenų subjektams teikiant filmuotą vaizdo medžiagą[23]. Kita vertus, atrinktuose sprendimo būduose neturėtų būti nebūtinų funkcijų (pvz., neribotas kamerų judėjimas, vaizdo mastelio didinimo galimybės, radijo signalo perdavimas, analizė ir garso įrašai). Numatytos funkcijos, kurios nėra būtinos, turi būti išjungtos.

130. Šia tema yra nemažai literatūros, įskaitant tarptautinius standartus ir technines specifikacijas, susijusias su fiziniu daugialypės terpės sistemų saugumu[24] ir bendro pobūdžio IT sistemų saugumu[25]. Todėl šiame skirsnyje pateikiama tik bendra šios temos apžvalga.

9.3.1 Organizacinės priemonės

131. Be galimo poreikio atlikti PDAV (žr. *10 skirsnį*), duomenų valdytojai, kurdami savo stebėjimo vaizdo kameromis politiką ir procedūras, turėtų apsvarstyti šias temas:

- Kas yra atsakingas už stebėjimo vaizdo kameromis sistemos valdymą ir veikimą.
- Stebėjimo vaizdo kameromis projekto tikslas ir taikymo sritis.
- Tinkamas ir draudžiamas naudojimas (kur ir kada leidžiamas stebėjimas vaizdo kameromis, o kur ir kada ne; pvz., slaptų kamerų naudojimas ir garso įrašymas kartu su vaizdo įrašymu)[26].
- Skaidrumo priemonės nurodytos *7 skirsnyje (Skaidrumo ir informavimo prievolės).*

[23] Tokių technologijų naudojimas tam tikrais atvejais gali būti netgi privalomas, kad būtų laikomasi 5 straipsnio 1 dalies c punkto. Bet kuriuo atveju jos gali būti geriausios praktikos pavyzdžiai.

[24] IEC TS 62045 „Daugialypės terpės saugumas: naudojamos ir nenaudojamos įrangos ir sistemų privatumo apsaugos gairės“.

[25] ISO/IEC 27000 – Informacijos saugumo valdymo sistemų serija.

[26] Tai gali priklausyti nuo nacionalinių įstatymų ir sektoriaus taisyklių.

- Vaizdo įrašo įrašymo būdas ir trukmė, įskaitant su saugumo incidentais susijusių vaizdo įrašų archyvavimą.
- Kas turi dalyvauti atitinkamuose mokymuose ir kada.
- Kas ir kokiais tikslais turi prieigą prie vaizdo įrašų.
- Veiklos procedūros (pvz., kas ir iš kur stebi vaizdo kamerų fiksuojamą vaizdą, kokių veiksmų reikia imtis, jeigu padaromas duomenų saugumo pažeidimas).
- Kokių procedūrų turi laikytis išorės šalys prašydamos įrašyti vaizdo įrašus ir kokios yra tokių prašymų atmetimo arba patenkinimo procedūros.
- Stebėjimo vaizdo kameromis sistemos viešojo pirkimo, įrengimo ir techninės priežiūros procedūros.
- Incidentų valdymo ir atkūrimo procedūros.

9.3.2 Techninės priemonės

132. **Sistemos saugumas** reiškia visų sistemos komponentų **fizinį saugumą** ir sistemos vientisumą, t. y. **apsauga nuo tyčinio ir netyčinio įsikišimo į jos įprastą veikimą ir atsparumas tokiam įsikišimui** ir **prieigos kontrolė**. Duomenų saugumas reiškia **konfidencialumą** (duomenys yra prieinami tik tiems asmenims, kuriems suteikta prieiga), **vientisumą** (prevenciją nuo duomenų praradimo arba manipuliavimo jais) ir **prieinamumą** (su duomenimis galima susipažinti tuomet, kai tai būtina).

133. **Fizinis saugumas** yra gyvybiškai svarbi duomenų apsaugos dalis ir pirmoji gynybos priemonė, nes ji padeda apsaugoti stebėjimo vaizdo kameromis sistemą nuo vagystės, vandalizmo, gaivalinių nelaimių, žmogaus sukeltų katastrofų ir atsitiktinės žalos (pvz., viršįtampiai, ekstremalios temperatūros ir išsiliejusi kava). Analoginių sistemų atveju fizinis saugumas atlieka pagrindinį vaidmenį užtikrinant sistemų apsaugą.

134. **Sistemos ir duomenų saugumas**, t. y. apsauga nuo tyčinio ir netyčinio kišimosi į jos įprastą veikimą, gali reikšti:

- Visos stebėjimo vaizdo kameromis sistemos infrastruktūros apsaugą (įskaitant nuotolines kameras, kabelių tiesimą ir energijos tiekimą) nuo fizinio sugadinimo ir vagystės;
- Filmuotos vaizdo medžiagos apsaugą perduodant ją ryšių kanalais, apsaugotais nuo perėmimo;
- Duomenų šifravimą;
- Aparatinės ir programinės įrangos naudojimu grindžiamų sprendimo būdų, pavyzdžiui, užkardų, antivirusinių ar įsibrovimo aptikimo sistemų, naudojimą siekiant apsisaugoti nuo kibernetinių išpuolių;
- Komponentų, programinės įrangos ir tarpusavio jungčių gedimų aptikimą;
- Priemones, kuriomis atkuriamas sistemos prieinamumas ir prieiga prie jos fizinio arba techninio incidento atveju.

135. **Prieigos kontrolė** padeda užtikrinti, kad prieiga prie sistemos ir duomenų būtų suteikta tik įgaliotiems asmenims, kartu neleidžiant to padaryti įgaliojimų neturintiems asmenims. Taikant fizines ir logines prieigos kontrolės priemones:

- Užtikrinama visų patalpų, kuriose stebėsena vykdoma naudojant stebėjimą vaizdo kameromis ir kuriose saugoma filmuota vaizdo medžiaga, apsauga nuo neprižiūrimos trečiųjų šalių prieigos;
- Monitoriai išdėstomi (ypač kai jie yra atvirose vietose, pvz., registratūroje) taip, kad juos galėtų matyti tik leidimą turintys operatoriai;
- Apibrėžiamos ir vykdomos fizinės ir loginės prieigos suteikimo, keitimo ir atšaukimo procedūros;

- Įgyvendinami naudotojo tapatybės nustatymo ir leidimų išdavimo, įskaitant slaptažodžių ilgį ir keitimo dažnumą, būdai ir priemonės;
- Įrašomi ir reguliariai peržiūrimi naudotojo atlikti veiksmai (susiję su sistema ir duomenimis);
- Nuolat stebimi ir nustatomi prieigos trūkumai ir kuo greičiau šalinami nustatyti trūkumai.

10 POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

136. Pagal BDAR 35 straipsnio 1 dalį reikalaujama, kad duomenų valdytojai atliktų poveikio duomenų apsaugai vertinimus (PDAV), jeigu, atsižvelgiant į duomenų tvarkymo rūšį, tikėtina, kad duomenų tvarkymas kels didelę riziką fizinių asmenų teisėms ir laisvėms. BDAR 35 straipsnio 3 dalies c punkte nustatyta, kad duomenų valdytojai privalo atlikti poveikio duomenų apsaugai vertinimus, jeigu duomenų tvarkymas reiškia sisteminę viešai prieinamos vietos stebėseną dideliu mastu. Be to, pagal BDAR 35 straipsnio 3 dalies b punktą poveikio duomenų apsaugai vertinimą taip pat reikalaujama atlikti tais atvejais, kai duomenų valdytojas ketina dideliu mastu tvarkyti asmens duomenis.

137. Poveikio duomenų apsaugai vertinimo gairėse[27] pateikiamos papildomos rekomendacijos ir išsamesni pavyzdžiai, susiję su stebėjimu vaizdo kameromis (pvz., dėl „kamerų sistemos naudojimo vairavimo įpročiams greitkeliuose stebėti“). Pagal BDAR 35 straipsnio 4 dalį reikalaujama, kad kiekviena priežiūros institucija skelbtų apie tas duomenų tvarkymo operacijų rūšis, dėl kurių jų šalyje privaloma atlikti PDAV. Šiuos sąrašus paprastai galima rasti institucijų svetainėse. Atsižvelgiant į tipinius stebėjimo vaizdo kameromis tikslus (žmonių ir turto apsauga, nusikalstamų veikų nustatymas, prevencija ir kontrolė, įrodymų rinkimas į įtariamųjų biometrinių duomenų nustatymas), galima pagrįstai daryti prielaidą, kad PDAV reikės atlikti dėl daugumos stebėjimo vaizdo kameromis atvejų. Todėl duomenų valdytojai turėtų atidžiai susipažinti su šiais dokumentais, kad nustatytų, ar tokį vertinimą reikia atlikti ir prireikus jį atlikti. Remiantis atlikto PDAV rezultatais, reikėtų nustatyti, kokias apsaugos priemones įgyvendins duomenų valdytojas.

138. Taip pat svarbu pažymėti, kad jeigu iš PDAV rezultatų matyti, kad dėl duomenų tvarkymo kiltų didelė rizika nepaisant duomenų valdytojo suplanuotų saugumo priemonių, tuomet prieš pradedant tvarkyti duomenis reikėtų pasikonsultuoti su atitinkama priežiūros institucija. Išsamią informaciją apie išankstines konsultacijas galima rasti 36 straipsnyje.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

(Andrea Jelinek)

[27] WP 248, 1-oji peržiūrėta versija, Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų, patvirtino EDAV.