edpb
European Data Protection Board

Ohjeet

Suuntaviivat 9/2022 yleisen tietosuoja-asetuksen mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta

Versio 2.0

Hyväksytty 28. maaliskuuta 2023

This language version has not yet been proofread.

Versiohistoria

Versio 1.0	10. lokakuuta 2022	Suuntaviivojen (tietosuojatyöryhmän hyväksymien ja Euroopan tietosuojaneuvoston 25. toukokuuta 2018 vahvistamien aiempien suuntaviivojen päivitetty versio WP250 (rev.01)) hyväksyminen kohdennettua julkista kuulemista varten.
Versio 2.0	28. maaliskuuta 2023	Suuntaviivojen hyväksyminen sen jälkeen, kun Euroopan talousalueelle sijoittautumattomille rekisterinpitäjille oli järjestetty kohdennettu julkinen kuuleminen henkilötietojen tietoturvaloukkauksen ilmoittamisesta.

SISÄLLYSLUETTELO

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 ja l alakohdan,

ottaa huomioon ETA-sopimuksen ja erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018[1],

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

ottaa huomioon 29 artiklan mukaisen tietosuojatyöryhmän suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta, WP250 rev.01,

ON ANTANUT SEURAAVAT SUUNTAVIIVAT

0 ESIPUHE

1. 29 artiklan mukainen tietosuojatyöryhmä, jäljempänä 'tietosuojatyöryhmä', hyväksyi 3. lokakuuta 2017 suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta (WP250 rev.01) [2] , jotka Euroopan tietosuojaneuvosto, jäljempänä 'tietosuojaneuvosto', hyväksyi ensimmäisessä täysistunnossaan[3]. Tämä asiakirja on päivitetty versio kyseisistä suuntaviivoista. Viittaukset tietosuojatyöryhmän suuntaviivoihin asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta (WP250 rev.01) olisi tästä lähtien tulkittava viittauksiksi näihin tietosuojaneuvoston suuntaviivoihin 9/2022.
2. Tietosuojaneuvosto totesi, että henkilötietojen tietoturvaloukkauksia koskevia ilmoitusvaatimuksia EU:n ulkopuolisissa toimipaikoissa oli tarpeen selventää. Tätä asiaa koskevaa kohtaa on tarkistettu ja päivitetty, mutta asiakirjan muut osat on jätetty ennalleen toimituksellisia muutoksia lukuun ottamatta. Tarkistus koskee tarkkaan ottaen asiakirjan II.C.2 osion 73 kohtaa.

JOHDANTO

3. Yleisessä tietosuoja-asetuksessa otettiin käyttöön vaatimus, että henkilötietojen tietoturvaloukkauksesta, jäljempänä 'tietoturvaloukkaus', on ilmoitettava toimivaltaiselle kansalliselle valvontaviranomaiselle [4] (tai rajatylittävän tietoturvaloukkauksen tapauksessa johtavalle valvontaviranomaiselle) sekä tietyissä tapauksissa niille henkilöille, joiden henkilötietoihin tietoturvaloukkaus on kohdistunut.
4. Ilmoittamisvelvollisuus tietoturvaloukkaustapauksissa oli tietyillä organisaatioilla, kuten yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajilla (direktiivin 2009/136/EY ja asetuksen (EU)

[1] Viittauksilla "jäsenvaltioihin" tarkoitetaan tässä asiakirjassa ETA:n jäsenvaltioita.
[2] Tietosuojatyöryhmän suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta (WP250 rev.01) (viimeksi tarkistettu ja päivitetty 6. helmikuuta 2018), saatavilla osoitteessa https://ec.europa.eu/newsroom/article29/items/612052.
[3] Ks. https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
[4] Ks. yleisen tietosuoja-asetuksen 4 artiklan 21 kohta.

N:o 611/2013 mukaisesti)[5]. Myös eräillä jäsenvaltioilla oli jo käytössä omat kansalliset tietoturvaloukkauksesta ilmoittamista koskevat velvoitteensa. Tähän saattoi sisältyä velvollisuus ilmoittaa tietoturvaloukkauksista, joihin liittyy rekisterinpitäjien ryhmiä yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien lisäksi (esimerkiksi Saksassa ja Italiassa), tai velvollisuus ilmoittaa kaikista tietoturvaloukkauksista, joihin liittyy henkilötietoja (esimerkiksi Alankomaissa). Muissa jäsenvaltioissa saattoi olla asiaan liittyviä käytännesääntöjä (esimerkiksi Irlannissa[6]). Vaikka monet EU:n tietosuojaviranomaiset kannustivat rekisterinpitäjiä ilmoittamaan tietoturvaloukkauksista, tietosuojadirektiivi 95/46/EY[7], joka yleisellä tietosuoja-asetuksella korvattiin, ei sisältänyt erityistä tietoturvaloukkauksista ilmoittamista koskevaa velvoitetta, ja tästä syystä tällainen vaatimus oli monille organisaatioille uusi. Yleisellä tietosuoja-asetuksella tehdään ilmoittamisesta pakollista kaikille rekisterinpitäjille, paitsi jos tietoturvaloukkaukseen ei todennäköisesti liity luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä[8]. Myös henkilötietojen käsittelijöillä on tärkeä rooli, ja niiden on ilmoitettava kaikista tietoturvaloukkauksista rekisterinpitäjälleen[9].

5. Tietosuojaneuvosto katsoo, että ilmoittamisvaatimuksesta on monia etuja. Ilmoittaessaan valvontaviranomaiselle rekisterinpitäjät voivat saada neuvontaa siitä, onko tietoturvaloukkauksesta ilmoitettava niille henkilöille, joihin se vaikuttaa. Valvontaviranomainen voi määrätä rekisterinpitäjän ilmoittamaan kyseisille henkilöille tietoturvaloukkauksesta[10]. Ilmoittamalla tietoturvaloukkauksesta henkilöille rekisterinpitäjä voi antaa tietoja tietoturvaloukkauksen aiheuttamista riskeistä sekä toimista, joita kyseiset henkilöt voivat toteuttaa suojautuakseen sen mahdollisilta seurauksilta. Kaikissa tietoturvaloukkauksia koskevissa valmiussuunnitelmissa olisi keskityttävä suojelemaan henkilöitä ja heidän henkilötietojaan. Näin ollen tietoturvaloukkauksesta ilmoittaminen olisi nähtävä henkilötietojen suojan noudattamista lisäävänä välineenä. Samalla on syytä huomauttaa, että tietoturvaloukkauksesta ilmoittamatta jättäminen joko henkilölle tai valvontaviranomaiselle saattaa merkitä sitä, että rekisterinpitäjälle voidaan 83 artiklan a alakohdan nojalla mahdollisesti määrätä seuraamuksia.

6. Tästä syystä rekisterinpitäjiä ja henkilötietojen käsittelijöitä kannustetaan suunnittelemaan ja ottamaan käyttöön ennakolta prosesseja, joiden avulla ne voivat havaita tietoturvaloukkauksen ja estää nopeasti sen leviämisen, arvioida henkilöille aiheutuvat riskit[11] ja tämän jälkeen määritellä, onko tietoturvaloukkauksesta tarpeen ilmoittaa toimivaltaiselle valvontaviranomaiselle sekä tarvittaessa ilmoittaa siitä asianomaisille henkilöille. Valvontaviranomaiselle ilmoittamisen olisi oltava osa tietoturvaloukkauksia koskevaa valmiussuunnitelmaa.

7. Yleinen tietosuoja-asetus sisältää säännöksiä siitä, milloin tietoturvaloukkauksesta on ilmoitettava ja kenelle, sekä siitä, mitä tietoja ilmoituksessa on toimitettava. Ilmoituksessa vaadittavat tiedot voidaan

---

[5] Ks. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:32009L0136 ja http://eur-lex.europa.eu/legalcontent/FI/TXT/?uri=CELEX%3A32013R0611

[6] Ks. https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[7] Ks. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex:31995L0046

[8] Oikeudet on kirjattu EU:n perusoikeuskirjaan, joka on saatavilla osoitteessa http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:12012P/TXT, available at http://eurlex.europa.eu/legal-content/FI/TXT/?uri=CELEX:12012P/TXT

[9] Ks. yleisen tietosuoja-asetuksen 33 artiklan 2 kohta. Se on käsitteellisesti samanlainen kuin asetuksen (EU) N:o 611/2013 5 artikla, jonka mukaan sähköisen viestintäpalvelun tarjonnassa alihankkijana käytettävän toisen palveluntarjoajan (joka ei ole suorassa sopimussuhteessa tilaajiin) on ilmoitettava henkilötietojen tietoturvaloukkauksesta sitä alihankkijana käyttävälle palveluntarjoajalle.

[10] Ks. yleisen tietosuoja-asetuksen 34 artiklan 4 alakohta ja 58 artiklan 2 kohta.

[11] Tämä voidaan varmistaa tietosuojaa koskevan vaikutustenarvioinnin valvonta- ja uudelleentarkasteluvaatimusten avulla. Tietosuojaa koskeva vaikutustenarviointi edellytetään käsittelytoimilta, jotka aiheuttavat todennäköisesti luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin (35 artiklan 1 ja 11 kohta).

toimittaa vaiheittain, mutta rekisterinpitäjien olisi joka tapauksessa reagoitava tietoturvaloukkauksiin viipymättä.

8. Lausunnossaan 3/2014 henkilötietojen tietoturvaloukkauksen ilmoittamisesta[12] tietosuojatyöryhmä antoi rekisterinpitäjille ohjeita, joiden avulla nämä voivat päättää, ilmoitetaanko tietoturvaloukkauksesta rekisteröidyille. Lausunnossa otettiin huomioon direktiiviin 2002/58/EY perustuvat sähköisen viestinnän palveluntarjoajien velvoitteet ja annettiin silloin ehdotusvaiheessa olleen tietosuoja-asetuksen hengessä esimerkkejä useilta eri aloilta ja esiteltiin kaikkia rekisterinpitäjiä koskevia hyviä käytäntöjä.

9. Näissä suuntaviivoissa selitetään yleisen tietosuoja-asetuksen sisältämät pakolliset tietoturvaloukkauksen ilmoittamista koskevat vaatimukset ja eräitä toimia, joita rekisterinpitäjät ja henkilötietojen käsittelijät voivat toteuttaa näiden velvoitteiden noudattamiseksi. Lisäksi annetaan esimerkkejä eri tyyppisistä tietoturvaloukkauksista sekä siitä, kenelle niistä olisi eri skenaarioissa ilmoitettava.

I. YLEISEN TIETOTURVA-ASETUKSEN MUKAINEN HENKILÖTIETOJEN TIETOTURVALOUKKAUKSEN ILMOITTAMINEN

A. Keskeisiä turvallisuutta koskevia näkökohtia

10. Yksi yleisen tietosuoja-asetuksen vaatimuksista on, että henkilötietoja on käsiteltävä tavalla, jolla varmistetaan asianmukaisten teknisten tai organisatoristen toimien avulla henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta[13].

11. Näin ollen yleisessä tietosuoja-asetuksessa edellytetään, että sekä rekisterinpitäjät että henkilötietojen käsittelijät toteuttavat asianmukaiset tekniset ja organisatoriset toimet varmistaakseen käsiteltäville henkilötiedoille aiheutuvaa riskiä vastaavan turvallisuustason. Näissä toimenpiteissä olisi otettava huomioon uusin tekniikka, toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä todennäköisyydeltään ja vakavuudeltaan vaihtelevat luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit[14]. Yleisessä tietosuoja-asetuksessa edellytetään myös, että kaikki asianmukaiset tekniset suojatoimenpiteet ja organisatoriset toimenpiteet on toteutettu, jotta voidaan selvittää välittömästi, onko tapahtunut tietoturvaloukkaus, mikä puolestaan määrää, sovelletaanko ilmoittamisvelvoitetta[15].

12. Näin ollen kaikkien tietosuojaa koskevien toimintalinjojen keskeinen osatekijä on kyky mahdollisuuksien mukaan estää tietoturvaloukkaus, ja jos se tästä huolimatta tapahtuu, reagoida siihen nopeasti.

B. Mikä on henkilötietojen tietoturvaloukkaus?

1. Määritelmä

13. Voidakseen puuttua tietoturvaloukkauksiin rekisterinpitäjän olisi ensin kyettävä tunnistamaan ne. Yleisen tietosuoja-asetuksen 4 artiklan 12 kohdan mukaan ’henkilötietojen tietoturvaloukkauksella’ tarkoitetaan:

---

[12] Ks. lausunto 3/2014 henkilötietojen tietoturvaloukkauksen ilmoittamisesta http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_fi.pdf

[13] Ks. 5 artiklan 1 kohdan f alakohta ja 32 artikla.

[14] Yleisen tietosuoja-asetuksen 32 artikla; ks. myös johdanto-osan 83 kappale.

[15] Ks. yleisen tietosuoja-asetuksen johdanto-osan 87 kappale.

”*tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin*”.

14. Se, mitä henkilötietojen ”tuhoamisella” tarkoitetaan, lienee täysin selvää: tällöin tietoja ei enää ole olemassa tai niitä ei enää ole olemassa rekisterinpitäjän kannalta käyttökelpoisessa muodossa. Myös ”vahingoittuminen” lienee suhteellisen selvää: tällöin henkilötietoja on muutettu, ne ovat vaurioituneet tai ne eivät enää ole täydelliset. Henkilötietojen ”häviäminen” olisi tulkittava siten, että tiedot saattavat yhä olla olemassa, mutta ne eivät ole rekisterinpitäjän valvonnassa tai sillä ei enää ole pääsyä niihin tai tiedot eivät enää ole rekisterinpitäjän hallussa. Luvattomaan tai laittomaan käsittelyyn saattaa sisältyä myös henkilötietojen luovuttaminen vastaanottajille, joilla ei ole lupaa ottaa niitä vastaan (tai tällaisten vastaanottajien pääsy tietoihin), tai mikä tahansa muu yleisen tietosuoja-asetuksen vastainen tietojen käsittelyn muoto.

Esimerkki

Yksi esimerkki henkilötietojen häviämisestä on tapaus, jossa rekisterinpitäjän asiakastietokannan kopion sisältävä laite on kadonnut tai varastettu. Toinen esimerkki häviämisestä saattaa olla tapaus, jossa ainoa henkilötietoja sisältävä kopio on salattu kiristysohjelmalla tai rekisterinpitäjä on salannut sen käyttäen salausavainta, joka ei enää ole sen hallussa.

15. Selvää on, että tietoturvaloukkaus on tietyntyyppinen turvapoikkeama. Yleistä tietosuoja-asetusta sovelletaan kuitenkin vain, jos tietoturvaloukkaus koskee henkilötietoja, kuten asetuksen 4 artiklan 12 kohdassa todetaan. Tällaisen tietoturvaloukkauksen seurauksena rekisterinpitäjä ei voi taata yleisen tietosuoja-asetuksen 5 artiklassa esitettyjen henkilötietojen käsittelyä koskevien periaatteiden noudattamista. Tämä tuo esiin turvapoikkeaman ja henkilötietojen tietoturvaloukkauksen välisen eron – tiivistetysti voidaan sanoa, että vaikka kaikki henkilötietojen tietoturvaloukkaukset ovat turvapoikkeamia, kaikki turvapoikkeamat eivät välttämättä ole henkilötietojen tietoturvaloukkauksia[16].

16. Tietoturvaloukkauksen mahdollisia haitallisia vaikutuksia henkilöille käsitellään jäljempänä.

2. Henkilötietojen tietoturvaloukkausten tyypit

17. Lausunnossaan 3/2014 henkilötietojen tietoturvaloukkausten ilmoittamisesta tietosuojatyöryhmä selitti, että tietoturvaloukkaukset voidaan luokitella seuraavien kolmen tunnetun tietoturvaperiaatteen mukaan[17]:

- ”**tietojen luottamuksellisuuteen vaikuttava tietoturvaloukkaus**” – henkilötietojen luvaton luovuttaminen tai käyttöön antaminen
- ”**tietojen eheyteen vaikuttava tietoturvaloukkaus**” – henkilötietojen luvaton tai tahaton muuttaminen
- ”**tietojen käytettävyyteen vaikuttava tietoturvaloukkaus**” – tahaton tai luvaton henkilötietoihin pääsyn menettäminen[18] tai henkilötietojen tuhoaminen.

[16] On syytä huomauttaa, että turvapoikkeama ei rajoitu uhkamalleihin, joissa organisaatioon kohdistuu hyökkäys ulkoisesta lähteestä, vaan siihen sisältyvät myös vaaratilanteet, jotka aiheutuvat turvallisuusperiaatteiden vastaisesta sisäisestä tietojenkäsittelystä.

[17] Ks. tietosuojatyöryhmän lausunto 3/2014.

[18] On laajalti tunnustettua, että ”pääsy” tietoihin on oleellinen osa niiden ”käytettävyyttä”. Ks. esimerkiksi asiakirja NIST SP800-SP80053rev4, jossa ”käytettävyys” (engl. ”availability”) määritellään oikea-aikaisen ja luotettavan tietoihin pääsyn ja tietojen käytön varmistamiseksi (”Ensuring timely and reliable access to and use of information”). Asiakirja on saatavilla verkko-osoitteessa

18. On myös syytä huomata, että tilanteesta riippuen tietoturvaloukkaus voi koskea samanaikaisesti luottamuksellisuutta, eheyttä ja käytettävyyttä tai mitä tahansa niiden yhdistelmää.

19. Sen määrittäminen, onko tapahtunut luottamuksellisuuteen tai eheyteen vaikuttava tietoturvaloukkaus, on suhteellisen selkeää, mutta se, onko tapahtunut käytettävyyteen vaikuttava tietoturvaloukkaus, saattaa olla vähemmän ilmeistä. Tietoturvaloukkauksen katsotaan aina vaikuttavan käytettävyyteen, jos henkilötietoja on hävinnyt tai tuhoutunut pysyvästi.

Esimerkki

Käytettävyys menetetään esimerkiksi tapauksissa, joissa tiedot on poistettu tahattomasti tai sellaisen henkilön toimesta, jolla ei ole tähän lupaa, tai salattujen tietojen salausavain on kadonnut. Jos rekisterinpitäjä ei voi palauttaa pääsyä tietoihin esimerkiksi varmuuskopion avulla, tätä pidetään käytettävyyden pysyvänä menettämisenä.

Käytettävyys saatetaan menettää myös silloin, jos organisaation normaalissa toiminnassa on ollut merkittävä häiriö esimerkiksi henkilötietojen käytettävyyden estävän sähkökatkoksen tai palvelunestohyökkäyksen vuoksi.

20. Voidaan kysyä, onko henkilötietojen käytettävyyden väliaikaista menettämistä pidettävä tietoturvaloukkauksena, ja jos on, olisiko siitä ilmoitettava. Yleisen tietoturva-asetuksen 32 artiklassa ”Käsittelyn turvallisuus” selitetään, että toteutettaessa riskiä vastaavan turvallisuustason varmistamiseksi asianmukaisia teknisiä ja organisatorisia toimenpiteitä olisi otettava huomioon muun muassa ”*kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus*” ja ”*kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa*”.

21. Näin ollen turvapoikkeama, joka johtaa henkilötietojen käytettävyyden menettämiseen joksikin aikaa, on myös yksi tietoturvaloukkauksen tyyppi, koska tietoihin pääsyn menettämisellä saattaa olla merkittävä vaikutus luonnollisten henkilöiden oikeuksiin ja vapauksiin. Selvyyden vuoksi on todettava, että jos henkilötiedot eivät ole käytettävissä suunnitellun järjestelmän huollon vuoksi, tämä ei ole yleisen tietosuoja-asetuksen 4 artiklan 12 kohdassa tarkoitettu ”tietoturvaloukkaus”.

22. Kuten henkilötietojen pysyvä häviäminen tai tuhoutuminen (tai yleensä minkä tahansa tyyppinen tietoturvaloukkaus), tietoturvaloukkaus, johon liittyy käytettävyyden väliaikainen häviäminen, olisi dokumentoitava yleisen tietosuoja-asetuksen 33 artiklan 5 kohdan mukaisesti. Tämä auttaa rekisterinpitäjää täyttämään osoitusvelvollisuutensa valvontaviranomaiselle, joka saattaa pyytää näitä tietoja [19]. Tietoturvaloukkaukseen liittyvistä olosuhteista riippuen se saattaa edellyttää tai olla edellyttämättä ilmoittamista valvontaviranomaiselle ja tietoturvaloukkauksen kohteina olleille henkilöille. Rekisterinpitäjän on arvioitava henkilötietojen käytettävyyden menetyksen seurauksena syntyvän, luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvan vaikutuksen todennäköisyys ja vakavuus. Rekisterinpitäjän on yleisen tietosuoja-asetuksen 33 artiklan mukaisesti ilmoitettava tietoturvaloukkauksesta, ellei ole epätodennäköistä, että se aiheuttaa riskin henkilöiden oikeuksille ja vapauksille. Tämä on luonnollisesti arvioitava tapauskohtaisesti.

---

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Asiakirjassa CNSSI-4009 käytettävyydellä tarkoitetaan myös valtuutettujen käyttäjien nopeaa ja luotettavaa pääsyä tietoihin (”Timely, reliable access to data and information services for authorized users”). Ks. https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. Myös standardissa ISO/IEC 27000:2016 tietojen ”käytettävyys” määritellään siten, että tiedot ovat pyynnöstä valtuutetun yksikön saatavilla ja käytettävissä (”Property of being accessible and usable upon demand by an authorized entity”): https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en

[19] Ks. yleisen tietosuoja-asetuksen 33 artiklan 5 kohta.

Esimerkki

Jos sairaalaympäristössä potilaiden kriittisen tärkeät lääketieteelliset tiedot eivät ole käytettävissä, vaikka väliaikaisestikin, tämä saattaa muodostaa riskin henkilöiden oikeuksille ja vapauksille; esimerkiksi leikkauksia saatetaan peruuttaa, jolloin ihmishenkiä vaarantuu.

Jos taas mediayrityksen järjestelmät eivät ole käytettävissä useiden tuntien ajan (esimerkiksi sähkökatkon vuoksi) ja kyseinen yritys ei tästä syystä pysty lähettämään uutiskirjeitä tilaajilleen, tämä ei todennäköisesti muodosta riskiä henkilöiden oikeuksille ja vapauksille.

23. On syytä huomata, että vaikka rekisterinpitäjän järjestelmien käytettävyyden menettäminen saattaa olla vain väliaikaista eikä ehkä vaikuta henkilöihin, rekisterinpitäjän on tärkeää ottaa huomioon tietoturvaloukkauksen kaikki mahdolliset seuraukset, koska se saattaa edellyttää ilmoittamista muista syistä.

Esimerkki

Kiristysohjelmat (haittaohjelmat, jotka salaavat rekisterinpitäjän tiedot, kunnes lunnaat maksetaan) saattavat aiheuttaa käytettävyyden väliaikaisen menettämisen, jos tiedot voidaan palauttaa varmuuskopiosta. Verkkotunkeutuminen on kuitenkin tapahtunut, ja se saattaa edellyttää ilmoittamista, jos turvapoikkeama katsotaan luottamuksellisuuteen vaikuttavaksi tietoturvaloukkaukseksi (eli hyökkääjä saa pääsyn henkilötietoihin) ja tämä aiheuttaa riskin henkilöiden oikeuksille ja vapauksille.

3. Henkilötietojen tietoturvaloukkauksen mahdolliset seuraukset

24. Tietoturvaloukkauksella saattaa mahdollisesti olla useita erilaisia henkilöihin kohdistuvia haittavaikutuksia, jotka voivat aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja. Yleisessä tietosuoja-asetuksessa selitetään, että niitä saattavat olla muun muassa omien henkilötietojen valvomiskyvyn menettäminen tai oikeuksien rajoittaminen, syrjintä, identiteettivarkaus tai petos, taloudelliset menetykset, pseudonymisoitumisen luvaton kumoutuminen, maineen vahingoittuminen ja salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetys. Niihin saattaa sisältyä myös muuta merkittävää taloudellista tai sosiaalista vahinkoa kyseisille henkilöille[20].

25. Näin ollen yleisessä tietosuoja-asetuksessa edellytetään, että rekisterinpitäjä ilmoittaa tietoturvaloukkauksesta toimivaltaiselle valvontaviranomaiselle, paitsi jos se ei todennäköisesti aiheuta tällaisten haittavaikutusten riskiä. Jos tällaisten haittavaikutusten riski on todennäköisesti korkea, yleisessä tietosuoja-asetuksessa edellytetään, että rekisterinpitäjä ilmoittaa tietoturvaloukkauksesta asianomaisille henkilöille niin pian kuin se on kohtuudella mahdollista[21].

26. Yleisen tietosuoja-asetuksen johdanto-osan 87 kappaleessa korostetaan, että on tärkeää tunnistaa tietoturvaloukkaus, arvioida henkilöille aiheutuva riski ja sitten ilmoittaa tietoturvaloukkauksesta tarvittaessa.

”*Olisi tarkistettava, onko kaikki asianmukaiset tekniset suojatoimenpiteet ja organisatoriset toimenpiteet toteutettu, jotta voidaan selvittää välittömästi, onko tapahtunut henkilötietojen tietoturvaloukkaus, ja saattaa asia viipymättä valvontaviranomaisen ja rekisteröidyn tiedoksi. Se, että ilmoitus tehtiin ilman aiheetonta viivytystä, olisi selvitettävä ottaen huomioon erityisesti henkilötietojen tietoturvaloukkauksen luonne ja vakavuus sekä tästä rekisteröidylle aiheutuvat seuraukset ja haittavaikutukset. Kyseinen ilmoitus voi johtaa siihen, että valvontaviranomainen puuttuu asiaan sille tässä asetuksessa säädettyjen tehtävien ja toimivaltuuksien mukaisesti.*”

[20] Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 85 ja 75 kappaleet.

[21] Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 86 kappale.

27. Lisäohjeita henkilöille aiheutuvien haittavaikutusten riskin arvioimisesta on osiossa IV.

28. Jos rekisterinpitäjät jättävät ilmoittamatta tietoturvaloukkauksesta joko valvontaviranomaiselle tai rekisteröidyille tai molemmille, vaikka yleisen tietosuoja-asetuksen 33 ja/tai 34 artiklan vaatimukset täyttyvät, valvontaviranomaisen on tehtävä päätös, jossa on harkittava kaikkia sen käytettävissä olevia korjaavia toimenpiteitä, kuten muun muassa asianmukaista hallinnollista sakkoa [22], joka voidaan määrätä yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan mukaisen korjaavan toimenpiteen lisäksi tai erikseen. Jos päätetään määrätä hallinnollinen sakko, sen määrä voi yleisen tietosuoja-asetuksen 83 artiklan 4 kohdan a alakohdan mukaan olla enintään 10 000 000 euroa tai 2 prosenttia yrityksen vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. On myös tärkeää muistaa, että joissain tapauksissa tietoturvaloukkauksesta ilmoittamatta jättäminen saattaa paljastaa joko turvaamistoimenpiteiden puutteen tai olemassa olevien turvaamistoimenpiteiden riittämättömyyden. Hallinnollisia sakkoja koskevissa tietosuojatyöryhmän suuntaviivoissa todetaan seuraavaa: ”*Jos tietyssä yksittäisessä tapauksessa rikkomisia on useita, valvontaviranomainen voi määrätä hallinnollisia sakkoja vakavimman rikkomisen rajoissa siinä määrin kuin on tehokasta, oikeasuhteista ja varoittavaa.*” Tässä tapauksessa valvontaviranomaisella on myös mahdollisuus määrätä seuraamuksia yhtäältä tietoturvaloukkauksesta ilmoittamatta jättämisestä (yleisen tietosuoja-asetuksen 33 ja 34 artikla) ja toisaalta (riittävien) turvatoimien puutteesta (yleisen tietosuoja-asetuksen 32 artikla), koska ne ovat kaksi erillistä sääntörikkomusta.

II 33 ARTIKLA – ILMOITTAMINEN VALVONTAVIRANOMAISELLE

A. Milloin ilmoitetaan?

1. 33 artiklan vaatimukset

29. Yleisen tietosuoja-asetuksen 33 artiklan 1 kohdassa säädetään seuraavaa:

> ”*Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta 55 artiklan mukaisesti toimivaltaiselle valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys.*”

30. Yleisen tietosuoja-asetuksen johdanto-osan 87 kappaleessa todetaan seuraavaa[23]:

> ”*Olisi tarkistettava, onko kaikki asianmukaiset tekniset suojatoimenpiteet ja organisatoriset toimenpiteet toteutettu, jotta voidaan selvittää välittömästi, onko tapahtunut henkilötietojen tietoturvaloukkaus, ja saattaa asia viipymättä valvontaviranomaisen ja rekisteröidyn tiedoksi. Se, että ilmoitus tehtiin ilman aiheetonta viivytystä, olisi selvitettävä ottaen huomioon erityisesti henkilötietojen tietoturvaloukkauksen luonne ja vakavuus sekä tästä rekisteröidylle aiheutuvat seuraukset ja haittavaikutukset. Kyseinen ilmoitus voi johtaa siihen, että valvontaviranomainen puuttuu asiaan sille tässä asetuksessa säädettyjen tehtävien ja toimivaltuuksien mukaisesti.*”

2. Milloin tietoturvaloukkaus ”tulee ilmi” rekisterinpitäjälle?

31. Kuten edellä on esitetty, yleisessä tietosuoja-asetuksessa edellytetään, että jos tapahtuu tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja

[22] Lisätietoja on asetuksessa 2016/679 tarkoitettujen hallinnollisten sakkojen soveltamista ja määräämistä koskevissa tietosuojatyöryhmän suuntaviivoissa, jotka ovat saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[23] Myös johdanto-osan 85 kappale on tässä yhteydessä merkittävä.

mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta. Tämä saattaa herättää kysymyksen siitä, milloin tietoturvaloukkauksen voidaan katsoa ”tulleen ilmi” rekisterinpitäjälle. Tietosuojaneuvosto katsoo, että tietoturvaloukkauksen olisi katsottava ”tulleen ilmi” rekisterinpitäjälle silloin, kun sillä on kohtuullinen varmuus siitä, että on tapahtunut henkilötietoja vaarantava turvapoikkeama.

32. Kuten edellä todettiin, yleisessä tietosuoja-asetuksessa edellytetään kuitenkin, että rekisterinpitäjä toteuttaa kaikki asianmukaiset tekniset suojatoimenpiteet ja organisatoriset toimenpiteet, jotta voidaan selvittää välittömästi, onko tapahtunut henkilötietojen tietoturvaloukkaus, ja saattaa asia viipymättä valvontaviranomaisen ja rekisteröityjen tiedoksi. Siinä todetaan myös, että se, että ilmoitus tehtiin ilman aiheetonta viivytystä, olisi selvitettävä ottaen huomioon erityisesti tietoturvaloukkauksen luonne ja vakavuus sekä tästä rekisteröidylle aiheutuvat seuraukset ja haittavaikutukset[24]. Tämä asettaa rekisterinpitäjälle velvoitteen varmistaa, että mahdolliset tietoturvaloukkaukset tulevat sille ”ilmi” ajoissa, jotta se voi toteuttaa asianmukaisia toimia.

33. Se, milloin tarkalleen tietyn tietoturvaloukkauksen voidaan katsoa tulleen rekisterinpitäjälle ”ilmi”, riippuu kunkin tietoturvaloukkauksen olosuhteista. Joissain tapauksissa on alusta lähtien suhteellisen selvää, että tietoturvaloukkaus on tapahtunut, kun taas toisissa tapauksissa saattaa kestää jonkin aikaa selvittää, ovatko henkilötiedot vaarantuneet. Olisi kuitenkin painotettava ripeitä toimia turvapoikkeaman tutkimiseksi, jotta voidaan määrittää, onko todella tapahtunut henkilötietojen tietoturvaloukkaus, ja jos on, toteutetaan korjaavia toimia ja ilmoitetaan siitä tarvittaessa.

Esimerkkejä

1. Jos salaamattomia henkilötietoja sisältävä USB-muistitikku katoaa, ei usein ole mahdollista selvittää varmasti, ovatko sivulliset saaneet pääsyn tietoihin. Vaikka rekisterinpitäjän ei ehkä ole mahdollista selvittää, onko luottamuksellisuuteen vaikuttava tietoturvaloukkaus tapahtunut, tällaisesta tapauksesta on kuitenkin ilmoitettava, koska on olemassa kohtuullinen varmuus siitä, että on tapahtunut käytettävyyteen vaikuttava tietoturvaloukkaus; se tulee ”ilmi” rekisterinpitäjälle tämän huomatessa, että USB-muistitikku on kadonnut.

2. Jokin kolmas osapuoli ilmoittaa rekisterinpitäjälle saaneensa vahingossa rekisterinpitäjän asiakkaan henkilötietoja ja toimittaa näyttöä luvattomasta luovuttamisesta. Koska rekisterinpitäjälle on esitetty selvää näyttöä luottamuksellisuuteen vaikuttavasta tietoturvaloukkauksesta, on täysin selvää, että tietoturvaloukkaus on tullut sille ”ilmi”.

3. Rekisterinpitäjä havaitsee, että sen verkkoon on mahdollisesti tunkeuduttu. Rekisterinpitäjä tarkastaa järjestelmänsä selvittääkseen, ovatko siinä säilytetyt henkilötiedot vaarantuneet, ja vahvistaa, että näin on tapahtunut. Koska rekisterinpitäjällä nyt on selvää näyttöä tietoturvaloukkauksesta, tässäkin tapauksessa on täysin selvää, että tietoturvaloukkaus on tullut sille ”ilmi”.

4. Verkkorikollinen ottaa yhteyttä rekisterinpitäjään tehtyään tietomurron tämän järjestelmään ja vaatii lunnaita. Tässä tapauksessa rekisterinpitäjällä on – tarkastettuaan järjestelmänsä ja vahvistettuaan, että siihen on kohdistunut hyökkäys – selvää näyttöä tietoturvaloukkauksen tapahtumisesta, ja on täysin selvää, että tietoturvaloukkaus on tullut sille ”ilmi”.

34. Kun rekisterinpitäjä on saanut tiedon mahdollisesta tietoturvaloukkauksesta yksityishenkilöltä, media-alan organisaatiolta tai muusta lähteestä tai jos se itse on havainnut turvapoikkeaman, se voi käyttää lyhyen ajan tutkiakseen, onko tietoturvaloukkaus todella tapahtunut. Tämän tutkinnan aikana ei voida katsoa, että tietoturvaloukkaus on tullut ”ilmi” rekisterinpitäjälle. Alustavan tutkinnan edellytetään kuitenkin alkavan mahdollisimman pian, ja sillä olisi selvitettävä kohtuullisen varmasti, onko tietoturvaloukkaus tapahtunut; tämän jälkeen voidaan suorittaa tarkempi tutkinta.

[24] Ks. yleisen tietosuoja-asetuksen johdanto-osan 87 kappale.

35. Kun tietoturvaloukkaus on tullut rekisterinpitäjälle ilmi, ilmoitettavasta tietoturvaloukkauksesta on ilmoitettava ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa. Tänä aikana rekisterinpitäjän olisi arvioitava henkilöille aiheutuva todennäköinen riski määrittääkseen, sovelletaanko ilmoittamisvelvollisuutta, sekä tietoturvaloukkauksen edellyttämät toimet. Rekisterinpitäjällä voi kuitenkin olla jo tietoturvaloukkauksesta mahdollisesti aiheutuvasta potentiaalisesta riskistä tehty alustava arvio, joka on osa ennen kyseisen käsittelytoimen suorittamista toteutettua tietosuojaa koskevaa vaikutustenarviointia[25]. Tietosuojaa koskeva vaikutustenarviointi saattaa kuitenkin olla luonteeltaan yleisempi verrattuna todellisen tietoturvaloukkauksen konkreettisiin olosuhteisiin, ja siksi on joka tapauksessa tehtävä täydentävä arviointi, jossa nämä olosuhteet otetaan huomioon. Lisätietoja riskin arvioinnista on osiossa IV.

36. Useimmissa tapauksissa nämä alustavat toimet olisi saatettava päätökseen pian ensimmäisen hälytyksen jälkeen (eli kun rekisterinpitäjä tai henkilötietojen käsittelijä epäilee, että on tapahtunut turvapoikkeama, johon liittyy henkilötietoja) – tämä saa kestää tätä kauemmin vain poikkeuksellisissa tapauksissa.

Esimerkki

Yksityishenkilö ilmoittaa rekisterinpitäjälle saaneensa sähköpostiviestin, jonka lähettäjä väittää olevansa rekisterinpitäjä ja joka sisältää henkilötietoja, jotka liittyvät henkilön suorittamaan rekisterinpitäjän palvelujen (todelliseen) käyttöön, ja jossa väitetään rekisterinpitäjän tietoturvan vaarantuneen. Rekisterinpitäjä suorittaa lyhytkestoisen tutkinnan ja havaitsee, että sen verkkoon on tunkeuduttu, ja löytää näyttöä luvattomasta pääsystä henkilötietoihin. Nyt tietoturvaloukkauksen katsottaisiin tulleen rekisterinpitäjälle ”ilmi”, ja ilmoittaminen valvontaviranomaiselle on tarpeen, paitsi jos on epätodennäköistä, että tietoturvaloukkaus aiheuttaa henkilöiden oikeuksiin ja vapauksiin kohdistuvan riskin. Rekisterinpitäjän on toteutettava tarvittavat korjaavat toimet tietoturvaloukkaukseen puuttumiseksi.

37. Tästä syystä rekisterinpitäjällä olisi oltava käytössä sisäiset prosessit, joiden avulla se voi havaita tietoturvaloukkauksen ja puuttua siihen. Esimerkiksi havaitakseen sääntöjenvastaisuuksia tietojenkäsittelyssä rekisterinpitäjä tai henkilötietojen käsittelijä voi käyttää tiettyjä teknisiä toimenpiteitä, kuten tietovuon ja tapahtumalokien analysointivälineitä, joiden avulla on mahdollista määritellä tapahtumia ja hälytyksiä korreloimalla tapahtumalokien tietoja[26]. On tärkeää, että kun tietoturvaloukkaus havaitaan, siitä raportoidaan ylöspäin asianmukaiselle johdon tasolle, jotta siihen voidaan puuttua ja siitä voidaan tarvittaessa ilmoittaa 33 artiklan ja mahdollisesti 34 artiklan mukaisesti. Tällaiset toimenpiteet ja raportointimekanismit voitaisiin kuvailla yksityiskohtaisesti rekisterinpitäjän turvapoikkeamia koskevissa valmiussuunnitelmissa ja/tai hallinnointijärjestelyissä. Nämä auttavat rekisterinpitäjää suunnittelemaan tehokkaasti ja määrittämään, kenellä organisaatiossa on operatiivinen vastuu tietoturvaloukkauksen hallinnoinnista ja porrastetaanko turvapoikkeama, ja jos porrastetaan, miten.

38. Lisäksi rekisterinpitäjällä olisi oltava järjestelyjä käyttämiensä henkilötietojen käsittelijöiden kanssa, joilla on velvollisuus ilmoittaa rekisterinpitäjälle tietoturvaloukkauksista (ks. jäljempänä).

39. Vaikka on rekisterinpitäjien ja henkilötietojen käsittelijöiden vastuulla ottaa käyttöön soveltuvat toimenpiteet, joiden avulla ne voivat ehkäistä tietoturvaloukkauksia, reagoida niihin ja torjua niitä, on eräitä käytännön toimia, jotka olisi toteutettava kaikissa tapauksissa.

---

[25] Ks. tietosuojatyöryhmän ohjeet tietosuojaa koskevasta vaikutustenarvioinnista WP248, jotka ovat saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[26] On syytä huomauttaa, että myös esimerkiksi tietojen säilyttämisen, muuttamisen tai poistamisen tarkastuksissa apuna käytettävät lokitiedot voidaan katsoa henkilötiedoiksi, jotka liittyvät henkilöön, joka on käynnistänyt kyseisen käsittelytoimen.

- Tiedot kaikista turvallisuuteen liittyvistä tapahtumista olisi osoitettava vastuuhenkilölle tai -henkilöille, joiden tehtävänä on käsitellä turvapoikkeamia, todeta tietoturvaloukkauksen tapahtuminen ja arvioida riski.
- Tämän jälkeen olisi arvioitava tietoturvaloukkauksesta henkilöille aiheutuva riski (ei riskiä tai riskin tai korkean riskin todennäköisyys) ja siitä olisi tiedotettava asiaan kuuluville organisaation osille.
- Tarvittaessa tietoturvaloukkauksesta olisi ilmoitettava valvontaviranomaiselle ja tarvittaessa niille henkilöille, joihin se vaikuttaa.
- Samalla rekisterinpitäjän olisi toteutettava toimia tietoturvaloukkauksen leviämisen estämiseksi ja sen korjaamiseksi. Tietoturvaloukkaus olisi dokumentoitava sitä mukaa, kun tilanne kehittyy.

40. Näin ollen pitäisi olla selvää, että rekisterinpitäjällä on velvollisuus reagoida alustavaan hälytykseen ja selvittää, onko tietoturvaloukkaus todella tapahtunut. Tänä lyhyenä aikana rekisterinpitäjän on mahdollista suorittaa jonkin verran tutkintaa ja kerätä näyttöä ja muita merkityksellisiä tietoja. Kun rekisterinpitäjä on todennut kohtuullisen varmasti, että tietoturvaloukkaus on tapahtunut, sen on ilmoitettava siitä valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa, mikäli yleisen tietosuoja-asetuksen 33 artiklan 1 kohdan ehdot täyttyvät[27]. Jos rekisterinpitäjä ei toimi nopeasti ja käy ilmi, että tietoturvaloukkaus on tapahtunut, tätä voidaan pitää yleisen tietosuoja-asetuksen 33 artiklassa säädetyn ilmoittamisvelvollisuuden laiminlyöntinä.

41. Yleisen tietosuoja-asetuksen 32 artiklassa todetaan selkeästi, että rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Valmiuksia havaita ja torjua tietoturvaloukkaus ja ilmoittaa siitä nopeasti olisi pidettävä näiden toimenpiteiden oleellisina osatekijöinä.

3. Yhteisrekisterinpitäjät

42. Yleisen tietosuoja-asetuksen 26 artikla koskee yhteisrekisterinpitäjiä, ja sen mukaan yhteisrekisterinpitäjien on määritettävä kunkin vastuualueet yleisen tietosuoja-asetuksen noudattamiseksi [28]. Tähän sisältyy sen määrittäminen, mikä osapuoli vastaa yleisen tietosuoja-asetuksen 33 ja 34 artiklan velvoitteiden noudattamisesta. Tietosuojaneuvosto suosittaa, että yhteisrekisterinpitäjien väliset sopimusjärjestelyt sisältävät määräyksiä, joissa määritetään, mikä rekisterinpitäjä on johtavassa asemassa tai vastuussa yleisen tietosuoja-asetuksen tietoturvaloukkauksen ilmoittamista koskevien velvoitteiden noudattamisesta.

4. Henkilötietojen käsittelijän velvollisuudet

43. Rekisterinpitäjällä on kokonaisvastuu henkilötietojen suojaamisesta, mutta henkilötietojen käsittelijällä on merkittävä rooli, jotta rekisterinpitäjä voi noudattaa velvoitteitaan; tähän sisältyy myös tietoturvaloukkauksen ilmoittaminen. Yleisen tietosuoja-asetuksen 28 artiklan 3 kohdassa täsmennetään, että henkilötietojen käsittelijän suorittama käsittely on määritettävä sopimuksella tai oikeudellisella asiakirjalla. Asetuksen 28 artiklan 3 kohdan f alakohdan mukaan sopimuksessa tai muussa oikeudellisessa asiakirjassa on säädettävä, että henkilötietojen käsittelijä ”auttaa rekisterinpitäjää varmistamaan, että 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan ottaen huomioon käsittelyn luonteen ja henkilötietojen käsittelijän saatavilla olevat tiedot”.

44. Yleisen tietosuoja-asetuksen 33 artiklan 2 kohdassa todetaan selvästi, että jos rekisterinpitäjä käyttää henkilötietojen käsittelijää, tämän on ilmoitettava rekisterinpitäjän puolesta käsittelemiensä henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ”ilman aiheetonta viivytystä saatuaan sen tietoonsa”. On syytä huomauttaa, ettei henkilötietojen käsittelijän tarvitse ensin arvioida

[27] Ks. asetus N:o 1182/71 määräaikoihin, päivämääriin ja määräpäiviin sovellettavista säännöistä, saatavilla verkko-osoitteessa: http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:31971R1182&from=FI

[28] Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 79 kappale.

tietoturvaloukkauksen aiheuttaman riskin todennäköisyyttä, ennen kuin se ilmoittaa siitä rekisterinpitäjälle; rekisterinpitäjän velvollisuutena on suorittaa tällainen arviointi saatuaan tietoturvaloukkauksen tietoonsa. Henkilötietojen käsittelijän on ainoastaan selvitettävä, onko tietoturvaloukkaus tapahtunut, ja ilmoitettava sitä sitten rekisterinpitäjälle. Rekisterinpitäjä käyttää henkilötietojen käsittelijää omiin tarkoituksiinsa; tästä syystä rekisterinpitäjän olisi lähtökohtaisesti katsottava saaneen tietoturvaloukkauksen ”tietoonsa”, kun henkilötietojen käsittelijä on ilmoittanut sille siitä. Henkilötietojen käsittelijän velvollisuus ilmoittaa rekisterinpitäjälle antaa tälle mahdollisuuden puuttua tietoturvaloukkaukseen ja määrittää, onko siitä tarpeen ilmoittaa valvontaviranomaiselle 33 artiklan 1 kohdan mukaisesti ja asianomaisille henkilöille 34 artiklan 1 kohdan mukaisesti. Rekisterinpitäjä saattaa myös haluta tutkia tietoturvaloukkauksen, sillä henkilötietojen käsittelijä ei ehkä tiedä kaikkia asiaan liittyviä merkityksellisiä seikkoja, kuten esimerkiksi sitä, onko rekisterinpitäjän hallussa yhä kopio tai varmuuskopio henkilötietojen käsittelijän tuhoamista tai kadottamista henkilötiedoista. Tämä saattaa vaikuttaa siihen, onko rekisterinpitäjän ilmoitettava tietoturvaloukkauksesta.

45. Yleisessä tietosuoja-asetuksessa ei säädetä tarkasta määräajasta, jonka kuluessa henkilötietojen käsittelijän on ilmoitettava asiasta rekisterinpitäjälle, vaan todetaan vain, että sen on tehtävä tämä ”ilman aiheetonta viivytystä”. Tästä syystä tietosuojaneuvosto suosittaa, että henkilötietojen käsittelijä ilmoittaa tietoturvaloukkauksesta rekisterinpitäjälle välittömästi ja toimittaa lisätietoja siitä sitä mukaa, kun tarkempia tietoja saadaan. Tämä on tärkeää, sillä se auttaa rekisterinpitäjää noudattamaan vaatimusta ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa.

46. Kuten edellä selitettiin, rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa olisi täsmennettävä, miten 33 artiklan 2 kohdassa säädetyt vaatimukset olisi täytettävä yleisen tietosuoja-asetuksen muiden säännösten lisäksi. Tähän voi sisältyä vaatimuksia henkilötietojen käsittelijän tekemästä varhaisesta ilmoituksesta, joka puolestaan tukee rekisterinpitäjän velvollisuuksia ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa.

47. Jos henkilötietojen käsittelijä toimittaa palveluja useille rekisterinpitäjille, joihin kaikkiin sama turvapoikkeama vaikuttaa, henkilötietojen käsittelijän on ilmoitettava tiedot turvapoikkeamasta jokaiselle rekisterinpitäjälle.

48. Henkilötietojen käsittelijä voi tehdä ilmoituksen rekisterinpitäjän puolesta, jos tämä on antanut henkilötietojen käsittelijälle asianmukaisen valtuutuksen ja tämä sisältyy rekisterinpitäjän ja henkilötietojen käsittelijän välisiin sopimusjärjestelyihin. Tällainen ilmoitus on tehtävä yleisen tietosuoja-asetuksen 33 ja 34 artiklan mukaisesti. On kuitenkin tärkeää muistaa, että oikeudellinen vastuu ilmoittamisesta säilyy rekisterinpitäjällä.

B. Tietojen toimittaminen valvontaviranomaiselle

1. Toimitettavat tiedot

49. Kun rekisterinpitäjä ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle, sen olisi yleisen tietosuoja-asetuksen 33 artiklan 3 kohdan mukaan vähintään

”a) kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;

(b) *ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;*

(c) *kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;*

(d) *kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.*”

50. Yleisessä tietosuoja-asetuksessa ei määritellä rekisteröityjen tai henkilötietotyyppien ryhmiä. Tietosuojaneuvosto ehdottaa kuitenkin, että rekisteröityjen ryhmillä viitataan eri tyyppisiin henkilöihin, joiden henkilötietoihin tietoturvaloukkaus on vaikuttanut: käytetyistä kuvaajista riippuen näitä voivat olla muun muassa lapset ja muut haavoittuvassa asemassa olevat ryhmät, vammaiset, työntekijät tai asiakkaat. Vastaavasti henkilötietotyyppien ryhmät voivat viitata rekisterinpitäjän hallussa mahdollisesti oleviin eri tyyppisiin tietoihin, kuten terveystietoihin, koulutustietoihin, sosiaalihuoltotietoihin, taloudellisiin tietoihin, pankkitilien numeroihin, passinumeroihin yms.

51. Yleisen tietosuoja-asetuksen johdanto-osan 85 kappaleessa todetaan selvästi, että ilmoittamisen yhtenä tarkoituksena on rajoittaa henkilöille aiheutuvia vahinkoja. Näin ollen jos rekisteröidyt tai henkilötiedot ovat sen tyyppisiä, että tietoturvaloukkauksen seurauksena voi olla riski tietyn vahingon aiheutumisesta (esimerkiksi identiteettivarkaus, petos, taloudelliset menetykset, salassapitovelvollisuuden vaarantuminen), on tärkeää, että ilmoituksessa mainitaan nämä ryhmät. Tällä tavoin ilmoitus kytkeytyy tietoturvaloukkauksen todennäköisen seurausten kuvaamista koskevaan vaatimukseen.

52. Sen, että tarkkoja tietoja (esimerkiksi tietoturvaloukkauksen kohteeksi joutuneiden rekisteröityjen tarkkaa määrää) ei ole saatavilla, ei pitäisi estää oikea-aikaista ilmoittamista. Yleisessä tietosuoja-asetuksessa sallitaan asianomaisten rekisteröityjen sekä henkilötietotyyppien arvioitujen lukumäärien käyttäminen. Painopiste olisi suunnattava tietoturvaloukkauksen haittavaikutusten torjumiseen pikemmin kuin tarkkojen lukujen toimittamiseen.

53. Näin ollen, kun on käynyt selväksi, että tietoturvaloukkaus on tapahtunut, mutta sen laajuus ei ole vielä tiedossa, vaiheittain tehtävä ilmoitus (ks. jäljempänä) on varma tapa täyttää ilmoittamisvelvollisuudet.

54. Yleisen tietosuoja-asetuksen 33 artiklan 3 kohdassa todetaan, että rekisterinpitäjän on toimitettava ilmoituksessa ”vähintään” nämä tiedot, joten rekisterinpitäjä voi tarvittaessa päättää toimittaa myös muita tietoja. Eri tyyppiset (luottamuksellisuuteen, eheyteen tai käytettävyyteen vaikuttavat) tietoturvaloukkaukset saattavat edellyttää lisätietojen toimittamista, jotta kunkin tapauksen olosuhteet selitetään kattavasti.

Esimerkki

Rekisterinpitäjä voi katsoa hyödylliseksi nimetä valvontaviranomaiselle tehtävässä ilmoituksessa henkilötietojen käsittelijänsä, jos se on tietoturvaloukkauksen perimmäinen aiheuttaja ja varsinkin jos se on aiheuttanut turvapoikkeaman, joka vaikuttaa monien muiden samaa henkilötietojen käsittelijää käyttävien rekisterinpitäjien henkilötietotyyppeihin.

55. Valvontaviranomainen voi joka tapauksessa pyytää lisätietoja osana tietoturvaloukkausta koskevaa tutkintaansa.

2. Vaiheittain tapahtuva ilmoittaminen

56. Tietoturvaloukkauksen luonteesta riippuen rekisterinpitäjän saattaa olla tarpeen suorittaa lisätutkimuksia kaikkien turvapoikkeamaan liittyvien merkityksellisten seikkojen selvittämiseksi. Tästä syystä yleisen tietosuoja-asetuksen 33 artiklan 4 kohdassa säädetään seuraavaa:

”*Jos ja siltä osin kuin tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä.*”

57. Yleisessä tietosuoja-asetuksessa tunnustetaan näin, että rekisterinpitäjät eivät aina saa kaikkia tarvittavia tietoja tietoturvaloukkauksesta 72 tunnin kuluessa sen ilmitulosta, sillä täydellisiä ja kattavia tietoja turvapoikkeamasta ei ehkä aina ole saatavilla tässä alkuvaiheessa. Näin ollen siinä sallitaan vaiheittain tapahtuva ilmoittaminen. Tätä sovelletaan todennäköisemmin monimutkaisemmissa tietoturvaloukkauksissa, kuten tietyntyyppisissä kyberturvallisuuspoikkeamissa, jotka saattavat edellyttää esimerkiksi perusteellista digitaalista rikosteknistä tutkimusta, jotta voidaan määrittää

kattavasti tietoturvaloukkauksen luonne ja se, missä määrin henkilötiedot ovat vaarantuneet. Tästä seuraa, että rekisterinpitäjän on monissa tapauksissa suoritettava lisätutkimuksia ja toimitettava täydentäviä tietoja myöhemmin. Tämä on sallittua, mikäli rekisterinpitäjä toimittaa viivästyksestä perustellun selityksen yleisen tietosuoja-asetuksen 33 artiklan 1 kohdan mukaisesti. Tietosuojaneuvosto suosittaa, että kun rekisterinpitäjä ensimmäisen kerran ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle, sen olisi myös ilmoitettava, jos sillä ei vielä ole kaikkia vaadittavia tietoja ja se aikoo toimittaa lisätietoja myöhemmin. Valvontaviranomaisen kanssa olisi sovittava, miten ja milloin lisätiedot toimitetaan. Tämä ei estä rekisterinpitäjää toimittamasta lisätietoja missä tahansa muussa vaiheessa, jos tietoturvaloukkauksesta tulee ilmi muita merkityksellisiä tietoja, jotka on toimitettava valvontaviranomaiselle.

58. Ilmoittamisvaatimuksen painopisteenä on rekisterinpitäjien kannustaminen reagoimaan nopeasti tietoturvaloukkaukseen, estämään sen leviäminen ja, mikäli mahdollista, palauttamaan vaarantuneet henkilötiedot sekä asiaa koskevien neuvojen pyytäminen valvontaviranomaiselta. Ilmoittamalla valvontaviranomaiselle ensimmäisten 72 tunnin aikana rekisterinpitäjä voi varmistaa, että henkilöille ilmoittamisesta tai ilmoittamatta jättämisestä tehtävät päätökset ovat oikeita.

59. Valvontaviranomaiselle ilmoittamisen tarkoituksena ei kuitenkaan ole ainoastaan ohjeiden saaminen siitä, ilmoitetaanko tietoturvaloukkauksesta sen kohteena oleville henkilöille. Joissain tapauksissa on ilmeistä, että tietoturvaloukkauksen luonteen ja riskin vakavuuden vuoksi rekisterinpitäjän on ilmoitettava siitä asianomaisille henkilöille viipymättä. Jos esimerkiksi on olemassa identiteettivarkauden välitön vaara tai jos tiettyjä henkilötietojen ryhmiä[29] paljastetaan verkossa, rekisterinpitäjän olisi toimittava ilman aiheetonta viivästystä tietoturvaloukkauksen rajoittamiseksi ja ilmoitettava siitä asianomaisille henkilöille (ks. osio III). Poikkeuksellisissa tilanteissa tämä voidaan tehdä jopa ennen valvontaviranomaiselle ilmoittamista. Valvontaviranomaiselle ilmoittaminen ei voi olla peruste jättää ilmoittamatta tietoturvaloukkauksesta rekisteröidylle tapauksissa, joissa tätä edellytetään.

60. Olisi myös oltava selvää, että ensimmäisen ilmoituksen jälkeen rekisterinpitäjä voi päivittää sitä valvontaviranomaiselle, jos jatkotutkimuksessa paljastuu näyttöä siitä, että turvapoikkeama torjuttiin eikä tietoturvaloukkausta itse asiassa tapahtunut. Nämä tiedot voidaan sitten lisätä valvontaviranomaiselle jo annettuihin tietoihin, ja turvapoikkeama voidaan rekisteröidä niiden mukaisesti muuna kuin tietoturvaloukkauksena. Sellaisen turvapoikkeaman raportoinnista, joka lopulta ei olekaan tietoturvaloukkaus, ei seuraa mitään rangaistusta.

Esimerkki

Rekisterinpitäjä ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa tietoturvaloukkauksen havaitsemisesta, että se on kadottanut USB-muistitikun, joka sisältää kopion joidenkin sen asiakkaiden henkilötiedoista. USB-muistitikku löydetään myöhemmin rekisterinpitäjän tiloista ja se palautetaan oikeaan paikkaan. Rekisterinpitäjä ilmoittaa tästä valvontaviranomaiselle ja pyytää ilmoituksen muuttamista.

61. On syytä huomauttaa, että vaiheittainen lähestymistapa ilmoittamiseen on jo olemassa direktiivin 2002/58/EY ja asetuksen (EU) N:o 611/2013 voimassa olevien vaatimusten ja muiden omatoimisesti ilmoitettavien turvapoikkeamien puitteissa.

3. Ilmoittamisen viivästyminen

62. Yleisen tietosuoja-asetuksen 33 artiklan 1 kohdassa todetaan selvästi, että jos ilmoitusta ei anneta valvontaviranomaiselle 72 tunnin kuluessa, rekisterinpitäjän on toimitettava tästä perusteltu selitys. Tällä sekä vaiheittaisen ilmoittamisen mallilla otetaan huomioon, että rekisterinpitäjä ei välttämättä

[29] Ks. yleisen tietosuoja-asetuksen 9 artikla.

aina pysty ilmoittamaan tietoturvaloukkauksesta tämän ajan kuluessa ja että ilmoittaminen myöhemmin saattaa olla hyväksyttävää.

63. Tällainen tilanne saattaa syntyä esimerkiksi silloin, kun rekisterinpitäjälle tapahtuu lyhyessä ajassa useita samanlaisia luottamuksellisuuteen vaikuttavia tietoturvaloukkauksia, jotka vaikuttavat suureen määrään rekisteröityjä samalla tavoin. Tietoturvaloukkaus saattaa tulla rekisterinpitäjän tietoon, ja aloittaessaan tutkintansa rekisterinpitäjä havaitsee ennen ilmoittamista muita samanlaisia tietoturvaloukkauksia, joilla on eri syyt. Olosuhteista riippuen saattaa kestää jonkin aikaa, ennen kuin rekisterinpitäjä on selvittänyt tietoturvaloukkausten laajuuden, ja sen sijaan, että se ilmoittaisi kustakin tietoturvaloukkauksesta erikseen, se laatii mielekkään ilmoituksen, joka koskee useita hyvin samanlaisia tietoturvaloukkauksia, jotka johtuvat mahdollisesti eri syistä. Tämä saattaa aiheuttaa sen, että ilmoittaminen valvontaviranomaiselle kestää yli 72 tuntia siitä, kun nämä tietoturvaloukkaukset tulevat ensimmäisen kerran rekisterinpitäjän tietoon.

64. Tiukasti ottaen jokainen yksittäinen tietoturvaloukkaus on turvapoikkeama, josta on ilmoitettava. Välttääkseen liiallisen vaivalloisuuden rekisterinpitäjä voi kuitenkin toimittaa ”niputetun” ilmoituksen kaikista näistä tietoturvaloukkauksista, mikäli ne koskevat saman tyyppisiä henkilötietoja, joita on loukattu samalla tavoin suhteellisen lyhyen ajan kuluessa. Jos tapahtuu useita tietoturvaloukkauksia, jotka koskevat eri tyyppisiä henkilötietoja, joita on loukattu eri tavoin, ilmoittaminen olisi tehtävä tavalliseen tapaan ja kustakin tietoturvaloukkauksesta olisi ilmoitettava 33 artiklan mukaisesti.

65. Vaikka yleisessä tietosuoja-asetuksessa sallitaan jonkinasteinen ilmoittamisen viivästyminen, tätä ei tulisi tapahtua säännöllisesti. On syytä huomauttaa, että niputettuja ilmoituksia voidaan tehdä myös sellaisista samanlaisista tietoturvaloukkauksista, joista ilmoitetaan 72 tunnin kuluessa.

C. Rajatylittävät tietoturvaloukkaukset ja EU:n ulkopuolisissa toimipaikoissa tapahtuvat tietoturvaloukkaukset

1. Rajatylittävät tietoturvaloukkaukset

66. Jos henkilötietojen käsitelly on rajatylittävää[30], tietoturvaloukkaus saattaa vaikuttaa rekisteröityihin useammassa kuin yhdessä jäsenvaltiossa. Yleisen tietosuoja-asetuksen 33 artiklan 1 kohdassa todetaan selvästi, että jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä toimivaltaiselle valvontaviranomaiselle 55 artiklan mukaisesti [31] . Yleisen tietosuoja-asetuksen 55 artiklan 1 kohdassa todetaan seuraavaa:

> ”*Jokaisella valvontaviranomaisella on sille tämän asetuksen mukaisesti annettujen tehtävien hoitoa ja valtuuksien käyttöä koskeva toimivalta oman jäsenvaltionsa alueella.*”

67. Yleisen tietosuoja-asetuksen 56 artiklan 1 kohdassa todetaan kuitenkin seuraavaa:

> ”*Rekisterinpitäjän tai henkilötietojen käsittelijän päätoimipaikan tai ainoan toimipaikan valvontaviranomaisella on toimivalta toimia johtavana valvontaviranomaisena kyseisen rekisterinpitäjän tai henkilötietojen käsittelijän toteuttaman rajatylittävän käsittelyn osalta 60 artiklassa säädetyn menettelyn mukaisesti, sanotun kuitenkaan rajoittamatta 55 artiklan soveltamista.*”

68. Lisäksi yleisen tietosuoja-asetuksen 56 artiklan 6 kohdassa todetaan seuraavaa:

> ”*Johtava valvontaviranomainen on rekisterinpitäjän tai henkilötietojen käsittelijän ainoa yhteystaho kyseisen rekisterinpitäjän tai henkilötietojen käsittelijän toteuttaman rajatylittävän käsittelyn osalta.*”

[30] Ks. yleisen tietosuoja-asetuksen 4 artiklan 23 kohta.

[31] Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 122 kappale.

69. Tämä tarkoittaa, että jos tietoturvaloukkaus tapahtuu rajatylittävän käsittelyn yhteydessä ja siitä on ilmoitettava, rekisterinpitäjän on ilmoitettava siitä johtavalle valvontaviranomaiselle[32]. Laatiessaan tietoturvaloukkauksia koskevaa valmiussuunnitelmaansa rekisterinpitäjän on tästä syystä arvioitava, mikä valvontaviranomainen on johtava valvontaviranomainen, jolle sen on ilmoitettava tietoturvaloukkauksista [33] . Näin toimiessaan rekisterinpitäjä voi reagoida nopeasti tietoturvaloukkaukseen ja täyttää 33 artiklan mukaiset velvoitteensa. Pitäisi olla selvää, että mikäli tietoturvaloukkaus liittyy rajatylittävään käsittelyyn, ilmoitus on tehtävä johtavalle valvontaviranomaiselle, joka ei välttämättä ole sen paikan valvontaviranomainen, jossa asianomaiset rekisteröidyt ovat tai jossa tietoturvaloukkaus on tapahtunut. Ilmoittaessaan tietoturvaloukkauksesta johtavalle valvontaviranomaiselle rekisterinpitäjän olisi ilmoitettava soveltuvin osin, koskeeko tietoturvaloukkaus muissa jäsenvaltioissa sijaitsevia toimipaikkoja ja missä jäsenvaltioissa tietoturvaloukkaus on todennäköisesti vaikuttanut rekisteröityihin. Jos rekisterinpitäjällä on epäselvyyttä siitä, mikä viranomainen on johtava valvontaviranomainen, sen olisi ilmoitettava ainakin sen paikan paikalliselle valvontaviranomaiselle, jossa tietoturvaloukkaus on tapahtunut.

2. EU:n ulkopuolisissa toimipaikoissa tapahtuvat tietoturvaloukkaukset

70. Yleisen tietosuoja-asetuksen 3 artikla koskee asetuksen maantieteellistä soveltamisalaa, mukaan lukien asetuksen soveltaminen sellaisen rekisterinpitäjän tai henkilötietojen käsittelijän suorittamaan henkilötietojen käsittelyyn, joka ei ole sijoittautunut unioniin. Yleisen tietosuoja-asetuksen 3 artiklan 2 kohdassa säädetään seuraavaa[34]:

> ”*Tätä asetusta sovelletaan unionissa olevia rekisteröityjä koskevien henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä tai henkilötietojen käsittelijä ei ole sijoittautunut unioniin, jos käsittely liittyy*
>
> (a) *tavaroiden tai palvelujen tarjoamiseen näille rekisteröidyille unionissa riippumatta siitä, edellytetäänkö rekisteröidyltä maksua; tai*
>
> (b) *näiden rekisteröityjen käyttäytymisen seurantaan siltä osin kuin heidän käyttäytymisensä tapahtuu unionissa.*”

71. Myös 3 artiklan 3 kohta on merkityksellinen, ja siinä säädetään seuraavaa[35]:

> ”*Tätä asetusta sovelletaan henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä ei ole sijoittautunut unioniin vaan toimii paikassa, jossa sovelletaan jonkin jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla.*”

72. Jos rekisterinpitäjään, joka ei ole sijoittautunut unioniin, sovelletaan yleisen tietosuoja-asetuksen 3 artiklan 2 tai 3 kohtaa ja siihen kohdistuu tietoturvaloukkaus, yleisen tietosuoja-asetuksen 33 ja 34 artiklan mukaiset ilmoittamisvelvoitteet sitovat sitä. Yleisen tietosuoja-asetuksen 27 artiklassa edellytetään, että sovellettaessa yleisen tietosuoja-asetuksen 3 artiklan 2 kohtaa rekisterinpitäjä (ja henkilötietojen käsittelijä) nimittää edustajan unionin aluetta varten.

73. Pelkkä edustajan läsnäolo jäsenvaltiossa ei kuitenkaan käynnistä yhden luukun järjestelmää.[36] Tästä syystä tietoturvaloukkauksesta on ilmoitettava jokaiselle valvontaviranomaiselle, jonka alueella

---

[32] Ks. tietosuojatyöryhmän ohjeet rekisterinpitäjän tai henkilötietojen käsittelijän johtavan valvontaviranomaisen määrittämiseen, saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=44102

[33] Kaikkien kansallisten tietosuojaviranomaisten yhteystiedot ovat saatavilla verkko-osoitteessa https://edpb.europa.eu/about-edpb/about-edpb/members_fi

[34] Ks. myös johdanto-osan 23 ja 24 kappale.

[35] Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 25 kappale.

[36] Ks. tietosuojatyöryhmän ohjeet rekisterinpitäjän tai henkilötietojen käsittelijän johtavan valvontaviranomaisen määrittämiseen, saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=44102

tietoturvaloukkauksen kohteena olevat rekisteröidyt asuvat. Ilmoittaminen on rekisterinpitäjän vastuulla.[37]

74. Vastaavasti jos henkilötietojen käsittelijään sovelletaan yleisen tietosuoja-asetuksen 3 artiklan 2 kohtaa, sitä sitovat henkilötietojen käsittelijöille asetetut velvoitteet, joista tässä yhteydessä erityisen merkittävä on yleisen tietosuoja-asetuksen 33 artiklan 2 kohdassa säädetty velvollisuus ilmoittaa tietoturvaloukkauksesta rekisterinpitäjälle.

D. Tilanteet, joissa ilmoittamista ei edellytetä

75. Yleisen tietosuoja-asetuksen 33 artiklan 1 kohdassa todetaan selvästi, että tietoturvaloukkaukset, joista ”ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä”, eivät edellytä ilmoittamista valvontaviranomaiselle. Esimerkki tästä voisi olla tapaus, jossa henkilötiedot ovat jo yleisesti saatavilla eikä niiden luovuttaminen aiheuta todennäköistä riskiä henkilöille. Tämä on ristiriidassa yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajiin sovellettavien voimassa olevien tietoturvaloukkausten ilmoittamista koskevien vaatimusten kanssa, joista säädetään direktiivissä 2009/136/EY ja joiden mukaan kaikki merkitykselliset tietoturvaloukkaukset on ilmoitettava toimivaltaiselle viranomaiselle.

76. Lausunnossaan 3/2014 henkilötietojen tietoturvaloukkauksen ilmoittamisesta[38] tietosuojatyöryhmä totesi, että henkilötietojen luottamuksellisuuden vaarantava tietoturvaloukkaus on henkilötietojen tietoturvaloukkaus, vaikka tiedot olisi suojattu uusimman tekniikan mukaisella algoritmilla, ja se on ilmoitettava. Jos salauksessa käytetyn avaimen luottamuksellisuus ei kuitenkaan ole vaarantunut – toisin sanoen avain ei ole vaarantunut missään tietoturvaloukkauksessa ja se on muodostettu siten, etteivät henkilöt, joilla ei ole lupa käyttää avainta, voi saada sitä selville käytettävissä olevan teknologian avulla – tiedot ovat periaatteessa sellaisessa muodossa, etteivät ne ole ymmärrettävissä. Tällöin tietoturvaloukkaus ei todennäköisesti vaikuta rekisteröityihin haitallisesti, eikä siitä siksi tarvitse ilmoittaa näille[39]. Vaikka tiedot olisi salattu, niiden katoaminen tai muuttaminen voi aiheuttaa rekisteröidyille kielteisiä seurauksia, jos rekisterinpitäjällä ei ole riittäviä varmuuskopioita. Tällaisessa tapauksessa rekisteröidyille olisi ilmoitettava, vaikka tiedot olisi suojattu asianmukaisella salauksella.

77. Tietosuojatyöryhmä totesi lisäksi, että näin on myös silloin, kun henkilötiedot, kuten salasanat, on suojattu turvallisesti tiivistyksen ja suolaamisen avulla, tiivistearvo on laskettu uusimman tekniikan mukaista kryptografista avaimellista tiivistefunktiota käyttäen, tietojen tiivistämiseen käytetty avain ei ole vaarantunut missään tietoturvaloukkauksessa ja tietojen tiivistämiseen käytetty avain on muodostettu siten, etteivät henkilöt, joilla ei ole lupa käyttää avainta, voi saada sitä selville käytettävissä olevan teknologian avulla.

78. Jos henkilötiedot on oleellisilta osin muutettu sellaiseen muotoon, että ne eivät ole sivullisten ymmärrettävissä tai jos ne ovat kopio tai niistä on olemassa varmuuskopio, luottamuksellisuuteen vaikuttavasta tietoturvaloukkauksesta, johon liittyy asianmukaisesti salattuja henkilötietoja, ei näin ollen välttämättä tarvitse ilmoittaa valvontaviranomaiselle. Tämä johtuu siitä, että tällainen tietoturvaloukkaus ei todennäköisesti aiheuta henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Tämä tarkoittaa luonnollisesti sitä, ettei myöskään henkilöille tarvitse ilmoittaa, koska riski ei

[37] Tietosuojaneuvosto katsoo yleisen tietosuoja-asetuksen alueellista soveltamisalaa (3 artikla) koskevien suuntaviivojen 3/2018 mukaisesti (saatavilla osoitteessa https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_fi), että unionissa olevan edustajan tehtävä ei ole yhteensopiva ulkoisen tietosuojavastaavan tehtävän kanssa, joten ilmoittaminen valvontaviranomaiselle henkilötietojen tietoturvaloukkauksesta on edelleen rekisterinpitäjän tehtävä yleisen tietosuoja-asetuksen 27 artiklan 5 kohdan mukaisesti. Edustaja voi kuitenkin olla mukana ilmoittamisprosessissa, jos siitä on nimenomaisesti määrätty kirjallisessa toimeksiannossa.

[38] Tietosuojatyöryhmä, lausunto 3/2014 tietoturvaloukkauksen ilmoittamisesta http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_fi.pdf

[39] Ks. myös asetuksen (EU) N:o 611/2013 4 artiklan 1 ja 2 kohta.

todennäköisesti ole korkea. Olisi kuitenkin muistettava, että vaikka ilmoittamista ei ehkä alkuvaiheessa edellytetä, mikäli henkilöiden oikeuksiin ja vapauksiin ei todennäköisesti kohdistu riskiä, tämä saattaa muuttua ajan myötä, jolloin riski olisi arvioitava uudelleen. Jos esimerkiksi salausavaimen havaitaan myöhemmin vaarantuneen tai salausohjelmassa paljastuu heikkous, ilmoitus saatetaan kuitenkin vaatia.

79. Lisäksi on syytä huomauttaa, että jos tietoturvaloukkauksen kohteena olleista salatuista henkilötiedoista ei ole varmuuskopioita, tietoturvaloukkaus vaikuttaa käytettävyyteen, mikä saattaa aiheuttaa riskejä henkilöille ja siten edellyttää ilmoittamista. Vastaavasti jos tietoturvaloukkaukseen liittyy salattujen tietojen häviämistä, siitä täytyy ehkä ilmoittaa, vaikka henkilötiedoista olisi olemassa varmuuskopio. Tämä riippuu siitä, kuinka kauan tietojen palauttaminen varmuuskopiosta kestää ja miten tämä käytettävyyden puute vaikuttaa henkilöihin. Kuten yleisen tietosuoja-asetuksen 32 artiklan 1 kohdan c alakohdassa todetaan, ”*kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa*” on merkittävä turvallisuustekijä.

Esimerkki

Tietoturvaloukkaus, joka ei edellytä ilmoittamista valvontaviranomaiselle, on esimerkiksi rekisterinpitäjän ja sen työntekijöiden käyttämän, turvallisesti salatun mobiililaitteen katoaminen. Mikäli salausavain säilyy varmasti rekisterinpitäjän hallussa eikä kyse ole henkilötietojen ainoasta kopiosta, hyökkäyksen tekijä ei pääse käsiksi henkilötietoihin. Tämä tarkoittaa, että tietoturvaloukkaus ei todennäköisesti aiheuta kyseisten rekisteröityjen oikeuksiin ja vapauksiin kohdistuvaa riskiä. Jos myöhemmin käy ilmi, että salausavain on vaarantunut tai salausohjelmassa tai -algoritmissa on heikkouksia, rekisteröityjen oikeuksiin ja vapauksiin kohdistuva riski muuttuu ja ilmoittaminen saattaa näin ollen olla tarpeen.

80. Jos rekisterinpitäjä ei tee ilmoitusta valvontaviranomaiselle tilanteessa, jossa tietoja ei tosiasiallisesti ole salattu turvallisesti, tämä merkitsee yleisen tietosuoja-asetuksen 33 artiklan noudattamatta jättämistä. Tästä syystä rekisterinpitäjien olisi salausohjelmistoja valitessaan punnittava huolellisesti tarjotun salauksen laatua ja asianmukaista toteuttamista sekä ymmärrettävä sen antaman suojan taso ja asianmukaisuus suhteessa riskeihin. Rekisterinpitäjien olisi myös tunnettava tarkasti salaustuotteensa toiminta. Laite saattaa esimerkiksi olla salattu, kun siitä on sammutettu virta, mutta valmiustilassa salaamaton. Joissain salausta käyttävissä tuotteissa on ”oletusarvoisia salausavaimia”, jotka kunkin asiakkaan on muutettava, jotta ne olisivat tehokkaita. Turvallisuusasiantuntijat saattavat myös pitää salausta tällä hetkellä riittävänä, mutta se voi vanhentua muutamassa vuodessa, mikä tarkoittaa, että on kyseenalaista, salaako kyseinen tuote tiedot riittävästi ja antaako se riittävän suojan tason.

III 34 ARTIKLA – ILMOITTAMINEN REKISTERÖIDYLLE

A. Ilmoittaminen yksittäisille henkilöille

81. Tietyissä tapauksissa rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta valvontaviranomaisen lisäksi myös henkilöille, joihin tietoturvaloukkaus kohdistuu.

Yleisen tietosuoja-asetuksen 34 artiklan 1 kohdassa säädetään seuraavaa:

”*Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.*”

82. Rekisterinpitäjien olisi muistettava, että ilmoittaminen valvontaviranomaiselle on pakollista, paitsi jos on epätodennäköistä, että tietoturvaloukkaus aiheuttaa henkilöiden oikeuksiin ja vapauksiin kohdistuvan riskin. Lisäksi jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin henkilöiden

oikeuksille ja vapauksille, myös näille henkilöille on ilmoitettava tietoturvaloukkauksesta. Näin ollen kynnys ilmoittaa tietoturvaloukkauksesta henkilöille on korkeampi kuin kynnys ilmoittaa valvontaviranomaiselle, eikä kaikista tietoturvaloukkauksista edellytetä ilmoitusta henkilöille, mikä suojelee heitä tarpeettomien ilmoitusten aiheuttamalta väsymykseltä.

83. Yleisen tietosuoja-asetuksen mukaan tietoturvaloukkauksesta olisi ilmoitettava henkilöille ”ilman aiheetonta viivästystä” eli mahdollisimman pian. Henkilöille ilmoittamisen päätavoitteena on antaa konkreettisia tietoja toimista, joita heidän olisi toteuttava suojellakseen itseään[40]. Kuten edellä todettiin, nopealla ilmoittamisella autetaan – tietoturvaloukkauksen luonteesta ja sen aiheuttamasta riskistä riippuen – henkilöitä toteuttamaan toimia suojellakseen itseään sen mahdollisilta kielteisiltä seurauksilta.

84. Näiden suuntaviivojen liitteessä B on ohjeellinen luettelo esimerkkitapauksista, joissa tietoturvaloukkaus todennäköisesti aiheuttaa henkilöille korkean riskin ja rekisterinpitäjän täytyy ilmoittaa siitä henkilöille, joihin tietoturvaloukkaus kohdistuu.

B. Toimitettavat tiedot

85. Henkilöille tehtävän ilmoituksen suhteen yleisen tietosuoja-asetuksen 34 artiklan 2 kohdassa säädetään seuraavaa:

> ”*Tämän artiklan 1 kohdassa tarkoitetussa rekisteröidylle annettavassa ilmoituksessa on kuvattava selkeällä ja yksinkertaisella kielellä henkilötietojen tietoturvaloukkauksen luonne ja annettava ainakin 33 artiklan 3 kohdan b, c ja d alakohdassa tarkoitetut tiedot ja toimenpiteet.*”

86. Tämän säännöksen mukaan rekisterinpitäjän on annettava vähintään seuraavat tiedot:

- kuvaus toimenpiteen luonteesta;
- tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste;
- kuvaus tietoturvaloukkauksen todennäköisistä seurauksista; ja
- kuvaus toimenpiteistä, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteistä mahdollisten haittavaikutusten lieventämiseksi.

87. Esimerkkinä toimenpiteistä, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut tietoturvaloukkauksen johdosta, se voi todeta ilmoittaneensa tietoturvaloukkauksesta valvontaviranomaiselle ja saaneensa tämän jälkeen neuvoja tietoturvaloukkauksen hoitamisesta ja sen vaikutusten vähentämisestä. Rekisterinpitäjän olisi myös tarvittaessa annettava henkilöille konkreettisia neuvoja, jotta nämä voivat suojautua tietoturvaloukkauksen mahdollisilta haittavaikutuksilta esimerkiksi vaihtamalla salasanan tapauksissa, joissa heidän kirjautumistietonsa ovat vaarantuneet. Tässäkin yhteydessä rekisterinpitäjä voi päättää toimittaa muita tietoja tässä edellytettyjen tietojen lisäksi.

C. Yhteydenotto henkilöihin

88. Periaatteessa tietoturvaloukkauksesta olisi ilmoitettava sen kohteena oleville rekisteröidyille välittömästi, ellei tästä ole kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla (yleisen tietosuoja-asetuksen 34 artiklan 3 kohdan c alakohta).

89. Kun tietoturvaloukkauksesta ilmoitetaan rekisteröidyille, tulisi lähettää nimenomaisesti tätä koskeva viesti, jota ei tule lähettää yhdessä muiden tietojen, kuten säännöllisten päivitysten, uutiskirjeiden tai

[40] Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 86 kappale.

vakiomuotoisten viestien, kanssa. Näin toimien ilmoitus tietoturvaloukkauksesta on selkeä ja läpinäkyvä.

90. Esimerkkejä läpinäkyvistä ilmoitusmenetelmistä ovat muun muassa viestit suoraan henkilöille (esimerkiksi sähköposti, tekstiviesti, pikaviesti), näkyvät palkit tai ilmoitukset verkkosivustoilla, postitetut ilmoitukset ja näkyvät ilmoitukset painetussa mediassa. Pelkästään lehdistötiedotteessa tai yrityksen blogissa annettava ilmoitus ei ole tehokas keino ilmoittaa tietoturvaloukkauksesta yksittäiselle henkilöille. Tietosuojaneuvosto suosittaa, että rekisterinpitäjät valitsevat välineen, jolla mahdollisuus saada tieto kaikille asianomaisille henkilöille on mahdollisimman suuri. Tämä saattaa olosuhteista riippuen edellyttää, että rekisterinpitäjä käyttää useita viestintämenetelmiä eikä vain yhtä kanavaa.

91. Rekisterinpitäjien on ehkä myös varmistettava, että ilmoitus on saatavilla sopivissa vaihtoehtoisissa muodoissa ja tarvittavilla kielillä, jotta henkilöt voivat varmasti ymmärtää saamansa tiedot. Esimerkiksi ilmoitettaessa tietoturvaloukkauksesta yksittäiselle henkilölle on aiemmassa tavanomaisessa viestinnässä vastaanottajan kanssa käytetty kieli yleensä asianmukainen. Jos tietoturvaloukkaus kuitenkin vaikuttaa rekisteröityihin, joiden kanssa rekisterinpitäjä ei aikaisemmin ole ollut tekemisissä, tai erityisesti sellaisiin rekisteröityihin, jotka asuvat toisessa jäsenvaltiossa tai muussa EU:n ulkopuolisessa maassa kuin siinä, johon rekisterinpitäjä on sijoittautunut, hyväksyttävä voisi olla paikallisella kielellä annettava ilmoitus vaadittavat resurssit huomioon ottaen. Keskeistä on auttaa rekisteröityjä ymmärtämään tietoturvaloukkauksen luonne ja toimenpiteet, joita he voivat toteuttaa suojatakseen itseään.

92. Rekisterinpitäjillä on parhaat edellytykset määrittää, mikä on asianmukaisin kanava ilmoittaa tietoturvaloukkauksesta yksittäisille henkilöille, varsinkin jos niiden kanssakäyminen asiakkaidensa kanssa on tiivistä. Rekisterinpitäjän on kuitenkin luonnollisesti varottava käyttämästä tietoturvaloukkauksen vaarantamaa yhteyskanavaa, sillä sitä voivat käyttää myös rekisterinpitäjäksi tekeytyvät hyökkäyksen tekijät.

93. Yleisen tietosuoja-asetuksen johdanto-osan 86 kappaleessa asiasta todetaan seuraavaa:

> ”*Tällainen ilmoitus rekisteröidylle olisi tehtävä niin pian kuin se on kohtuudella mahdollista ja tiiviissä yhteistyössä valvontaviranomaisen kanssa noudattaen valvontaviranomaisen tai muiden asiaankuuluvien viranomaisten (kuten lainvalvontaviranomaisten) antamia ohjeita. Esimerkiksi tarve lieventää välittömien haittojen riskiä edellyttää sitä, että rekisteröidyille ilmoitetaan viipymättä, kun taas tarve toteuttaa asianmukaiset toimenpiteet tietoturvaloukkauksen jatkumisen tai vastaavien henkilötietojen tietoturvaloukkausten estämiseksi voivat olla perusteena pidemmälle ilmoitusajalle.*”

94. Tästä syystä rekisterinpitäjät saattavat haluta kuulla valvontaviranomaista pyytääkseen neuvoja paitsi tietoturvaloukkauksen ilmoittamisesta rekisteröidyille 34 artiklan mukaisesti myös asianmukaisista henkilöille lähetettävistä viesteistä ja asianmukaisimmasta tavasta ottaa näihin yhteyttä.

95. Tähän liittyy yleisen tietosuoja-asetuksen johdanto-osan 88 kappaleessa annettu neuvo, jonka mukaan tietoturvaloukkauksesta ilmoitettaessa ”olisi myös otettava huomioon lainvalvontaviranomaisten oikeutetut edut tapauksissa, joissa varhainen ilmoittaminen voisi tarpeettomasti haitata henkilötietojen tietoturvaloukkauksen tutkintaa.” Tämä saattaa tarkoittaa sitä, että tietyissä tilanteissa, joissa tämä on perusteltua ja lainvalvontaviranomaiset näin neuvovat, rekisterinpitäjä saattaa viivyttää tietoturvaloukkauksesta ilmoittamista asianomaisille henkilöille, kunnes tämä ei vaaranna tällaista tutkintaa. Tämän jälkeen rekisteröidyille on kuitenkin ilmoitettava tietoturvaloukkauksesta nopeasti.

96. Jos rekisterinpitäjän ei ole mahdollista ilmoittaa tietoturvaloukkauksesta henkilölle, koska sillä ei ole riittävästi tietoja tämän tavoittamiseksi, rekisterinpitäjän olisi ilmoitettava kyseiselle henkilölle heti, kun se on kohtuudella mahdollista (esimerkiksi kun henkilö käyttää 15 artiklan mukaista oikeuttaan

saada tutustua henkilötietoihinsa ja toimittaa rekisterinpitäjälle tarvittavat lisätiedot yhteyden ottamiseksi).

D. Tilanteet, joissa ilmoittamista ei edellytetä

97. Yleisen tietosuoja-asetuksen 34 artiklan 3 kohdassa säädetään kolmesta ehdosta, joiden täyttyessä tietoturvaloukkauksesta ei tarvitse ilmoittaa henkilöille. Ne ovat seuraavat:

    - Rekisterinpitäjä on ennen tietoturvaloukkausta soveltanut asianmukaisia teknisiä ja organisatorisia toimenpiteitä suojatakseen henkilötiedot, erityisesti toimenpiteitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin. Tähän saattaa sisältyä esimerkiksi henkilötietojen suojaaminen uusimman tekniikan mukaisella salauksella tai tokenisoinnilla.
    - Rekisterinpitäjä on välittömästi tietoturvaloukkauksen jälkeen toteuttanut toimia varmistaakseen, että henkilöiden oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu. Rekisterinpitäjä on voinut tapauksen olosuhteista riippuen esimerkiksi välittömästi tunnistaa henkilötietoihin päässeen henkilön ja toteuttaa toimia tätä vastaan ennen kuin tämä pystyi tekemään tiedoilla mitään. On kuitenkin edelleen otettava asianmukaisesti huomioon mahdollisen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen seuraukset kyseisten tietojen luonteesta riippuen.
    - Yhteyden ottaminen henkilöihin vaatisi kohtuutonta vaivaa[41] esimerkiksi siinä tapauksessa, että heidän yhteystietonsa ovat hävinneet tietoturvaloukkauksen seurauksena tai niitä ei ole ollut alun perinkään. Esimerkki tästä on tapaus, jossa tilastotoimiston varastossa on tapahtunut vesivahinko ja henkilötietoja sisältävät asiakirjat oli tallennettu vain paperimuodossa. Tällöin rekisterinpitäjän on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla henkilöille tiedotetaan yhtä tehokkaalla tavalla. Jos ilmoittaminen vaatisi kohtuutonta vaivaa, voidaan myös harkita teknisiä järjestelyjä, joilla tiedot tietoturvaloukkauksesta asetetaan saataville pyynnöstä. Tämä saattaa olla hyödyllistä niiden henkilöiden kohdalla, joihin tietoturvaloukkaus saattaa vaikuttaa, mutta joihin rekisterinpitäjä ei muulla tavoin saa yhteyttä.

98. Osoitusvelvollisuusperiaatteen mukaisesti rekisterinpitäjien olisi pystyttävä osoittamaan valvontaviranomaiselle täyttävänsä yhden tai useamman näistä ehdoista [42]. Olisi muistettava, että vaikka ilmoittamista ei ehkä alkuvaiheessa edellytetä, mikäli luonnollisten henkilöiden oikeuksiin ja vapauksiin ei kohdistu riskiä, tämä saattaa muuttua ajan myötä ja riski olisi arvioitava uudelleen.

99. Jos rekisterinpitäjä päättää olla ilmoittamatta tietoturvaloukkauksesta yksittäisille henkilöille, valvontaviranomainen voi yleisen tietosuoja-asetuksen 34 artiklan 4 kohdan nojalla vaatia sitä tekemään sen, jos viranomainen katsoo, että tietoturvaloukkaus todennäköisesti aiheuttaa henkilöille korkean riskin. Vaihtoehtoisesti se voi katsoa, että yleisen tietosuoja-asetuksen 34 artiklan 3 kohdan ehdot täyttyvät, jolloin ilmoittamista henkilöille ei edellytetä. Jos valvontaviranomainen katsoo, että päätös olla ilmoittamatta tietoturvaloukkauksesta rekisteröidyille ei ole hyvin perusteltu, se voi harkita käytettävissään olevien valtuuksien ja seuraamuksien käyttöä.

---

[41] Ks. läpinäkyvyyttä koskevat tietosuojatyöryhmän ohjeet, joissa käsitellään kohtuuttoman vaivan käsitettä, saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[42] Ks. yleisen tietosuoja-asetuksen 5 artiklan 2 kohta.

IV RISKIN JA KORKEAN RISKIN ARVIOINTI

A. Riski ilmoittamisen käynnistäjänä

100. Vaikka yleisessä tietosuoja-asetuksessa säädetään velvollisuudesta ilmoittaa tietoturvaloukkauksesta, tätä ei vaadita kaikissa tilanteissa:

- Ilmoitus valvontaviranomaiselle on tehtävä, paitsi jos tietoturvaloukkaukseen ei todennäköisesti liity luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.
- Tietoturvaloukkauksesta on ilmoitettava henkilöille vain, jos se todennäköisesti aiheuttaa korkean riskin heidän oikeuksilleen ja vapauksilleen.

101. Tämä tarkoittaa, että rekisterinpitäjän on heti saatuaan tietoturvaloukkauksen tietoonsa erittäin tärkeää paitsi pyrkiä rajoittamaan turvapoikkeaman leviäminen myös arvioida siitä mahdollisesti aiheutuva riski. Tähän on kaksi tärkeää syytä: ensinnäkin tieto henkilöön kohdistuvan vaikutuksen todennäköisyydestä ja mahdollisesta vakavuudesta auttaa rekisterinpitäjää toteuttamaan tehokkaita toimia tietoturvaloukkauksen leviämisen estämiseksi ja sen torjumiseksi; toiseksi, tämän avulla se voi määrittää, onko tietoturvaloukkauksesta ilmoitettava valvontaviranomaiselle ja tarvittaessa asianomaisille henkilöille.

102. Kuten edellä selostettiin, tietoturvaloukkauksesta on ilmoitettava, paitsi jos se ei todennäköisesti aiheuta luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Keskeinen rekisteröidyille tehtävän ilmoituksen laukaiseva seikka on se, aiheuttaako tietoturvaloukkaus todennäköisesti *korkean* riskin henkilöiden oikeuksille ja vapauksille. Tällainen riski on olemassa, jos tietoturvaloukkaus voi aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja henkilöille, joiden tietosuojaa on loukattu. Tällaisia vahinkoja ovat esimerkiksi syrjintä, identiteettivarkaus tai petos, taloudelliset menetykset ja maineen vahingoittuminen. Jos tietoturvaloukkaukseen liittyy henkilötietoja, jotka koskevat rotua tai etnistä alkuperää, poliittisia mielipiteitä, uskonnollista tai filosofista vakaumusta tai ammattiliittoon kuulumista tai jotka sisältävät geneettisiä tietoja tai terveyttä ja seksuaalista käyttäytymistä tai rikostuomioita ja rikkomuksia tai niihin liittyviä turvatoimia koskevia tietoja, tällaisten vahinkojen aiheutumista olisi pidettävä todennäköisenä[43].

B. Riskiä arvioitaessa huomioon otettavat tekijät

103. Yleisen tietosuoja-asetuksen johdanto-osan 75 ja 76 kappaleessa todetaan, että riskiä arvioitaessa olisi yleisesti otettava huomioon sekä rekisteröityjen oikeuksille ja vapauksille aiheutuvan riskin todennäköisyys että sen vakavuus. Lisäksi niissä todetaan, että riski olisi arvioitava objektiivisen arvioinnin perusteella.

104. On syytä huomauttaa, että arvioitaessa tietoturvaloukkauksen aiheuttamaa riskiä henkilöiden oikeuksille ja vapauksille keskitytään eri asioihin kuin tietosuojaa koskevassa vaikutustenarvioinnissa[44]. Tietosuojaa koskevassa vaikutustenarvioinnissa otetaan huomioon sekä riskit, jotka aiheutuvat, kun tiedonkäsittely suoritetaan suunnitellusti, että riskit, jotka aiheutuvat tietoturvaloukkauksesta. Mahdollisen tietoturvaloukkauksen osalta siinä tarkastellaan yleisesti tietoturvaloukkauksen todennäköisyyttä ja siitä rekisteröidylle mahdollisesti aiheutuvia vahinkoja; toisin sanoen siinä arvioidaan hypoteettista tapahtumaa. Todellisen tietoturvaloukkauksen kohdalla tapahtuma on jo toteutunut, ja näin ollen painopiste on täysin siitä aiheutuvassa henkilöihin kohdistuvien vaikutusten riskissä.

---

[43] Ks. johdanto-osan 75 ja 85 kappale.

[44] Ks. tietosuojatyöryhmän ohjeet tietosuojaa koskevasta vaikutustenarvioinnista, jotka ovat saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Esimerkki

Tietosuojaa koskevan vaikutustenarvioinnin mukaan tietyn suojausohjelmiston käyttö henkilötietojen suojaamiseksi on sopiva toimenpide, jolla varmistetaan turvallisuustaso, joka on tietojenkäsittelyn muutoin henkilöille aiheuttamaan riskiin nähden asianmukainen. Jos kuitenkin myöhemmin saataisiin tietää, että ohjelmistossa on heikkous, tämä muuttaisi ohjelmiston soveltuvuutta suojeltuihin henkilötietoihin kohdistuvan riskin torjumiseen ja se olisi arvioitava uudelleen osana jatkuvaa tietosuojaa koskevaa vaikutustenarviointia. Tuotteessa olevaa heikkoutta käytetään myöhemmin hyväksi, ja tapahtuu tietoturvaloukkaus. Rekisterinpitäjän olisi arvioitava tietoturvaloukkauksen erityiset olosuhteet, tiedot, joihin se vaikuttaa, henkilöihin kohdistuvien vaikutusten mahdollinen taso sekä tämän riskin toteutumistodennäköisyys.

105. Näin ollen rekisterinpitäjän olisi tietoturvaloukkauksesta henkilöille aiheutuvaa riskiä arvioidessaan otettava huomioon tietoturvaloukkauksen erityiset olosuhteet, muun muassa mahdollisten vaikutusten vakavuus ja niiden toteutumisen todennäköisyys. Tästä syystä tietosuojaneuvosto suosittaa, että arvioinnissa olisi otettava huomioon seuraavat kriteerit[45]:

- **Tietoturvaloukkaustyypit**

106. Tapahtuneen tietoturvaloukkauksen tyyppi saattaa vaikuttaa henkilöille aiheutuvan riskin tasoon. Esimerkiksi luottamuksellisuuteen vaikuttavalla tietoturvaloukkauksella, jossa terveystietoja on luovutettu sivullisille, saattaa olla erilaisia seurauksia henkilölle kuin tietoturvaloukkauksella, jossa henkilön terveystiedot ovat kadonneet eivätkä ne enää ole käytettävissä.

- **Henkilötietojen luonne, arkaluonteisuus ja määrä**

107. Riskiä arvioitaessa keskeinen tekijä on luonnollisesti tietoturvaloukkauksessa vaarantuneiden henkilötietojen tyyppi ja arkaluonteisuus. Mitä arkaluonteisempia tiedot ovat, sitä korkeampi on yleensä asianomaisille henkilöille aiheutuvien vahinkojen riski, mutta huomioon olisi otettava myös muut henkilötiedot, joita rekisteröidystä saattaa jo olla saatavilla. Esimerkiksi henkilön nimen ja osoitteen paljastaminen ei tavanomaisissa olosuhteissa todennäköisesti aiheuta huomattavaa vahinkoa. Jos kuitenkin adoptiovanhemman nimi ja osoite luovutetaan biologiselle vanhemmalle, sekä adoptiovanhemmalle että lapselle aiheutuvat seuraukset voivat olla hyvin vakavia.

108. Terveystietoja, henkilöllisyysasiakirjoja tai luottokorttitietojen kaltaisia taloudellisia tietoja koskevat tietoturvaloukkaukset voivat aiheuttaa vahinkoa sellaisenaan, mutta yhdessä niitä voidaan käyttää identiteettivarkauteen. Henkilötietojen yhdistelmä on tavallisesti arkaluonteisempi kuin yksittäinen henkilötieto.

109. Jotkin henkilötietotyypit saattavat ensi näkemältä vaikuttaa suhteellisen harmittomilta, mutta olisi pohdittava huolellisesti, mitä tällaiset tiedot saattavat paljastaa asianomaisesta henkilöstä. Luettelo asiakkaista, joille toimitetaan tavaraa säännöllisesti, ei ehkä ole erityisen arkaluonteinen, mutta samat tiedot asiakkaista, jotka ovat keskeyttäneet toimitukset lomansa ajaksi, ovat hyödyllisiä rikollisille.

110. Vastaavasti pienellä määrällä erittäin arkaluonteisia henkilötietoja voi olla suuri vaikutus henkilöön, ja suuri määrä yksityiskohtia voi paljastaa suuremman määrän tietoa kyseisestä henkilöstä. Samoin tietoturvaloukkauksella, joka kohdistuu suureen määrään monien rekisteröityjen henkilötietoja, voi olla vaikutus suureen määrään henkilöitä.

[45] Asetuksen (EU) N:o 611/2013 3 artiklan 2 kohdassa annetaan ohjeita tekijöistä, jotka olisi otettava huomioon ilmoitettaessa tietoturvaloukkauksista sähköisten viestintäpalvelujen alalla. Niistä voi olla hyötyä yleisen tietosuoja-asetuksen mukaisen ilmoittamisen yhteydessä. Ks. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fi:PDF

- **Henkilöiden tunnistamisen helppous**

111. Tärkeä huomioon otettava tekijä on se, kuinka helppoa vaarantuneisiin henkilötietoihin pääsevän osapuolen on tunnistaa yksittäisiä henkilöitä tai yhdistellä henkilötietoja muihin tietoihin henkilöiden tunnistamiseksi. Tilanteesta riippuen tunnistaminen saattaa olla mahdollista suoraan vaarantuneista henkilötiedoista ilman erityisiä tutkimuksia henkilön henkilöllisyyden selvittämiseksi tai henkilötietojen yhdistäminen tiettyyn henkilöön saattaa olla äärimmäisen vaikeaa, mutta kuitenkin mahdollista tietyissä olosuhteissa. Tunnistaminen vaarantuneista tiedoista voi olla mahdollista suoraan tai välillisesti, mutta se voi myös riippua kontekstista, jossa tietoturvaloukkaus tapahtuu, ja tietoturvaloukkaukseen liittyvien henkilötietojen julkisesta saatavuudesta. Tällä saattaa olla enemmän merkitystä luottamuksellisuuteen ja käytettävyyteen vaikuttavien tietoturvaloukkausten kohdalla.

112. Kuten edellä todettiin, riittävän tasoisella salauksella suojatut henkilötiedot eivät ole sivullisten ymmärrettävissä ilman salausavainta. Lisäksi asianmukaisesti toteutettu pseudonymisoiminen (jolla yleisen tietosuoja-asetuksen 4 artiklan 5 kohdan mukaan tarkoitetaan ”*henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu*”) voi myös vähentää henkilöiden tunnistamisen todennäköisyyttä tietoturvaloukkauksen tapahtuessa. Ei kuitenkaan voida katsoa, että tiedot voidaan pelkästään pseudonymisoimistekniikoilla muuttaa sellaisiksi, että ne eivät ole ymmärrettävissä.

- **Henkilöille aiheutuvien seurausten vakavuus**

113. Tietoturvaloukkaukseen liittyvien henkilötietojen luonteesta riippuen henkilöille mahdollisesti aiheutuva vahinko voi olla erityisen vakava, etenkin jos tietoturvaloukkaus voi johtaa identiteettivarkauteen tai petokseen, fyysisiin vahinkoihin, ahdistukseen, nöyryytykseen tai maineen vahingoittumiseen. Jos tietoturvaloukkaus koskee haavoittuvassa asemassa olevien henkilöiden henkilötietoja, näihin henkilöihin saattaa kohdistua suurempi riski joutua kärsimään haittaa.

114. Se, onko rekisterinpitäjä tietoinen siitä, että henkilötietoja on sellaisten henkilöiden hallussa, joiden tarkoitusperät ovat tuntemattomat tai mahdollisesti pahantahtoiset, saattaa vaikuttaa mahdollisen riskin tasoon. Saattaa tapahtua luottamuksellisuuteen vaikuttava tietoturvaloukkaus, jossa henkilötietoja luovutetaan vahingossa 4 artiklan 10 kohdassa määritellylle kolmannelle osapuolelle tai muulle vastaanottajalle. Näin voi tapahtua esimerkiksi silloin, kun henkilötietoja lähetetään vahingossa organisaation väärälle osastolle tai yleisesti käytetylle tavarantoimittajaorganisaatiolle. Rekisterinpitäjä voi pyytää vastaanottajaa joko palauttamaan tai turvallisella tavalla tuhoamaan saamansa tiedot. Molemmissa tapauksissa vastaanottajaa voidaan pitää ”luotettavana”, koska rekisterinpitäjän suhde tähän on jatkuva ja rekisterinpitäjä saattaa olla tietoinen vastaanottajan menettelyistä, historiasta ja muista merkityksellisistä seikoista. Toisin sanoen rekisterinpitäjällä voi olla sen tasoinen varmuus vastaanottajasta, että se voi kohtuudella odottaa, ettei tämä osapuoli lue tai käytä erehdyksessä lähetettyjä tietoja, vaan noudattaa ohjeita palauttaa ne. Vaikka tietoihin olisi päästy, rekisterinpitäjä voi silti mahdollisesti luottaa siihen, ettei vastaanottaja toteuta tiedoilla muita toimia, vaan palauttaa tiedot rekisterinpitäjälle nopeasti ja tekee yhteistyötä niiden palauttamiseksi. Tällaisissa tapauksissa tämä voidaan ottaa huomioon riskinarvioinnissa, jonka rekisterinpitäjä tekee tietoturvaloukkauksen jälkeen. Se, että vastaanottajaan luotetaan, saattaa poistaa seurausten vakavuuden, mutta ei tarkoita sitä, ettei tietoturvaloukkausta olisi tapahtunut. Tämä puolestaan voi poistaa henkilöille aiheutuvan riskin todennäköisyyden, jolloin tietoturvaloukkauksesta ei enää tarvitse ilmoittaa valvontaviranomaiselle tai asianomaisille henkilöille. Myös tämä on tapauskohtaista. Tästä huolimatta rekisterinpitäjän on silti säilytettävä tietoturvaloukkausta koskevat tiedot osana yleistä velvollisuutta pitää rekisteriä tietoturvaloukkauksista (ks. jäljempänä osio V).

115. Myös henkilöille aiheutuvien seurausten pysyvyys olisi otettava huomioon. Vaikutuksia voidaan pitää suurempina, jos ne ovat pitkäaikaisia.

- **Henkilön erityiset ominaisuudet**

116. Tietoturvaloukkaus voi vaikuttaa henkilötietoihin, jotka koskevat lapsia tai muita haavoittuvassa asemassa olevia henkilöitä. Heihin saattaa tämän seurauksena kohdistua suurempi riski. Saattaa olla myös muita henkilöön liittyviä tekijöitä, jotka voivat vaikuttaa siihen, kuinka suuri tietoturvaloukkauksen vaikutus näihin henkilöihin on.

- **Rekisterinpitäjän erityiset ominaisuudet**

117. Rekisterinpitäjän ja sen toiminnan luonne ja rooli saattavat vaikuttaa siihen, kuinka suuri tietoturvaloukkauksesta henkilöille aiheutuva riski on. Jos esimerkiksi lääketieteellinen organisaatio käsittelee erityisiä henkilötietojen ryhmiä, tämä tarkoittaa, että henkilöihin kohdistuu heidän henkilötietojensa vaarantuessa suurempi uhka kuin jos kyseessä olisi jonkin sanomalehden postituslista.

- **Niiden henkilöiden määrä, joihin tietoturvaloukkaus vaikuttaa**

118. Tietoturvaloukkaus saattaa vaikuttaa vain yhteen tai muutamaan henkilöön tai moneen tuhanteen tai vielä useampaan henkilöön. Yleisesti voidaan todeta, että mitä useampaan henkilöön tietoturvaloukkaus vaikuttaa, sitä suurempi vaikutus sillä voi olla. Tietoturvaloukkaus voi kuitenkin vaikuttaa vakavasti vain yhteenkin henkilöön henkilötietojen luonteesta ja niiden vaarantumisen asiayhteydestä riippuen. Tässäkin yhteydessä on keskeistä ottaa huomioon kohteena oleviin henkilöihin kohdistuvan vaikutuksen todennäköisyys ja vakavuus.

- **Yleisiä seikkoja**

119. Arvioidessaan tietoturvaloukkauksesta todennäköisesti aiheutuvaa riskiä rekisterinpitäjän olisi näin ollen otettava huomioon sekä henkilöiden oikeuksiin ja vapauksiin kohdistuvien mahdollisten vaikutusten vakavuus ja niiden toteutumisen todennäköisyys. On selvää, että jos tietoturvaloukkauksen seuraukset ovat vakavammat, riski on suurempi, kuten myös silloin, jos niiden toteutumisen todennäköisyys on suurempi. Jos asia on epäselvä, rekisterinpitäjän on parempi olla liian varovainen ja ilmoittaa tietoturvaloukkauksesta. Liitteessä B esitetään joitakin hyödyllisiä esimerkkejä eri tyyppisistä tietoturvaloukkauksista, joihin liittyy korkea riski henkilöille.

120. Euroopan unionin verkko- ja tietoturvavirasto (ENISA) on laatinut tietoturvaloukkauksen vakavuuden arviointimenetelmää koskevia suosituksia, joista voi olla hyötyä rekisterinpitäjille ja henkilötietojen käsittelijöille näiden laatiessa tietoturvaloukkauksia koskevaa valmiussuunnitelmaansa[46].

V. OSOITUSVELVOLLISUUS JA REKISTERIN PITÄMINEN

A. Tietoturvaloukkausten dokumentointi

121. Riippumatta siitä, onko tietoturvaloukkauksesta ilmoitettava valvontaviranomaiselle, rekisterinpitäjän on dokumentoitava kaikki tietoturvaloukkaukset, sillä yleisen tietosuoja-asetuksen 33 artiklan 5 kohdassa todetaan seuraavaa:

> *”Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, mukaan lukien henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet. Valvontaviranomaisen on voitava tämän dokumentoinnin avulla tarkistaa, että tätä artiklaa on noudatettu.”*

[46] ENISA: Recommendations for a methodology of the assessment of severity of personal data breaches, saatavilla verkko-osoitteessahttps://www.enisa.europa.eu/publications/dbn-severity

122. Tämä liittyy yleisen tietosuoja-asetuksen 5 artiklan 2 kohtaan sisältyvään osoitusvelvollisuuden periaatteeseen. Sekä sellaisten tietoturvaloukkausten, joista ei tarvitse ilmoittaa, että ilmoitettavien tietoturvaloukkausten rekisteröinti liittyy myös yleisen tietosuoja-asetuksen 24 artiklan mukaisiin rekisterinpitäjän velvollisuuksiin, ja valvontaviranomainen voi pyytää saada nähdä nämä rekisterit. Tästä syystä rekisterinpitäjiä kannustetaan perustamaan sisäinen tietoturvaloukkausten rekisteri katsomatta siihen, onko niistä ilmoitettava vai ei[47].

123. Vaikka rekisterinpitäjä voi päättää, mitä menetelmää ja rakennetta se käyttää tietoturvaloukkausten dokumentoinnissa, kirjattavien tietojen suhteen on eräitä keskeisiä elementtejä, jotka olisi sisällytettävä tietoihin kaikissa tapauksissa. Kuten yleisen tietosuoja-asetuksen 33 artiklan 5 kohdassa edellytetään, rekisterinpitäjän on rekisteröitävä tietoturvaloukkausta koskevat tiedot, muun muassa sen syyt, mitä tapahtui ja mihin henkilötietoihin se vaikutti. Lisäksi olisi kirjattava tietoturvaloukkauksen vaikutukset ja seuraukset sekä rekisterinpitäjän toteuttamat korjaavat toimet.

124. Yleisessä tietosuoja-asetuksessa ei täsmennetä, kuinka kauan tällaista dokumentaatiota on säilytettävä. Jos tällaiset rekisterit sisältävät henkilötietoja, rekisterinpitäjän velvollisuutena on määrittää asianmukainen säilytysaika henkilötietojen käsittelyyn liittyvien periaatteiden[48] mukaisesti ja käsittelyn lainmukaisuuden täyttämiseksi[49]. Sen on säilytettävä dokumentaatio yleisen tietosuoja-asetuksen 33 artiklan 5 kohdan mukaisesti, koska sitä voidaan pyytää osoittamaan valvontaviranomaiselle, että se on noudattanut kyseistä artiklaa tai yleisemmin osoitusvelvollisuutta. On selvää, että jos itse rekisterit eivät sisällä henkilötietoja, säilyttämistä rajoittavaa yleisen tietosuoja-asetuksen periaatetta[50] ei sovelleta.

125. Tietosuojaneuvosto suosittaa, että näiden tietojen lisäksi rekisterinpitäjä dokumentoi myös tietoturvaloukkauksen torjumiseksi tehtyjen päätösten perustelut. Erityisesti jos tietoturvaloukkauksesta ei ilmoiteta, tätä koskevan päätöksen perustelut olisi dokumentoitava. Tähän olisi sisällyttävä syyt siihen, miksi rekisterinpitäjä katsoo, ettei tietoturvaloukkaus todennäköisesti aiheuta luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä[51]. Jos rekisterinpitäjä taas katsoo, että jokin yleisen tietosuoja-asetuksen 34 artiklan 3 kohdan ehdoista täyttyy, sen olisi voitava toimittaa tätä tukeva asianmukainen näyttö.

126. Jos rekisterinpitäjä ei ilmoita tietoturvaloukkauksesta valvontaviranomaiselle, vaan ilmoittaminen viivästyy, rekisterinpitäjän on voitava esittää viivästymisen syyt; tätä koskeva dokumentaatio voi auttaa osoittamaan, että ilmoittamisen viivästyminen on perusteltu eikä kohtuuton.

127. Jos rekisterinpitäjä ilmoittaa tietoturvaloukkauksesta sen kohteena olleille henkilöille, sen olisi tiedotettava tietoturvaloukkauksesta läpinäkyvästi, tehokkaasti ja nopeasti. Tällaista ilmoitusta koskevan näytön säilyttäminen voi auttaa rekisterinpitäjää todistamaan osoitusvelvollisuutensa ja säännösten noudattamisen.

128. Yleisen tietosuoja-asetuksen 33 ja 34 artiklan noudattamisen helpottamiseksi sekä rekisterinpitäjillä että henkilötietojen käsittelijöillä olisi hyvä olla käytössä dokumentoitu ilmoitusmenettely, jossa esitetään tietoturvaloukkauksen havaitsemisen jälkeen noudatettava prosessi, muun muassa se, miten turvapoikkeaman leviäminen estetään, miten sitä hallitaan ja miten tiedot palautetaan sekä miten riski arvioidaan ja tietoturvaloukkauksesta ilmoitetaan. Yleisen tietosuoja-asetuksen noudattamisen osoittamiseksi saattaa tässä suhteessa olla hyödyllistä myös

[47] Rekisterinpitäjä voi päättä dokumentoida tietoturvaloukkaukset osana yleisen tietosuoja-asetuksen 30 artiklan nojalla ylläpidettävää selostetta käsittelytoimista. Erillistä rekisteriä ei edellytetä, mikäli tietoturvaloukkausta koskevat tiedot ovat selvästi tunnistettavissa tällaisiksi tiedoiksi ja ne voidaan hakea pyynnöstä.

[48] Ks. yleisen tietosuoja-asetuksen 5 artikla.

[49] Ks. yleisen tietosuoja-asetuksen 6 artikla ja myös 9 artikla.

[50] Ks. yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohta.

[51] Ks. yleisen tietosuoja-asetuksen johdanto-osan 85 kappale.

osoittaa, että työntekijöille on tiedotettu tällaisten menettelyjen ja mekanismien olemassaolosta ja että nämä tietävät, miten tietoturvaloukkauksiin reagoidaan.

129. On syytä huomauttaa, että tietoturvaloukkauksen asianmukaisen dokumentoinnin laiminlyönti saattaa johtaa siihen, että valvontaviranomainen käyttää yleisen tietosuoja-asetuksen 58 artiklan mukaisia valtuuksiaan tai määrää hallinnollisen sakon yleisen tietosuoja-asetuksen 83 artiklan mukaisesti.

B. Tietosuojavastaavan rooli

130. Rekisterinpitäjällä tai henkilötietojen käsittelijällä voi olla tietosuojavastaava[52] joko yleisen tietosuoja-asetuksen 37 artiklan vaatimusten perusteella tai vapaaehtoisesti hyvää käytäntöä noudattaen. Yleisen tietosuoja-asetuksen 39 artiklassa säädetään useista tietosuojavastaavan pakollisista tehtävistä, mutta sillä ei estetä rekisterinpitäjää osoittamasta tietosuojavastaavalle tarvittaessa muita tehtäviä.

131. Erityisen merkittävää tietoturvaloukkauksesta ilmoittamisen kannalta on, että tietosuojavastaavan pakollisiin tehtäviin sisältyy muun muassa tietosuojaa koskevan neuvonnan ja tietojen antaminen rekisterinpitäjälle tai henkilötietojen käsittelijälle, yleisen tietosuoja-asetuksen noudattamisen valvominen sekä tietosuojaa koskevia vaikutustenarviointeja koskevien neuvojen antaminen. Tietosuojavastaavan on myös tehtävä yhteistyötä valvontaviranomaisen kanssa ja toimittava tämän ja rekisteröityjen yhteyspisteenä. On myös huomattava, että ilmoitettaessa tietoturvaloukkauksesta valvontaviranomaiselle yleisen tietosuoja-asetuksen 33 artiklan 3 kohdan b alakohdassa edellytetään, että rekisterinpitäjä ilmoittaa tietosuojavastaavan nimen ja yhteystiedot tai muun yhteyspisteen.

132. Tietoturvaloukkausten dokumentoinnin yhteydessä rekisterinpitäjä tai henkilötietojen käsittelijä voivat pyytää tietosuojavastaavan lausunnon tällaisen dokumentoinnin rakenteesta, laatimisesta ja hallinnoinnista. Tietosuojavastaavan tehtäväksi voidaan antaa myös tällaisten rekisterien ylläpitäminen.

133. Näiden seikkojen vuoksi tietosuojavastaavalla olisi oltava keskeinen rooli pyrittäessä ehkäisemään tietoturvaloukkauksia tai valmistautumaan niihin antamalla neuvoja ja valvomalla säännösten noudattamista sekä tietoturvaloukkauksen aikana (eli ilmoitettaessa valvontaviranomaiselle) samoin kuin valvontaviranomaisen mahdollisesti myöhemmin suorittaman tutkinnan aikana. Tästä syystä tietosuojaneuvosto suosittaa, että tietosuojavastaavalle ilmoitetaan viipymättä tietoturvaloukkauksesta ja että se on mukana koko tietoturvaloukkauksen hallinta- ja ilmoittamisprosessin ajan.

VI MUIHIN SÄÄDÖKSIIN PERUSTUVAT ILMOITTAMISVELVOLLISUUDET

134. Yleiseen tietosuoja-asetukseen perustuvan tietoturvaloukkausten ilmoittamisen lisäksi ja siitä erikseen rekisterinpitäjien olisi oltava tietoisia myös muun asiaan liittyvän lainsäädännön nojalla niihin mahdollisesti sovellettavista turvapoikkeamien ilmoittamista koskevista vaatimuksista sekä siitä, onko niiden ehkä samalla ilmoitettava valvontaviranomaiselle henkilötietojen tietoturvaloukkauksesta. Tällaiset vaatimukset saattavat olla eri jäsenvaltioissa erilaisia, mutta seuraavassa on esimerkkejä muihin säädöksiin sisältyvistä ilmoittamisvaatimuksista ja niiden suhteesta yleiseen tietosuoja-asetukseen.

[52] Ks. tietosuojavastaavia koskevat tietosuojatyöryhmän ohjeet, jotka ovat saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- *Asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla (eIDAS-asetus)*[53].

135. eIDAS-asetuksen 19 artiklan 2 kohdassa edellytetään luottamuspalvelujen tarjoajien ilmoittavan valvontaelimelleen tietoturvaloukkauksista ja eheyden menetyksistä, joilla on huomattavia vaikutuksia tarjottuun luottamuspalveluun tai sen puitteissa ylläpidettyihin henkilötietoihin. Tarvittaessa – eli jos tällainen tietoturvaloukkaus tai eheyden menetys on myös yleisen tietosuoja-asetuksen mukainen henkilötietojen tietoturvaloukkaus – luottamuspalvelun tarjoajan olisi ilmoitettava asiasta myös valvontaviranomaiselle.

- *Direktiivi (EU) 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (verkko- ja tietoturvadirektiivi)*[54].

136. Verkko- ja tietoturvadirektiivin 14 ja 16 artiklassa edellytetään keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien ilmoittavan turvapoikkeamista toimivaltaiselle viranomaiselleen. Kuten verkko- ja tietoturvadirektiivin[55] johdanto-osan 63 kappaleessa todetaan, turvapoikkeamiin voi usein sisältyä henkilötietojen vaarantuminen. Vaikka verkko- ja tietoturvadirektiivissä edellytetään toimivaltaisten viranomaisten ja valvontaviranomaisten tekevän yhteistyötä ja vaihtavan tietoja tässä yhteydessä, näiden palvelun tarjoajien on poikkeamien ilmoittamista koskevien verkko- ja tietoturvadirektiivin vaatimusten lisäksi ilmoitettava poikkeamista valvontaviranomaiselle, jos ne ovat tai niistä tulee yleisen tietosuoja-asetuksen mukaisia henkilötietojen tietoturvaloukkauksia.

Esimerkki

Pilvipalvelun tarjoajan, joka ilmoittaa tietoturvaloukkauksesta verkko- ja tietoturvadirektiivin nojalla, voi olla tarpeen ilmoittaa siitä myös rekisterinpitäjälle, jos siihen liittyy henkilötietojen tietoturvaloukkaus. Vastaavasti eIDAS-asetuksen nojalla ilmoituksen tekevän luottamuspalvelun tarjoajan täytyy ehkä ilmoittaa tapahtuneesta tietoturvaloukkauksesta myös asianomaiselle tietosuojaviranomaiselle.

- *Direktiivi 2009/136/EY (kansalaisten oikeuksia koskeva direktiivi) ja asetus (EU) N:o 611/2013 (tietoturvaloukkauksesta ilmoittamista koskeva asetus).*

137. Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien on direktiivin 2002/58/EY[56] puitteissa ilmoitettava tietoturvaloukkauksista toimivaltaisille kansallisille viranomaisille.

138. Rekisterinpitäjien olisi oltava tietoisia myös muihin sovellettaviin järjestelmiin perustuvista muista mahdollisista oikeudellisista, lääketieteellisistä tai ammatillisista ilmoittamisvelvollisuuksista.

[53] Ks. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.FIN

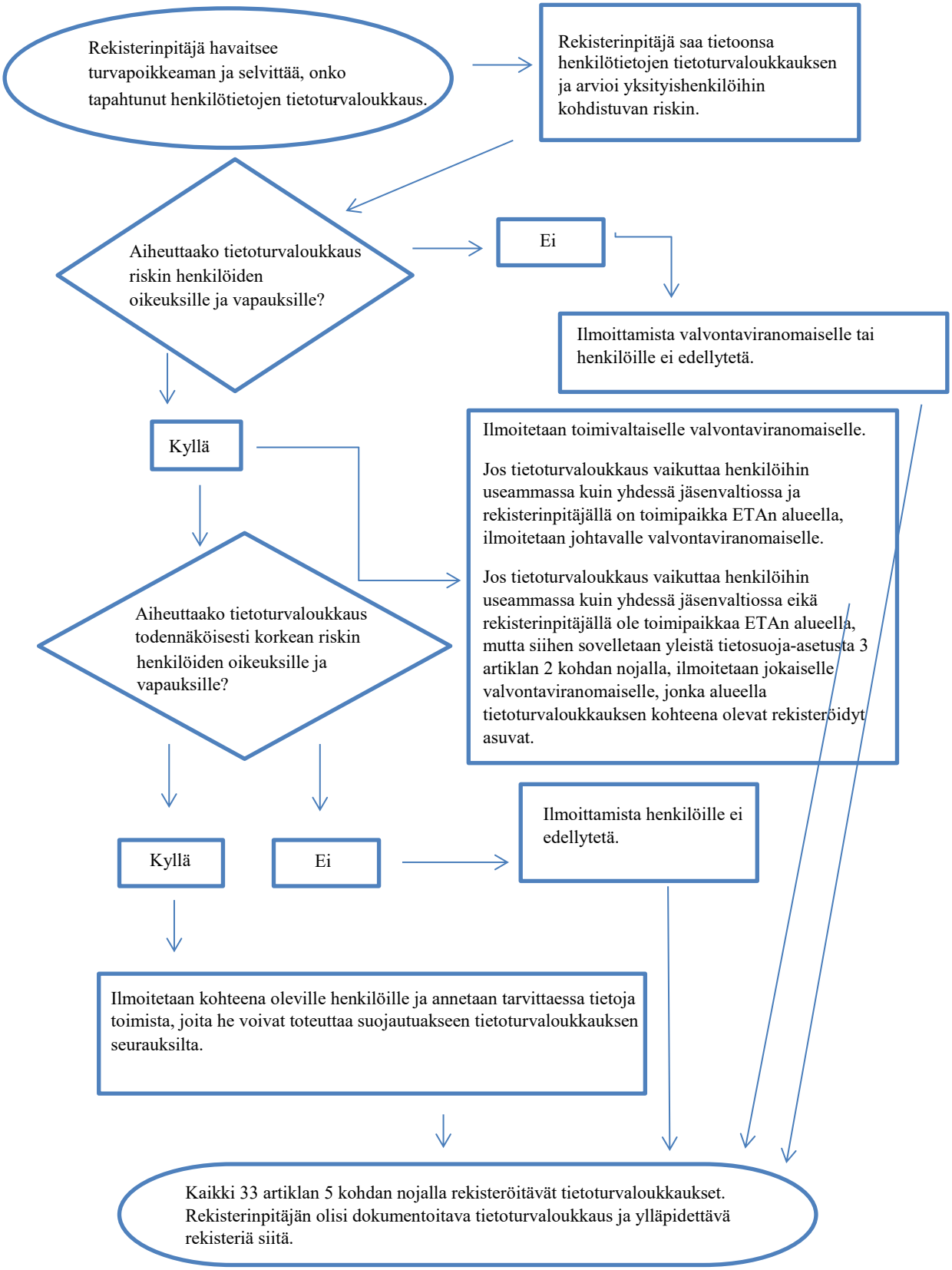
[54] Ks. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.FIN

[55] Johdanto-osan 63 kappale: *"Poikkeamat vaarantavat monissa tapauksissa henkilötietoja. Toimivaltaisten viranomaisten ja tietosuojaviranomaisten olisi tässä yhteydessä tehtävä yhteistyötä ja vaihdettava tietoja kaikista asiaankuuluvista seikoista, jotta voidaan puuttua poikkeamista johtuviin henkilötietojen tietoturvaloukkauksiin."*

[56] Euroopan komissio julkaisi 10. tammikuuta 2017 ehdotuksen sähköisen viestinnän tietosuoja-asetukseksi, jolla korvataan direktiivi 2009/136/EY ja kumotaan ilmoittamisvaatimukset. Nykyiset ilmoittamisvaatimukset pysyvät kuitenkin voimassa, kunnes Euroopan parlamentti on hyväksynyt kyseisen ehdotuksen, ks. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

VII LIITE

A. Vuokaavio ilmoittamisvaatimuksista



B. Esimerkkejä henkilötietojen tietoturvaloukkauksista ja siitä, kenelle niistä ilmoitetaan

Seuraavien esimerkkien tarkoituksena on auttaa rekisterinpitäjiä määrittämään, onko niiden tehtävä ilmoitus erilaisissa henkilötietojen tietoturvaloukkaustilanteissa. Nämä esimerkit voivat myös olla avuksi määritettäessä, kohdistuuko henkilöiden oikeuksiin ja vapauksiin riski ja onko kyseessä korkea riski.

	Esimerkki	Ilmoitetaanko valvonta-viranomaiselle?	Ilmoitetaanko rekisteröidylle?	Huomautukset/ suositukset
i	Rekisterinpitäjä on tallentanut salatun varmuuskopion henkilötietoja sisältävästä arkistosta USB-muistitikulle. Muistitikku varastetaan tiloihin tehdyn murron yhteydessä.	Ei.	Ei.	Mikäli tiedot on salattu uusimman tekniikan mukaisella algoritmilla, tiedoista on varmuuskopioita, yksilöllinen salausavain ei vaarannu ja tiedot voidaan palauttaa ajoissa, tästä tietoturvaloukkauksesta ei välttämättä tarvitse ilmoittaa. Jos tiedot kuitenkin myöhemmin vaarantuvat, ilmoittaminen on tarpeen.
ii	Rekisterinpitäjä ylläpitää verkkopalvelua. Palveluun tehdyn verkkohyökkäyksen seurauksena henkilöiden henkilötietoja varastetaan. Rekisterinpitäjällä on asiakkaita vain yhdessä jäsenvaltiossa.	Kyllä, ilmoitetaan valvontaviranomaiselle, jos henkilöille todennäköisesti aiheutuu seurauksia.	Kyllä, ilmoitetaan henkilöille kohteena olleiden henkilötietojen luonteesta riippuen ja jos henkilöille todennäköisesti aiheutuvien seurausten vakavuus on suuri.	
iii	Rekisterinpitäjän puhelinpalvelukeskuksessa tapahtuu lyhyt, useita minuutteja kestävä sähkökatko, jonka vuoksi asiakkaat eivät voi soittaa rekisterinpitäjälle ja päästä tietoihinsa.	Ei.	Ei.	Tämä ei ole ilmoitettava tietoturvaloukkaus, mutta se on silti 33 artiklan 5 kohdan mukaisesti rekisteröitävä turvapoikkeama. Rekisterinpitäjän olisi ylläpidettävä tarvittavaa rekisteriä.

iv	Rekisterinpitäjään kohdistuu kiristysohjelmahyökkäys, jonka seurauksena kaikki tiedot salataan. Varmuuskopioita ei ole, eikä tietoja voida palauttaa. Tutkinnassa käy ilmi, että kiristysohjelma ainoastaan salasi tiedot eikä järjestelmässä ollut muita haittaohjelmia.	Kyllä, ilmoitetaan valvontaviranomaiselle, jos henkilöille todennäköisesti aiheutuu seurauksia, koska käytettävyys on hävinnyt.	Kyllä, ilmoitetaan henkilöille, kohteena olleiden henkilötietojen luonteesta ja tietojen käytettävyyden menettämisen mahdollisesta vaikutuksesta sekä muista todennäköisistä seurauksista riippuen.	Jos saatavilla oli varmuuskopio ja tiedot pystyttiin palauttamaan nopeasti, valvontaviranomaiselle tai henkilöille ei tarvitse ilmoittaa, koska käytettävyyttä tai luottamuksellisuutta ei menetetty pysyvästi. Jos valvontaviranomainen kuitenkin sai turvapoikkeaman tietoonsa muilla keinoin, se voi harkita tutkintaa arvioidakseen 32 artiklan laajempien turvallisuusvaatimusten noudattamista.

v	Henkilö soittaa pankin puhelinpalvelukeskukseen ja ilmoittaa tietoturvaloukkauksesta. Hän on saanut jonkun muun henkilön kuukausittaisen tiliotteen. Rekisterinpitäjä suorittaa lyhyen tutkinnan (joka saatetaan päätökseen 24 tunnin kuluessa) ja selvittää kohtuullisella varmuudella, että on tapahtunut henkilötietojen tietoturvaloukkaus, sekä sen, onko sen järjestelmissä vika, jonka vuoksi tietoturvaloukkaus vaikuttaa tai voi vaikuttaa muihinkin henkilöihin.	Kyllä.	Vain tietoturva-loukkauksen kohteena oleville henkilöille ilmoitetaan, jos on olemassa korkea riski ja on selvää, ettei tietoturvaloukkaus vaikuta muihin henkilöihin.	Jos lisätutkinnan jälkeen havaitaan, että tietoturvaloukkaus vaikuttaa useampiin henkilöihin, ilmoitus valvontaviranomaiselle on päivitettävä ja rekisterinpitäjän on ilmoitettava myös kyseisille muille henkilöille, jos näihin kohdistuu korkea riski.

vi	Rekisterinpitäjä ylläpitää sähköistä markkinapaikkaa, ja sillä on asiakkaita useissa jäsenvaltioissa. Markkinapaikkaan tehdään verkkohyökkäys, ja hyökkäyksen tekijä julkaisee verkossa käyttäjänimiä, salasanoja ja ostohistoriaa.	Kyllä, ilmoitetaan johtavalle valvontaviranomaiselle, jos asiaan liittyy rajatylittävää tietojenkäsittelyä.	Kyllä, sillä voi aiheutua korkea riski.	Rekisterinpitäjän olisi toteutettava toimia, esimerkiksi vaadittava käyttäjiä uusimaan kohteena olleiden tilien salasanat sekä toteutettava muita toimenpiteitä riskin lieventämiseksi. Rekisterinpitäjän olisi otettava huomioon myös mahdolliset muut ilmoittamisvelvollisuudet, jotka perustuvat esimerkiksi verkko- ja tietoturvadirektiiviin, koska se on digitaalisen palvelun tarjoaja.
vii	Henkilötietojen käsittelijänä toimiva verkkosivustoja isännöivä yritys havaitsee virheen koodissa, jolla hallitaan käyttäjien hyväksyntää. Vian vaikutuksesta kuka tahansa käyttäjä voi päästä kenen tahansa muun käyttäjän tilin tietoihin.	Henkilötietojen käsittelijänä verkkosäilytyspalveluja tarjoavan yrityksen on ilmoitettava viipymättä asiakkailleen (rekisterinpitäjille), joihin vika vaikuttaa. Olettaen, että verkkosäilytyspalveluja tarjoava yritys on suorittanut oman tutkintansa, kohteena olevilla rekisterinpitäjillä pitäisi olla kohtuullinen varmuus siitä, ovatko ne olleet tietoturvaloukkauksen kohteena, ja siksi pidetään todennäköisenä, että tietoturvaloukkaus on tullut niiden tietoon, kun verkkosäilytyspalveluja tarjoava yritys (henkilötietojen käsittelijä) on ilmoittanut niille loukkauksista. Tämän jälkeen rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta valvontaviranomaiselle.	Jos henkilöille ei todennäköisesti aiheudu korkeaa riskiä, heille ei tarvitse ilmoittaa.	Verkkosivustoja isännöivän yrityksen (henkilötietojen käsittelijän) on otettava huomioon mahdolliset muut ilmoittamisvelvollisuudet (esimerkiksi verkko- ja tietoturvadirektiivin nojalla, koska se on digitaalisen palvelun tarjoaja). Jos ei ole näyttöä siitä, että jokin rekisterinpitäjistä olisi käyttänyt hyväkseen tätä järjestelmän heikkoutta, ei ehkä ole tapahtunut ilmoitettavaa tietoturvaloukkausta, mutta kyseessä on todennäköisesti rekisteröitävä tietoturvaloukkaus tai 32 artiklan noudattamatta jättäminen.
viii	Sairaalan potilastiedot ovat poissa käytöstä 30 tunnin ajan verkkohyökkäyksen vuoksi.	Kyllä, sairaalalla on velvollisuus ilmoittaa tästä, koska potilaiden hyvinvoinnille ja yksityisyydensuojalle	Kyllä, kohteena oleville henkilöille ilmoitetaan.	

		saattaa aiheutua korkea riski.		
ix	Suuren opiskelijamäärän henkilötiedot lähetetään erehdyksessä väärälle postituslistalle, jolla on yli tuhat vastaanottajaa.	Kyllä, ilmoitetaan valvontaviranomaiselle.	Kyllä, ilmoitetaan henkilöille, asianomaisten henkilötietojen laajuudesta ja tyypistä sekä mahdollisten seurausten vakavuudesta riippuen.	
x	Suoramarkkinointi-sähköpostiviesti lähetetään ”vastaanottaja”- tai ”kopio”-kentissä luetelluille vastaanottajille, jolloin kaikki vastaanottajat voivat nähdä muiden vastaanottajien sähköpostiosoitteet.	Kyllä, valvontaviranomaiselle ilmoittaminen saattaa olla pakollista, jos tämä vaikuttaa suureen määrään henkilöitä, jos paljastetaan arkaluonteisia tietoja (esimerkiksi psykoterapeutin postituslista) tai jos jotkin muut tekijät aiheuttavat korkeita riskejä (sähköpostiviesti sisältää esimerkiksi kirjautumisessa käytettäviä salasanoja).	Kyllä, ilmoitetaan henkilöille, asianomaisten henkilötietojen laajuudesta ja tyypistä sekä mahdollisten seurausten vakavuudesta riippuen.	Ilmoittaminen ei ehkä ole tarpeen, jos arkaluonteisia tietoja ei paljasteta ja jos paljastuneita sähköpostiosoitteita on vain vähän.