Suunised 3/2019 isikuandmete töötlemise kohta videoseadmetes

Versioon 2.0

Vastu võetud 29. jaanuaril 2020

Versiooniajalugu

Versioon 2.0	29. jaanuar 2020	Suuniste vastuvõtmine pärast avalikku konsultatsiooni
Versioon 1.0	10. juuli 2019	Suuniste vastuvõtmine avalikuks konsulteerimiseks

Sisukord

Euroopa Andmekaitsenõukogu,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta; edaspidi „isikuandmete kaitse üldmäärus“) artikli 70 lõike 1 punkti e,

võttes arvesse Euroopa Majanduspiirkonna (EMP) lepingut, eriti selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018[1],

võttes arvesse kodukorra artiklit 12 ja artiklit 22,

ON VASTU VÕTNUD JÄRGMISED SUUNISED

1 SISSEJUHATUS

1. Videoseadmete aktiivne kasutamine mõjutab kodanike käitumist. Selliste vahendite ulatuslik rakendamine paljudes eluvaldkondades paneb üksikisikule lisasurve vältida võimaliku normist kõrvalekaldumisena tajutava käitumise avastamist. Tegelikult võivad need tehnoloogialahendused piirata anonüümse liikumise ja teenuste anonüümse kasutamise võimalusi ning üldiselt ka märkamatuks jäämise võimalust. See avaldab andmekaitsele väga suurt mõju.

2. Kuigi üksikisikud võivad tunda end mugavalt, kui tegemist on näiteks teataval turvaeesmärgil sisse seatud videovalvega, tuleb luua tagatised, et vältida väärkasutust täiesti teistsugustel ja andmesubjekti jaoks ootamatutel eesmärkidel (nt turundus, töötajate tulemuslikkuse jälgimine jne). Lisaks võetakse nüüd kasutusele arvukalt vahendeid, mis võimaldavad salvestatud kujutisi ära kasutada ja muuta tavapärased kaamerad nutikaamerateks. Videote abil loodavate andmete hulk koos nende vahendite ja tehnikalahendustega suurendab teisese kasutamise (olenemata sellest, kas see on seotud süsteemile algselt määratud eesmärgiga või mitte) või isegi väärkasutuse ohtu. Videovalve puhul tuleks alati hoolikalt arvesse võtta isikuandmete kaitse üldmääruses sätestatud üldpõhimõtteid (artikkel 5).

3. Videovalvesüsteemid muudavad mitmeti viisi, kuidas avaliku ja erasektori spetsialistid toimivad eravaldustes või avalikes kohtades, et suurendada turvalisust, teha sihtrühma analüüsi, pakkuda personaalset reklaami jne. Videovalve on muutunud aruka videoanalüüsi üha suurema rakendamise tulemusena väga tõhusaks. Selline tehnika võib olla rohkem sekkuv (nt keerukas biomeetriline tehnoloogia) või vähem sekkuv (nt lihtsad loendamisalgoritmid). Üldiselt on üha keerulisem anonüümseks jääda ja privaatsust säilitada. Eri olukordades võivad tekkida erinevad andmekaitsega seotud probleemid, samuti on õiguslik analüüs konkreetsest kasutatavast tehnoloogiast olenevalt erinev.

[1] Kõiki selle arvamuse viiteid liikmesriikidele tuleb mõista kui viiteid EMP liikmesriikidele.

4. Peale privaatsusprobleemide esineb ka nende seadmete võimalike riketega ja neist tuleneva võimaliku kallutatusega seotud riske. Uurijate teatel toimib näotuvastuseks, äratundmiseks või analüüsiks kasutatav tarkvara erinevalt olenevalt tuvastatava isiku vanusest, soost ja etnilisest kuuluvusest. Algoritmid toimiksid erinevatel demograafilistel alustel ja seega võib näotuvastuse kallutatus suurendada ühiskonna eelarvamusi. Seetõttu peavad vastutavad töötlejad tagama ka selle, et videovalvest saadavate biomeetriliste andmete töötlemise asjakohasust ja tagatiste piisavust hinnatakse korrapäraselt.

5. Videovalve ei ole vaikimisi vajadus, juhul kui selle eesmärgi saavutamiseks on olemas muid vahendeid. Vastasel juhul võivad kultuurinormid muutuda, nii et privaatsuse puudumist hakatakse tunnistama üldise eeldusena.

6. Käesolevate suuniste eesmärk on anda juhiseid selle kohta, kuidas kohaldada isikuandmete kaitse üldmäärust seoses isikuandmete töötlemisega videoseadmetes. Näited ei ole ammendavad ja üldisi põhjendusi saab kohaldada kõigi võimalike kasutusvaldkondade suhtes.

2 KOHALDAMISALA[2]

2.1 Isikuandmed

7. Teatava ala süstemaatiline automatiseeritud jälgimine optiliste või audiovisuaalsete vahendite abil peamiselt vara või üksikisiku elu ja tervise kaitsmise eesmärgil on saavutanud märkimisväärse ulatuse. Selle tegevuse käigus kogutakse ja säilitatakse visuaalset või audiovisuaalset teavet kõikide isikute kohta, kes sisenevad jälgitavale alale ja on oma välimuse või muude konkreetsete elementide põhjal tuvastatavad. Nende andmete alusel võib kindlaks teha asjaomaste isikute isikusamasuse. Samuti võimaldab see isikuandmeid isikute konkreetsel alal viibimise ja käitumise seisukohast edasi töödelda. Nende andmete väärkasutamise oht suureneb vastavalt jälgitava ala mõõtmetele ja seda ala kasutavate inimeste arvule. Seda asjaolu kajastatakse isikuandmete kaitse üldmääruse artikli 35 lõike 3 punktis c, milles nõutakse andmekaitsealase mõjuhinnangu tegemist avalike alade ulatusliku süstemaatilise jälgimise korral, ning artikli 37 lõike 1 punktis b, milles nõutakse, et volitatud töötlejad määraksid andmekaitseametniku, kui töötlemistoiminguga kaasneb andmesubjektide korrapärane ja süstemaatiline jälgimine.

8. Määrust ei kohaldata siiski selliste andmete töötlemise suhtes, mis ei viita kuidagi isikule, näiteks kui isikut ei ole võimalik otseselt või kaudselt tuvastada.

> Näide. Isikuandmete kaitse üldmäärust ei kohaldata võltskaamerate suhtes (st kaamerate suhtes, mis ei tööta kaamerana ja ei töötle seega isikuandmeid). *Küll aga võidakse mõnes liikmesriigis kohaldada selle suhtes muid õigusakte.*
>
> Näide. Suurtel kõrgustel tehtud salvestised kuuluvad isikuandmete kaitse üldmääruse kohaldamisalasse üksnes juhul, kui töödeldavaid andmeid saab neis tingimustes seostada konkreetse isikuga.
>
> Näide. Autosse on paigaldatud parkimisabi eesmärgil videokaamera. Isikuandmete kaitse üldmäärust ei kohaldata, kui kaamera on konstrueeritud või seda on kohandatud nii, et see ei kogu füüsilise isikuga seotud teavet (nt numbrimärgid või teave, mille abil on võimalik möödujaid tuvastada).

9.

2.2 Õiguskaitsedirektiivi (direktiiv (EL) 2016/680) kohaldamine

10. Direktiivi (EL) 2016/680 kohaldamisalasse kuulub eelkõige isikuandmete töötlemine, mida teostavad pädevad asutused süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil.

2.3 Kodust tegevust käsitlev erand

11. Vastavalt isikuandmete kaitse üldmääruse artikli 2 lõike 2 punktile c ei kuulu määruse kohaldamisalasse isikuandmete töötlemine, kui isikuandmeid töötleb füüsiline isik eranditult isiklike või koduste tegevuste käigus.[3]

---

[2] Euroopa Andmekaitsenõukogu märgib, et kui isikuandmete kaitse üldmäärus seda lubab, võidakse kohaldada liikmesriikide õigusaktides sätestatud erinõudeid.

[3] Vt ka põhjendus 18.

12. Seda sätet – nn kodust tegevust käsitlevat erandit – tuleb videovalve kontekstis tõlgendada kitsalt. Nagu on leidnud Euroopa Kohus, tuleb seega nn kodust tegevust käsitlevat erandit „tõlgendada nii, et see puudutab ainult tegevust, mis mahub isiku era- või perekonnaelu raamidesse, nagu see ilmselgelt ei ole siis, kui isikuandmete töötlemine seisneb nende internetis avaldamises, nii et andmed on tehtud kättesaadavaks määratlemata isikute ringile“.[4] Lisaks, kui videovalvesüsteem isikuandmete pidevat salvestamist ja säilitamist hõlmavas osas „kasvõi osaliselt ulatub avalikku ruumi ja on seetõttu suunatud selle vahendi abil andmete töötleja isiklikust sfäärist väljapoole, ei saa seda pidada tegevuseks, millega tegeldakse üksnes „isiklikel või kodustel“ eesmärkidel direktiivi 95/46 artikli 3 lõike 2 teise taande tähenduses“[5].

13. Eraisiku valdustes kasutatavad videoseadmed võivad kuuluda kodust tegevust käsitleva erandi alla. See sõltub mitmest tegurist, mida tuleb järelduse tegemisel arvesse võtta. Lisaks eespool nimetatud elementidele, mis on esitatud Euroopa Kohtu otsustes, peab koduse videovalve kasutaja uurima, kas tal on andmesubjektiga teatavat laadi isiklik suhe, kas jälgimise ulatus või sagedus viitab temapoolsele teatavat laadi kutsealasele tegevusele ning milline on jälgimise võimalik kahjulik mõju andmesubjektidele. Mõne eespool nimetatud elemendi olemasolu ei tähenda tingimata, et töötlemine ei kuulu kodust tegevust käsitleva erandi alla; selle kindlakstegemiseks on vaja teha üldine hindamine.

Näide. Turist salvestab oma puhkuse jäädvustamiseks videoid nii mobiiltelefoni kui ka videokaameraga. Ta näitab salvestist sõpradele ja pereliikmetele, kuid ei tee seda kättesaadavaks määramata arvule inimestele. See kuulub kodust tegevust käsitleva erandi alla.

Näide. Mägilaskumist harrastav jalgrattur tahab jäädvustada oma laskumise toimekaameraga. Ta sõidab kõrvalises piirkonnas ja kavatseb kasutada salvestisi üksnes kodus isikliku meelelahutuse otstarbel. See kuulub kodust tegevust käsitleva erandi alla isegi siis, kui isikuandmeid teataval määral töödeldakse.

Näide. Keegi jälgib ja salvestab oma isiklikku aeda. Krunt on tarastatud ning aias käivad korrapäraselt ainult vastutav töötleja ise ja tema pereliikmed. See kuulub kodust tegevust käsitleva erandi alla, tingimusel et videovalve ei laiene isegi osaliselt avalikule alale või naaberkrundile.

14.

[4] Kohtuotsus, Euroopa Kohus, 6. november 2003, kriminaalasi, milles süüdistatav on Bodil Lindqvist, C-101/01, punkt 47.

[5] Kohtuotsus, Euroopa Kohus, 11. detsember 2014, František Ryneš *vs.* Úřad pro ochranu osobních údajů, C-212/13, punkt 33.

3 ANDMETÖÖTLUSE SEADUSLIKKUS

15. Enne andmetöötluse kasutamist tuleb selle eesmärgid täpselt kindlaks määrata (artikli 5 lõike 1 punkt b). Videovalve võib täita mitut eesmärki, näiteks toetada kinnisvara ja muu vara kaitset, toetada üksikisikute elu ja füüsilise puutumatuse kaitset ning koguda tõendeid tsiviilhagide jaoks.[6] Need jälgimiseesmärgid tuleb kirjalikult dokumenteerida (artikli 5 lõige 2) ja iga kasutatava valvekaamera kohta täpselt kindlaks määrata. Kaamerad, mida samal eesmärgil kasutab üks vastutav töötleja, võib koos dokumenteerida. Lisaks tuleb kooskõlas artikliga 13 (*vt 7. jagu „Läbipaistvus ja teavitamiskohustused“*) teavitada andmesubjekte töötlemise eesmärgist. Videovalvel, mis põhineb üksnes „turvalisuse“ või „teie turvalisuse“ eesmärgil, ei ole piisavalt täpne eesmärk (artikli 5 lõike 1 punkt b). Pealegi on see vastuolus põhimõttega, et isikuandmete töötlemine peab olema seaduslik, õiglane ja andmesubjektile läbipaistev (vt artikli 5 lõike 1 punkt a).

16. Põhimõtteliselt võib videovalve andmete töötlemise õiguslikuks aluseks olla iga artikli 6 lõike 1 kohane õiguslik alus. Kui liikmesriigi õiguses on sätestatud videovalve kohustus, kohaldatakse näiteks artikli 6 lõike 1 punkti c.[7] Praktikas kasutatakse siiski kõige tõenäolisemalt järgmisi sätteid:

- artikli 6 lõike 1 punkt f (õigustatud huvi),
- artikli 6 lõike 1 punkt e (vajalik avalikes huvides oleva ülesande täitmiseks või avaliku võimu teostamiseks).

Üsna erandlikel juhtudel võib vastutav töötleja kasutada õigusliku alusena artikli 6 lõike 1 punkti a (nõusolek).

3.1 Õigustatud huvi – artikli 6 lõike 1 punkt f

17. Artikli 6 lõike 1 punkti f õiguslik hinnang peaks põhinema järgmistel kriteeriumidel kooskõlas põhjendusega 47.

3.1.1 Õigustatud huvi olemasolu

18. Videovalve on seaduslik, kui see on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused (artikli 6 lõike 1 punkt f). Vastutava töötleja või kolmanda isiku õigustatud huvid võivad olla õiguslikud,[8] majanduslikud või mittemateriaalsed.[9] Vastutav töötleja peaks siiski arvestama, et kui andmesubjektid esitavad jälgimise suhtes vastuväiteid kooskõlas artikliga 21, võib vastutav töötleja jätkata kõnealuse andmesubjekti videovalvet üksnes juhul, kui on olemas *mõjuv* õigustatud huvi, mis kaalub üles andmesubjekti huvid, õigused ja vabadused, või õigusnõuete koostamise, esitamise või kaitsmise eesmärgil.

19. Võttes arvesse tegelikku ja ohtlikku olukorda, võib eesmärk kaitsta vara sissemurdmise, varguse või vandalismi eest kujutada endast õigustatud huvi kasutada videovalvet.

---

[6] Tsiviilhagide jaoks tõendite kogumise eeskirjad on liikmesriigiti erinevad.

[7] Nendes suunistes ei analüüsita ega käsitleta üksikasjalikult liikmesriikide õigusakte, mis võivad liikmesriigiti erineda.

[8] Kohtuotsus, Euroopa Kohus, 4. mai 2017, Rīgas satiksme, C-13/16.

[9] Vt WP 217, artikli 29 töörühm.

20. Õigustatud huvi peab olema tegelikult olemas ja see peab olema aktuaalne küsimus (st see ei tohi olla fiktiivne ega spekulatiivne)[10]. Enne valvetegevuse alustamist peab olema käes tegelik hädaolukord, näiteks varasem kahju või varasemad tõsised juhtumid. Võttes arvesse vastutuse põhimõtet, soovitatakse vastutavatel töötlejatel dokumenteerida asjaomased juhtumid (kuupäev, viis, rahaline kahju) ja nendega seotud kriminaalsüüdistused. Need dokumenteeritud juhtumid võivad olla kindlaks tõendiks õigustatud huvi olemasolu kohta. Õigustatud huvi olemasolu ja jälgimise vajalikkust tuleks korrapäraselt uuesti hinnata (nt kord aastas olenevalt asjaoludest).

> Näide. Kaupluse omanik soovib avada uue poe ja paigaldada vandalismi ärahoidmiseks videovalvesüsteemi. Ta suudab statistika abil näidata, et lähinaabruses on vandalismi tõenäosus suur. Kasu on ka naaberkaupluste kogemusest. Ei ole vajalik, et asjaomane vastutav töötleja oleks kahju kandnud. Kui naabruskonnas tekitatud kahju viitab ohule või sarnasele riskile, võib see järelikult viidata õigustatud huvi olemasolule. Kuritegevuse riikliku või üldise statistika esitamisest ilma kõnealuse piirkonna või seda konkreetset kauplust ähvardavate ohtude analüüsita siiski ei piisa.

21.

22. Vahetud ohuolukorrad võivad kujutada endast õigustatud huvi, näiteks kui on tegemist panga või vääriskaupu müüva kauplusega (nt juveelipood) või alaga, mis on varaga seotud õigusrikkumiste puhul teadaolevalt tüüpiline kuriteopaik (nt tankla).

23. Isikuandmete kaitse üldmääruses on ka selgelt sätestatud, et avaliku sektori asutused ei saa oma ülesannete täitmisel isikuandmeid töödeldes tugineda õigustatud huvile (artikli 6 lõike 1 teine lause).

3.1.2 Andmetöötluse vajalikkus

24. Isikuandmed peaksid olema asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt („võimalikult väheste andmete kogumine“) – vt artikli 5 lõike 1 punkt c. Enne videovalvesüsteemi paigaldamist peaks vastutav töötleja alati kriitiliselt uurima, kas see meede on esiteks sobiv soovitud tulemuse saavutamiseks ning teiseks piisav ja vajalik selle eesmärkide saavutamiseks. Videovalvemeetmed tuleks valida üksnes juhul, kui töötlemise eesmärki ei ole võimalik mõistlikult saavutada muude vahenditega, mis riivavad vähem andmesubjekti põhiõigusi ja -vabadusi.

25. Olukorras, kus vastutav töötleja soovib ennetada varavastaseid kuritegusid, võiks vastutav töötleja videovalvesüsteemi paigaldamise asemel võtta ka alternatiivseid turvameetmeid, nagu tarastamine, turvatöötajate korrapäraste patrullide sisseseadmine, väravavalvurite kasutamine, parem valgustus, turvalukkude, avamiskindlate akende ja uste paigaldamine või graffitivastase katte või fooliumi paigaldamine seintele. Need meetmed võivad olla sissemurdmise, varguse ja vandalismi vastu sama tõhusad kui videovalvesüsteemid. Vastutav töötleja peab iga juhtumi puhul eraldi hindama, kas sellised meetmed võivad olla mõistlikuks lahenduseks.

26. Enne kaamerasüsteemi kasutamist on vastutav töötleja kohustatud hindama, kus ja millal on videovalvemeetmed tingimata vajalikud. Tavaliselt täidab vastutava töötleja vajadused tema vara ähvardavate ohtude ennetamise järele öösel ja väljaspool tavapärast tööaega töötav valvesüsteem.

[10] Vt WP 217, artikli 29 töörühm, lk 24 jj. Vt ka kohtuotsus, Euroopa Kohus, C-708/18, punkt 44.

27. Üldjuhul lõpeb vajadus kasutada videovalvet vastutavate töötlejate valduste kaitsmiseks vara piiridel.[11] Esineb siiski juhtumeid, kus vara jälgimine ei ole tõhusa kaitse tagamiseks piisav. Mõnel üksikjuhul võib olla vajalik laiendada videovalvet valduste vahetule ümbrusele. Sel juhul peaks vastutav töötleja kaaluma füüsiliste ja tehniliste vahendite kasutamist, näiteks mitteasjakohaste alade blokeerimist või pikseldamise abil hägustamist.

> Näide. Raamatupood soovib kaitsta oma ruume vandalismi eest. Üldjuhul peaksid kaamerad filmima üksnes ruume, sest ei ole tarvidust valvata sel eesmärgil raamatupoe ruumide naabruses olevaid valdusi või avalikke alasid.

28.

29. Töötlemise vajalikkust puudutavad küsimused tekivad ka seoses tõendite säilitamise viisiga. Mõnel juhul võib olla vaja kasutada musta kasti lahendusi, mille puhul salvestis pärast teatavat säilitamisaega automaatselt kustutatakse ja sellele pääseb juurde ainult juhtumi toimumisel. Muudes olukordades ei pruugi videomaterjali salvestamine üldse vajalik olla, vaid selle asemel on asjakohasem kasutada reaalajas jälgimist. Otsus, kas kasutada musta kasti lahendust või reaalajas jälgimist, peaks põhinema ka taotletaval eesmärgil. Kui videovalve eesmärk on näiteks tõendite säilitamine, siis reaalajal põhinevad meetodid tavaliselt ei sobi. Ka võib reaalajas jälgimine olla mõnikord sekkuvam kui materjali salvestamine ja automaatne kustutamine pärast piiratud ajavahemikku (nt kui keegi jälgib kuvarit pidevalt, võib see olla sekkuvam kui see, et kuvarit ei olegi ja materjal salvestatakse otse musta kasti). Selles kontekstis tuleb arvesse võtta võimalikult väheste andmete kogumise põhimõtet (artikli 5 lõike 1 punkt c). Samuti tuleks meeles pidada, et vastutav töötleja võib kasutada videovalve asemel turvatöötajaid, kes on võimelised viivitamata reageerima ja sekkuma.

3.1.3 Huvide tasakaalustamine

30. Eeldades, et videovalve on vajalik vastutava töötleja õigustatud huvide kaitsmiseks, võib videovalvesüsteemi kasutusele võtta üksnes juhul, kui andmesubjekti huvid või põhiõigused ja -vabadused ei kaalu üles vastutava töötleja või kolmanda isiku õigustatud huve (nt vara või füüsilise puutumatuse kaitse). Vastutav töötleja peab kaaluma, 1) mil määral mõjutab jälgimine üksikisikute huve, põhiõigusi ja -vabadusi ning 2) kas see põhjustab andmesubjekti õiguste rikkumist või negatiivseid tagajärgi tema õigustele. Huvide tasakaalustamine on tegelikult kohustuslik. Hoolikalt tuleb hinnata ja tasakaalustada ühelt poolt põhiõigusi ja -vabadusi ning teiselt poolt vastutava töötleja õigustatud huve.

> Näide. Eraparklat pidav ettevõtja on dokumenteerinud pargitud autodest varastamise korduva probleemi. Parkla on avatud ala, kuhu igaüks võib hõlpsasti minna, kuid see on selgelt tähistatud ala ümber paigutatud märkide ja teetõkistega. Parkimisettevõtjal on õigustatud huvi (varguste vältimine klientide autodest) jälgida seda ala probleemsetel kellaaegadel. Andmesubjektide jälgimine toimub piiratud aja jooksul, nad ei ole sellel alal meelelahutuslikel eesmärkidel ning varguste ärahoidmine on ka nende endi huvides. Vastutava töötleja õigustatud huvi kaalub kirjeldatud juhul üles andmesubjektide huvi, et neid ei jälgitaks.
>
> Näide. Restoranipidaja otsustab paigaldada tualettruumidesse videokaamerad, et kontrollida sanitaarruumide korrasolekut. Sellisel juhul kaaluvad andmesubjektide õigused selgelt üles vastutava töötleja huvid, mistõttu ei saa kaameraid sinna paigaldada.

31.

[11] Ka see võib kuuluda mõne liikmesriigi õigusaktide kohaldamisalasse.

3.1.3.1 Juhtumipõhiste otsuste tegemine

32. Kuna huvide tasakaalustamine on määruse kohaselt kohustuslik, tuleb otsus teha igal üksikjuhul eraldi (vt artikli 6 lõike 1 punkt f). Abstraktsetele olukordadele viitamine või sarnaste juhtumite võrdlemine ei ole piisav. Vastutav töötleja peab hindama andmesubjekti õiguste rikkumise ohtu; siinkohal on otsustav kriteerium see, kui intensiivselt sekkutakse üksikisiku õigustesse ja vabadustesse.

33. Intensiivsuse võib muu hulgas määratleda kogutava teabe liigi (teabesisu), ulatuse (teabetihedus, ruumiline ja geograafiline ulatus), asjaomaste andmesubjektide arvu (kas konkreetse arvuna või osana asjaomasest elanikkonnast), kõnealuse olukorra, andmesubjektide rühma tegelike huvide, alternatiivsete vahendite ning andmete hindamise laadi ja ulatuse alusel.

34. Olulised tasakaalustavad tegurid võivad olla jälgitava ala suurus ja jälgitavate andmesubjektide arv. Videovalve kasutamist kõrvalises piirkonnas (nt metsloomade jälgimiseks või elutähtsa taristu, näiteks eraomandis oleva raadioantenni kaitsmiseks) tuleb hinnata teisiti kui videovalvet jalakäijate alal või kaubanduskeskuses.

> Näide. Kui paigaldatakse pardakaamera (nt tõendite kogumiseks õnnetuse korral), on oluline tagada, et kaamera ei salvesta pidevalt liiklust ega tee lähedal viibivaid inimesi. Vastasel juhul ei õigusta huvi kasutada videosalvestist tõendina teoreetilise liiklusõnnetuse korral sellist tõsist sekkumist andmesubjektide õigustesse.[11]

35.

3.1.3.2 Andmesubjektide mõistlikud ootused

36. Põhjenduse 47 kohaselt tuleb õigustatud huvi olemasolu hoolikalt hinnata. Seejuures tuleb arvesse võtta andmesubjekti mõistlikke ootusi tema isikuandmete töötlemise ajal ja kontekstis. Süstemaatilise jälgimise korral võib andmesubjekti ja vastutava töötleja vaheline suhe oluliselt erineda ning mõjutada andmesubjekti võimalikke mõistlikke ootusi. Mõistlike ootuste mõiste tõlgendamine ei tohiks põhineda üksnes kõnealustel subjektiivsetel ootustel. Pigem peab otsustavaks kriteeriumiks olema see, kas objektiivne kolmas isik võib mõistlikult eeldada ja järeldada, et selles konkreetses olukorras teda jälgitakse.

37. Näiteks enamikul juhtudel töötaja tõenäoliselt ei oota, et tööandja jälgib teda töökohal.[12] Peale selle ei oodata jälgimist oma eraaias, eluruumides ega läbivaatus- ja raviruumides. Samamoodi ei ole mõistlik eeldada jälgimist sanitaarruumides või saunas – selliste alade jälgimine on andmesubjekti õiguste tugev riive. Andmesubjektide mõistlik ootus on, et nendel aladel ei tehta videovalvet. Teisalt võib panga klient oodata, et teda jälgitakse pangas või sularahaautomaadi juures.

38. Samuti võivad andmesubjektid eeldada, et neid ei jälgita avalikel aladel, eriti kui neid alasid kasutatakse tavaliselt puhkamiseks, taastumiseks ja vaba aja veetmiseks, samuti kohtades, kus inimesed viibivad ja/või suhtlevad, näiteks istumisalad, restoranilauad, pargid, kinod ja spordirajatised. Siin kaaluvad andmesubjekti huvid või õigused ja vabadused sageli üles vastutava töötleja õigustatud huvid.

> Näide. Andmesubjektid eeldavad, et tualettides neid ei jälgita. Videovalve näiteks õnnetuste ärahoidmise eesmärgil ei ole proportsionaalne.

39.

[12] Vt ka artikli 29 töörühm, arvamus 2/2017 andmete töötlemise kohta töökohal (WP 249), vastu võetud 8. juunil 2017.

40. Märgid, mis teavitavad andmesubjekti videovalvest, ei ole olulised selle kindlaksmääramisel, mida andmesubjekt võib objektiivselt oodata. See tähendab, et kui näiteks märk kaupluse sissepääsu juures teavitab isikut valvest, ei saa kaupluse omanik ainuüksi sel põhjusel eeldada, et klientidel on *objektiivselt* mõistlikud ootused, et neid jälgitakse.

3.2 Vajadus täita avalikes huvides olevat ülesannet või teostada vastutava andmetöötleja avalikku võimu – artikli 6 lõike 1 punkt e

41. Artikli 6 lõike 1 punkti e kohaselt võib isikuandmeid töödelda videovalve kaudu, kui see on vajalik avalikes huvides oleva ülesande täitmiseks või avaliku võimu teostamiseks.[13] Võib juhtuda, et avaliku võimu teostamine ei võimalda sellist töötlemist, kuid muud õiguslikud alused, nagu „tervishoid ja ohutus“ külastajate ja töötajate kaitseks, võivad pakkuda töötlemiseks piiratud võimalusi, võttes siiski arvesse isikuandmete kaitse üldmäärusest tulenevaid kohustusi ja andmesubjektide õigusi.

42. Liikmesriigid võivad säilitada või kehtestada videovalvet käsitlevad konkreetsed õigusaktid, et kohandada isikuandmete kaitse üldmääruse eeskirjade kohaldamist, määrates täpsemalt kindlaks töötlemise erinõuded, tingimusel et see on kooskõlas isikuandmete kaitse üldmääruses sätestatud põhimõtetega (nt säilitamise piirang, proportsionaalsus).

3.3 Nõusolek – artikli 6 lõike 1 punkt a

43. Nõusolek peab olema vabatahtlik, konkreetne, teadlik ja ühemõtteline, nagu on kirjeldatud nõusolekut käsitlevates suunistes.[14]

44. Mis puudutab süstemaatilist jälgimist, siis artikli 7 kohaselt võib andmesubjekti nõusolek olla õiguslik alus ainult erandjuhtudel (vt põhjendus 43). Valve laadist tulenevalt jälgitakse selle tehnoloogia abil korraga teadmata arvu inimesi. Vastutav töötleja ei suuda ilmselt tõendada, et andmesubjekt on andnud enne oma isikuandmete töötlemist nõusoleku (artikli 7 lõige 1). Kui andmesubjekt võtab oma nõusoleku tagasi, on vastutaval töötlejal keeruline tõendada, et isikuandmeid enam ei töödelda (artikli 7 lõige 3).

> Näide. Sportlased võivad taotleda jälgimist üksikute harjutuste sooritamise ajal, et analüüsida oma tehnikat ja tulemusi. Kui aga spordiklubi algatab samal eesmärgil kogu meeskonna jälgimise, ei ole nõusolek sageli kehtiv, sest üksikud sportlased võivad tunda nõusoleku andmiseks survet, et nende keeldumine nõusoleku andmisest ei kahjustaks meeskonnakaaslasi.

45.

[13] Nimetatud töötlemise alus sätestatakse liidu või liikmesriigi õiguses ja see on „vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks“ (artikli 6 lõige 3).

[14] Artikli 29 töörühm, „Suunised määruse (EL) 2016/679 kohase nõusoleku kohta“ (WP 259 rev. 01), mille on heaks kiitnud Euroopa Andmekaitsenõukogu.

46. Kui vastutav töötleja soovib tugineda nõusolekule, on tal kohustus tagada, et iga videovalve all olevale alale sisenev andmesubjekt on andnud oma nõusoleku. Nõusolek peab vastama artikli 7 tingimustele. Tähistatud jälgitavale alale sisenemine (nt inimestel palutakse jälgitavale alale sisenemiseks läbida teatav koridor või värav) ei kujuta endast nõusoleku saamiseks vajalikku avaldust või selget kinnitust andvat toimingut, välja arvatud juhul, kui see vastab artiklites 4 ja 7 sätestatud kriteeriumidele, nagu on kirjeldatud nõusoleku andmist käsitlevates suunistes.[15]

47. Võttes arvesse tööandjate ja töötajate võimu ebavõrdsust, ei tohiks tööandjad enamikul juhtudel tugineda isikuandmete töötlemisel nõusolekule, sest see ei ole tõenäoliselt antud vabatahtlikult. Selles kontekstis tuleks arvesse võtta nõusoleku andmist käsitlevaid suuniseid.

48. Liikmesriigi õiguses või kollektiivlepingutes (sh ettevõttesisesed lepingud) võib ette näha erieeskirjad, millega reguleeritakse töötajate isikuandmete töötlemist töösuhete kontekstis (vt artikkel 88).

[15] Arvesse tuleks võtta artikli 29 töörühma suuniseid määruse (EL) 2016/679 kohase nõusoleku kohta (WP 259 rev. 01), mille on heaks kiitnud Euroopa Andmekaitsenõukogu.

4 VIDEOSALVESTISTE AVALIKUSTAMINE KOLMANDATELE ISIKUTELE

49. Põhimõtteliselt kohaldatakse videosalvestiste kolmandatele isikutele avaldamise suhtes isikuandmete kaitse üldmääruse üldsätteid.

4.1 Videosalvestiste avalikustamine üldiselt kolmandatele isikutele

50. Artikli 4 punktis 2 on avalikustamine määratletud kui edastamine (nt individuaalne teabevahetus), levitamine (nt avaldamine internetis) või muul moel kättesaadavaks tegemine. Kolmandad isikud on määratletud artikli 4 punktis 10. Kui teave avalikustatakse kolmandatele riikidele või rahvusvahelistele organisatsioonidele, kohaldatakse ka artikli 44 ja järgnevate artiklite erisätteid.

51. Isikuandmete mis tahes avalikustamine on isikuandmete eri laadi töötlemine, mille jaoks peab vastutava töötlejal olema artiklis 6 sätestatud õiguslik alus.

> Näide. Vastutaval töötlejal, kes soovib salvestist internetti üles laadida, peab olema selliseks töötlemiseks õiguslik alus, näiteks andmesubjektilt artikli 6 lõike 1 punkti a kohaselt saadud nõusolek.

52.

53. Videosalvestiste edastamine kolmandatele isikutele muul eesmärgil kui see, milleks andmeid koguti, on võimalik artikli 6 lõikes 4 sätestatud eeskirjade kohaselt.

> Näide. Kahjujuhtumite lahendamiseks paigaldatakse tõkkepuu videovalve (parklasse). Kahju tekib ja salvestis edastatakse asja menetlemiseks advokaadile. Sellisel juhul on salvestamisel sama eesmärk mis edastamisel.
>
> Näide. Kahjujuhtumite lahendamiseks paigaldatakse tõkkepuu videovalve (parklasse). Salvestis avaldatakse internetis üksnes meelelahutuslikel põhjustel. Sellisel juhul on eesmärk muutunud ega ole kooskõlas esialgse eesmärgiga. Lisaks oleks sellise töötlemise (avaldamise) õigusliku aluse kindlaksmääramine probleemne.

54.

55. Kolmandast isikust vastuvõtja peab tegema oma õigusliku analüüsi, määrates eelkõige kindlaks oma töötlemise õigusliku aluse vastavalt artiklile 6 (nt materjali vastuvõtmine).

4.2 Videosalvestiste avalikustamine õiguskaitseasutustele

56. Videosalvestiste avalikustamine õiguskaitseasutustele on samuti iseseisev protsess, mis nõuab vastutavalt töötlejalt eraldi põhjendust.

57. Artikli 6 lõike 1 punkti c kohaselt on töötlemine seaduslik, kui see on vajalik vastutava töötleja juriidilise kohustuse täitmiseks. Kuigi kohaldatav politseiõigus kuulub liikmesriikide ainukontrolli alla, on igas liikmesriigis suure tõenäosusega olemas üldnormid, mis reguleerivad tõendite edastamist õiguskaitseasutustele. Andmeid üle andva vastutava töötleja poolne töötlemine on reguleeritud isikuandmete kaitse üldmäärusega. Kui liikmesriigi õigusaktides nõutakse, et vastutav töötleja teeks õiguskaitseasutustega koostööd (nt uurimise käigus), on andmete üleandmise õiguslik alus artikli 6 lõike 1 punkti c kohane juriidiline kohustus.

58. Seega ei ole artikli 6 lõikes 4 sätestatud eesmärgi piiritlemine sageli probleemne, sest avalikustamine toimub sõnaselgelt liikmesriigi õiguse kohaselt. Seetõttu ei ole eesmärgi muutmise erinõuete kaalumine punktide a–e tähenduses vajalik.

59. Näide. Kaupluse omanik filmib kaameraga kaupluse sissepääsu. Salvestisel on näha isik, kes varastab teise isiku rahakoti. Politsei palub vastutaval töötlejal uurimisele kaasa aitamiseks materjal üle anda. Sellisel juhul kasutab kaupluse omanik artikli 6 lõike 1 punkti c kohast õiguslikku alust (juriidiline kohustus) koostoimes asjakohaste liikmesriigi õigusaktidega töötlemise ülemineku kohta.

60. Näide. Kauplusesse paigaldatakse turvakaalutlustel kaamera. Kaupluse omanik usub, et ta on salvestanud midagi kahtlast ja otsustab saata materjali politseile (ilma et käimasoleva uurimise kohta oleks vähimatki viidet). Sellisel juhul peab kaupluse omanik hindama, kas on täidetud (enamikul juhtudel) artikli 6 lõike 1 punktis f sätestatud tingimused. Tavaliselt on see nii, kui kaupluse omanikul on põhjendatud kahtlus, et toime on pandud kuritegu.

61. Kui isikuandmeid töötlevad õiguskaitseasutused ise, ei järgi nad mitte isikuandmete kaitse üldmäärust (vt artikli 2 lõike 2 punkt d), vaid õiguskaitsedirektiivi (direktiiv (EL) 2016/680).

5 ANDMETE ERILIIKIDE TÖÖTLEMINE

62. Videovalvesüsteemid koguvad tavaliselt suurel hulgal isikuandmeid, mis võivad paljastada väga isiklikke andmeid ja isegi andmete eriliike. Algselt video kaudu kogutud andmeid, mis on näiliselt väheolulised, võidakse kasutada muu teabe tuletamiseks, et saavutada teistsugune eesmärk (nt saada ülevaade isiku harjumustest). Siiski ei peeta videovalvet mitte alati isikuandmete eriliikide töötlemiseks.

> Näide. Iseenesest ei loeta isikuandmete eriliigiks videosalvestist, kus on näha prille kandvat või ratastooli kasutavat andmesubjekti.

63.

64. Kui aga seda videosalvestist töödeldakse andmete eriliikide tuletamiseks, kohaldatakse artiklit 9.

> Näide. Poliitilisi seisukohti võib tuletada näiteks piltidest, millel on näha tuvastatavad andmesubjektid, kes osalevad üritusel, streigis jne. See kuuluks artikli 9 kohaldamisalasse.
>
> Näide. Kui haiglas paigaldatakse patsiendi terviseseisundi jälgimiseks videokaamera, käsitatakse seda isikuandmete eriliikide töötlemisena (artikkel 9).

65.

66. Üldiselt tuleks videovalvesüsteemi paigaldamisel võtta hoolikalt arvesse võimalikult väheste andmete kogumise põhimõtet. Seega peaks vastutav töötleja isegi juhul, kui artikli 9 lõiget 1 ei kohaldata, püüdma eesmärgist olenemata alati vähendada ohtu, et salvestised paljastavad muid tundlikke andmeid (lisaks artiklile 9).

> Näide. Kiriku videovalve ei kuulu iseenesest artikli 9 kohaldamisalasse. Vastutav töötleja peab siiski läbi viima artikli 6 lõike 1 punkti f kohase eriti hoolika hindamise, võttes andmesubjekti huvide hindamisel arvesse andmete laadi ja muude tundlike andmete (lisaks artiklile 9) kogumise ohtu.

67.

68. Kui videovalvesüsteemi kasutatakse andmete eriliikide töötlemiseks, peab vastutav töötleja tegema kindlaks nii artikli 9 kohase andmete eriliikide töötlemise erandi (st erandi üldreeglist, et andmete eriliike ei tohiks töödelda) kui ka artikli 6 kohase õigusliku aluse.

69. Näiteks võidakse teoreetiliselt ja erandjuhul kasutada artikli 9 lõike 2 punkti c („[...] töötlemine on vajalik selleks, et kaitsta andmesubjekti või teise füüsilise isiku elulisi huve [...]“), kuid vastutav töötleja peaks seda põhjendama kui absoluutset vajadust kaitsta isiku elulisi huve ja tõendama, et see „[...] andmesubjekt on füüsiliselt või õiguslikult võimetu nõusolekut andma“. Lisaks ei lubata vastutaval töötlejal süsteemi kasutada ühelgi muul põhjusel.

70. Siinkohal on oluline märkida, et iga artiklis 9 loetletud erand ei õigusta tõenäoliselt andmete eriliikide töötlemist videovalve abil. Täpsemalt öeldes ei saa vastutavad töötlejad, kes neid andmeid videovalve raames töötlevad, tugineda artikli 9 lõike 2 punktile e, mis lubab töödelda isikuandmeid, mille andmesubjekt on ilmselgelt avalikustanud. Lihtsalt kaamera vaatevälja sisenemine ei tähenda, et andmesubjekt kavatseb avalikustada temaga seotud andmete eriliike.

71. Pealegi nõuab andmete eriliikide töötlemine suuremat ja pidevat tähelepanelikkust teatavate kohustuste suhtes; näiteks vajaduse korral kõrgetasemelist turvalisust ja andmekaitse mõjuhinnangut.

Näide. Tööandja ei tohi streikijate tuvastamiseks kasutada videovalvesalvestisi, millel kujutatakse demonstratsiooni.

72.

5.1 Üldised kaalutlused biomeetriliste andmete töötlemisel

73. Biomeetriliste andmete ja eelkõige näotuvastuse kasutamisega kaasnevad suuremad ohud andmesubjektide õigustele. On väga oluline, et sellise tehnoloogia kasutamisel järgitaks nõuetekohaselt isikuandmete kaitse üldmääruses sätestatud seaduslikkuse, vajalikkuse, proportsionaalsuse ja võimalikult väheste andmete kogumise põhimõtteid. Kuigi selle tehnoloogia kasutamist võib pidada eriti tõhusaks, peaksid vastutavad töötlejad kõigepealt hindama mõju põhiõigustele ja -vabadustele ning kaaluma töötlemise õiguspärase eesmärgi saavutamiseks vähem sekkuvate vahendite kasutamist.

74. Selleks et kvalifitseerida andmed isikuandmete kaitse üldmääruses määratletud biomeetriliste andmetena, peab toorandmete, näiteks isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste töötlemine hõlmama nende omaduste mõõtmist. Kuna biomeetrilised andmed on selliste mõõtmiste tulemus, on isikuandmete kaitse üldmääruse artikli 4 punktis 14 sätestatud, et need andmed on „[...] konkreetse tehnilise töötlemise abil saadavad isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist [...]“. Isikust tehtud videosalvestist ei saa siiski iseenesest käsitada biomeetriliste andmetena artikli 9 tähenduses, kui seda ei ole spetsiaalselt tehniliselt töödeldud, et aidata kaasa isiku tuvastamisele.[16]

75. Selleks et töötlemist saaks käsitada isikuandmete eriliikide töötlemisena (artikkel 9), on nõutav, et biomeetrilisi andmeid töödeldakse „füüsilise isiku kordumatuks tuvastamiseks“.

76. Kokkuvõttes tuleb artikli 4 punkti 14 ja artiklit 9 silmas pidades võtta arvesse kolme kriteeriumi:

- **andmete laad:** andmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta;
- **töötlemisvahendid ja -viis:** „konkreetse tehnilise töötlemise abil saadavad“ andmed;
- **töötlemise eesmärk:** andmeid tuleb kasutada füüsilise isiku kordumatuks tuvastamiseks.

77. Videovalve, sealhulgas biomeetrilise tuvastamise funktsiooni kasutamine eraõiguslike üksuste poolt nende enda tarbeks (nt turundus, statistika või isegi turvalisus) nõuab enamikul juhtudel kõigi andmesubjektide sõnaselget nõusolekut (artikli 9 lõike 2 punkt a), kuid kohaldada võib ka mõnda muud artiklis 9 sätestatud sobivat erandit.

[16] Seda analüüsi toetab isikuandmete kaitse üldmääruse põhjendus 51, milles märgitakse, et „[...] [f]otode töötlemist ei peaks süstemaatiliselt käsitlema isikuandmete eriliikide töötlemisena, kuna need on hõlmatud üksnes biomeetriliste andmete määratlusega, kui neid töödeldakse konkreetsete tehniliste vahenditega, mis võimaldavad füüsilist isikut kordumatult tuvastada või autentida. […]“.

Näide. Eraettevõtja asendab oma teenuse parandamiseks lennujaamas asuvad reisijate tuvastamise kontrollpunktid (pagasi äraandmine, pardaleminek) videovalvesüsteemidega, mis kasutavad näotuvastustehnikat, et kontrollida nende reisijate isikusamasust, kes on sellise menetlusega nõustunud. Kuna töötlemine kuulub artikli 9 kohaldamisalasse, peavad reisijad, kes on eelnevalt andnud oma sõnaselge ja teadliku nõusoleku, registreeruma näiteks automaatterminalis, et luua ja registreerida oma näokujutis, mis on seotud nende pardakaardi ja isikuga. Näotuvastusega kontrollpunktid peavad olema selgelt eraldatud, näiteks peab süsteem olema paigaldatud estakaadile, et vältida nende isikute biomeetriliste mallide salvestamist, kes ei ole nõusolekut andnud. Biomeetrilise süsteemiga varustatud estakaadi kasutavad ainult reisijad, kes on eelnevalt andnud nõusoleku ja registreerunud.

Näide. Vastutav töötleja haldab sisenemist oma hoonesse näotuvastusmeetodi abil. Inimesed võivad seda sisenemisviisi kasutada ainult siis, kui nad on eelnevalt andnud sõnaselge teadliku nõusoleku (artikli 9 lõike 2 punkti a kohaselt). Selleks et tagada, et ei pildistataks kedagi, kes ei ole eelnevat nõusolekut andnud, peaks näotuvastusmeetodi käivitama andmesubjekt ise, näiteks vajutades nuppu. Töötlemise seaduslikkuse tagamiseks peab vastutav töötleja alati pakkuma hoonesse sisenemiseks biomeetrilise töötlemiseta alternatiivset viisi, näiteks sissepääsukaarte või võtmeid.

78.

79. Biomeetriliste mallide loomise korral tagavad vastutavad töötlejad, et kui tulemuseks on saadud kokkulangevus või kokkulangevuse puudumine, kustutatakse viivitamata ja turvaliselt kõik vahemallid, mis on käigu pealt koostatud (andmesubjekti sõnaselgel ja teadliku nõusolekul), et võrrelda neid andmesubjektide poolt registreerimise ajal loodud mallidega. Registreerimiseks loodud malle tuleks hoida ainult töötlemise eesmärgi saavutamiseks ning neid ei tohiks säilitada ega arhiveerida.

80. Kui aga töötlemise eesmärk on näiteks eristada ühte isikute kategooriat teisest, kuid mitte kedagi üheselt tuvastada, ei kuulu töötlemine artikli 9 kohaldamisalasse.

Näide. Kaupluse omanik soovib kohandada oma reklaami klientide soo ja vanuse alusel, mille registreerib videovalvesüsteem. Kui selle süsteemiga ei looda biomeetrilisi malle isikute kordumatuks tuvastamiseks, vaid need füüsilised omadused tuvastatakse lihtsalt isiku klassifitseerimiseks, ei kuulu töötlemine artikli 9 kohaldamisalasse (seni, kuni ei töödelda andmete muid eriliike).

81.

82. Artiklit 9 kohaldatakse siiski juhul, kui vastutav töötleja säilitab biomeetrilisi andmeid (enamasti mallide abil, mis on loodud biomeetriliste andmete toorvormist põhielementide eraldamise teel (nt näo mõõtmed kujutiselt)), et isik kordumatult tuvastada. Kui vastutav töötleja soovib tuvastada andmesubjekti, kes siseneb alale uuesti või siseneb teisele alale (näiteks selleks, et kuvada pidevat kohandatud reklaami), on eesmärk isik kordumatult tuvastada, mis tähendab, et toiming kuuluks algusest peale artikli 9 kohaldamisalasse. Nii võib see olla juhul, kui vastutav töötleja säilitab loodud malle, et pakkuda veelgi kohandatumat reklaami mitmel reklaamtahvlil kaupluse eri kohtades. Kuna süsteem kasutab füüsilisi omadusi, et tuvastada ja jälgida konkreetseid isikuid, kes tulevad tagasi kaamera nägemisulatusse (nagu ostukeskuse külastajad), oleks see biomeetrilise tuvastamise meetod, sest selle eesmärk on tuvastamine konkreetse tehnilise töötlemise abil.

Näide. Kaupluse omanik on paigaldanud oma kauplusesse näotuvastussüsteemi, et kohandada oma reklaami üksikisikutele. Enne biomeetrilise süsteemi kasutamist ja kohandatud reklaami esitamist peab vastutav töötleja saama kõigilt andmesubjektidelt sõnaselge ja teadliku nõusoleku. Süsteem oleks ebaseaduslik, kui see salvestaks külastajaid või möödujaid, kes ei ole andnud nõusolekut oma biomeetrilise malli loomiseks, isegi kui nende mall kustutatakse võimalikult lühikese aja jooksul. Need ajutised mallid kujutavad endast biomeetrilisi andmeid, mida töödeldakse selleks, et tuvastada kordumatult isik, kellel ei pruugi olla soovi saada suunatud reklaami.

83.

84. Euroopa Andmekaitsenõukogu märgib, et mõned biomeetrilised süsteemid on paigaldatud kontrollimatusse keskkonda,[17] mis tähendab, et süsteem salvestab käigu pealt kõigi kaamerast mööduvate isikute, sealhulgas biomeetrilise seadmega mittenõustunud isikute näokujutisi ja loob seeläbi biomeetrilisi malle. Neid malle võrreldakse mallidega, mis on loodud andmesubjektidest, kes on andnud andmete registreerimise protsessi käigus eelneva nõusoleku (st biomeetrilise seadme kasutaja), et vastutav töötleja saaks kindlaks teha, kas isik on biomeetrilise seadme kasutaja või mitte. Sellisel juhul on süsteem sageli loodud diskrimineerima isikuid, keda ta soovib andmebaasis eristada neist, kes ei ole registreeritud. Kuna eesmärk on kordumatult tuvastada füüsilised isikud, on kõigi kaameraga salvestatud isikute puhul ikkagi vaja isikuandmete kaitse üldmääruse artikli 9 lõike 2 kohast erandit.

Näide. Hotell kasutab videovalvet, et automaatselt teavitada hotellijuhti väga tähtsa isiku saabumisest, kui külastaja nägu on ära tuntud. Enne selleks loodud andmebaasi kandmist on need väga tähtsad isikud andnud eelneva sõnaselge nõusoleku näotuvastuse kasutamiseks. Need biomeetriliste andmete töötlemise süsteemid oleksid ebaseaduslikud, välja arvatud juhul, kui kõik teised jälgitavad külalised (eesmärgiga tuvastada väga tähtsad isikud) on andnud isikuandmete töötlemiseks nõusoleku vastavalt isikuandmete kaitse üldmääruse artikli 9 lõike 2 punktile a.

Näide. Vastutav töötleja paigaldab tema hallatava kontserdisaali sissepääsu juurde näotuvastusega videovalvesüsteemi. Vastutav töötleja peab tagama selgelt eraldatud sissepääsud; üks biomeetrilise süsteemiga ja teine ilma (näiteks selline, kus skannitakse hoopis pilet). Biomeetriliste seadmetega varustatud sissepääsud tuleb paigaldada ja teha juurdepääsetavaks nii, et süsteem ei saaks salvestada nende kontserdikülastajate biomeetrilisi malle, kes ei ole nõusolekut andnud.

85.

86. Kui isikuandmete kaitse üldmääruse artikli 9 kohaselt on nõutav nõusoleku olemasolu, ei tohi vastutav töötleja seada oma teenustele juurdepääsu tingimuseks nõusolekut biomeetrilise töötlemisega. Eelkõige juhul, kui biomeetrilist töötlemist kasutatakse autentimise eesmärgil, peab vastutav töötleja seega pakkuma alternatiivset lahendust, mis ei hõlma biomeetrilist töötlemist, ilma et sellega kaasneks piiranguid või lisakulusid andmesubjektile. Sellist alternatiivset lahendust on vaja ka isikutele, kes ei vasta biomeetrilise seadme piirangutele (biomeetriliste andmete registreerimine või lugemine ei ole võimalik, selle kasutamise muudab keeruliseks puue jne), ning arvestades biomeetrilise seadme

[17] See tähendab, et biomeetriline seade asub üldsusele avatud ruumis ja töötab kõigi peal, kes mööduvad, erinevalt kontrollitavas keskkonnas asuvatest biomeetrilistest süsteemidest, mida saab kasutada üksnes isiku nõusolekul.

kättesaadamatuse võimalust (nt seadme talitlushäire), tuleb luua erandkorras kasutatav varulahendus, et tagada kavandatud teenuse järjepidevus. Erandjuhtudel võib tekkida olukord, kus biomeetriliste andmete töötlemine on lepingu alusel osutatava teenuse põhitegevus: näiteks kui muuseum paneb näotuvastusseadme kasutamise demonstreerimiseks üles näituse, ei saa andmesubjekt keelduda biomeetriliste andmete töötlemisest, kui ta soovib näitusel osaleda. Sellisel juhul on artikli 9 alusel nõutav nõusolek endiselt kehtiv, kui artikli 7 nõuded on täidetud.

5.2 Soovitatavad meetmed riskide vähendamiseks biomeetriliste andmete töötlemisel

87. Kooskõlas võimalikult väheste andmete kogumise põhimõttega peavad vastutavad töötlejad tagama, et digitaalsest kujutisest malli koostamiseks eraldatud andmed ei ole ülemäärased ja sisaldavad üksnes konkreetseks otstarbeks vajalikku teavet, vältides seega võimalikku edasist töötlemist. Tuleks kehtestada meetmed, millega tagatakse, et malle ei saa biomeetriliste süsteemide vahel üle kanda.

88. Tuvastamine ja autentimine/kontrollimine nõuavad tõenäoliselt malli säilitamist hilisemaks võrdlemiseks. Vastutav töötleja peab leidma andmete säilitamiseks kõige sobivama koha. Kontrollitavas keskkonnas (piiratud koridorid või kontrollpunktid) salvestatakse mallid kasutaja käes ja tema ainukontrolli all olevale üksikseadmele (nutitelefon või ID-kaart) või – kui see on vajalik konkreetsetel eesmärkidel ja objektiivsete vajaduste korral – keskandmebaasi krüpteeritud kujul, kasutades võtit/salasõna, mis on üksnes selle isiku käes, et takistada volitamata juurdepääsu mallile või säilitamiskohale. Kui vastutav töötleja ei saa vältida juurdepääsu mallidele, peab ta võtma asjakohased meetmed, et tagada säilitatavate andmete turvalisus. See võib hõlmata malli krüpteerimist krüptoalgoritmi abil.

89. Igal juhul peab vastutav töötleja võtma kõik vajalikud ettevaatusabinõud, et säilitada töödeldavate andmete kättesaadavus, terviklus ja konfidentsiaalsus. Selleks võtab vastutav töötleja eelkõige järgmised meetmed: eraldab andmed nende edastamise ja säilitamise ajal, säilitab biomeetrilisi malle ja toorandmeid või identiteediandmeid eraldi andmebaasides, krüpteerib biomeetrilised andmed, eelkõige biomeetrilised mallid, ning määrab kindlaks krüpteerimise ja võtmehalduse põhimõtted, integreerib korralduslikku ja tehnilise meetme pettuste avastamiseks, ühendab tervikluse koodi andmetega (näiteks allkiri või räsi) ning keelab igasuguse välise juurdepääsu biomeetrilistele andmetele. Need meetmed peavad arenema koos tehnoloogia arenguga.

90. Lisaks selle peaksid vastutavad töötlejad toorandmed (näokujutised, kõnesignaalid, kõnnak jne) kustutama ja tagama selle kustutamise tõhususe. Kui töötlemiseks ei ole enam õiguslikku alust, tuleb toorandmed kustutada. Kui biomeetrilised mallid tulenevad sellistest andmetest, võib arvata, et andmebaaside loomine võib kujutada endast samaväärset, kui mitte isegi suuremat ohtu (kuna biomeetrilist malli ei pruugi alati olla lihtne lugeda, kui ei ole teada, kuidas see on programmeeritud, samas kui toorandmed on mis tahes malli koostisosad). Kui vastutaval töötlejal peaks olema vaja selliseid andmeid säilitada, tuleb uurida müra lisamise meetodeid (nt vesimärgistamine), mis muudaksid malli loomise ebatõhusaks. Vastutav töötleja peab biomeetrilised andmed ja mallid kustutama ka volitamata juurdepääsu korral lugemis-võrdlusterminalile või salvestusserverile ning kustutama kõik andmed, mis ei ole biomeetrilise seadme kasutusea lõpus edasiseks töötlemiseks kasulikud.

6 ANDMESUBJEKTI ÕIGUSED

91. Videovalve kasutamisel toimuva andmetöötluse laadi tõttu tuleb täiendavalt selgitada andmesubjekti õigusi, mis tulenevad isikuandmete kaitse üldmäärusest. See peatükk ei ole siiski ammendav; videovalve tegemisel toimuva isikuandmete töötlemise suhtes kohaldatakse kõiki isikuandmete kaitse üldmäärusest tulenevaid õigusi.

6.1 Õigus tutvuda andmetega

92. Andmesubjektil on õigus saada vastutavalt töötlejalt kinnitus selle kohta, kas tema isikuandmeid töödeldakse või mitte. Videovalve puhul tähendab see, et kui andmeid ühelgi viisil ei säilitata ega edastata, võib vastutav töötleja pärast reaalajas jälgimise lõppemist anda üksnes teavet, et isikuandmeid enam ei töödelda (lisaks artiklis 13 sätestatud üldistele teavitamiskohustustele, vt *7. jagu „Läbipaistvus ja teavitamiskohustused“*). Kui aga päringu esitamise ajal andmeid ikkagi töödeldakse (st kui andmeid säilitatakse või töödeldakse pidevalt mis tahes muul viisil), peaks andmesubjektil olema kooskõlas artikliga 15 õigus tutvuda andmete ja teabega.

93. Siiski võidakse mõnel juhul kohaldada andmetega tutvumise õiguse suhtes mitut piirangut.

- Isikuandmete kaitse üldmääruse artikli 15 lõige 4 – teiste isikute õiguste kahjustamine

94. Kuna samas videovalve salvestise lõigus võib olla salvestatud mis tahes arvul andmesubjekte, põhjustaks salvestise läbivaatamine teiste andmesubjektide isikuandmete täiendavat töötlemist. Kui andmesubjekt soovib saada materjali koopiat (artikli 15 lõige 3), võib see kahjustada materjalis hõlmatud teiste andmesubjektide õigusi ja vabadusi. Seepärast peaks vastutav töötleja võtma sellise mõju vältimiseks arvesse, et videosalvestise sekkuva olemuse tõttu ei tohiks vastutav töötleja mõnel juhul videosalvestist välja anda, juhul kui on võimalik tuvastada teisi andmesubjekte. Kolmandate isikute õiguste kaitset ei tohiks siiski kasutada ettekäändena, et ennetada üksikisikute õigustatud nõudmist andmetega tutvuda; sellistel juhtudel peaks vastutav töötleja rakendama andmetega tutvumise taotluste rahuldamiseks tehnilisi meetmeid (näiteks kujutise muutmine, nagu maskeerimine või peitmine). Vastutavad töötlejad ei ole siiski kohustatud selliseid tehnilisi meetmeid võtma, kui nad saavad muul viisil tagada, et nad on võimelised reageerima artikli 15 kohasele taotlusele artikli 12 lõikes 3 sätestatud aja jooksul.

- Isikuandmete kaitse üldmääruse artikli 11 lõige 2 – vastutav töötleja ei suuda andmesubjekti tuvastada

95. Kui videosalvestises ei ole võimalik isikuandmeid otsida (st vastutav töötleja peaks vaatama läbi suure hulga salvestatud materjali, et leida asjaomane andmesubjekt), ei pruugi vastutav töötleja suuta andmesubjekti tuvastada.

96. Nendel põhjustel peaks andmesubjekt (lisaks enda tuvastamisele, sh isikut tõendava dokumendiga või isiklikult) täpsustama oma taotluses vastutavale töötlejale, millal ta sisenes jälgitavale alale – mõistliku ajavahemiku piires, mis on proportsionaalne registreeritud andmesubjektide arvuga. Vastutav töötleja peaks andmesubjekti eelnevalt teavitama sellest, millist teavet on vastutaval töötlejal taotluse täitmiseks vaja. Kui vastutav töötleja suudab tõendada, et tal ei ole võimalik andmesubjekti tuvastada, peab ta andmesubjekti sellest võimaluse korral teavitama. Sellises olukorras peaks vastutav töötleja täpsustama oma vastuses andmesubjektile jälgitud ala, kasutusel olnud kaamerate kontrollimise andmed jne, et andmesubjekt saaks täielikult aru, milliseid tema isikuandmeid võidi töödelda.

Näide. Kui andmesubjekt taotleb koopiat oma isikuandmetest, mida töödeldi kaubanduskeskuse (kus käib päevas 30 000 külastajat) sissepääsu juurde paigaldatud videovalve abil, peaks andmesubjekt täpsustama umbes ühe tunni täpsusega, millal ta möödus jälgitavast alast. Kui vastutav töötleja ikkagi töötleb materjali, tuleks esitada videosalvestise koopia. Kui samas materjalis on võimalik tuvastada teisi andmesubjekte, tuleks see materjali osa enne taotluse esitanud andmesubjektile koopia andmist anonüümseks muuta (näiteks koopia või selle osade hägustamisega).

Näide. Kui vastutav töötleja kustutab automaatselt kõik salvestised näiteks kahe päeva jooksul, ei saa vastutav töötleja pärast nimetatud kahte päeva salvestisi andmesubjektile edastada. Kui vastutav töötleja saab taotluse pärast kahe päeva möödumist, tuleks andmesubjekti asjakohaselt teavitada.

97.

- Isikuandmete kaitse üldmääruse artikkel 12 – ülemäärased taotlused

98. Andmesubjekti ülemääraste või selgelt põhjendamatute taotluste korral võib vastutav töötleja küsida mõistlikku tasu isikuandmete kaitse üldmääruse artikli 12 lõike 5 punkti a kohaselt või keelduda taotletud meetmete võtmisest (isikuandmete kaitse üldmääruse artikli 12 lõike 5 punkt b). Vastutav töötleja peab suutma tõendada, et taotlus on selgelt põhjendamatu või ülemäärane.

6.2 Õigus andmete kustutamisele ja õigus esitada vastuväiteid

6.2.1 Õigus andmete kustutamisele (õigus olla unustatud)

99. Kui vastutav töötleja jätkab isikuandmete töötlemist lisaks reaalajas jälgimisele (nt säilitamine), võib andmesubjekt taotleda isikuandmete kustutamist isikuandmete kaitse üldmääruse artikli 17 alusel.

100. Taotluse korral on vastutav töötleja kohustatud isikuandmed põhjendamatu viivituseta kustutama, kui esineb mõni isikuandmete kaitse üldmääruse artikli 17 lõikes 1 loetletud asjaoludest (ja ei kehti ükski isikuandmete kaitse üldmääruse artikli 17 lõikes 3 loetletud erand). See hõlmab kohustust kustutada isikuandmed, kui neid ei ole enam vaja eesmärgil, milleks neid algselt säilitati, või kui töötlemine on ebaseaduslik (vt ka *8. jagu „Säilitamise ajavahemikud ja kustutamise kohustus“*). Peale selle tuleks töötlemise õiguslikust alusest olenevalt kustutada isikuandmed järgmistel juhtudel:

- *nõusoleku puhul* alati, kui nõusolek võetakse tagasi (ja muud õiguslikku alust töötlemiseks ei ole);
- *õigustatud huvi* korral:
    - kui andmesubjekt kasutab oma õigust esitada vastuväiteid (vt *punkt 6.2.2*) ja töötlemiseks ei ole mõjuvaid õiguspäraseid põhjuseid või
    - otseturunduse korral (sh profiilianalüüs), kui andmesubjekt esitab töötlemise suhtes vastuväiteid.

101. Kui vastutav töötleja on videosalvestise avalikustanud (nt ringhäälingus või voogedastus internetis), tuleb võtta mõistlikke meetmeid, et teavitada teisi vastutavaid töötlejaid (kes nüüd kõnealuseid isikuandmeid töötlevad) isikuandmete kaitse üldmääruse artikli 17 lõike 2 kohasest taotlusest. Mõistlike meetmete hulgas peaksid olema tehnilised meetmed, võttes arvesse olemasolevat tehnoloogiat ja rakendamise kulusid. Isikuandmete kustutamise korral peaks vastutav töötleja teavitama võimalikult paljusid isikuid, kellele isikuandmed on varem avalikustatud, kooskõlas isikuandmete kaitse üldmääruse artikliga 19.

102. Lisaks vastutava töötleja kohustusele kustutada isikuandmed andmesubjekti taotlusel on vastutav töötleja isikuandmete kaitse üldmääruse üldpõhimõtete kohaselt kohustatud piirama säilitatavate isikuandmete hulka (vt *8. jagu*).

103. Videovalve puhul väärib märkimist, et isikuandmete kustutamiseks vastavuses isikuandmete kaitse üldmäärusega loetakse näiteks pildi hägustamist ilma võimaluseta pildil varem sisaldunud isikuandmeid taastada.

> Näide. Esmatarbekaupade kauplusel on probleeme vandalismiga, eriti välisfassaadi puhul, ning seetõttu kasutab ta väljaspool sissepääsu videovalvet, mis hõlmab sissepääsuga külgnevaid seinu. Mööduja taotleb oma isikuandmete kustutamist alates möödumise hetkest. Vastutav töötleja on kohustatud vastama taotlusele põhjendamatu viivituseta ja hiljemalt ühe kuu jooksul. Kuna kõnealune salvestis ei täida enam eesmärki, milleks see algselt salvestati (andmesubjekti möödumise ajal ei esinenud vandalismi), puudub taotluse esitamise ajal õigustatud huvi andmete säilitamiseks, mis kaaluks üles andmesubjektide huvid. Vastutav töötleja peab isikuandmed kustutama.

104.

6.2.2 Õigus esitada vastuväiteid

105. Videovalve puhul, mis põhineb *õigustatud huvil* (isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt f) või vajadusel täita *avalikes huvides* olevat ülesannet (isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt e), on andmesubjektil igal ajal õigus esitada oma konkreetse olukorraga seotud põhjustel vastuväiteid isikuandmete töötlemise suhtes kooskõlas isikuandmete kaitse üldmääruse artikliga 21. Vastuväite esitanud isiku isikuandmete töötlemine peab siis lõppema, välja arvatud juhul, kui vastutav töötleja tõendab, et andmeid töödeldakse mõjuval õiguspärasel põhjusel, mis kaalub üles andmesubjekti õigused ja huvid. Vastutav töötleja peaks olema kohustatud vastama andmesubjekti taotlustele põhjendamatu viivituseta ja hiljemalt ühe kuu jooksul.

106. Videovalve kontekstis võib selle vastuväite esitada kas jälgitavale alale sisenemisel, seal viibimise ajal või pärast sealt lahkumist. Praktikas tähendab see, et välja arvatud juhul, kui vastutaval töötlejal on mõjuvad õiguspärased põhjused, on sellise ala jälgimine, kus on võimalik tuvastada füüsilisi isikuid, seaduslik ainult järgmistel juhtudel:

    (1) kui vastutav töötleja saab taotluse korral viivitamata peatada kaamera kasutamise isikuandmete töötlemiseks või

    (2) kui jälgitav ala on nii täpselt piiratud, et vastutav töötleja saab tagada andmesubjekti heakskiidu enne alale sisenemist, ning see ei ole ala, millele andmesubjektil kui kodanikul on õigus juurde pääseda.

107. Käesolevate suuniste eesmärk ei ole kindlaks teha, mida peetakse *mõjuvaks* õigustatud huviks (isikuandmete kaitse üldmääruse artikkel 21).

108. Videovalve kasutamisel otseturunduse eesmärgil on andmesubjektil õigus esitada oma äranägemisel isikuandmete töötlemise suhtes vastuväiteid, kuna õigus esitada vastuväiteid on selles kontekstis absoluutne (isikuandmete kaitse üldmääruse artikli 21 lõiked 2 ja 3).

109.

Näide. Ettevõttele tekitab probleeme turvanõuete rikkumine tema avaliku sissepääsu juures ja ettevõte kasutab videovalvet õigustatud huvi alusel eesmärgiga tabada ebaseaduslikult sisenevad isikud. Külastaja ei nõustu oma andmete töötlemisega videovalvesüsteemi abil põhjustel, mis on seotud tema konkreetse olukorraga. Kõnealusel juhul lükkab ettevõte taotluse siiski tagasi selgitusega, et salvestatud materjali on vaja käimasoleva sisejuurdluse tõttu, mis annab talle mõjuvad õiguspärased põhjused isikuandmete töötlemise jätkamiseks.

7 LÄBIPAISTVUS JA TEAVITAMISKOHUSTUSED[18]

110. Euroopa andmekaitseõigusele on pikka aega olnud omane, et andmesubjektid peaksid olema teadlikud videovalve toimimisest. Neid tuleks jälgitavatest kohtadest täpselt teavitada.[19] Isikuandmete kaitse üldmääruse kohaselt on üldine läbipaistvus ja teavitamiskohustused sätestatud isikuandmete kaitse üldmääruse artiklis 12 ja sellele järgnevates artiklites. Lisateave on esitatud artikli 29 töörühma suunistes määruse 2016/679 kohase läbipaistvuse kohta (WP 260), mille Euroopa Andmekaitsenõukogu kiitis heaks 25. mail 2018. Kooskõlas WP 260 punktiga 26 kohaldatakse isikuandmete kaitse üldmääruse artiklit 13, kui isikuandmeid kogutakse „[...] andmesubjektilt vaatluse alusel (nt automatiseeritud andmehõive seadmete või andmehõivetarkvara, nt kaamerate [...] abil) [...]“).

111. Pidades silmas teabe mahtu, mis tuleb andmesubjektile esitada, võivad vastutavad töötlejad järgida kihilist lähenemisviisi juhul, kui nad otsustavad kasutada läbipaistvuse tagamiseks kombineeritud meetodeid (WP 260, punkt 35; WP 89, punkt 22). Videovalve puhul tuleks kõige olulisem teave kuvada hoiatusmärgil (esimene kiht) ja kohustusliku lisateabe võib esitada muul viisil (teine kiht).

7.1 Esimese kihi teave (hoiatusmärk)

112. Esimene kiht puudutab esmast viisi, kuidas vastutav töötleja andmesubjektiga esmakordselt suhtleb. Selles etapis võivad vastutavad töötlejad kasutada hoiatusmärki, millel on asjakohane teave. Kuvatava teabe võib esitada koos ikooniga, et anda kavandatavast töötlemisest selgelt nähtaval, arusaadaval ja loetaval viisil sisuline ülevaade (isikuandmete kaitse üldmääruse artikli 12 lõige 7). Teabe vormingut tuleks kohandada konkreetsele asukohale (WP 89, punkt 22).

7.1.1 Hoiatusmärgi paigutus

113. Teave tuleks paigutada nii, et andmesubjektil on lihtne enne jälgitavale alale sisenemist märgata jälgimisega seotud asjaolusid (ligikaudu silmade tasandil). Kaamera asukohta ei ole vaja näidata, kui ei ole kahtlust, milliseid alasid jälgitakse, ning jälgimise konteksti on üheselt selgitatud (WP 89, punkt 22). Andmesubjektil peab olema võimalik hinnata, milline ala on kaamera vaateväljas, et ta saaks vajaduse korral jälgimist vältida või oma käitumist kohandada.

7.1.2 Esimese kihi sisu

114. Esimese kihi teave (hoiatusmärk) peaks üldjuhul edastama kõige olulisemad andmed, nt andmed töötlemise eesmärkide, vastutava töötleja isiku ja andmesubjekti õiguste olemasolu kohta ning teabe töötlemise suurima mõju kohta.[20] See võib hõlmata näiteks vastutava töötleja (või kolmanda isiku) õigustatud huve ja andmekaitseametniku kontaktandmeid (kui see on asjakohane). Samuti tuleb selles viidata üksikasjalikumale teisele teabekihile ning sellele, kust ja kuidas seda leida.

115. Lisaks peaks märk sisaldama ka mis tahes teavet selle kohta, mis võib andmesubjekti üllatada (WP 260, punkt 38). See võib olla näiteks edastamine kolmandatele isikutele, eriti kui need asuvad väljaspool ELi, ja säilitamisaeg. Kui seda teavet ei esitata, peaks andmesubjektil olema võimalik olla kindel, et tegemist on üksnes reaalajas jälgimisega (ilma andmete salvestamise või kolmandatele isikutele edastamiseta).

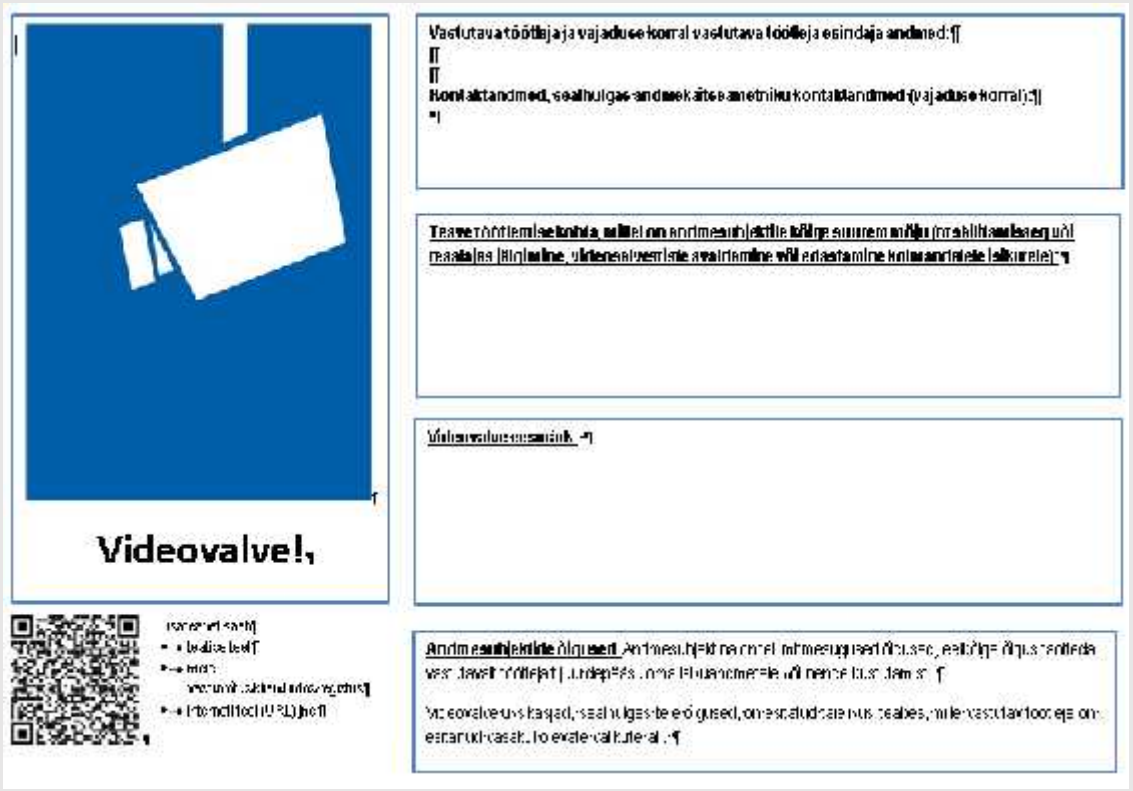
---

[18] Kohaldada võidakse liikmesriigi õigusaktide erinõudeid.

[19] Vt WP 859, artikli 29 töörühma arvamus 4/2004 isikuandmete töötlemise kohta videovalve abil.

[20] Vt WP 260, punkt 38.

Näide (mittesiduv soovitus)



116.

7.2 Teise kihi teave

117. Ka teise kihi teave peab olema andmesubjektile kättesaadav kergesti juurdepääsetavas kohas, näiteks keskses kohas (nt infolauas, vastuvõtus või kassas) kättesaadava täieliku teabelehena või lihtsasti juurdepääsetaval plakatil. Nagu eespool märgitud, tuleb esimese kihi hoiatusmärgil selgelt viidata teise kihi teabele. Lisaks on kõige parem, kui esimese kihi teabes viidatakse teise kihi digitaalsele allikale (nt ruutkood või veebisaidi aadress). Teave peaks siiski olema kergesti kättesaadav ka muul viisil kui digitaalselt. Teise kihi teabega peaks olema võimalik tutvuda jälgitavale alale minemata, eriti kui teavet antakse digitaalselt (seda on võimalik saavutada näiteks lingi abil). Muu asjakohane teave võiks olla telefoninumber, millele saab helistada. Olenemata sellest, kuidas teave esitatakse, peab see sisaldama kogu teavet, mis on isikuandmete kaitse üldmääruse artikli 13 kohaselt kohustuslik.

118. Lisaks neile võimalustele ja nende tõhustamise eesmärgil edendab Euroopa Andmekaitsenõukogu tehnoloogiliste vahendite kasutamist andmesubjektide teavitamisel. See võib hõlmata näiteks järgmist: geopositsioneerivad kaamerad ja teabe lisamine kaardirakendustesse või veebisaitidele, et üksikisikud saaksid esiteks hõlpsasti kindlaks teha ja täpsustada oma õiguste teostamisega seotud videoallikaid ning teiseks saada üksikasjalikumat teavet töötlemistoimingu kohta.

Näide. Kaupluse omanik jälgib oma kauplust. Artikli 13 järgimiseks piisab esimese kihi teavet sisaldava hoiatusmärgi paigaldamisest hõlpsasti nähtavasse kohta kaupluse sissepääsu juures. Lisaks peab omanik tegema teise kihi teavet sisaldava teabelehe kättesaadavaks kas kassas või kaupluse mis tahes muus keskses ja kergesti juurdepääsetavas kohas.

119.

8 SÄILITAMISE AJAVAHEMIKUD JA KUSTUTAMISE KOHUSTUS

120. Isikuandmeid ei tohi säilitada kauem, kui on vajalik eesmärkidel, milleks neid töödeldakse (isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktid c ja e). Kooskõlas isikuandmete kaitse üldmääruse artikli 6 lõikega 2 võivad mõnes liikmesriigis kehtida erisätted säilitamise ajavahemike kohta seoses videovalvega.

121. Seda, kas isikuandmeid on vaja säilitada, tuleks kontrollida lühikese aja jooksul. Üldjuhul on videovalve õiguspärased eesmärgid sageli vara kaitse või tõendite säilitamine. Tekkinud kahju saab tavaliselt kindlaks teha ühe või kahe päeva jooksul. Selleks et hõlbustada andmekaitseraamistiku nõuetele vastavuse tõendamist, on vastutava töötleja huvides võtta eelnevalt korralduslikke meetmeid (nt nimetada vajaduse korral esindaja, kes videomaterjali läbi vaatab ja seda turvab). Võttes arvesse isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktides c ja e sätestatud põhimõtteid, nimelt võimalikult väheste andmete kogumist ja säilitamise piirangut, tuleks isikuandmed enamikul juhtudel (nt vandalismi avastamiseks) kustutada – ideaaljuhul automaatselt – mõne päeva pärast. Mida pikem on ettenähtud säilitamisaeg (eriti kui see on pikem kui 72 tundi), seda rohkem tuleb põhjendada eesmärgi õiguspärasust ja säilitamise vajalikkust. Kui vastutav töötleja kasutab videovalvet mitte ainult oma ruumide jälgimiseks, vaid kavatseb andmeid ka säilitada, peab vastutav töötleja tagama, et säilitamine on eesmärgi saavutamiseks tegelikult vajalik. Kui säilitamine on vajalik, tuleb säilitamisaeg iga konkreetse eesmärgi puhul selgelt kindlaks määrata ja eraldi kehtestada. Vastutav töötleja vastutab säilitamisaja kindlaksmääramise eest kooskõlas vajalikkuse ja proportsionaalsuse põhimõttega ning isikuandmete kaitse üldmääruse sätete järgimise tõendamise eest.

> Näide. Väikepoe omanik saab tavaliselt vandalismist teada samal päeval. Seetõttu piisab korrapärasest 24-tunnisest säilitamisajast. Siiski võivad pikema säilitamisaja põhjuseks olla kinniolek nädalavahetustel või pikemad pühad. Kui avastatakse kahju, võib omanikul olla vaja säilitada videomaterjali ka pikema aja jooksul, et võtta õigusrikkuja vastu õiguslikke meetmeid.

122.

9 TEHNILISED JA KORRALDUSLIKUD MEETMED

123. Nagu on sätestatud isikuandmete kaitse üldmääruse artikli 32 lõikes 1, peab isikuandmete töötlemine videovalve ajal olema õiguslikult lubatud ning vastutavad töötlejad ja volitatud töötlejad peavad selle piisavalt turvaliseks muutma. Võetud **korralduslikud ja tehnilised meetmed** peavad olema **proportsionaalsed füüsiliste isikute õigusi ja vabadusi ähvardavate ohtudega**, mis tulenevad videovalve andmete juhuslikust või ebaseaduslikust hävitamisest, kaotsiminekust, muutmisest ja loata avalikustamisest või neile juurdepääsust. Isikuandmete kaitse üldmääruse artiklite 24 ja 25 kohaselt peavad vastutavad töötlejad rakendama tehnilisi ja korralduslikke meetmeid ka selleks, et tagada töötlemise ajal kõigi andmekaitse põhimõtete järgimine, ning looma andmesubjektidele vahendid nende isikuandmete kaitse üldmääruse artiklites 15–22 sätestatud õiguste teostamiseks. Andmete vastutavad töötlejad peaksid vastu võtma siseraamistiku ja -põhimõtted, mis tagavad sellise rakendamise nii töötlemisvahendite kindlaksmääramise kui ka töötlemise ajal, sealhulgas vajaduse korral andmekaitsealaste mõjuhinnangute tegemise.

9.1 Videovalvesüsteemi ülevaade

124. Videovalvesüsteem[21] koosneb analoog- ja digitaalseadmetest ning tarkvarast, mille eesmärk on salvestada kujutisi sündmuskohast, neid töödelda ja operaatorile kuvada. Selle osad on jagatud järgmistesse kategooriatesse.

- Videokeskkond: kujutise salvestamine, ühendused ja pilditöötlus:
  - kujutise salvestamise eesmärk on luua reaalmaailmast selline kujutis, mida saaks kasutada ülejäänud süsteemis;
  - mõiste „ühendused“ tähistab igasugust andmeedastust videokeskkonnas, st ühendusi ja sidet. Ühendused on näiteks kaablid, digivõrgud ja juhtmeta ülekanded. Mõiste „side“ tähistab kõiki video- ja andmesignaale, mis võivad olla digitaal- või analoogsignaalid;
  - pilditöötlus hõlmab pildi või kujutiste jada analüüsi, salvestamist ja esitamist.
- Süsteemi haldamise seisukohast on videovalvesüsteemil järgmised loogilised funktsioonid:
  - andmehaldus ja tegevuse juhtimine, mis hõlmab operaatori käskude töötlemist ja süsteemi loodud tegevusi (häiremenetlused, operaatorite hoiatamine);
  - teiste süsteemidega ühendavad liidesed võivad hõlmata ühendust teiste turvasüsteemidega (juurdepääsukontroll, tulekahjuhäire) ja muude kui turvasüsteemidega (hoonehaldussüsteemid, numbrimärkide automaattuvastus).
- Videovalvesüsteemi turvalisuse loovad süsteemi ja andmete konfidentsiaalsus, terviklus ja kättesaadavus:
  - süsteemi turvalisus hõlmab kõigi süsteemikomponentide füüsilist turvalisust ja videovalvesüsteemile juurdepääsu kontrollimist;
  - andmeturve hõlmab andmete kaotsimineku või manipuleerimise ärahoidmist.

[21] Isikuandmete kaitse üldmäärus ei sisalda videovalvesüsteemi määratlust, tehniline kirjeldus on esitatud näiteks standardis EN 62676-1-1:2014 „Turvarakendustes kasutatavad videovalvesüsteemid. Osa 1-1: Süsteemi nõuded“.

125.

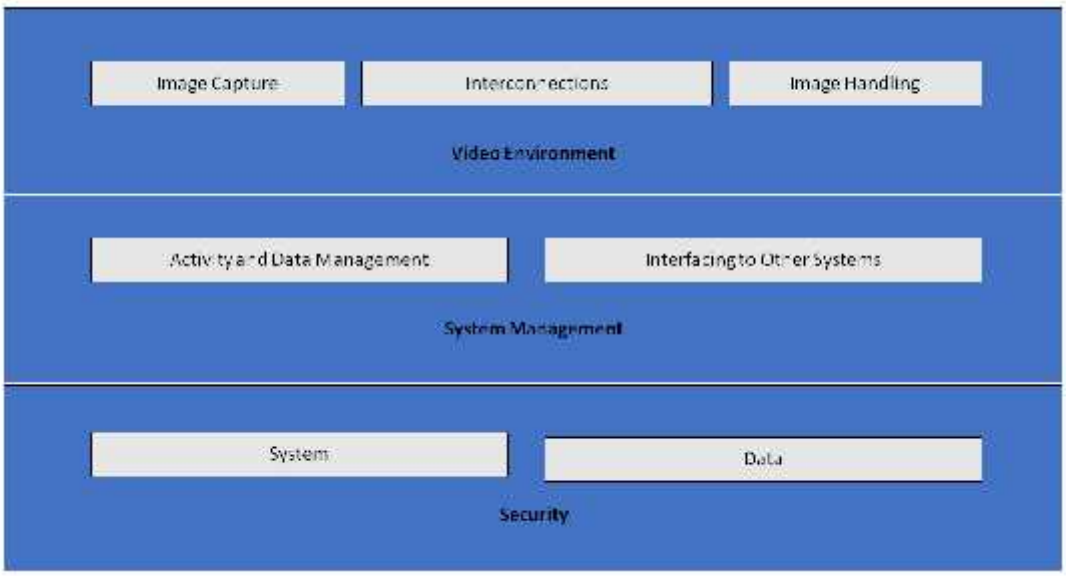


Image Capture	Kujutise salvestamine
Interconnections	Ühendused
Image Handling	Pilditöötlus
Video Environment	Videokeskkond
Activity and Data Management	Tegevuse ja andmete haldus
Interfacing to Other Systems	Teiste süsteemidega ühendavad liidesed
System Management	Süsteemi haldamine
System	Süsteem
Data	Andmed
Security	Turvalisus

Joonis 1. Videovalvesüsteem

9.2 Lõimitud andmekaitse ja vaikimisi andmekaitse

126. Nagu on sätestatud isikuandmete kaitse üldmääruse artiklis 25, peavad vastutavad töötlejad rakendama asjakohaseid andmekaitsealaseid tehnilisi ja korralduslikke meetmeid kohe, kui nad kavandavad videovalvet, st enne, kui nad alustavad videosalvestiste kogumist ja töötlemist. Need põhimõtted rõhutavad vajadust privaatsust edendavate tehnoloogialahenduste, andmetöötlust vähendavate vaikeseadete ning isikuandmete võimalikult kõrgetasemelist kaitset võimaldavate vajalike vahendite järele[22].

127. Vastutavad töötlejad peaksid lisama andmekaitse ja privaatsuse kaitse nii tehnoloogia väljatöötamise tehnilistesse kirjeldustesse kui ka korralduslikesse tavadesse. Korralduslike tavadega seoses peaks vastutav töötleja võtma vastu asjakohase juhtimisraamistiku ning kehtestama videovalvega seotud põhimõtted ja menetlused ning tagama nende järgimise. Tehnilisest seisukohast peaksid süsteemi tehniline kirjeldus ja ülesehitus hõlmama isikuandmete töötlemise nõudeid kooskõlas isikuandmete kaitse üldmääruse artiklis 5 sätestatud põhimõtetega (töötlemise seaduslikkus, eesmärk ja andmete piiramine, vaikimisi võimalikult väheste andmete kogumine isikuandmete kaitse üldmääruse artikli 25

[22] WP 168, arvamus eraelu puutumatuse tuleviku kohta, artikli 29 alusel asutatud andmekaitse töörühma ning politsei- ja kohtukoostöö töörühma ühispanus Euroopa Komisjoni arutellu isikuandmete kaitsmise põhiõiguse õigusraamistiku üle (vastu võetud 1. detsembril 2009).

lõike 2 tähenduses, terviklus ja konfidentsiaalsus, vastutus jne). Kui vastutav töötleja kavatseb omandada kaubandusliku videovalvesüsteemi, peab vastutav töötleja lisama need nõuded ostutingimustesse. Vastutav töötleja peab tagama nende nõuete täitmise, kohaldades neid süsteemi kõigi osade ja kõigi töödeldavate andmete suhtes kogu nende olelusringi jooksul.

9.3 Konkreetsed näited asjakohaste meetmete kohta

128. Enamik meetmeid, mida saab kasutada videovalve turvamiseks, eriti juhul, kui kasutatakse digitaalseadmeid ja -tarkvara, ei erine teistes IT-süsteemides kasutatavatest meetmetest. Olenemata valitud lahendusest peab vastutav töötleja ikkagi piisavalt kaitsma videovalvesüsteemi kõiki komponente ja andmeid kõikides etappides, st salvestamise (sisestatud andmed), edastamise (edastatavad andmed) ja töötlemise (kasutatavad andmed) ajal. Selleks on vaja, et vastutavad töötlejad ja volitatud töötlejad kombineeriksid korralduslikke ja tehnilisi meetmeid.

129. Tehniliste lahenduste valimisel peaks vastutav töötleja kaaluma privaatsust soodustavaid tehnoloogialahendusi ka seetõttu, et need suurendavad turvalisust. Sellised tehnoloogialahendused on näiteks süsteemid, mis võimaldavad andmesubjektidele videosalvestisi andes peita või hägustada alasid, mis ei ole jälgimise seisukohast olulised, või lõigata välja kolmandate isikute kujutisi.[23] Teisest küljest ei tohiks valitud lahendused pakkuda funktsioone, mis ei ole vajalikud (nt kaamerate piiramatu liikumine, suumimise võimalus, raadioülekanne, analüüs ja helisalvestised). Valikus olevad, kuid ebavajalikud funktsioonid tuleb desaktiveerida.

130. Sellel teemal on olemas palju kirjandust, sealhulgas rahvusvahelised standardid ja tehnilised kirjeldused multimeediasüsteemide füüsilise turvalisuse[24] ja üldiste IT-süsteemide turvalisuse kohta[25]. Seetõttu esitatakse käesolevas jaos ainult selle teema üldine ülevaade.

9.3.1 Korralduslikud meetmed

131. Peale võimaliku vajaliku andmekaitsealase mõjuhinnangu (vt *10. jagu*) peaksid vastutavad töötlejad võtma oma videovalve põhimõtete ja menetluste väljatöötamisel arvesse järgmisi teemasid:

- kes vastutab videovalvesüsteemi haldamise ja toimimise eest;
- videovalveprojekti eesmärk ja ulatus;
- asjakohane ja keelatud kasutamine (kus ja millal videovalve on lubatud või ei ole lubatud; nt varjatud kaamerate ja audioseadmete kasutamine lisaks video salvestamisele)[26];
- *7. jaos* (*Läbipaistvus ja teavitamiskohustused*) nimetatud läbipaistvusmeetmed;
- video salvestamise viis ja kestus, sealhulgas turvaintsidentidega seotud videosalvestiste arhiveerimine;
- kes ja millal peavad läbima asjakohase koolituse;
- kellel ja milleks on juurdepääs videosalvestistele;
- töökord (nt kes ja kust videovalvet jälgib, mida teha andmenõuete rikkumise korral);

---

[23] Selliste tehnoloogialahenduste kasutamine võib mõnel juhul olla artikli 5 lõike 1 punkti c järgimiseks isegi kohustuslik. Igal juhul võivad need olla parimate tavade näiteks.

[24] IEC TS 62045 – Multimedia security – Guideline for privacy protection of equipment and systems in and out of use (Multimeedia turvalisus. Juhend kasutuses olevate ja kasutuses mitteolevate seadmete ja süsteemide privaatsuse kaitsmise kohta).

[25] ISO/IEC 27000 – Information security management systems series (Infoturbe haldamise süsteemide seeriad).

[26] See võib oleneda liikmesriigi õigusaktidest ja valdkondlikest eeskirjadest.

- milliseid menetlusi peavad välised pooled videosalvestiste taotlemiseks läbima ning selliste taotluste tagasilükkamise või täitmise menetlused;
- videovalvesüsteemi hankimise, paigaldamise ja hooldamise kord;
- intsidentide haldamine ja neist taastumise kord.

9.3.2 Tehnilised meetmed

132. **Süsteemi turvalisus** tähendab süsteemi kõigi komponentide **füüsilist turvalisust** ja süsteemi terviklust, st **kaitset tahtliku ja tahtmatu sekkumise eest süsteemi tavapärasesse töösse ja vastupidavust** ning **juurdepääsukontrolli**. Andmeturve tähendab **konfidentsiaalsust** (andmetele on juurdepääs ainult juurdepääsuõigusega isikutel), **terviklust** (andmete kaotsimineku või manipuleerimise ärahoidmine) ja **kättesaadavust** (andmetega on võimalik vajaduse korral tutvuda).

133. **Füüsiline turvalisus** on andmekaitse ja esimese kaitseliini oluline osa, sest see kaitseb videovalvesüsteemi seadmeid varguse, vandalismi, loodusõnnetuste, inimtegevusest tingitud katastroofide ja juhuslike kahjustuste eest (nt ülepinge, äärmuslike temperatuuride või mahaloksunud kohvi tõttu). Analoogsüsteemide kaitses on peamine osa füüsilisel turvalisusel.

134. **Süsteemi ja andmete turvalisus**, st kaitse selle tavapärasesse töösse tahtliku ja tahtmatu sekkumise eest, võib hõlmata järgmist:

- kogu videovalvesüsteemi taristu (sh kaugkaamerad, kaablid ja toiteallikad) kaitsmine füüsilise kahjustamise ja varguse eest;
- edastatavate salvestiste kaitsmine pealtkuulamiskindlate sidekanalite abil;
- andmete krüpteerimine;
- riist- ja tarkvarapõhiste lahenduste, näiteks tulemüüride, viirusetõrje või küberründevastaste sissetungi avastamise süsteemide kasutamine;
- komponentide, tarkvara ja ühenduste tõrgete avastamine;
- vahendid süsteemi kättesaadavuse ja sellele juurdepääsu taastamiseks füüsilise või tehnilise intsidendi korral.

135. **Juurdepääsukontroll** tagab, et süsteemile ja andmetele pääsevad juurde üksnes volitatud isikud, samal ajal kui teised seda teha ei saa. Füüsilist ja loogilist juurdepääsukontrolli toetavad meetmed hõlmavad järgmist:

- tagatakse, et kõik ruumid, kus tehakse videovalvet ja kus säilitatakse videosalvestisi, on kaitstud kolmandate isikute järelevalveta juurdepääsu eest;
- kuvarid paigutatakse nii (eriti kui need asuvad avatud aladel, nagu vastuvõtt), et neid saavad vaadata ainult volitatud operaatorid;
- füüsilise ja loogilise juurdepääsu andmise, muutmise ja tühistamise kord on kindlaks määratud ja seda täidetakse;
- rakendatakse kasutajate autentimise ja volitamise meetodeid ja vahendeid, sealhulgas näiteks paroolide pikkus ja muutmise sagedus;
- kasutaja tehtud toimingud (nii süsteemis kui ka andmetega) registreeritakse ja vaadatakse korrapäraselt läbi;
- juurdepääsuga seotud tõrkeid jälgitakse ja tuvastatakse pidevalt ning tuvastatud puudused kõrvaldatakse võimalikult kiiresti.

10 ANDMEKAITSEALANE MÕJUHINNANG

136. Isikuandmete kaitse üldmääruse artikli 35 lõike 1 kohaselt peavad vastutavad töötlejad tegema andmekaitsealaseid mõjuhinnanguid, kui teatavat liiki andmetöötlusega kaasneb tõenäoliselt suur oht füüsiliste isikute õigustele ja vabadustele. Isikuandmete kaitse üldmääruse artikli 35 lõike 3 punktis c on sätestatud, et vastutavad töötlejad peavad tegema andmekaitsealaseid mõjuhinnanguid, kui töötlemine kujutab endast avalike alade ulatuslikku süstemaatilist jälgimist. Lisaks sellele on isikuandmete kaitse üldmääruse artikli 35 lõike 3 punkti b kohaselt andmekaitsealane mõjuhinnang nõutav ka siis, kui vastutav töötleja kavatseb ulatuslikult töödelda andmete eriliike.

137. Andmekaitsealast mõjuhinnangut käsitlevates suunistes[27] on esitatud lisanõuanded ja üksikasjalikumad näited videovalve kohta (nt seoses kaamerasüsteemi kasutamisega sõidukäitumise jälgimiseks maanteedel). Isikuandmete kaitse üldmääruse artikli 35 lõike 4 kohaselt peab iga järelevalveasutus avaldama loetelu töötlemistoimingutest, mille suhtes kohaldatakse nende riigis kohustuslikku andmekaitsealast mõjuhinnangut. Need loetelud on tavaliselt kättesaadavad ametiasutuste veebisaitidel. Võttes arvesse videovalve tüüpilisi eesmärke (inimeste ja vara kaitse, süütegude avastamine, ennetamine ja kontroll, tõendite kogumine ja kahtlusaluste biomeetriline tuvastamine), on mõistlik eeldada, et paljude videovalve juhtumite kohta on vaja teha andmekaitsealane mõjuhinnang. Seetõttu peaksid vastutavad töötlejad hoolikalt tutvuma nende dokumentidega, et teha kindlaks, kas selline hindamine on vajalik, ja tegema vajaduse korral hindamise. Andmekaitsealase mõjuhinnangu tulemus peaks näitama, milliseid andmekaitsemeetmeid vastutav töötleja rakendab.

138. Oluline on märkida ka seda, et kui andmekaitsealase mõjuhinnangu tulemustest nähtub, et töötlemisega kaasneb vastutava töötleja kavandatud turvameetmetest hoolimata suur oht, tuleb enne töötlemist konsulteerida asjaomase järelevalveasutusega. Üksikasjalik teave eelneva konsulteerimise kohta on esitatud artiklis 36.

Euroopa Andmekaitsenõukogu nimel

eesistuja

(Andrea Jelinek)

[27] WP 248 rev.01, „Suunised, mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ vastavalt määrusele 2016/679“; heaks kiidetud Euroopa Andmekaitsenõukogu poolt.