

Ohjeet



Ohjeet 3/2019 henkilötietojen käsittelystä videolaitteilla

Versio 2.0

Annettu 29. tammikuuta 2020

Aiemmat versiot

Versio 2.0	29. tammikuuta 2020	Ohjeiden hyväksyminen julkisen kuulemisen jälkeen
Versio 1.0	10. heinäkuuta 2019	Ohjeiden hyväksyminen julkista kuulemista varten

Sisällysluettelo

1	Johdanto.....	5
2	Soveltamisala.....	7
2.1	Henkilötiedot.....	7
2.2	Lainvalvontadirektiivin (direktiivin (EU) 2016/680) soveltaminen.....	7
2.3	Kotitalouksia koskeva poikkeus.....	7
3	Käsittelyn lainmukaisuus.....	9
3.1	Oikeutettu etu, 6 artiklan 1 kohdan f alakohta.....	9
3.1.1	Oikeutettujen etujen olemassaolo.....	9
3.1.2	Käsittelyn tarpeellisuus.....	10
3.1.3	Etujen tasapainottaminen.....	11
3.2	Käsittelyn tarpeellisuus yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi, 6 artiklan 1 kohdan e alakohta.....	13
3.3	6 artiklan 1 kohdan a alakohta.....	14
4	Videoaineiston luovuttaminen kolmansille osapuolille.....	15
4.1	Videoaineiston luovuttaminen kolmansille osapuolille yleisesti.....	15
4.2	Videoaineiston luovuttaminen lainvalvontaviranomaisille.....	15
5	Erityisiä henkilötietoryhmiä koskeva käsittely.....	17
5.1	Biometrinen tietojen käsittelyyn liittyvät yleiset näkökohdat.....	18
5.2	Riskien minimoimiseksi ehdotetut toimenpiteet biometrinen tietojen käsittelyssä.....	21
6	Rekisteröidyn oikeudet.....	23
6.1	Oikeus saada pääsy tietoihin.....	23
6.2	Oikeus tietojen poistamiseen ja vastustamisoikeus.....	24
6.2.1	Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi).....	24
6.2.2	Vastustamisoikeus.....	25
7	Läpinäkyvyyttä ja tiedottamista koskevat velvollisuudet.....	27
7.1	Ensimmäisen tason tiedot (varoituserkki).....	27
7.1.1	Varoituserkin sijainti.....	27
7.1.2	Ensimmäisen tason sisältö.....	27
7.2	Toisen tason tiedot.....	28
8	Säilytysajat ja poistamisvelvollisuus.....	29
9	Tekniset ja organisatoriset toimenpiteet.....	29
9.1	Katsaus videovalvontajärjestelmään.....	29
9.2	Sisäänrakennettu ja oletusarvoinen tietosuojajärjestelmä.....	31
9.3	Konkreettisia esimerkkejä asiaankuuluvista toimenpiteistä.....	32

9.3.1	Organisatoriset toimenpiteet	32
9.3.2	Tekniset toimenpiteet	33
10	Tietosuojaa koskeva vaikutustenarviointi	34

Euroopan tietosuojaneuvosto, joka

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679, jäljempänä 'yleinen tietosuoja-asetus', 70 artiklan 1 kohdan e alakohdan,

ottaa huomioon ETA-sopimuksen sekä erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018¹,

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

ON ANTANUT SEURAAVAT OHJEET:

1 JOHDANTO

1. Videolaitteiden laaja käyttö vaikuttaa kansalaisten käytökseen. Tällaisten välineiden huomattava käyttöönotto useilla ihmiselämän aloilla aiheuttaa lisäpainetta ihmisille estää poikkeavuuksiksi mahdollisesti katsottavien asioiden havaitsemisen. Tällaisilla teknologioilla voidaan tosiasiallisesti rajoittaa mahdollisuuksia tuntemattomana liikkumiseen ja palvelujen anonyymiin käyttöön sekä yleisesti rajoittaa mahdollisuutta pysyä huomaamattomana. Vaikutukset tietosuojaan ovat valtavat.
2. Vaikka ihmisiä ei ehkä haittaa esimerkiksi turvallisuutta varten käytettävä videovalvonta, on taattava, että sitä ei käytetä väärin täysin toisenlaisiin ja – rekisteröidyn kannalta – odottamattomiin tarkoituksiin (esimerkiksi markkinointiin tai työntekijöiden suoritusten seurantaan jne.). Nykyään otetaan käyttöön myös useita työkaluja, joiden avulla hyödynnetään otettuja kuvia ja muunnetaan perinteisistä kameroista älykameroita. Videolla tuotetun tiedon määrä yhdistettynä näihin työkaluihin ja tekniikoihin lisää toissijaisen käytön riskejä (riippumatta siitä, liittyykö se järjestelmälle osoitettuun alkuperäiseen tarkoitukseen) ja jopa väärinkäytön riskejä. Yleisen tietosuoja-asetuksen yleiset periaatteet (5 artikla) on otettava aina huolellisesti huomioon videovalvonnassa.
3. Videovalvontajärjestelmät muuttavat monin tavoin tapaa, jolla yksityisen ja julkisen sektorin ammattilaiset toimivat vuorovaikutuksessa yksityisissä tai julkisissa paikoissa, jotta voidaan parantaa turvallisuutta, saada yleisöanalyseja, toteuttaa yksilöllistä mainontaa jne. Videovalvonnasta on tullut erittäin tehokasta älykkään videoanalyysin kasvavan käyttöönoton ansiosta. Nämä tekniikat voivat olla aiempaa tunkeilevampia (esim. monimutkaiset biometriset teknologiat) tai vähemmän tunkeileviä (esim. yksinkertaiset laskualgoritmit). Yleisesti ottaen tuntemattomana pysyminen ja yksityisyyden varjeleminen vaikeutuvat jatkuvasti. Kunkin tilanteen herättämät tietosuojakysymykset voivat olla erilaisia, ja myös oikeudellinen analyysi voi vaihdella sen mukaan, mitä näistä teknologioista käytetään.
4. Yksityisyyden suojaa koskevien kysymysten lisäksi riskejä liittyy myös näiden laitteiden mahdollisiin häiriöihin ja niiden aikaansaamiin vääristymiin. Tutkijoiden mukaan kasvotunnistusta, tunnistamista tai analyysia varten käytettävät ohjelmistot toimivat eri tavoin riippuen tunnistamisen kohteena

¹ Viittauksilla "jäsenvaltioihin" tarkoitetaan kauttaaltaan tässä lausunnossa ETAn jäsenvaltioita.

olevan henkilön iästä, sukupuolesta ja etnisestä taustasta. Algoritmit toimivat eri tavoin eri väestöryhmien osalta, joten kasvontunnistuksen vääristymä uhkaa vahvistaa yhteiskunnan ennakkoluuloja. Rekisterinpitäjien on siksi myös varmistettava, että videovalvonnasta saatavien biometristen tietojen käsittelyn merkitystä ja annettujen takeiden riittävyttä arvioidaan säännöllisesti.

5. Videovalvonta ei ole oletusarvoisesti välttämätöntä, kun sen perustana olevan tarkoituksen saavuttamiseksi on olemassa muita keinoja. Muutoin kulttuuriset normit saattavat muuttua siten, että yksityisyyden puutteesta tulisi hyväksyttävää yleisenä lähtökohtana.
6. Tämän ohjeen tarkoituksena on antaa neuvoja siitä, miten yleistä tietosuoja-asetusta sovelletaan videolaitteilla saatavien henkilötietojen käsittelyn yhteydessä. Esimerkit eivät ole tyhjentyviä, ja yleisiä perusteluita voidaan soveltaa kaikilla mahdollisilla käyttöaloilla.

2 SOVELTAMISALA²

2.1 Henkilötiedot

7. Tietyn tilan järjestelmällisestä automaattisesta valvonnasta optisilla tai audiovisuaalisilla keinoilla on tullut nykyään merkittävä ilmiö. Tällaista valvontaa suoritetaan pääsääntöisesti omaisuuden suojaamista varten ja ihmisten hengen ja terveyden suojelemiseksi. Toiminnassa kerätään ja säilytetään kuvallista tai audiovisuaalista tietoa kaikista valvottuun tilaan tulevista ihmisistä, jotka voidaan tunnistaa heidän ulkonäkönsä tai muiden erityisten tekijöiden perusteella. Ihmisten henkilöllisyys voidaan vahvistaa näiden yksityiskohtien perusteella. Siinä voidaan myös edelleen käsitellä henkilötietoja, jotka koskevat henkilöiden läsnäoloa ja käyttäytymistä tietyssä tilassa. Näiden tietojen väärinkäytön mahdollinen riski kasvaa suhteessa valvotun tilan kokoon sekä tilassa käyvien henkilöiden määrään. Tämä seikka näkyy yleisen tietosuoja-asetuksen 35 artiklan 3 kohdan c alakohdassa, jonka mukaan tietosuoja koskeva vaikutustenarviointi on tehtävä, kun on kyse yleisölle avoimen alueen järjestelmällisestä valvonnasta laajamittaisesti, sekä 37 artiklan 1 kohdan b alakohdassa, jonka mukaan henkilötietojen käsittelijöiden on nimettävä tietosuojavastaavat, jos käsittelytoimet edellyttävät luonteensa vuoksi rekisteröityjen säännöllistä ja järjestelmällistä seuranta.
8. Asetusta ei kuitenkaan sovelleta tietojenkäsittelyyn, joka ei liity henkilöön, esimerkiksi, jos henkilöä ei voida tunnistaa suoraan tai välillisesti.

Esimerkki: Yleistä tietosuoja-asetusta ei sovelleta valekameroihin (eli kameroihin, jotka eivät toimi kamerana eivätkä siten käsittele henkilötietoja). *Joissakin jäsenvaltioissa siihen voidaan kuitenkin soveltaa muuta lainsäädäntöä.*

Esimerkki: Erittäin korkealta tehdyt tallennukset kuuluvat yleisen tietosuoja-asetuksen soveltamisalaan vain, jos käsitellyt tiedot voidaan kyseisissä olosuhteissa liittää tiettyyn henkilöön.

Esimerkki: Autoon on asennettu videokamera auttamaan pysäköinnissä. Jos kamera on rakennettu tai sitä säädetään niin, että se ei kerää luonnolliseen henkilöön liittyviä tietoja (kuten rekisterikilpiä tai tietoja, joista voidaan tunnistaa ohikulkijat), yleistä tietosuoja-asetusta ei sovelleta.

- 9.
10. Erityisesti toimivaltaisten viranomaisten suorittama henkilötietojen käsittely rikosten torjumista, tutkimista, selvittämistä ja syytteen esenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä yleiseen turvallisuuteen kohdistuvilta uhkilta suojele ja tällaisten uhkien ehkäisy kuuluvat direktiivin (EU) 2016/680 soveltamisalaan.

2.2 Lainvalvontadirektiivin (direktiivin (EU) 2016/680) soveltaminen

2.3 Kotitalouksia koskeva poikkeus

11. Yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan c alakohdan mukaan henkilötietojen käsittely, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitaloutta koskevassa

² Euroopan tietosuojaneuvosto huomauttaa, että kansallisen lainsäädännön erityisiä vaatimuksia voidaan soveltaa, jos se sallitaan yleisessä tietosuoja-asetuksessa.

toiminnassa, johon voi kuulua myös toiminta verkossa, ei kuulu yleisen tietosuojasetuksen soveltamisalaan³.

12. Tätä säännöstä – niin sanottua kotitalouksia koskevaa poikkeusta – on tulkittava suppeasti videovalvonnan yhteydessä. Kuten Euroopan unionin tuomioistuimien totesikin, niin sanottua kotitalouksia koskevaa poikkeusta on ”*tulkittava niin, että se kohdistuu ainoastaan toimintaan, joka kuuluu yksityisen henkilön yksityis- tai perhe-elämään, mistä ei ilmeisestikään ole kysymys sellaisessa henkilötietojen käsittelyssä, jossa tiedot julkaistaan Internet-sivulla siten, että ne saatetaan ennalta määrittelemättömän henkilöryhmän saataville*”⁴. Lisäksi, jos videovalvontajärjestelmään kuuluu henkilötietojen jatkuvaa tallentamista ja säilyttämistä ja se ulottuu ”*vaikka osittainkin julkiseen tilaan ja kohdistuu tämän vuoksi tietoja tällä tavoin käsittelevän tahon yksityisen piirin ulkopuolelle, sitä ei voida pitää yksinomaan ’henkilökohtaisena tai kotitaloutta koskevana’ toimintana direktiivin 95/46 3 artiklan 2 kohdan toisessa luetelmakohdassa tarkoitettu tavoin*”⁵.
13. Yksityishenkilön tiloissa käytettävät videolaitteet voivat kuulua kotitalouksia koskevaan poikkeuksen piiriin. Tämä riippuu useista tekijöistä, jotka on kaikki otettava huomioon johtopäätöksen tekemiseksi. Edellä mainittujen unionin tuomioistuimen päätöksissä määritettyjen seikkojen lisäksi kotona videovalvontaa käyttävän on mietittävä: onko hänellä jonkinlaista henkilökohtaista suhdetta rekisteröityyn, viittaako videovalvonnan laajuus tai tiheys jonkinlaiseen ammattimaiseen toimintaan hänen puoleltaan ja vaikuttaako valvonta mahdollisesti haitallisesti rekisteröityihin. Minkään yksittäisen edellä mainitun tekijän käsillä olo ei välttämättä tarkoita, että käsittely ei kuulu kotitalouksia koskevan poikkeuksen soveltamisalaan, vaan sen määrittämiseksi on tehtävä kokonaisarvio.

Esimerkki: Matkailija dokumentoi lomaansa kuvaamalla videoita sekä matkapuhelimellaan että videokameralla. Hän näyttää videon ystävilleen ja perheelleen mutta ei anna sitä määrittelemättömän ihmismäärän saataville. Tähän sovelletaan kotitalouksia koskevaa poikkeusta.

Esimerkki: Alamäkipyöräilijä haluaa kuvata ajonsa toimintakameralla. Hän ajaa syrjäisellä alueella ja aikoo käyttää tallenteita vain omaksi ilokseen kotona. Tähän sovelletaan kotitalouksia koskevaa poikkeusta, vaikka henkilötietoja käsitellään jonkin verran.

Esimerkki: Henkilö seuraa ja kuvaa omaa puutarhaansa. Kiinteistö on aidattu, ja vain rekisterinpitäjä ja hänen perheensä käyvät puutarhassa säännöllisesti. Tähän sovelletaan kotitalouksia koskevaa poikkeusta, mikäli videovalvonta ei ulotu edes osittain yleiseen tilaan tai naapurikiinteistölle.

14.

³ Ks. myös johdanto-osan 18 kappale.

⁴ Unionin tuomioistuin, tuomio asiassa C-101/01, *rikosoikeudenkäynti vastaan Bodil Lindqvist*, 6.11.2003, 47 kohta.

⁵ Unionin tuomioistuin, tuomio asiassa C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11.12.2014, 33 kohta.

3 KÄSITTELYN LAINMUKAISUUS

15. Käsittelyn tarkoitus on määritettävä yksityiskohtaisesti ennen käyttöä (5 artiklan 1 kohdan b alakohta). Videovalvonnalla voi olla monia tarkoituksia, esimerkiksi kiinteistön ja muun omaisuuden suojelun tukeminen, ihmisten hengen ja fyysisen koskemattomuuden suojelun tukeminen tai todisteiden kerääminen siviilikanteita varten⁶. Nämä valvontatarkoitukset on dokumentoitava kirjallisesti (5 artiklan 2 kohta), ja ne on erikseen yksilöitävä jokaisen käytössä olevan valvontakameran osalta. Kamerat, joita yksi rekisterinpitäjä käyttää samaa tarkoitusta varten, voidaan dokumentoida yhdessä. Rekisteröidyille on myös ilmoitettava käsittelyn tarkoituksesta tai tarkoituksista 13 artiklan mukaisesti (ks. 7 jakso *Läpinäkyvyyttä ja tiedottamista koskevat velvollisuudet*). Videovalvonnan perustetta ei ole yksilöity riittävästi, jos perusteena on pelkästään ”turvallisuus” tai ”oman turvallisuus” (5 artiklan 1 kohdan b alakohta). Tämä on myös vastoin periaatetta, jonka mukaan henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (ks. 5 artiklan 1 kohdan a alakohta).
16. Periaatteessa kaikki 6 artiklan 1 kohdan mukaiset lainmukaiset perusteet voivat tulla kyseeseen videovalvontatietojen käsittelyn oikeusperusteena. Esimerkiksi 6 artiklan 1 kohdan c alakohtaa sovelletaan, jos kansallisessa lainsäädännössä säädetään velvollisuudesta suorittaa videovalvontaa⁷. Käytännössä todennäköisimmin käytettävät säännökset ovat kuitenkin:
-) 6 artiklan 1 kohdan f alakohta (oikeutettu etu)
 -) 6 artiklan 1 kohdan e alakohta (käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi).

Melko poikkeuksellisissa tapauksissa rekisterinpitäjä voi käyttää 6 artiklan 1 kohdan a alakohtaa (suostumus) käsittelyn oikeusperusteena.

3.1 Oikeutettu etu, 6 artiklan 1 kohdan f alakohta

17. Asetuksen 6 artiklan 1 kohdan f alakohdan oikeudellisen arvioinnin pitäisi perustua seuraaviin kriteereihin johdanto-osan 47 kappaleen mukaisesti.

3.1.1 Oikeutettujen etujen olemassaolo

18. Videovalvonta on lainmukaista, jos se on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutetun edun tarkoituksen täyttämiseksi, paitsi silloin kun rekisteröidyn edut perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut (6 artiklan 1 kohdan f alakohta). Rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut voivat olla oikeudellisia⁸, taloudellisia tai aineettomia etuja⁹. Rekisterinpitäjän on kuitenkin otettava huomioon, että jos rekisteröity vastustaa valvontaa 21 artiklan mukaisesti, rekisterinpitäjä voi jatkaa videovalvontaa kyseisen rekisteröidyn osalta vain silloin, jos kyseessä on *huomattavan tärkeä* oikeutettu etu, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet, taikka oikeusvaateiden laatimiseksi, esittämiseksi tai puolustamiseksi.
19. Todellinen vaaratilanne, omaisuuden suojele murroilta, varkauksilta tai ilkivallalta voivat muodostaa oikeutetun edun harjoittaa videovalvontaa.

⁶ Säännöt todisteiden keräämisestä siviilikanteita varten vaihtelevat jäsenvaltioittain.

⁷ Näissä ohjeissa ei analysoida eikä käsitellä yksityiskohtaisesti kansallista lainsäädäntöä, joka voi vaihdella jäsenvaltioittain.

⁸ Unionin tuomioistuin, tuomio asiassa C-13/16, *Rīgas satiksme*, 4.5.2017

⁹ Ks. tietosuojatyöryhmän asiakirja WP217.

20. Oikeutetun edun on oltava todellinen ja välitön (eli se ei saa olla kuvitteellinen tai spekulatiivinen)¹⁰. Todellisen elämän hätätilanteen - kuten vaurioiden tai aiempien vakavien häiriöiden – on oltava käsillä välittömästi ennen valvonnan aloittamista. Osoitusvelvollisuuden periaatteen vuoksi rekisterinpitäjien olisi viisasta dokumentoida nämä häiriöt (päivämäärä, tapa, taloudelliset tappiot) ja niihin liittyvät rikossyytteet. Näistä dokumentoiduista häiriötilanteista voidaan saada vahvaa näyttöä oikeutetusta edusta. Oikeutetun edun olemassaoloa sekä valvonnan tarpeellisuutta on arvioitava uudelleen määräajoin (esim. kerran vuodessa, olosuhteiden mukaisesti).

Esimerkki: Kauppias haluaa avata uuden kaupan ja asentaa siihen videovalvontajärjestelmän ilkivallan estämiseksi. Hän pystyy tilastojen avulla osoittamaan, että lähiympäristössä ilkivalta on erittäin todennäköistä. Myös naapurikaupan kokemukset ovat hyödyllisiä. Vahingon ei ole tarvinnut tapahtua kyseessä olevalle rekisterinpitäjälle. Jos lähiympäristön vahingot viittaavat vaaraan tai vastaavaan, ne voivat olla osoitus oikeutetusta edusta. Kansallisten tai yleisten rikostilastojen esittäminen ei kuitenkaan riitä, jos kyseessä olevaa aluetta tai nimenomaiselle kaupalle koituvia vaaroja ei analysoida.

- 21.
22. Välittömät vaaratilanteet voivat muodostaa oikeutetun edun esimerkiksi pankeissa tai arvotavaroita myyvissä kaupoissa (esim. kultasepäneliikkeet) tai alueilla, joilla tunnetusti tapahtuu omaisuusrikoksia (esim. huoltoasemat).
23. Yleisessä tietosuoja-asetuksessa myös todetaan selkeästi, että viranomaiset eivät voi käyttää käsittelynsä perusteena oikeutettua etua, jos ne suorittavat tehtäviään (6 artiklan 1 kohdan toinen lause).

3.1.2 Käsittelyn tarpeellisuus

24. Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään ("tietojen minimointi"), ks. 5 artiklan 1 kohdan c alakohta. Ennen videovalvontajärjestelmän asentamista rekisterinpitäjän pitäisi aina arvioida huolellisesti, ensinnäkin, onko tämä toimenpide sopiva halutun tavoitteen saavuttamiseksi ja, toiseksi, onko toimenpide asianmukainen ja tarpeellinen käsittelyn tarkoituksia varten. Videovalvontatoimenpiteet pitäisi valita vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa sellaisilla keinoilla, joilla ei puututa niin paljon rekisteröidyn perusoikeuksiin ja -vapauksiin.
25. Kun rekisterinpitäjä haluaa estää omaisuusrikokset, videovalvontajärjestelmän asentamisen sijasta, rekisterinpitäjä voisi myös toteuttaa vaihtoehtoisia turvatoimenpiteitä. Niitä voisivat olla esimerkiksi kiinteistön aitaaminen, vartijoiden säännöllinen partiointi, portinvartijajärjestelmän käyttö, valaistuksen parantaminen, turvalukkojen asentaminen, peukaloinnilla suojatut ikkunat ja ovet tai graffiteilta suojaavien pinnoitteiden tai päällysteiden levittäminen seiniin. Nämä toimenpiteet voivat olla murtoja, varkauksia ja ilkivaltaa vastaan yhtä tehokkaita kuin videovalvontajärjestelmät. Rekisterinpitäjän on arvioitava tapauskohtaisesti, voisivatko kyseiset toimenpiteet olla kohtuullinen ratkaisu.
26. Ennen kamerajärjestelmän käyttöä rekisterinpitäjän on arvioitava, missä ja milloin videovalvontatoimenpiteet ovat ehdottoman tarpeellisia. Yöaikaan ja aukioloaikojen ulkopuolella

¹⁰ Ks. tietosuojatyöryhmän asiakirja WP217, s. 24 ja seuraavat sivut, ks. myös unionin tuomioistuimen asia C-08/18, s. 44.

käytettävä valvontajärjestelmä täyttää tavallisesti rekisterinpitäjän tarpeet tämän omaisuudelle aiheutuvien vaarojen estämisessä.

27. Yleisesti ottaen rekisterinpitäjän tilojen suojaamiseen käytettävän videovalvonnan tarpeellisuus päättyy kiinteistön rajoihin.¹¹ Joissakin tapauksissa kiinteistön valvonta ei kuitenkaan riitä takaamaan tehokasta suojaa. Joissakin yksittäisissä tapauksissa voi olla tarpeen ulottaa videovalvonta tilojen välittömään läheisyyteen. Tässä yhteydessä rekisterinpitäjän olisi pohdittava fyysisiä ja teknisiä keinoja, esimerkiksi asiaankuulumattomien alueiden sulkemista pois kuvasta tai niiden pikselöintiä.

Esimerkki: Kirjakauppa haluaa suojella tilojaan ilkeiltä. Kameroilla pitäisi yleisesti kuvata vain itse tiloja, koska suojelua varten ei ole tarpeen vahtia naapuritiloja tai yleisiä alueita kirjakaupan tilojen lähellä.

- 28.
29. Käsittelyn tarpeellisuudesta herättää kysymyksiä myös tapa, jolla todisteita säilytetään. Joissakin tapauksissa voi olla tarpeen käyttää mustan laatikon kaltaisia ratkaisuja, joissa tallenne poistetaan automaattisesti tietyn säilytysajan jälkeen ja sitä voi käyttää vain häiriön tapahtuessa. Joissain tilanteissa ei ehkä ole tarpeen tallentaa videoaineistoa lainkaan, vaan käyttää sen sijaan reaaliaikaista valvontaa. Mustan laatikon kaltaisten ratkaisujen ja reaaliaikaisen valvonnan välisen valinnan pitäisi myös perustua tavoiteltuun tarkoitukseen. Jos videovalvonnan tarkoituksena on esimerkiksi säilyttää todisteita, reaaliaikaiset menetelmät eivät ole tavallisesti sopivia. Joskus reaaliaikainen valvonta voi myös olla tunkeilevampaa kuin aineiston säilyttäminen ja poistaminen automaattisesti tietyn ajan päästä (esimerkiksi, jos joku seuraa monitoria jatkuvasti, se voi olla tunkeilevampaa kuin se, että monitoria ei ole lainkaan ja kaikki aineisto tallennetaan suoraan mustaan laatikkoon). Tässä yhteydessä on otettava huomioon tietojen minimoinnin periaate (5 artiklan 1 kohdan c alakohta). Olisi myös pidettävä mielessä, että rekisterinpitäjä voisi mahdollisesti käyttää videovalvonnan sijasta turvallisuushenkilöstöä, joka pystyy reagoimaan ja puuttumaan asioihin välittömästi.

3.1.3 Etujen tasapainottaminen

30. Jos katsotaan, että videovalvonta on tarpeen rekisterinpitäjän oikeutettujen etujen suojaamiseksi, videovalvontajärjestelmä voidaan ottaa käyttöön vain, jos rekisteröidyn edut tai perusoikeudet ja -vapaudet eivät syrjäytä rekisterinpitäjän tai kolmannen osapuolen oikeutettuja etuja (esimerkiksi omaisuuden tai fyysisen koskemattomuuden suoja). Rekisterinpitäjän on otettava huomioon, 1) missä määrin valvonta vaikuttaa yksilöiden etuihin, perusoikeuksiin ja -vapauksiin ja 2) loukkaako se rekisteröidyn oikeuksia tai aiheuttaako se niille kielteisiä seurauksia. Etujen tasapainottaminen on siis pakollista. Siinä on arvioitava ja punnittava huolellisesti toisaalta perusoikeuksia ja -vapauksia ja toisaalta rekisterinpitäjän oikeutettuja etuja.

¹¹ Joissakin jäsenvaltioissa tästä voi myös olla kansallista lainsäädäntöä.

Esimerkki: Yksityinen pysäköintiyhtiö on dokumentoinut toistuvasti varkauksia alueelleen pysäköidyissä autoissa. Pysäköintialue on avoin alue, johon kuka tahansa pääsee helposti. Se on kuitenkin merkitty selkeästi aluetta ympäröivillä merkeillä ja liikenne-esteillä. Pysäköintiyhtiöllä on oikeutettu etu (varkauksien estäminen asiakkaiden autoissa) valvoa aluetta siihen aikaan päivästä, kun ongelmia esiintyy. Rekisteröityjä valvotaan rajattu aika, he eivät ole alueella viettämässä vapaa-aikaa, ja varkauksien estäminen on myös heidän etunsa mukaista. Tässä tapauksessa rekisterinpitäjän oikeutettu etu syrjäyttää rekisteröityjen edun olla joutumatta valvonnan kohteeksi.

Esimerkki: Ravintola päättää asentaa videokameroita WC-tiloihin niiden siisteyden valvomiseksi. Tässä tapauksessa rekisteröityjen oikeudet syrjäyttävät selkeästi rekisterinpitäjän edun, ja siksi kameroita ei voida asentaa.

31.

3.1.3.1 Tapauskohtaisten päätösten tekeminen

32. Koska etujen tasapainottaminen on asetuksen mukaan pakollista, päätös on tehtävä tapauskohtaisesti (ks. 6 artiklan 1 kohdan f alakohta). Abstrakteihin tilanteisiin viittaaminen tai samankaltaisten tapausten vertailu toisiinsa ei riitä. Rekisterinpitäjän on arvioitava rekisteröidyn oikeuksiin puuttumisen riskejä. Siinä ratkaisevaa on, miten voimakkaasti yksilön oikeuksiin ja vapauksiin puututaan.

33. Puuttumisen voimakkuuden arvioinnissa voidaan ottaa huomioon muun muassa kerättyjen tietojen tyyppiä (tietosisältöä), laajuutta (tietojen tallennustiheyttä, alueellista ja maantieteellistä laajuutta), kyseessä olevien rekisteröityjen määrää (joko yksilöiden määränä tai osuutena asiaankuuluvasta väestöstä), kyseessä olevaa tilannetta, rekisteröityjen ryhmän tosiasiallisia intressejä, vaihtoehtoisia keinoja sekä tietojen arvioinnin luonnetta ja laajuutta.

34. Tärkeitä tekijöitä tasapainottamisessa voivat olla valvottavan alueen koko ja valvottavien rekisteröityjen määrä. Videovalvonnan käyttöä syrjäisellä alueella (esimerkiksi luonnonvaraisten eläinten tarkkailuun tai kriittisen infrastruktuurin, kuten yksityisomisteisen radioantennin, suojeluun) on arvioitava eri tavalla kuin videovalvontaa jalankulkijoille tarkoitettulla alueella tai ostoskeskuksessa.

Esimerkki: Jos asennetaan autokamera (esimerkiksi todisteiden keräämiseksi onnettomuuden sattuessa), on tärkeää varmistaa, että kamera ei kuvaa jatkuvasti liikennettä eikä lähellä tietä olevia henkilöitä. Jos niin ei tehdä, etu, joka koskee videotallenteiden saamista todisteeksi melko teoreettisessa liikenneonnettomuuden tapauksessa, ei voi oikeuttaa tätä vakavaa puuttumista rekisteröityjen oikeuksiin.¹¹

35.

3.1.3.2 Rekisteröityjen kohtuulliset odotukset

36. Johdanto-osan 47 kappaleen mukaisesti oikeutetun edun olemassaoloa on arvioitava huolellisesti. Siihen on otettava mukaan rekisteröidyn kohtuulliset odotukset hänen henkilötietojensa käsittelyn aikana ja sen yhteydessä. Järjestelmällisessä valvonnassa rekisteröidyn ja rekisterinpitäjän välinen suhde voi vaihdella huomattavasti, ja se voi vaikuttaa siihen, mitä kohtuullisia odotuksia rekisteröidyllä voi olla. Kohtuullisten odotusten käsitteen tulkintaa ei pitäisi perustaa ainoastaan subjektiivisiin odotuksiin. Ratkaisevana kriteerinä pitäisi sen sijaan olla se, voisiko objektiivinen kolmas osapuoli kohtuudella odottaa ja päätellä joutuvansa valvonnan kohteeksi kyseisessä nimenomaisessa tilanteensa.

37. Työntekijä ei esimerkiksi useimmiten odota joutuvansa työpaikalla työnantajansa valvomaksi¹². Valvontaa ei myöskään odoteta omassa puutarhassa, asuinalueilla tai sairaalan tutkimus- ja hoituhuoneissa. Valvontaa ei ole myöskään kohtuullista odottaa pesu- tai saunatiloissa – tällaisissa tiloissa valvonta on voimakasta puuttumista rekisteröidyn oikeuksiin. Rekisteröidyt voivat kohtuullisesti odottaa, että kyseisissä tiloissa ei ole videovalvontaa. Pankin asiakas voi puolestaan odottaa, että häntä valvotaan pankin sisäpuolella tai pankkiautomaatilla.
38. Rekisteröidyt voivat odottaa myös, että valvontaa ei ole yleisessä käytössä olevilla alueilla etenkin, jos kyseisiä alueita käytetään tavallisesti rentoutumiseen, elpymiseen ja vapaa-ajan toimiin, sekä paikoissa, joissa ihmiset oleskelevat ja/tai ovat yhteydessä toisiinsa, kuten oleskelutiloissa, ravintoloiden pöydissä, puistoissa, elokuvissa ja kuntosaleilla. Näissä tapauksissa rekisteröidyn edut tai oikeudet ja vapaudet usein syrjäyttävät rekisterinpitäjän oikeudet edut.

Esimerkki: Rekisteröidyt eivät odota, että heitä valvotaan WC-tiloissa. Esimerkiksi tapaturmien ehkäisyyn käytettävä videovalvonta ei ole oikeasuhteista.

- 39.
40. Merkeillä, joilla rekisteröidylle ilmoitetaan videovalvonnasta, ei ole merkitystä määrittäessä, mitä rekisteröity voi kohtuudella odottaa. Tämä tarkoittaa, että esimerkiksi kauppias ei voi vedota siihen, että asiakkailta olisi *objektiivisesti* kohtuullisia odotuksia valvonnan kohteeksi joutumisesta vain siksi, että siitä ilmoitetaan heille sisäänkäynnin luona olevassa merkissä.

3.2 Käsittelyn tarpeellisuus yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi, 6 artiklan 1 kohdan e alakohta

41. Henkilötietoja voitaisiin käsitellä videovalvonnan kautta 6 artiklan 1 kohdan e alakohdan nojalla, jos se on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi.¹³ Tällainen käsittely ei ehkä ole mahdollista julkisen vallan käytön perusteella, mutta muut lainsäädännölliset perusteet, kuten vierailijoiden ja työntekijöiden ”terveyden ja turvallisuuden” suojeleminen, voivat tarjota rajoitetut mahdollisuudet käsittelylle, samalla ottaen huomioon yleisessä tietosuojasetuksessa säädettyt velvollisuudet ja rekisteröidyn oikeudet.
42. Jäsenvaltiot voivat pitää voimassa tai ottaa käyttöön videovalvontaa koskevaa erityistä kansallista lainsäädäntöä, kun ne haluavat mukauttaa yleisen tietosuojasetuksen sääntöjen soveltamista, ja määrittää asetusta täsmällisemmin käsittelyä koskevat erityisvaatimukset. Kansallisen lainsäädännön on oltava yleisessä tietosuojasetuksessa esitettyjen periaatteiden mukaista (esim. säilytyksen rajoittaminen, oikeasuhteisuus).

¹² Ks. myös Tietosuojatyöryhmä, lausunto 2/2017 tietojenkäsittelystä työpaikalla, WP249, hyväksytty 8.6.2017.

¹³ Kyseessä olevan käsittelyn perusteesta on säädettävä joko unionin oikeudessa tai jäsenvaltion lainsäädännössä, ja ”sen on oltava tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi” (6 artiklan 3 kohta).

3.3 6 artiklan 1 kohdan a alakohta

43. Suostumuksen on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen toimi, kuten suostumusta koskevassa ohjeessa määritetään¹⁴.
44. Järjestelmällisessä valvonnassa rekisteröityjen suostumusta voidaan käyttää 7 artiklan mukaisena oikeudellisena perusteena (ks. johdanto-osan 43 kappale) poikkeustapauksissa. Valvonnan luonteen mukaisesti tässä teknologiassa valvotaan yhdellä kerralla tuntematonta ihmismäärää. Rekisterinpitäjä tuskin pystyy todistamaan, että rekisteröity on antanut suostumuksensa ennen henkilötietojensa käsittelyä (7 artiklan 1 kohta). Jos oletetaan, että rekisteröity peruuttaa suostumuksensa, rekisterinpitäjän on vaikeaa todistaa, että henkilötietoja ei enää käsitellä (7 artiklan 3 kohta).

Esimerkki: Urheilijat voivat pyytää, että heitä seurataan yksittäisissä harjoituksissa heidän tekniikkansa ja suorituskykynsä analysoimiseksi. Jos taas koko joukkuetta seurataan urheiluseuran aloitteesta samaa tarkoitusta varten, suostumus ei usein ole pätevä, koska yksittäiset urheilijat saattavat tuntea, että heitä on painostettu antamaan suostumus, jotta heidän suostumuksensa ei vaikuttaisi haitallisesti joukkueveroihin.

- 45.
46. Jos rekisterinpitäjä haluaa vedota suostumukseen, sen velvollisuutena on varmistaa, että kaikki videovalvonnan kattavalle alueelle tulevat rekisteröidyt ovat antaneet suostumuksensa. Suostumuksen on täytettävä 7 artiklan ehdot. Merkitylle valvotulle alueelle tuleminen (esimerkiksi, jos ihmisiä pyydetään kulkemaan käytävästä tai portista valvotulle alueelle päästäkseen) ei ole suostumukseen tarvittava lausuma eikä selkeästi suostumusta ilmaiseva toimi, ellei se täytä 4 ja 7 artiklan mukaisia vaatimuksia, kuten kuvattu suostumusta koskevassa ohjeessa¹⁵.
47. Koska työnantajien ja työntekijöiden välillä on vallan epätasapaino, työnantajien ei useimmissa tapauksissa pitäisi perustaa henkilötietojen käsittelyä suostumukselle, koska suostumus on epätodennäköisesti annettu vapaaehtoisesti. Tässä yhteydessä olisi otettava huomioon suostumusta koskeva ohje.
48. Jäsenvaltioiden lainsäädännössä tai työehtosopimuksissa, myös työsopimuksissa, voidaan antaa erityisiä sääntöjä työntekijöiden henkilötietojen käsittelystä työsuhteen yhteydessä (ks. 88 artikla).

¹⁴ Tietosuojatyöryhmä, asetuksen 2016/679 mukaista suostumusta koskevat suuntaviivat (WP 259, rev. 01) – tietosuojaneuvoston hyväksymät

¹⁵ Tietosuojatyöryhmä, asetuksen 2016/679 mukaista suostumusta koskevat suuntaviivat (WP 259), jotka tietosuojaneuvosto on hyväksynyt ja jotka olisi otettava huomioon.

4 VIDEOAINEISTON LUOVUTTAMINEN KOLMANSILLE OSAPUOLILLE

49. Yleisen tietosuoja-asetuksen yleisiä säännöksiä sinänsä sovelletaan videotallenteiden luovuttamiseen kolmansille osapuolille.

4.1 Videoaineiston luovuttaminen kolmansille osapuolille yleisesti

50. Yleisen tietosuoja-asetuksen 4 artiklan 2 kohdassa luovuttaminen määritellään tietojen siirtämiseksi (esim. yksittäinen kommunikaatio), levittämiseksi (esim. verkkojulkaisu) tai asettamiseksi muutoin saataville. Kolmannet osapuolet määritellään 4 artiklan 10 kohdassa. Jos luovutus tehdään kolmansiin maihin tai kansainvälisille järjestöille, sovelletaan myös 44 artiklan ja sitä seuraavien artiklojen erityissäännöksiä.
51. Kaikki henkilötietojen luovuttaminen on erillistä henkilötietojen käsittelyä, jota varten rekisterinpitäjällä on oltava käsittelyn oikeusperuste 6 artiklan mukaisesti.

Esimerkki: Rekisterinpitäjällä, joka haluaa ladata tallenteen verkkoon, on oltava käsittelyn oikeusperuste kyseistä käsittelyä varten. Sen on esimerkiksi saatava rekisteröidyltä suostumus 6 artiklan 1 kohdan a alakohdan mukaisesti.

- 52.
53. Videoaineisto voidaan siirtää kolmansille osapuolille muuta kuin sitä tarkoitusta varten, jonka vuoksi tiedot on kerätty, 6 artiklan 4 kohdan sääntöjen mukaisesti.

Esimerkki: Pysäköintialueen esteeseen on asennettu videovalvonta vaurioiden selvittämistä varten. Vaurio tapahtuu, ja tallenne siirretään asianajajalle kanteen nostamiseksi. Tässä tapauksessa tallenteen tarkoitus on sama kuin siirtämisen tarkoitus.

Esimerkki: Pysäköintialueen esteeseen on asennettu videovalvonta vaurioiden selvittämistä varten. Tallenne julkaistaan verkossa pelkästään ajanvietteeksi. Tässä tapauksessa tarkoitus on muuttunut, eikä se ole yhteensopiva alkuperäisen tarkoituksen kanssa. Tälle käsittelylle (julkaisulle) olisi lisäksi ongelmallista löytää käsittelyn oikeusperustetta.

- 54.
55. Ulkopuolisen vastaanottajan on tehtävä oma oikeudellinen analyysinsä ja erityisesti määritettävä käsittelyn oikeusperuste 6 artiklan mukaisesti omaa käsittelyään varten (esim. aineiston vastaanotto).

4.2 Videoaineiston luovuttaminen lainvalvontaviranomaisille

56. Videotallenteiden luovuttaminen lainvalvontaviranomaisille on myös itsenäinen prosessi, joka edellyttää rekisterinpitäjältä erillistä perustelua.
57. Yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohdan mukaan käsittely on laillista, jos se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Vaikka sovellettava poliisilainsäädäntö kuuluu ainoastaan jäsenvaltioiden toimivaltaan, jokaisen jäsenvaltion yleisissä säännöissä todennäköisesti säädetään todisteiden siirtämistä lainvalvontaviranomaisille. Yleisen tietosuoja-asetuksen säännöksiä sovelletaan tiedot luovuttavan rekisterinpitäjän suorittamaan käsittelyyn. Jos rekisterinpitäjän on kansallisen lainsäädännön mukaan tehtävä yhteistyötä lainvalvonnan kanssa (esim. tutkinnassa), tietojen luovuttamisen käsittelyn oikeusperuste on 6 artiklan 1 kohdan c alakohdan lakisääteinen velvollisuus.

58. Käyttötarkoitussidonnaisuus 6 artiklan 4 kohdassa ei siksi yleensä aiheuta ongelmia, koska luovuttaminen perustuu yksiselitteisesti jäsenvaltion lainsäädäntöön. Siksi ei ole tarpeellista ottaa huomioon a–e alakohdassa tarkoitettuja tarkoituksen muutosta koskevia erityisvaatimuksia.

Esimerkki: Kauppias kuvaa kauppansa sisäänkäyntiä. Tallennuksessa näkyy, kun henkilö varastaa toisen henkilön lompakon. Poliisi pyytää rekisterinpitäjää luovuttamaan aineiston tutkimuksen avuksi. Siinä tapauksessa kauppias käyttäisi käsittelyn oikeusperusteena 6 artiklan 1 kohdan c alakohtaa (lakisääteinen velvollisuus) luettuna yhdessä asiaan sovellettavan kansallisen lainsäädännön kanssa, joka koskee poliisin suorittamaa siirrettyjen tietojen käsittelyä.

59.

Esimerkki: Kauppaan on asennettu kamera turvallisuussyistä. Kauppias uskoo, että siihen on tallentunut jotakin epäilyttävää, ja päättää lähettää aineiston poliisille (ilman tietoa minkäänlaisen tutkinnan käynnissä olosta). Tässä tapauksessa kauppiaan on yleensä arvioitava täyttyvätkö 6 artiklan 1 kohdan f alakohdan edellytykset. Näin on yleensä silloin, jos kauppialla on kohtuulliset syyt epäillä, että rikos tapahtunut.

60.

61. Itse lainvalvontaviranomaisten suorittamassa henkilötietojen käsittelyssä ei noudateta yleistä tietosuojasetusta (ks. 2 artiklan 2 kohdan d alakohta) vaan direktiiviä lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta ((EU) 2016/680).

5 ERITYISIÄ HENKILÖTIETORYHMIÄ KOSKEVA KÄSITTELY

62. Videovalvontajärjestelmien kautta kerätään tavallisesti valtavia määriä henkilötietoja, jotka voivat paljastaa luonteeltaan erittäin henkilökohtaisia tietoja ja jopa kuulua erityisiin henkilötietoryhmiä. Alun perin videoiden avulla kerättyjä, nähtävästi merkityksettömiä tietoja, voidaan käyttää siten, että niiden avulla päätellään muita tietoja eri tarkoituksen saavuttamiseksi (esim. kartoittamaan yksilön tapoja). Videovalvontaa ei kuitenkaan aina katsota erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyksi.

Esimerkki: Videoaineistoa, joka näyttää rekisteröidyn käyttämässä silmälaseja tai pyörätuolia, ei sellaisenaan katsota erityisesti henkilötietoryhmiksi.

- 63.
64. Jos videota kuitenkin käsitellään erityisiin henkilötietoryhmiin kuuluvien tietojen päättelemiseksi, sovelletaan 9 artiklaa.

Esimerkki: Poliittiset mielipiteet voitaisiin esimerkiksi päätellä kuvista, joissa esitetään tunnistettavia rekisteröityjä osallistumassa tapahtumaan, lakkoon jne. Tämä kuuluisi 9 artiklan soveltamisalaan.

Esimerkki: Videokameran asentaminen sairaalaan potilaiden terveydentilan seuraamiseksi katsottaisiin erityisten henkilötietoryhmien käsittelyksi (9 artikla).

- 65.
66. Yleisesti ottaen aina videovalvontajärjestelmää asennettaessa on periaatteessa otettava huolellisesti huomioon tietojen minimoinnin periaate. Näin ollen, vaikka 9 artiklan 1 kohtaa ei sovelleta, rekisterinpitäjän pitäisi aina pyrkiä minimoimaan riski siitä, että muita arkaluonteisia tietoja (9 artiklan mukaisten tietojen lisäksi) paljastavaa materiaalia tallennettaisiin, niiden tarkoituksesta riippumatta.

Esimerkki: Kirkkoa kuvaava videovalvonta ei sellaisenaan kuulu 9 artiklan soveltamisalaan. Rekisterinpitäjän on kuitenkin rekisteröidyn etuja arvioidessaan tehtävä erityisen huolellisesti 6 artiklan 1 kohdan f alakohdan mukainen arviointi ja otettava huomioon tietojen luonne sekä riski muiden (9 artiklan mukaisten tietojen lisäksi) arkaluonteisten tietojen kuvaamisesta.

- 67.
68. Jos videovalvontajärjestelmää käytetään erityisten henkilötietoryhmien käsittelyyn, rekisterinpitäjän on yksilöitävä sekä erityisten henkilötietoryhmien käsittelyä koskeva 9 artiklan mukainen poikkeus (toisin sanoen poikkeus yleisestä säännöstä, jonka mukaan erityisiä henkilötietoryhmiin kuuluvia tietoja ei pitäisi käsitellä) ja 6 artiklan mukainen käsittelyn oikeusperuste.
69. Esimerkiksi 9 artiklan 2 kohdan c alakohtaa ”*käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi*” voitaisiin – teoriassa ja poikkeuksellisesti – käyttää, mutta rekisterinpitäjän olisi perusteltava, että on ehdottoman välttämätöntä suojata henkilön elintärkeitä etuja, todistettava, että tämä ”*rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan*”. Rekisterinpitäjä ei saa myöskään käyttää järjestelmää mihinkään muuhun tarkoitukseen.
70. Tässä on tärkeää panna merkille, että jokaista 9 artiklassa lueteltua poikkeusta ei todennäköisesti voida käyttää perustelemaan erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyä videovalvonnassa. Tarkemmin sanottuna videovalvonnan yhteydessä kyseisiä tietoja käsittelevät rekisterinpitäjät eivät voi vedota 9 artiklan 2 kohdan e alakohtaan, jossa sallitaan käsittely, joka koskee

henkilötietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi. Pelkästään kameran kuvausalueelle tuleminen ei tarkoita, että rekisteröity aikoo saattaa julkisiksi itseensä liittyviä erityisiä henkilötietoryhmiä.

71. Erityisiä henkilötietoryhmiä koskeva käsittely edellyttää lisäksi tiettyjen velvollisuuksien tavallista tarkempaa jatkuvaa noudattamista, esimerkiksi tarvittaessa erittäin korkeaa turvallisuustasoa ja tietosuojaa koskevaa vaikutustenarviointia.

Esimerkki: Työnantaja ei saa käyttää mielenosoitusta esittäviä videovalvontatallenteita lakkoilijoiden tunnistamiseksi.

72.

5.1 Biometrinen tietojen käsittelyyn liittyvät yleiset näkökohdat

73. Biometrinen tietojen ja erityisesti kasvotunnistuksen käyttöön sisältyy suuria riskejä rekisteröityjen oikeuksille. On ratkaisevan tärkeää, että näiden teknologioiden käytössä noudatetaan asianmukaisesti yleisessä tietosuojasetuksessa esitettyjä lainmukaisuuden, tarpeellisuuden, oikeasuhteisuuden ja tietojen minimoinnin periaatteita. Ottaen huomioon, että näiden teknologioiden käyttö voidaan katsoa erityisen tehokkaaksi, rekisterinpitäjien pitäisi aivan ensin arvioida sen vaikutus perusoikeuksiin ja -vapauksiin ja miettiä, voidaanko käsittelyn laillinen tarkoitus saavuttaa vähemmän tunkeilevilla keinoilla.
74. Jotta tiedot voitaisiin katsoa yleisessä tietosuojasetuksessa määritellyiksi biometrisiksi tiedoiksi, käsittelemättömien tietojen, kuten luonnollisen henkilön fyysisten, fysiologisten tai käyttäytymisen ominaisuuksien, käsittelystä on seurattava näiden ominaisuuksien mittaamista. Koska biometriset tiedot ovat tulosta tällaisista mittauksista, yleisen tietosuojasetuksen 4 artiklan 14 kohdassa todetaan, että ne ovat *”luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, (...), joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa”*. Henkilöä koskevaa videoaineistoa ei siis voida sellaisenaan katsoa 9 artiklan mukaisesti biometrisiksi tiedoiksi, jos sitä ei ole erityisesti teknisesti käsitelty siten, että voidaan myötävaikuttaa henkilön tunnistamiseen.¹⁶
75. Jotta biometrinen tietojen käsittely voidaan katsoa (9 artiklan mukaisesti) erityisten henkilötietoryhmien käsittelyksi, biometrisiä tietoja on käsiteltävä *”henkilön yksiselitteistä tunnistamista varten”*.
76. Yhteenvetona voidaan todeta, että 4 artiklan 14 kohdan ja 9 artiklan nojalla on otettava huomioon kolme kriteeriä:
- **tietojen luonne:** luonnollisen henkilön fyysisiin, fysiologisiin tai käyttäytymisen ominaisuuksiin liittyvät tiedot
 - **käsittelyn keinot ja tapa:** *”teknisellä käsittelyllä”* saadut tiedot

¹⁶ Yleisen tietosuojasetuksen johdanto-osan 51 kappaleessa tuetaan tätä analyysia toteamalla, että *”[v]alokuvien käsittelyä ei olisi automaattisesti katsottava henkilötietojen erityisryhmien käsittelyksi, koska valokuvat kuuluvat biometrinen tietojen määrittelyn piiriin ainoastaan siinä tapauksessa, että niitä käsitellään erityisin teknisin menetelmin, jotka mahdollistavat luonnollisen henkilön yksilöllisen tunnistamisen tai todentamisen”*.

- **käsittelyn tarkoitus:** tietoja on käytettävä luonnollisen henkilön yksiselitteistä tunnistamista varten.

77. Biometrisen tunnistamistoiminnon sisältävän videovalvonnan käyttö, jonka yksityiset tahot ovat asentaneet omia tarkoituksiaan varten (esimerkiksi markkinointia, tilastoja ja jopa turvallisuutta varten), edellyttää useimmissa tapauksissa kaikkien rekisteröityjen nimenomaista suostumusta (9 artiklan 2 kohdan a alakohta), mutta myös muuta soveltuvaa 9 artiklan poikkeusta voidaan käyttää.

Esimerkki: Palveluaan parantaakseen yksityinen yritys vaihtaa lentoaseman matkustajien tarkastuspisteet (matkatavaroiden luovutusasteissa, koneeseen noustaessa) videovalvontajärjestelmiin, joissa käytetään kasvontunnistustekniikoita sellaisten matkustajien henkilöllisyyden todentamiseksi, jotka ovat antaneet suostumuksensa kyseiseen menettelyyn. Koska käsittely kuuluu 9 artiklan soveltamisalaan, matkustajien, jotka ovat antaneet aiemmin nimenomaisen ja tietoisin suostumuksensa, on rekisteröitävä itsensä esimerkiksi automaattisella päätteellä voidakseen luoda ja rekisteröidä tarkastuskorttiinsa liittyvän kasvokuvan, josta heidät tunnistetaan. Tarkastuspisteet, joissa on kasvontunnistus, on erotettava selvästi. Ne on esimerkiksi asennettava telineen sisälle, jotta ei kuvattaisi niiden henkilöiden biometrisiä malleja, jotka eivät ole antaneet suostumustaan. Vain matkustajat, jotka ovat antaneet aiemmin suostumuksensa ja rekisteröityneet, käyttävät biometrisellä järjestelmällä varustettua telinettä.

Esimerkki: Rekisterinpitäjä valvoo rakennukseensa pääsyä kasvontunnistusmenetelmällä. Ihmiset voivat käyttää tätä pääsytapaa vain, jos he ovat antaneet nimenomaisen tietoisin suostumuksensa (9 artiklan 2 kohdan mukaisesti) etukäteen. Sen varmistamiseksi, että ketään, joka ei ole antanut ennalta suostumustaan, ei kuvata, rekisteröidyn olisi kuitenkin itse käynnistettävä kasvontunnistusmenetelmä, esimerkiksi nappia painamalla. Käsittelyn lainmukaisuuden varmistamiseksi rekisterinpitäjän on aina tarjottava rakennukseen pääsulle vaihtoehtoinen tapa, johon ei kuulu biometristä käsittelyä, esimerkiksi kulkuluvat tai avaimet.

- 78.
79. Tämän tyyppisissä tapauksissa, joissa luodaan biometrisiä malleja, rekisterinpitäjien on varmistettava, että kun on saatu tulos, joka vastaa mallia tai ei vastaa sitä, kaikki väliaikaiset mallit poistetaan välittömästi ja suojatusti. Väliaikaisella mallilla tarkoitetaan malleja, jotka tehdään menettelyn aikana (rekisteröidyn nimenomaisen ja tietoisin suostumuksen perusteella) niiden vertaamiseksi rekisteröityjen rekisteröitymisen aikana tekemiin malleihin. Rekisteröitymistä varten luotuja malleja pitäisi säilyä vain käsittelyn tarkoituksen toteuttamista varten, eikä niitä pitäisi säilyttää tai arkistoida.
80. Jos käsittelyn tarkoituksena kuitenkin on esimerkiksi yhden ihmisryhmän erottaminen toisesta mutta ei kenenkään yksiselitteinen tunnistaminen, käsittely ei kuulu 9 artiklan soveltamisalaan.

Esimerkki: Kauppias haluaisi mukauttaa mainontaansa sellaisten asiakkaiden sukupuoleen ja ikään liittyvien ominaisuuksien perusteella, jotka on kuvattu videovalvontajärjestelmällä. Jos järjestelmä ei luo biometrisiä malleja, joilla voidaan tunnistaa henkilöt yksiselitteisesti, vaan se vain havaitsee kyseiset fyysiset ominaisuudet, joiden nojalla henkilö voidaan luokitella, käsittely ei kuulu 9 artiklan soveltamisalaan (kunhan muunlaisia erityisiin henkilötietoryhmiin kuuluvia tietoja ei käsitellä).

- 81.
82. Asetuksen 9 artiklaa sovelletaan kuitenkin, jos rekisterinpitäjä säilyttää biometrisiä tietoja (useimmiten malleilla, jotka luodaan erottamalla keskeiset ominaisuudet käsittelemättömistä biometrisistä tiedoista (esim. kasvojen mittaukset kuvasta), jotta henkilö voidaan tunnistaa

yksiselitteisesti. Jos rekisterinpitäjä haluaa havaita rekisteröidyn, kun tämä tulee uudelleen alueelle tai menee toiselle alueelle (esimerkiksi jatkuvan mukautetun mainonnan suunnittelemiseksi), tarkoituksena olisi silloin luonnollisen henkilön yksiselitteinen tunnistaminen, jolloin käsittely kuuluisi alusta alkaen 9 artiklan soveltamisalaan. Tästä voisi olisi kyse, jos rekisterinpitäjä säilyttäisi luotuja malleja tarjotakseen lisää yksilöllistä mainontaa useilla mainostauluilla eri paikoissa kaupan sisällä. Koska järjestelmä käyttää fyysisiä ominaisuuksia tiettyjen kameran kuvausalueelle takaisin tulevien henkilöiden (kuten ostoskeskuksessa kävijöiden) havaitsemiseen ja seuraamiseen, se olisi biometrinen tunnistusmenetelmä, koska sillä on tarkoitus tunnistaa henkilö käyttämällä tiettyä teknistä käsittelyä.

Esimerkki: Kauppias on asentanut kasvotunnistusjärjestelmän kauppaansa voidakseen mukauttaa ihmisille kohdistamaansa mainontaa. Rekisterinpitäjän on saatava kaikilta rekisteröidyiltä nimenomainen ja tietoinen suostumus ennen tämän biometrisen järjestelmän käyttöä ja yksilöllisen mainonnan toteuttamista. Järjestelmä olisi lainvastainen, jos siinä kuvataan kävijöitä tai ohikulkijoita, jotka eivät ole antaneet suostumustaan biometrisen mallinsa luomiseen, vaikka heidän mallinsa poistettaisiinkin mahdollisimman lyhyen ajan kuluessa. Tällaiset väliaikaiset mallit ovat kuin ovatkin biometrisiä tietoja, joita käsitellään sellaisen henkilön tunnistamiseksi yksiselitteisesti, joka ei välttämättä halua saada kohdennettua mainontaa.

83.

84. Tietosuojaneuvosto huomauttaa, että joitakin biometrisiä järjestelmiä asennetaan valvomattomiin ympäristöihin¹⁷, mikä tarkoittaa, että järjestelmään sisältyy kaikkien kameran kuvausalueen ohittavien ihmisten kasvojen valikoimatonta kuvaamista, myös henkilöiden, jotka eivät ole antaneet suostumustaan biometriselle laitteelle eivätkä siten biometrinen mallien luomiselle. Näitä malleja verrataan malleihin, jotka on luotu rekisteröidyistä, jotka ovat antaneet suostumuksensa etukäteen rekisteröitymisprosessissa (eli biometrisen laitteen käyttäjistä), jotta rekisterinpitäjä voisi tunnistaa, onko henkilö biometrisen laitteen käyttäjä vai ei. Tässä tapauksessa järjestelmä on usein suunniteltu erottamaan henkilöt, jotka se haluaa tunnistaa tietokannasta, niiden joukosta, jotka eivät ole rekisteröityneet. Koska tarkoituksena on luonnollisten henkilöiden yksiselitteinen tunnistaminen, yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan mukainen poikkeusperuste tarvitaan edelleen kaikilta, jotka tulevat kameran kuvaamaksi.

¹⁷ Tämä tarkoittaa, että biometrinen laite sijaitsee yleisölle avoimessa tilassa ja se pystyy toimimaan kaikkien ohikulkevien osalta toisin kuin valvotuissa ympäristöissä olevat biometriset järjestelmät, joita voidaan käyttää vain suostumuksen antaneen henkilön osallistuessa.

Esimerkki: Hotellissa käytetään videovalvontaa, joka ilmoittaa hotellinjohtajalle automaattisesti VIP-vieraan saapumisesta, kun vieraiden kasvoja tunnistetaan. Nämä VIP-vieraat ovat antaneet etukäteen nimenomaisen suostumuksensa kasvontunnistuksen käyttöön, ennen kuin heidät on rekisteröity sitä varten perustettuun tietokantaan. Nämä biometrinen tietojen käsittelyjärjestelmät olisivat lainvastaisia, paitsi jos kaikki muut (VIP-vieraiden tunnistamiseksi) seuratut vieraat ovat antaneet suostumuksensa käsittelylle yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohdan mukaisesti.

Esimerkki: Rekisterinpitäjä asentaa kasvontunnistuksella varustetun videovalvontajärjestelmän johtamansa konserttisalin sisäänkäyntiin. Rekisterinpitäjän on perustettava selvästi erotetut sisäänkäynnit: yksi, jossa on biometrinen järjestelmä, ja yksi ilman sitä (jossa esimerkiksi skannataan lippu). Biometrisillä laitteilla varustetut sisäänkäynnit on asennettava ja niille kulku on järjestettävä siten, että järjestelmä ei kuvaa niiden katsojien biometriä malleja, jotka eivät ole antaneet suostumustaan.

85.

86. Kun yleisen tietosuoja-asetuksen 9 artiklan mukaan vaaditaan suostumusta, rekisterinpitäjä ei saa asettaa palvelujensa saatavuuden ehdoksi biometrisen käsittelyn hyväksymistä. Toisin sanoen, varsinkin silloin, kun biometrinen käsittelyä käytetään henkilöllisyyden todentamistarkoituksiin, rekisterinpitäjän on tarjottava vaihtoehtoinen ratkaisu, johon ei kuulu biometrinen käsittely – ilman rajoituksia tai lisäkustannuksia rekisteröidylle. Tätä vaihtoehtoista ratkaisua tarvitaan myös sellaisia henkilöitä varten, jotka eivät täytä biometrisen laitteen asettamia rajoituksia (rekisteröinti tai biometrinen tietojen lukeminen ei onnistu, käyttö on vaikeaa vammaisuuden vuoksi jne.). Lisäksi sen varalta, että biometrinen laite ei ole käytössä (kuten laitteen toimintahäiriö), on otettava käyttöön vararatkaisu, jolla varmistetaan ehdotetun palvelun jatkuvuus, mutta joka voidaan kuitenkin rajoittaa poikkeukselliseen käyttöön. Poikkeustapauksissa kyseessä voi olla tilanne, jossa biometrinen tietojen käsittely on sopimuksen nojalla tarjotun palvelun ydintoimintaa. Tästä käy esimerkiksi museo, jossa järjestetään näyttely kasvontunnistuslaitteen käytöstä, jolloin rekisteröity ei voi kieltäytyä biometrinen tietojen käsittelystä, jos hän haluaa osallistua näyttelyyn. Tällaisessa tapauksessa 9 artiklan mukaisesti edellytetty suostumus on edelleen pätevä, jos 7 artiklan vaatimukset täytetään.

5.2 Riskien minimoimiseksi ehdotetut toimenpiteet biometrinen tietojen käsittelyssä

87. Tietojen minimoinnin periaatteen mukaisesti rekisterinpitäjien on varmistettava, että mallin rakentamiseen käytetystä digitaalikuvasta otetut tiedot eivät ole kohtuuttomia ja että ne sisältävät vain erityistarkoitukseen tarvittavat tiedot. Näin estetään mahdollinen jatkokäsittely. Käyttöön olisi otettava toimenpiteitä, joilla varmistetaan, että malleja ei voida siirtää biometrinen järjestelmien välillä.
88. Tunnistaminen ja todentaminen/vahvistaminen edellyttävät todennäköisesti mallin säilyttämistä myöhempää vertailua varten. Rekisterinpitäjän on mietittävä, mikä on asianmukaisin paikka tietojen säilyttämiseen. Valvotussa ympäristössä (rajatuissa käytävissä tai tarkastuspisteissä) mallit on tallennettava käyttäjän pitämään yksittäiseen laitteeseen, joka on yksinomaan hänen valvonnassaan (älypuhelin tai henkilökortti), tai – kun se on tarpeen erityistarkoituksia varten ja kun kyse on objektiivisista tarpeista – tallennettava keskitettyyn tietokantaan salatusta muodossa, jonka avain/salasana on vain kyseisen henkilön hallussa, jotta voidaan estää luvaton pääsy malliin tai säilytyspaikkaan. Jos rekisterinpitäjä ei pysty estämään malleihin pääsyä, sen on toteutettava asianmukaiset toimenpiteet, joilla varmistetaan tallennettujen tietojen turvallisuus. Tähän voi kuulua mallin salaaminen salausalgoritmia käyttämällä.

89. Rekisterinpitäjän on joka tapauksessa toteutettava asianmukaiset varotoimet, jotta käsiteltyjen tietojen saatavuus, eheys ja luottamuksellisuus voidaan säilyttää. Tätä varten rekisterinpitäjän on toteutettava erityisesti seuraavat toimenpiteet: tietojen jakaminen osiin siirtämisen ja säilyttämisen aikana, biometrinen mallien ja käsittelemättömien tietojen tai henkilöllisyyttä koskevien tietojen tallentaminen erillisiin tietokantoihin, biometrinen tietojen (erityisesti biometrinen mallien) salaaminen, salausta ja avaimenhallintaa koskevan käytännön määrittäminen, organisatoristen ja teknisten toimenpiteiden käyttöönotto petosten paljastamiseksi, eheyskoodin (esimerkiksi allekirjoituksen tai tunnisteen) liittäminen tietoihin ja ulkopuolisten pääsyn estäminen biometrisiin tietoihin. Tällaisia toimenpiteitä on kehitettävä entisestään teknologian edistyessä.
90. Rekisterinpitäjien on myös poistettava käsittelemättömät tiedot (kasvokuvat, äänisignaalit, kävelyntunnistus jne.) ja varmistettava, että poistaminen on tehokasta. Jos käsittelylle ei ole enää lainmukaista käsittelyn oikeusperustaa, käsittelemättömät tiedot on poistettava. Mikäli biometrisiä malleja johdetaan tällaisista tiedoista, voidaan todellakin katsoa, että tietokantojen luominen on vähintään yhtä suuri uhka (koska aina ei ole ehkä helppoa lukea biometristä mallia tietämättä, miten se on ohjelmoitu, kun taas käsittelemättömät tiedot ovat kaikkien mallien rakenneosia). Jos rekisterinpitäjän pitäisi säilyttää kyseiset tiedot, on tutkittava kohinaa lisääviä menetelmiä (kuten vesileimausta), joilla mallin luomisesta tehtäisiin mahdotonta. Rekisterinpitäjän on myös poistettava biometriset tiedot ja mallit, jos luku- ja vertailupäätteeseen tai tallennuspalvelimelle päästään luvattomasti, ja poistettava kaikki tiedot, jotka eivät ole hyödyllisiä myöhempää käsittelyä varten biometrisen laitteen elinkaaren loppuun.

6 REKISTERÖIDYN OIKEUDET

91. Videovalvonnan avulla suoritettujen henkilötietojen käsittelyn tiettyjen ominaisuuksien vuoksi, joitakin yleisen tietosuoja-asetuksen mukaisia rekisteröidyn oikeuksia on selkeytettävä. Tämä luku ei kuitenkaan ole tyhjentävä, ja kaikkia yleisen tietosuoja-asetuksen mukaisia oikeuksia sovelletaan henkilötietojen käsittelyyn videovalvonnassa.

6.1 Oikeus saada pääsy tietoihin

92. Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä. Videovalvonnassa tämä tarkoittaa, että jos tietoja ei säilytetä tai siirretä millään tavalla, kun reaaliaikaisen seurannan hetki on ohi, rekisterinpitäjä voi antaa tietoa vain siitä, että henkilötietoja ei enää käsitellä (lukuun ottamatta 13 artiklan mukaisia yleisiä tiedotusvelvollisuuksia, ks. 7 jakso – *Läpinäkyvyyttä ja tiedottamista koskevat velvollisuudet*) Jos tietoja kuitenkin edelleen käsitellään, kun pyyntö tehdään (eli jos tietoja säilytetään tai käsitellään jatkuvasti jollakin muulla tavalla), rekisteröidyn pitäisi saada pääsy tietoihin ja inormatiota15 artiklan mukaisesti.
93. Tietoihin pääsyä koskevaan oikeuteen voidaan kuitenkin soveltaa useita rajoituksia joissakin tapauksissa.
-) Yleisen tietosuoja-asetuksen 15 artiklan 4 kohdan mukainen haitallinen vaikuttaminen muiden oikeuksiin
94. Koska samaan videovalvonnan jaksoon voidaan kuvata rekisteröityjä miten paljon tahansa, seulonta aiheuttaisi muiden rekisteröityjen henkilötietojen lisäkäsittelyä. Jos rekisteröity haluaa saada jäljennöksen aineistosta (15 artiklan 3 kohta), se voi vaikuttaa haitallisesti muiden aineistossa olevien rekisteröityjen oikeuksiin ja vapauksiin. Sen estämiseksi rekisterinpitäjän olisi siksi otettava huomioon, että videon tunkeilevan luonteen vuoksi rekisterinpitäjän ei pitäisi tietyissä tapauksissa luovuttaa videota, jos muita rekisteröityjä voidaan tunnistaa. Kolmansien osapuolten suojaamista ei pitäisi kuitenkaan käyttää tekosyynä estämään yksilöiden tietoihin pääsyä koskevia laillisia vaatimuksia. Tällaisissa tapauksissa rekisterinpitäjän pitäisi ottaa käyttöön teknisiä toimenpiteitä tietoihin pääsyä koskevan pyynnön täyttämiseksi (esimerkiksi kuvanmuokkaus, kuten naamiointi tai salausta). Rekisterinpitäjillä ei kuitenkaan ole velvollisuutta toteuttaa tällaisia teknisiä toimenpiteitä, jos ne pystyvät muutoin varmistamaan, että ne pystyvät vastaamaan 15 artiklan mukaiseen pyyntöön 12 artiklan 3 kohdassa säädetyssä määräajassa.
-) Yleisen tietosuoja-asetuksen 11 artiklan 2 kohdan mukaisesti rekisterinpitäjä ei pysty tunnistamaan rekisteröityä
95. Jos videolta ei pystytä hakemaan henkilötietoja (eli rekisterinpitäjän pitäisi todennäköisesti käydä läpi suuri määrä tallennettua aineistoa löytääkseen kyseessä olevan rekisteröidyn), rekisterinpitäjä ei ehkä pysty tunnistamaan rekisteröityä.
96. Näistä syistä rekisteröidyn pitäisi (sen lisäksi, että hän osoittaa henkilöllisyytensä henkilöasiakirjalla tai asioimalla henkilökohtaisesti) rekisterinpitäjälle osoittamassaan pyynnössä yksilöidä, milloin – kohtuullisessa aikavälissä, joka on oikeassa suhteessa kuvattujen rekisteröityjen määrään – hän tuli valvotulle alueelle. Rekisterinpitäjän pitäisi ilmoittaa rekisteröidylle etukäteen, mitä tietoja tarvitaan, jotta rekisterinpitäjä voi noudattaa pyyntöä. Jos rekisterinpitäjä pystyy osoittamaan, ettei se pysty tunnistamaan rekisteröityä, rekisterinpitäjän on ilmoitettava asiasta rekisteröidylle, jos tämä on mahdollista. Tällaisessa tilanteessa

rekisterinpitäjän olisi rekisteröidylle antamassaan vastauksessa ilmoitettava täsmällisestä seurantaan kuuluneesta alueesta, käytössä olleiden kameroiden tarkastamisesta jne., jotta rekisteröity ymmärtää täysin, mitä henkilötietoja hänestä on ehkä käsitelty.

Esimerkki: Jos rekisteröity pyytää jäljennöstä henkilötiedoistaan, joita on käsitelty sellaisen ostoskeskuksen sisäänkäynnin videovalvonnassa, jossa käy päivittäin 30 000 ihmistä, rekisteröidyn on yksilöitävä noin tunnin tarkkuudella, milloin hän ohitti valvotun alueen. Jos rekisterinpitäjä käsittelee aineistoa edelleen, videosta olisi annettava jäljennös. Jos samasta aineistosta voidaan tunnistaa muita rekisteröityjä, aineiston kyseinen osa olisi anonymisoitava (esimerkiksi sumentamalla jäljennös tai sen osia) ennen kuin jäljennös annetaan sitä pyytäneelle rekisteröidylle.

Esimerkki: Jos rekisterinpitäjä poistaa automaattisesti kaiken videoaineiston esimerkiksi kahden päivän kuluessa, rekisterinpitäjä ei pysty toimittamaan rekisteröidylle videokuvaa niiden kahden päivän jälkeen. Jos rekisterinpitäjä saa pyynnön niiden kahden päivän jälkeen, rekisteröidylle olisi ilmoitettava tästä.

97.

) Yleisen tietosuoja-asetuksen 12 artiklan mukaiset kohtuuttomat pyynnöt

98.

Jos rekisteröity esittää kohtuuttomia tai ilmeisen perusteettomia pyyntöjä, rekisterinpitäjä voi joko periä kohtuullisen maksun yleisen tietosuoja-asetuksen 12 artiklan 5 kohdan a alakohdan mukaisesti tai kieltäytyä suorittamasta pyydettyä toimea yleisen tietosuoja-asetuksen 12 artiklan 5 kohdan b alakohdan mukaisesti. Rekisterinpitäjän on pystyttävä osoittamaan pyynnön ilmeinen perusteettomuus tai kohtuuttomuus.

6.2 Oikeus tietojen poistamiseen ja vastustamisoikeus

6.2.1 Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi)

99.

Jos rekisterinpitäjä jatkaa henkilötietojen käsittelyä reaaliaikaisen seurannan jälkeen (esimerkiksi säilyttämällä tietoja), rekisteröity voi pyytää henkilötietojen poistamista yleisen tietosuoja-asetuksen 17 artiklan mukaisesti.

100.

Rekisterinpitäjällä on pyynnön perusteella velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä, mikäli jokin yleisen tietosuoja-asetuksen 17 artiklan 1 kohdassa luetelluista edellytyksistä täyttyy (eikä mikään yleisen tietosuoja-asetuksen 17 artiklan 3 kohdassa luetelluista poikkeuksista täyty). Tähän kuuluu velvollisuus poistaa henkilötiedot, kun niitä ei enää tarvita niihin tarkoituksiin, joita varten ne alun perin kerättiin, tai kun käsittely on lainvastaista (ks. myös 8 jakso – *Säilytysajat ja poistamisvelvollisuus*). Henkilötiedot pitäisi poistaa myös seuraavissa tapauksissa käsittelyn oikeudellisen perusteen mukaan:

- kun käsittelyn perustana on *suostumus*, aina kun suostumus peruutetaan (eikä käsittelyyn ole muuta laillista perustetta)
- kun käsittelyn perustana on *oikeutettu etu*:
 - o aina kun rekisteröity käyttää vastustamisoikeutta (ks. 6.2.2 kohta), eikä käsittelylle ole olemassa huomattavan tärkeää ja perusteltua syytä, tai
 - o kun kyse on suoramarkkinoinnista (myös profiloinnista), aina kun rekisteröity vastustaa käsittelyä.

101. Jos rekisterinpitäjä on julkistanut videoaineiston (esimerkiksi julkaissut tai lähettänyt sen suoratoistona verkossa), on toteutettava kohtuulliset toimenpiteet, jotta muille rekisterinpitäjille (jotka nyt käsittelevät kyseisiä henkilötietoja) voidaan ilmoittaa pyynnöstä yleisen tietosuoja-asetuksen 17 artiklan 2 kohdan mukaisesti. Kohtuullisiin toimenpiteisiin pitäisi kuulua teknisiä toimenpiteitä otettaessa huomioon käytettävissä oleva teknologia ja toteuttamiskustannukset. Yleisen tietosuoja-asetuksen 19 artiklan mukaan rekisterinpitäjän olisi mahdollisuuksien mukaan ilmoitettava – henkilötietoja poistettaessa – kaikille, joille henkilötietoja on aiemmin luovutettu.
102. Rekisterinpitäjän velvollisuuden poistaa henkilötiedot rekisteröidyn pyynnöstä lisäksi, rekisterinpitäjällä on velvollisuus yleisen tietosuoja-asetuksen yleisten periaatteiden mukaisesti rajoittaa henkilötietojen säilyttämistä (ks. 8 jakso).
103. Videovalvonnan kannalta kannattaa panna merkille, että jos kuva esimerkiksi sumennetaan niin, että kuvan aiemmin sisältämiä henkilötietoja ei voida saada takautuvasti palautetuksi, henkilötiedot katsotaan poistetuksi yleisen tietosuoja-asetuksen mukaisesti.

Esimerkki: Lähikaupalla on ilkeältäan liittyviä ongelmia erityisesti kaupan ulkopuolella. Siksi kaupassa käytetään sisäänkäynnin ulkopuolella videovalvontaa, joka on yhdistetty suoraan seiniin. Ohikulkija pyytää poistamaan ohikulkuaan koskevat henkilötiedot. Rekisterinpitäjän on vastattava pyyntöön ilman aiheutonta viivytystä ja viimeistään kuukauden kuluessa. Koska kyseinen aineisto ei enää täytä tarkoitusta, jota varten se oli alun perin tallennettu (ilkeältä ei tapahtunut rekisteröidyn kulkiessa ohi), pyynnön tekemisen aikaan rekisteröidyn tietojen säilyttämiseen ei ole oikeutettua etua, joka syrjäyttäisi rekisteröityjen edut. Rekisterinpitäjän on poistettava henkilötiedot.

104.

6.2.2 Vastustamisoikeus

105. Videovalvonnassa, joka perustuu *oikeutettuun etuun* (yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohta) tai *yleistä etua* koskevan tehtävän suorittamisen tarpeeseen (yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohta), rekisteröidyllä on oikeus – milloin tahansa – henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella vastustaa käsittelyä yleisen tietosuoja-asetuksen 21 artiklan mukaisesti. Ellei rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn oikeudet ja edut, vastustaneen henkilön tietojen käsittely on lopetettava. Rekisterinpitäjän on vastattava rekisteröidyn pyyntöön ilman aiheutonta viivytystä, viimeistään kuukauden kuluessa.
106. Videovalvonnan yhteydessä tämä vastustus voidaan tehdä joko valvotulle alueelle tultaessa, siellä olon aikana tai sieltä lähtemisen jälkeen. Käytännössä tämä tarkoittaa, jollei rekisterinpitäjällä ole huomattavan tärkeitä ja perusteltuja syitä, sellaisen alueen valvonta, jossa luonnolliset henkilöt voitaisiin tunnistaa, on lainmukaista vain, jos
- (1) rekisterinpitäjä pystyy välittömästi pyydettyä pysäyttämään kameran käsittelemästä henkilötietoja, tai
 - (2) jos valvottu alue on niin yksityiskohtaisesti rajattu, että rekisterinpitäjä voi varmistaa rekisteröidyn hyväksynnän saamisen ennen tämän saapumista alueelle, ja jos se ei ole alue, johon rekisteröidyllä on kansalaisena oikeus tulla.
107. Näiden ohjeiden tarkoituksena ei ole määrittellä, mikä katsotaan *huomattavan tärkeäksi ja perustelluksi syyksi* (yleisen tietosuoja-asetuksen 21 artikla).

108. Kun videovalvontaa käytetään suoramarkkinointitarkoituksiin, rekisteröidyllä on oikeus vastustaa käsittelyä oman harkintansa mukaan, koska siinä yhteydessä vastustamisoikeus on ehdoton (yleisen tietosuojasetuksen 21 artiklan 2 ja 3 kohta).

Esimerkki: Yrityksellä on asiakassisääkäyntinsä turvallisuusrikkomuksiin liittyviä ongelmia, ja se käyttää videovalvontaa oikeutetun edun perusteella, jotta lainvastaisesti sisään tulevat voitaisiin saada kiinni. Kävijä vastustaa henkilötietojensa käsittelyä videovalvontajärjestelmässä henkilökohtaiseen erityistilanteeseensa liittyvällä perusteella. Tässä tapauksessa yhtiö kuitenkin hylkää pyynnön, koska tallennettua videoaineistoa tarvitaan jatkuvaan sisäiseen tutkintaan, ja sillä on siksi huomattavan tärkeä ja perusteltu syy henkilötietojen käsittelyn jatkamiseen.

- 109.

7 LÄPINÄKYVYYTTÄ JA TIEDOTTAMISTA KOSKEVAT VELVOLLISUUDET¹⁸

110. Euroopan tietosuojalainsäädännössä on kauan ollut periaatteena, että rekisteröityjen olisi oltava tietoisia käynnissä olevassa videovalvonnasta. Heidän on saatava yksityiskohtaista informaatiota valvottavista paikoista¹⁹. Yleisen tietosuoja-asetuksen 12 artiklassa ja sitä seuraavissa artikloissa esitetään yleiset läpinäkyvyyttä ja informointia koskevat velvollisuudet. Tietosuojatyöryhmän asetuksen 2016/679 mukaista läpinäkyvyyttä koskevissa suuntaviivoissa (WP 260), joita tietosuojaneuvosto kannatti²⁵ toukokuuta 2018, annetaan lisätietoja. Suuntaviivojen 26 kohdan mukaan yleisen tietosuoja-asetusten 13 artikla koskee tilannetta, jossa henkilötietoja kerätään "[...] rekisteröidystä havainnoimalla (esim. käyttämällä automaattisia tiedonkeruun välineitä tai tiedonkeruuohjelmistoa, kuten kameroita [...])."
111. Koska rekisteröidyille on toimitettava paljon informaatiota, rekisterinpitäjät voivat hyödyntää monitasoista esitystapaa, jossa läpinäkyvyyden varmistamisessa käytetään eri menetelmien yhdistelmää (WP 260, 35 kohta, WP 89, 22 kohta). Videovalvonnassa tärkein informaatio tulisi esittää itse varoitusmerkissä (ensimmäinen taso) ja pakolliset lisätiedot voidaan antaa toisin keinoin (toinen taso).

7.1 Ensimmäisen tason informaatio (varoituserkki)

112. Ensimmäinen taso koskee ensisijaista tapaa, jolla rekisterinpitäjä on ensimmäiseksi tekemisissä rekisteröidyn kanssa. Tässä vaiheessa rekisterinpitäjät voivat käyttää varoituserkkiä asiaankuuluvan informaation esittämiseen. Esitettävät tiedot voidaan antaa yhdessä kuvakkeen kanssa, jotta suunnitellusta käsittelystä voidaan antaa mielekäs yleiskuva helposti erottuvalla, ymmärrettävällä ja selvästi luettavissa olevalla tavalla (yleisen tietosuoja-asetuksen 12 artiklan 7 kohta). Informaation esitysmuotoa pitäisi mukauttaa yksittäisen paikan mukaan (WP 89, 22 kohta).

7.1.1 Varoituserkin sijainti

113. Informaatio olisi sijoitettava siten, että rekisteröity pystyy helposti havaitsemaan valvontaolosuhteet ennen tuloaan valvotulle alueelle (noin silmien korkeudella). Kameran sijaintia ei tarvitse paljastaa, kunhan ei jää epäilystä siitä, mitä alueita valvotaan, ja kunhan valvonnan tausta on selitetty yksiselitteisesti (WP 89, 22 kohta). Rekisteröidyn on pystyttävä arvioimaan, mitä aluetta kameralla kuvataan, jotta hän voisi välttää valvonnan tai mukauttaa tarvittaessa käytöstään.

7.1.2 Ensimmäisen tason sisältö

114. Ensimmäisen tason informaatiossa (varoituserkki) pitäisi yleisesti välittää tärkeimmät tiedot, esimerkiksi käsittelytarkoitusten yksityiskohdat, rekisterinpitäjän identiteetti, tieto rekisteröidyn oikeuksien olemassaolosta ja tiedot henkilötietojen käsittelyn merkittävimmistä vaikutuksista²⁰. Niihin voivat kuulua esimerkiksi rekisterinpitäjän (tai kolmannen osapuolen) oikeutetut edut ja (soveltuvin osin) tietosuojavastaavan yhteystiedot. Niissä on myös viitattava yksityiskohtaisempiin toisen tason informaatioon ja siihen, mistä ja miten ne löytyvät.
115. Lisäksi merkin pitäisi sisältää kaikki tiedot, jotka voivat tulla rekisteröidylle yllätyksenä (WP260, 38 kohta). Niitä voivat olla esimerkiksi siirtäminen kolmansille osapuolille erityisesti, jos ne sijaitsevat EU:n ulkopuolella, ja säilytysaika. Jos näitä tietoja ei ilmoiteta, rekisteröidyn pitäisi voida luottaa siihen,

¹⁸ Kansallisen lainsäädännön erityisiä vaatimuksia voidaan soveltaa.

¹⁹ Ks. WP89, tietosuojatyöryhmän lausunto 4/2004 henkilötietojen käsittelystä videovalvonnan keinoin.

²⁰ Ks. WP260, 38 kohta.

että seuranta on pelkästään reaaliaikaista (ilman tietojen säilyttämistä tai siirtämistä kolmansille osapuolille).

Esimerkki (ei-sitova ehdotus):



Lisätietoja on saatavilla
] ilmoituksesta
] vastaanotosta/asiakastiedoista/rekisteristä
] internetistä (osoitteesta...)

Rekisterinpitäjän ja asian niin vaatiessa rekisterinpitäjän edustajan henkilöllisyys:

Yhteystiedot, myös tietosuojavastaavan (asian niin vaatiessa):

Tiedot käsittelystä, jolla on merkittävin vaikutus rekisteröityyn (esim. säilytysaika tai reaaliaikainen seuranta, videoaineiston julkaiseminen tai siirtäminen kolmansille osapuolille):

Videovalvonnan tarkoitus tai tarkoitukset:

Rekisteröityjen oikeudet: Rekisteröitynä sinulla on käytettävissäsi useita oikeuksia, erityisesti oikeus pyytää rekisterinpitäjältä pääsy omiin henkilötietoihisi tai oikeus pyytää tietojen poistamista.

Rekisterinpitäjä on asettanut saataville yksityiskohtaista informaatiota tästä videovalvonnasta ja oikeuksistasi. Tiedot ovat saatavilla vasemmalla olevien vaihtoehtojen kautta.

116.

7.2 Toisen tason informaatio

117. Myös toisen tason tiedot on asetettava saataville paikassa, johon rekisteröity pääsee helposti. Se voi olla esimerkiksi kattava tiedote, joka on saatavilla keskeisessä paikassa (esimerkiksi neuvontapalvelussa, vastaanotossa tai kassalla), tai helposti ymmärrettävä juliste. Kuten edellä mainitaan, ensimmäisen tason varoitusmerkissä on viitattava selvästi toisen tason informaatioon. Parasta olisi lisäksi, jos ensimmäisen tason informaatioon viitattaisiin toisen tason digitaaliseen lähteeseen (esim. QR-koodiin tai verkkosivustoon). Informaation pitäisi kuitenkin olla helposti saatavilla myös muuten kuin digitaalisesti. Pitäisi olla mahdollista saada pääsy toisen tason informaatioon ilman valvotulle alueelle menoa erityisesti, jos informaatio annetaan digitaalisesti (tämä voidaan toteuttaa esimerkiksi linkillä). Toinen asianmukainen keino on puhelinnumero, johon voi soittaa. Informaation on sisällettävä kaikki tiedot, jotka ovat pakollisia yleisen tietosuoja-asetuksen 13 artiklan perusteella riippumatta siitä, miten ne annetaan.
118. Näiden vaihtoehtojen lisäksi sekä niiden tehostamiseksi tietosuojaneuvosto suosittelee käyttämään teknisiä keinoja informaation antamiseksi rekisteröidyille. Niitä voivat olla esimerkiksi geopaikannuskamerat, jotka voivat sisältää informaatiota karttasovelluksissa tai verkkosivustoissa. Näin henkilöt voivat toisaalta tunnistaa ja yksilöidä helposti oikeuksiensa käyttöön liittyvät videolähteet ja toisaalta saada yksityiskohtaisempaa informaatiota käsittelytoimesta.

Esimerkki: Kauppias valvoo kauppaansa. Yleisen tietosuoja-asetuksen 13 artiklan noudattamiseksi riittää, että kaupan sisäänkäyntiin sijoitetaan helposti näkyvälle paikalle varoitusmerkki, jossa on ensimmäisen tason informaation. Kauppiaan on lisäksi annettava kassalla tai muussa keskeisessä ja helposti saavutettavassa paikassa kaupassaan saataville tiedote, joka sisältää toisen tason informaation.

119.

8 SÄILYTYSAJAT JA POISTAMISVELVOLLISUUS

120. Henkilötietoja saa säilyttää vain niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten (yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c ja e alakohta). Joissakin jäsenvaltioissa voi olla videovalvontaa koskevista säilytysajoista erityissäännöksiä yleisen tietosuoja-asetuksen 6 artiklan 2 kohdan mukaisesti.
121. Sitä, onko henkilötietojen säilyttäminen tarpeellista, tulisi kontrolloida lyhyen ajanjakson sisällä. Yleisesti ottaen videovalvonnan laillisia tarkoituksia ovat usein omaisuuden suojelu tai todisteiden säilyttäminen. Tapahtuneet vauriot voidaan tavallisesti havaita 1–2 päivässä. Tietosuojalainsäädännön noudattamisen osoittamisen helpottamiseksi rekisterinpitäjän etujen mukaista on tehdä organisatorisia järjestelyjä etukäteen (esimerkiksi nimittää tarvittaessa edustaja videoaineiston seulontaan ja siitä huolehtimiseen). Kun otetaan huomioon yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan c ja e alakohtan periaatteet eli tietojen minimointi ja säilytyksen rajoittaminen, henkilötiedot pitäisi useimmissa tapauksissa (esimerkiksi ilkevallan havaitsemista varten) poistaa, mielellään automaattisesti, muutaman päivän kuluessa. Mitä kauemmin säilyttäminen kestää (erityisesti, jos se kestää yli 72 tuntia), sitä enemmän tarvitaan perusteluja tarkoituksen laillisuudesta ja säilytyksen tarpeellisuudesta. Jos rekisterinpitäjä aikoo käyttää videovalvontaa tilojensa seurantaan ja lisäksi säilyttää tiedot, rekisterinpitäjän on varmistettava, että säilyttäminen todella on tarpeen tarkoituksen saavuttamiseksi. Jos se on tarpeen, säilytysaika on määritettävä selkeästi ja asetettava yksittäin kutakin erityistä tarkoitusta varten. Rekisterinpitäjän vastuulla on määrittää säilytysaika tarpeellisuutta ja oikeasuhteisuutta koskevien periaatteiden mukaisesti ja osoittaa yleisen tietosuoja-asetusten säännösten noudattaminen.

Esimerkki: Pienen kaupan kauppias huomaisi tavallisesti ilkevallan samana päivänä. Siksi tavanomainen 24 tunnin säilytysaika on riittävä. Kaupan kiinniolo viikonloppuisin tai pitkät lomamatkat voivat kuitenkin olla peruste pidemmälle säilytysajalle. Jos vahinko havaitaan, kauppiaan on ehkä myös säilytettävä videoaineistoa pidempään, jotta rikoksentehtäjiä vastaan voitaisiin ryhtyä oikeustoimiin.

122.

9 TEKNISET JA ORGANISATORISET TOIMENPITEET

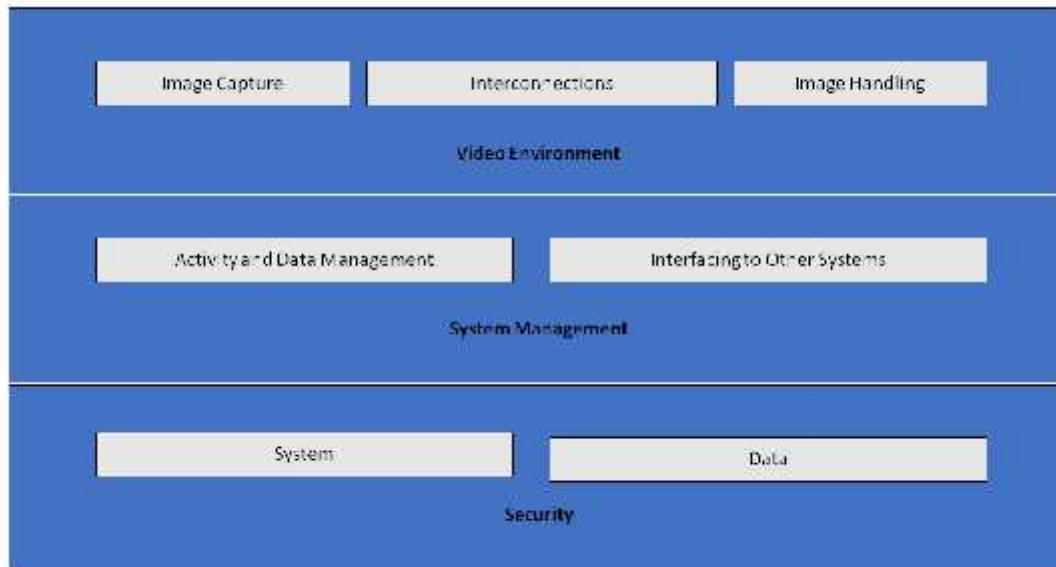
123. Kuten yleisen tietosuoja-asetuksen 32 artiklan 1 kohdassa todetaan, ei riitä, että henkilötietojen käsittely videovalvonnan yhteydessä on lain mukaan luvallista vaan rekisterinpitäjien ja henkilötietojen käsittelijöiden on myös suojattava se asianmukaisesti. Toteutettujen **organisatoristen ja teknisten toimenpiteiden** on oltava **oikeassa suhteessa luonnollisten henkilöiden oikeuksille ja vapauksille aiheutuviin riskeihin**, jotka johtuvat videovalvontatietojen vahingossa tapahtuvasta tai laittomasta tuhoamisesta, häviämisestä, muuttamisesta, luvattomasta luovuttamisesta tai niihin pääsystä. Yleisen tietosuoja-asetuksen 24 ja 25 artiklan mukaan rekisterinpitäjien on toteutettava teknisiä ja organisatorisia toimenpiteitä myös, jotta kaikki tietosuojaperiaatteiden toteutuminen voidaan varmistaa käsittelyn aikana ja jotta rekisteröidyille tarjotaan keinot käyttää yleisen tietosuoja-asetuksen 15–22 artiklassa määriteltyjä oikeuksiaan. Rekisterinpitäjien olisi otettava käyttöön sisäinen viitekehys ja käytäntöjä, joilla näiden toteuttaminen varmistetaan sekä käsittelytoimien määrittämisen aikana että itse käsittelyn aikana, tarvittaessa myös tehtäessä tietosuoja koskevia vaikutustenarviointoja.

9.1 Katsaus videovalvontajärjestelmään

124. Videovalvontajärjestelmässä²¹ on analogisia ja digitaalisia laitteita sekä ohjelmisto, joiden tarkoituksena on ottaa kuvia tilanteesta, käsitellä kuvia ja näyttää niitä käyttäjälle. Sen osat ryhmitellään seuraavasti:

-) Videoympäristö: kuvien ottaminen, yhteenkytkennät ja kuvankäsittely:
 - o kuvan ottamisen tarkoituksena on kuvan luominen reaali maailmasta muodossa, jota muu järjestelmä voi käyttää
 - o yhteenkytkennät kuvaavat kaikkea tietojen siirtämistä videoympäristössä eli liitäntöjä ja viestintää. Liitäntöjä ovat muun muassa johdot, digitaaliset verkot ja langaton siirto. Viestintä kuvaa kaikkia video- ja valvontatietosignaaleja, jotka voivat olla digitaalisia tai analogisia
 - o kuvankäsittely sisältää kuvan tai kuvasarjojen analyysin, säilyttämisen ja esittämisen.
-) Järjestelmän hallinnan kannalta videovalvontajärjestelmässä on seuraavat loogiset toiminnot:
 - o tietojen hallinta ja toiminnan hallinta, joihin kuuluu käyttäjän komentojen ja järjestelmän luomien toimien hallinta (hälytysmenettelyt, käyttäjälle ilmoittaminen)
 - o rajapinnat toisiin järjestelmiin voivat sisältää liitoksen muihin turvallisuusjärjestelmiin (pääsynvalvonta, palohälytys) ja muihin kuin turvallisuusjärjestelmiin (rakennusten hallintajärjestelmät, automaattinen rekisterikilven tunnistaminen).
-) Videovalvontajärjestelmään kuuluu järjestelmän ja tietojen luottamuksellisuus, eheys ja saatavuus:
 - o järjestelmäturvallisuuteen sisältyy kaikkien järjestelmän osien fyysinen turvallisuus ja videovalvontajärjestelmään pääsyn valvonta
 - o tietoturvaan kuuluu tietojen häviämisen tai manipuloinnin estäminen.

²¹ Yleisessä tietosuojasetuksessa ei ole videovalvonnan määritelmää, mutta sen tekninen kuvaus on esimerkiksi standardissa EN 62676-1-1:2014 Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 1-1: Järjestelmävaatimukset. Yleiset vaatimukset.



125.

Image Capture	Kuvan ottaminen
Interconnections	Yhteenkytkennät
Image Handling	Kuvankäsittely
Video Environment	Videoympäristö
Activity and Data Management	Toiminnan ja tietojen hallinta
Interfacing to Other Systems	Rajapinnat muihin järjestelmiin
System Management	Järjestelmähallinta
System	Järjestelmä
Data	Tiedot
Security	Turvallisuus

Kuva 1 – videovalvontajärjestelmä

9.2 Sisäänrakennettu ja oletusarvoinen tietosuojaja

126. Kuten yleisen tietosuojaja-asetuksen 25 artiklassa todetaan, rekisterinpitäjien on toteutettava tietosuojaja varten asianmukaiset tekniset ja organisatoriset toimenpiteet heti videovalvontaa suunnitellessaan – ennen videoaineiston keräämisen ja käsittelyn aloittamista. Näissä periaatteissa korostetaan, että tarvitaan sisäänrakennettuja yksityisyyttä edistäviä teknologioita, oletusasetuksia, joilla tietojenkäsittely minimoidaan, ja tarpeellisia työkaluja, joiden avulla henkilötietoja voidaan suojata mahdollisimman hyvin²².
127. Rekisterinpitäjien olisi sisällytettävä tietosuojaja ja yksityisyyttä koskevat suoja-toimet sekä teknologian suunnittelu-eritelmiin että organisatorisiin käytäntöihin. Organisatoristen käytäntöjen osalta rekisterinpitäjän pitäisi ottaa käyttöön asianmukainen hallintakehys sekä laadittava ja täytäntöön pantava käytäntöjä ja menettelyjä, jotka liittyvät videovalvontaan. Teknisestä näkökulmasta järjestelmän eritelmiin ja suunnitteluun pitäisi kuulua vaatimuksia henkilötietojen käsittelystä yleisen tietosuojaja-asetuksen 5 artiklassa esitettyjen periaatteiden (käsittelyn lainmukaisuus, tarkoituksen ja tietojen rajoittaminen, yleisen tietosuojaja-asetuksen 25 artiklan

²² WP 168, lausunto "The Future of Privacy", tietosuojatyöryhmän ja poliisi- ja oikeusasioden työryhmän yhteinen kannanotto Euroopan komission kuulemiseen henkilötietojen suojaaja koskevan perusoikeuden oikeudellisesta kehyksestä (annettu 1. joulukuuta 2009).

2 kohdassa tarkoitettu oletusarvoinen tietojen minimointi, eheys ja luottamuksellisuus, osoitusvelvollisuus jne.) mukaisesti. Jos rekisterinpitäjä aikoo hankkia kaupallisen videovalvontajärjestelmän, rekisterinpitäjän on sisällytettävä nämä vaatimukset hankintaeritelmiin. Rekisterinpitäjän on varmistettava vaatimusten noudattaminen soveltamalla niitä järjestelmän kaikkiin osiin ja kaikkiin sillä käsiteltäviin tietoihin koko niiden elinkaaren ajan.

9.3 Konkreettisia esimerkkejä asiaankuuluvista toimenpiteistä

128. Useimmat toimenpiteet, joita voidaan käyttää videovalvonnan suojaamisessa erityisesti silloin, kun käytetään digitaalisia laitteita ja ohjelmistoja, eivät eroa muissa tietoteknisissä järjestelmissä käytetyistä suojatoimenpiteistä. Valitusta ratkaisusta riippumatta rekisterinpitäjän on suojattava asianmukaisesti kaikki videovalvontajärjestelmän ja tietojen osat kaikissa vaiheissa eli säilyttämisen (levossa olevat tiedot), siirtämisen (matkalla olevat tiedot) ja käsittelyn (käytössä olevat tiedot) aikana. Tätä varten rekisterinpitäjien ja henkilötietojen käsittelijöiden on yhdistettävä organisatorisia ja teknisiä toimenpiteitä.
129. Teknisiä ratkaisuja valitessaan rekisterinpitäjän olisi otettava huomioon yksityisyyttä edistävät teknologiat myös siksi, että ne edistävät turvallisuutta. Tällaisia teknologioita ovat esimerkiksi järjestelmät, joiden avulla voidaan naamioida tai salata alueet, jotka eivät ole tärkeitä valvonnassa, tai muokata kolmansien henkilöiden kuvat pois, kun videoaineistoa annetaan rekisteröidyille.²³ Toisaalta valituissa ratkaisuissa ei pitäisi olla toimintoja, jotka eivät ole tarpeen (esimerkiksi kameroiden rajaton liikkuminen, tarkennusvalmiudet, radiolähetys, analyysi ja ääninauhitus). Toiminnot, jotka ratkaisuissa on mutta joita ei tarvita, on otettava pois käytöstä.
130. Tästä aiheesta on saatavilla paljon kirjallisuutta, muun muassa kansainvälisiä standardeja ja teknisiä eritelmiä multimediajärjestelmien fyysisestä turvallisuudesta²⁴ ja yleisten tietoteknisten järjestelmien turvallisuudesta²⁵. Tässä jaksossa tehdään siksi vain hyvin yleinen katsaus aiheeseen.

9.3.1 Organisatoriset toimenpiteet

131. Mahdollisesti tarvittavan tietosuojaa koskevan vaikutustenarvioinnin (ks. 10 jakso) lisäksi rekisterinpitäjien olisi pohdittava seuraavia asioita luodessaan omia videovalvonnan käytäntöjään ja menettelyitään:

-)] Kuka vastaa videovalvontajärjestelmän hallinnasta ja käytöstä?
-)] Videovalvontahankkeen tarkoitus ja laajuus.
-)] Asianmukainen ja kielletty käyttö (missä ja milloin videovalvonta sallitaan ja missä ja milloin ei, esim. piilokameroiden käyttö ja äänitys videotallennuksen lisäksi)²⁶.
-)] Edellä 7 jaksossa (Läpinäkyvyyttä ja tiedottamista koskevat velvollisuudet) tarkoitetut läpinäkyvyystoimet.
-)] Miten video tallennetaan ja mikä sen kesto on, myös turvallisuushäiriöihin liittyvien videotallenteiden arkistointi?
-)] Kenen on käytävä asiaankuuluva koulutus ja milloin?
-)] Kenellä on pääsy videotallenteisiin ja mitä tarkoituksia varten?

²³ Tällaisten teknologioiden käyttö voi jopa olla joissakin tapauksissa pakollista 5 artiklan 1 kohdan c alakohdan noudattamiseksi. Niitä voidaan joka tapauksessa käyttää parhaan käytännön esimerkkeinä.

²⁴ IEC TS 62045 – Multimedia-suojaus – Ohje käytössä olevien ja käytöstä poistettujen laitteiden yksityisyyden suojalle.

²⁵ ISO/IEC 27000 – Tietoturvallisuuden hallintajärjestelmien sarja.

²⁶ Tämä voi riippua kansallisista laeista ja alakohtaisista määräyksistä.

- J Operatiiviset menettelyt (esim. kuka videovalvontaa seuraa ja mistä sitä seurataan, mitä tehdään tietoturvaloukkauksen sattuessa?).
- J Mitä menettelyjä ulkopuolisten osapuolten on noudatettava videotallenteiden pyytämiseksi ja mitä menettelyjä on kyseisten pyyntöjen hylkäämiseksi tai niiden hyväksymiseksi?
- J Menettelyt videovalvontajärjestelmän hankintaa, asentamista ja huoltoa varten.
- J Häiriöiden hallinta- ja palautusmenettelyt.

9.3.2 Tekniset toimenpiteet

132. **Järjestelmäturvallisuudella** tarkoitetaan kaikkien järjestelmien osien **fyysistä turvallisuutta** ja järjestelmän eheyttä eli **suojaaja ja kestävyyttä tahalliselta tai tahattomalta häiriöltä järjestelmän tavanomaisissa toimissa ja pääsynvalvonnassa**. Tietoturvalta tarkoitetaan **luottamuksellisuutta** (tietoihin pääsevät vain ne, joilla on siihen lupa), **eheyttä** (tietojen häviämisen tai manipuloinnin estämistä) ja **saatavuutta** (tietoihin pääsee tarvittaessa).
133. **Fyysinen turvallisuus** on olennainen osa tietosuojaa ja ensimmäinen puolustuslinja, koska se suojaa videovalvontajärjestelmää varkauksilta, ilkvallalta, luonnonkatastrofeilta, ihmisen aiheuttamilta katastrofeilta ja tahattomilta vahingoilta (esim. sähköpiikeiltä, ääriämpötiloilta ja kaatuneelta kahvilta). Analogisissa järjestelmissä fyysisen turvallisuuden osuus on niiden suojelussa keskeinen osa.
134. **Järjestelmä- ja tietoturvaluuteen** eli suojaamiseen tahalliselta ja tahattomalta puuttumiselta tavanomaisissa toimissa voi kuulua
- J koko videovalvontajärjestelmän infrastruktuurin (myös etäkameroiden, kaapeleiden ja virransyötön) suojaaminen fyysiseltä peukaloinnilta ja varkauksilta
 - J aineiston lähettämisen suojaaminen salakuuntelulta suojatuissa viestintäkanavissa
 - J tietojen salaus
 - J laitteisto- ja ohjelmistopohjaisten ratkaisujen, kuten palomuurien, virus- tai tunkeutumisentorjuntajärjestelmien, käyttö verkkohyökkäyksiä vastaan
 - J osien, ohjelmistojen ja yhteenkytkentöjen vikojen havaitseminen
 - J keinot, joilla palautetaan nopeasti henkilötietojen saatavuus ja pääsy henkilötietoihin fyysisen tai teknisen vian sattuessa.
135. **Pääsynvalvonnalla** varmistetaan, että vain luvan saaneet henkilöt pääsevät järjestelmään ja tietoihin, kun taas muita estetään pääsemästä. Toimenpiteitä, joilla tuetaan fyysistä ja loogista pääsyä, ovat muun muassa
- J sen varmistaminen, että kaikki tilat, joissa seuranta toteutetaan videovalvonnalla ja joissa videoaineistoa säilytetään, on turvattu kolmansien osapuolten valvomattomalta pääsylvä
 - J monitorien sijoittaminen (erityisesti silloin, kun ne ovat avoimilla alueilla, kuten vastaanotossa) niin, että vain luvan saaneet käyttäjät pystyvät näkemään ne
 - J fyysisen ja loogisen pääsyn myöntämistä, muuttamista ja kumoamista koskevien menettelyjen määrittäminen ja valvonta
 - J käyttäjien todentamista ja luvan myöntämistä koskevien menetelmien ja keinojen, esimerkiksi salasanojen pituus ja muuttamistiheys, käyttöönotto
 - J käyttäjien (sekä järjestelmälle että tiedoille) suorittamien toimien tallentaminen ja säännöllinen tarkastaminen
 - J pääsyä koskevien virheiden jatkuva seuranta ja havainnointi, ja havaittuihin heikkouksiin puuttuminen mahdollisimman pian.

10 TIETOSUOJAA KOSKEVA VAIKUTUSTENARVIOINTI

136. Yleisen tietosuojasetuksen 35 artiklan 1 kohdan mukaan rekisterinpitäjän on tehtävä tietosuojaa koskeva vaikutustenarviointi, jos tietyn tyyppinen käsittely todennäköisesti aiheuttaa luonnollisten henkilöiden oikeuksien ja vapauksien kannalta korkean riskin. Yleisen tietosuojasetuksen 35 artiklan 3 kohdan c alakohdassa säädetään, että rekisterinpitäjien on tehtävä tietosuojaa koskeva vaikutustenarviointi, jos käsittelyyn kuuluu yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti. Yleisen tietosuojasetuksen 35 artiklan 3 kohdan b alakohdan mukaisesti tietosuojaa koskeva vaikutustenarviointi vaaditaan myös, kun rekisterinpitäjä aikoo käsitellä erityisiä henkilötietoryhmiä laajamittaisesti.
137. Tietosuojaa koskevasta vaikutustenarvioinnista annetussa ohjeessa²⁷ annetaan lisää neuvoja ja yksityiskohtaisempia esimerkkejä videovalvonnasta (esim. kamerajärjestelmän käytöstä ajotavan seurantaan valtateilla). Yleisen tietosuojasetuksen 35 artiklan 4 kohdan mukaan kunkin valvontaviranomaisen on julkaistava luettelo käsittelytoimien tyypeistä, joiden yhteydessä vaaditaan tietosuojaa koskeva vaikutustenarviointi heidän jäsenvaltiossaan. Tällaiset luettelot ovat tavallisesti viranomaisten verkkosivustoilla. Videovalvonnan tyypillisten tarkoitusten (ihmisten ja omaisuuden suojeleminen, rikosten havaitseminen, estäminen ja torjunta, todisteiden ja epäiltyjen biometristen tunnistetietojen kerääminen) vuoksi on kohtuullista olettaa, että useat videovalvontatapaukset edellyttävät tietosuojaa koskevan vaikutustenarvioinnin tekemistä. Rekisterinpitäjien on siksi tutustuttava huolellisesti näihin asiakirjoihin voidakseen päättää siitä, tarvitaanko kyseistä arviointia, ja tehdä sen tarvittaessa. Rekisterinpitäjän pitäisi valita tehdyn tietosuojaa koskevan vaikutustenarvioinnin perusteella toteutettavat tietosuojatoimenpiteet.
138. On myös tärkeää panna merkille, että jos tietosuojaa koskevan vaikutustenarvioinnin tuloksista käy ilmi, että käsittely aiheuttaisi korkean riskin rekisterinpitäjän suunnittelemissa turvallisuustoimenpiteistä huolimatta, ennen käsittelyä on kuultava asiaankuuluvia valvontaviranomaisia. Ennakkokuulemisesta on saatavilla lisätietoa 36 artiklassa.

Euroopan tietosuojaneuvosto

Puheenjohtaja

(Andrea Jelinek)

²⁷ WP 248 rev. 01, ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”. – tietosuojaneuvoston hyväksymät