TIETOSUOJATYÖRYHMÄ

18/FI

WP250rev.01

Suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta

Annettu 3. lokakuuta 2017

Viimeksi tarkistettu ja hyväksytty 6. helmikuuta 2018

Tietosuojatyöryhmä on perustettu direktiivin 95/46/EY 29 artiklalla. Se on riippumaton EU:n neuvoa-antava elin, joka käsittelee tietosuojaan ja yksityisyyden suojaan liittyviä kysymyksiä. Sen tehtävät määritellään direktiivin 95/46/EY 30 artiklassa ja direktiivin 2002/58/EY 15 artiklassa.

Työryhmän sihteeristön tehtävistä huolehtii Euroopan komission oikeusasioiden pääosaston linja C (perusoikeudet ja kansalaisuus), toimisto MO-59 02/013, B-1049 Bryssel, Belgia.

Verkkosivusto: http://ec.europa.eu/justice/data-protection/index_en.htm

TIETOSUOJATYÖRYHMÄ, joka

on perustettu 24 päivänä lokakuuta 1995 annetulla Euroopan parlamentin ja neuvoston direktiivillä 95/46/EY,

ottaa huomioon mainitun direktiivin 29 ja 30 artiklan,

ottaa huomioon työjärjestyksensä,

ON ANTANUT SEURAAVAT SUUNTAVIIVAT:

SISÄLLYSTOC

JOHDANTO

Yleisessä tietosuoja-asetuksessa säädetään vaatimuksesta, jonka mukaan henkilötietojen tietoturvaloukkauksesta (jäljempänä 'tietoturvaloukkaus') on ilmoitettava toimivaltaiselle kansalliselle valvontaviranomaiselle[1] (tai rajatylittävän tietoturvaloukkauksen tapauksessa johtavalle valvontaviranomaiselle) sekä tietyissä tapauksissa niille henkilöille, joiden henkilötietoihin tietoturvaloukkaus on kohdistunut.

Ilmoittamisvelvollisuus tietoturvaloukkaustapauksissa on tällä hetkellä tietyillä organisaatioilla, kuten yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajilla (direktiivin 2009/136/EY ja asetuksen (EU) N:o 611/2013 mukaisesti)[2]. Myös eräillä EU:n jäsenvaltioilla on jo käytössä omat kansalliset tietoturvaloukkauksesta ilmoittamista koskevat velvoitteensa. Niihin saattaa sisältyä myös muiden rekisterinpitäjien ryhmien kuin yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien velvollisuus ilmoittaa tietoturvaloukkauksista (esimerkiksi Saksassa ja Italiassa) tai velvollisuus ilmoittaa kaikista tietoturvaloukkauksista, joihin liittyy henkilötietoja (esimerkiksi Alankomaissa). Muissa jäsenvaltioissa saattaa olla asiaan liittyviä käytännesääntöjä (esimerkiksi Irlannissa[3]). Monet EU:n tietosuojaviranomaiset kannustavat nykyisin rekisterinpitäjiä ilmoittamaan tietoturvaloukkauksista. Tietosuojadirektiivi 95/46/EY[4], joka yleisellä tietosuoja-asetuksella korvataan, ei kuitenkaan sisällä erityistä tietoturvaloukkauksista ilmoittamista koskevaa velvoitetta, ja tästä syystä tällainen vaatimus on monille organisaatioille uusi. Yleisellä tietosuoja-asetuksella ilmoittamisesta tehdään nyt pakollista kaikille rekisterinpitäjille, paitsi jos tietoturvaloukkaukseen ei todennäköisesti liity luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä[5]. Myös henkilötietojen käsittelijöillä on tärkeä rooli, ja niiden on ilmoitettava kaikista tietoturvaloukkauksista rekisterinpitäjälleen[6].

Tietosuojatyöryhmä katsoo, että uudesta ilmoittamisvaatimuksesta saadaan monenlaisia hyötyjä. Ilmoittaessaan valvontaviranomaiselle rekisterinpitäjät voivat saada neuvontaa siitä, onko tietoturvaloukkauksesta ilmoitettava niille henkilöille, joihin se vaikuttaa. Valvontaviranomainen voi määrätä rekisterinpitäjän ilmoittamaan kyseisille henkilöille tietoturvaloukkauksesta[7]. Ilmoittaessaan 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

---

[1] Ks. yleisen tietosuoja-asetuksen 4 artiklan 21 kohta.

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

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

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

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

[6] Ks. 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.

[7] Ks. 34 artiklan 4 kohta ja 58 artiklan 2 kohdan e alakohta.

huomauttaa, että tietoturvaloukkauksesta ilmoittamatta jättäminen joko henkilölle tai valvontaviranomaiselle saattaa merkitä sitä, että rekisterinpitäjälle voidaan 83 artiklan nojalla mahdollisesti määrätä seuraamus.

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[8] ja tämän jälkeen määritellä, onko tietoturvaloukkauksesta tarpeen ilmoittaa toimivaltaiselle valvontaviranomaiselle sekä tarvittaessa ilmoittaa siitä asianomaisille henkilöille. Valvontaviranomaiselle ilmoittamisen olisi oltava osa tietoturvaloukkauksia koskevaa valmiussuunnitelmaa.

Yleinen tietosuoja-asetus sisältää säännöksiä siitä, milloin tietoturvaloukkauksesta on ilmoitettava ja kenelle, sekä siitä, mitä tietoja ilmoituksessa on toimitettava. Ilmoituksessa vaadittavat tiedot voidaan toimittaa vaiheittain, mutta rekisterinpitäjien olisi joka tapauksessa reagoitava tietoturvaloukkauksiin viipymättä.

Lausunnossaan 3/2014 henkilötietojen tietoturvaloukkauksen ilmoittamisesta[9] 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.

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

I. Yleisen tietoturva-asetuksen mukainen henkilötietojen tietoturvaloukkauksen ilmoittaminen

A. Keskeisiä turvallisuutta koskevia näkökohtia

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

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

[8] 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).

[9] Ks. lausunto 3/2014 henkilötietojen tietoturvaloukkauksen ilmoittamisesta http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_fi.pdf

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

huomioon uusin tekniikka, toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä todennäköisyydeltään ja vakavuudeltaan vaihtelevat luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit[11]. 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[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

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

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

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 lainvastaiseen 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 on tapaus, jossa ainoa henkilötietoja sisältävä kopio on salattu kiristysohjelmalla tai rekisterinpitäjä on salannut sen käyttäen salausavainta, joka ei enää ole sen hallussa.

Lienee selvää, että tietoturvaloukkaus on yksi turvapoikkeamien tyyppi. 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

[11] 32 artikla; ks. myös johdanto-osan 83 kappale.

[12] Ks. johdanto-osan 87 kappale.

– tiivistetysti voidaan sanoa, että vaikka kaikki henkilötietojen tietoturvaloukkaukset ovat turvapoikkeamia, kaikki turvapoikkeamat eivät välttämättä ole henkilötietojen tietoturvaloukkauksia[13].

Tietoturvaloukkauksen mahdollisia haitallisia vaikutuksia henkilöille käsitellään jäljempänä.

2. Henkilötietojen tietoturvaloukkausten tyypit

Lausunnossaan 3/2014 henkilötietojen tietoturvaloukkausten ilmoittamisesta tietosuojatyöryhmä selitti, että tietoturvaloukkaukset voidaan luokitella seuraavien kolmen tunnetun tietoturvaperiaatteen mukaan[14]:

- ”Tietojen luottamuksellisuuteen vaikuttava tietoturvaloukkaus” – henkilötietojen luvaton tai vahingossa tapahtuva luovuttaminen tai pääsy tietoihin.
- ”Tietojen eheyteen vaikuttava tietoturvaloukkaus” – henkilötietojen luvaton tai vahingossa tapahtuva muuttaminen.
- ”Tietojen käytettävyyteen vaikuttava tietoturvaloukkaus” – vahingossa tapahtuva tai luvaton henkilötietoihin pääsyn häviäminen[15] tai henkilötietojen tuhoaminen.

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

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 häviää esimerkiksi tapauksissa, joissa tiedot on poistettu vahingossa 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 häviämisenä.

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

[13] 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.

[14] Ks. lausunto 3/2014.

[15] On laajalti tunnustettua, että ”pääsy” tietoihin on oleellinen osa niiden ”käytettävyyttä”. Ks. esimerkiksi asiakirja NIST SP800-53rev4, 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 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Myös asiakirjassa CNSSI-4009 käytettävyydellä tarkoitetaan valtuutettujen käyttäjien nopeaa ja luotettavaa pääsyä tietoihin Ks. https://rmf.org/wp-content/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:iso-iec:27000:ed-4:v1:en

Voidaan kysyä, onko henkilötietojen käytettävyyden väliaikaista häviämistä 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”.

Näin ollen myös turvapoikkeama, joka johtaa henkilötietojen käytettävyyden häviämiseen joksikin aikaa, on yksi tietoturvaloukkauksen tyyppi, koska tietoihin pääsyn häviämisellä 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 4 artiklan 12 kohdassa tarkoitettu ”tietoturvaloukkaus”.

Kuten henkilötietojen pysyvä häviäminen tai tuhoutuminen (tai yleensä minkä tahansa tyyppinen tietoturvaloukkaus), tietoturvaloukkaus, johon liittyy käytettävyyden väliaikainen häviäminen, olisi dokumentoitava 33 artiklan 5 kohdan mukaisesti. Tämä auttaa rekisterinpitäjää täyttämään osoitusvelvollisuutensa valvontaviranomaiselle, joka saattaa pyytää näitä tietoja[16]. Tietoturvaloukkaukseen liittyvistä olosuhteista riippuen se saattaa edellyttää tai olla edellyttämättä ilmoittamista valvontaviranomaiselle ja tietoturvaloukkauksen kohteina olleille henkilöille. Rekisterinpitäjän on arvioitava henkilötietojen käytettävyyden häviämisen seurauksena syntyvän, luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvan vaikutuksen todennäköisyys ja vakavuus. Rekisterinpitäjän on 33 artiklan mukaisesti ilmoitettava tietoturvaloukkauksesta, ellei ole epätodennäköistä, että se aiheuttaa riskin henkilöiden oikeuksille ja vapauksille. Tämä on luonnollisesti arvioitava tapauskohtaisesti.

Esimerkkejä

Jos sairaalaympäristössä kriittisen tärkeät potilastiedot ovat poissa käytöstä, vaikka väliaikaisestikin, tämä saattaa muodostaa riskin henkilöiden oikeuksille ja vapauksille; esimerkiksi leikkauksia saatetaan peruuttaa, jolloin ihmishenkiä vaarantuu.

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

On syytä huomata, että vaikka rekisterinpitäjän järjestelmien käytettävyyden häviäminen 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 häviämisen väliaikaisesti, 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

[16] Ks. 33 artiklan 5 kohta.

Tietoturvaloukkauksella saattaa olla useita erilaisia henkilöihin kohdistuvia haittavaikutuksia, jotka voivat aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja. Yleisessä tietosuoja-asetuksessa mainitaan, 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[17].

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[18].

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.”

Lisäohjeita henkilöille aiheutuvien haittavaikutusten riskin arvioimisesta on osiossa IV.

Jos rekisterinpitäjät jättävät ilmoittamatta tietoturvaloukkauksesta joko valvontaviranomaiselle tai rekisteröidyille tai molemmille, vaikka 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[19], joka voidaan määrätä 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 euroa tai kaksi prosenttia yrityksen vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. On myös tärkeää muistaa, että joissain tapauksissa tietoturvaloukkauksesta ilmoittamatta jättäminen saattaa paljastaa joko turvatoimien puutteen tai olemassa olevien turvatoimien riittämättömyyden. Tietosuojatyöryhmän hallinnollisia sakkoja koskevissa 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 (33 ja 34 artikla) ja toisaalta (riittävien) turvatoimien puutteesta (32 artikla), koska ne ovat kaksi erillistä sääntörikkomusta.

[17] Ks. myös johdanto-osan 85 ja 75 kappale.

[18] Ks. myös johdanto-osan 86 kappale.

[19] Lisätietoja on asetuksessa 2016/679 tarkoitettujen hallinnollisten sakkojen soveltamista ja määräämistä koskevissa tietosuojatyöryhmän suuntaviivoissa, jotka ovat saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

II. 33 artikla – Ilmoittaminen valvontaviranomaiselle

A. Milloin ilmoitetaan?

1. 33 artiklan vaatimukset

Direktiivin 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.”

Johdanto-osan 87 kappaleessa todetaan seuraavaa[20]:

> ”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?

Kuten edellä on esitetty, yleisessä tietosuoja-asetuksessa edellytetään, että jos tapahtuu tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta. Tämä saattaa herättää kysymyksen siitä, milloin tietoturvaloukkauksen voidaan katsoa ”tulleen ilmi” rekisterinpitäjälle. Tietosuojatyöryhmä katsoo, että rekisterinpitäjän olisi katsottava tulleen tietoiseksi tietoturvaloukkauksesta silloin, kun sillä on kohtuullinen varmuus siitä, että on tapahtunut henkilötietoja vaarantava turvapoikkeama.

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[21]. Tämä asettaa rekisterinpitäjälle velvoitteen varmistaa, että mahdolliset tietoturvaloukkaukset tulevat sille ”ilmi” ajoissa, jotta se voi toteuttaa asianmukaisia toimia.

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

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

[21] Ks. johdanto-osan 87 kappale.

turvapoikkeaman tutkimiseksi, jotta voidaan määrittää, onko todella tapahtunut henkilötietojen tietoturvaloukkaus, ja jos on, toteutetaan korjaavia toimia ja ilmoitetaan tietoturvaloukkauksesta 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 yhden asiakkaan henkilötietoja ja toimittaa näytön luvattomasta luovuttamisesta. Koska rekisterinpitäjälle on esitetty selvä näyttö 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 selvä näyttö 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 – selvä näyttö tietoturvaloukkauksen tapahtumisesta, ja on täysin selvää, että tietoturvaloukkaus on tullut sille ”ilmi”.

Kun rekisterinpitäjä on saanut tiedon mahdollisesta tietoturvaloukkauksesta yksityishenkilöltä, media-alan organisaatiolta tai muusta lähteestä tai jos se itse on havainnut turvapoikkeaman, se voi vähän aikaa tutkia, 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.

Kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta, 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[22]. 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.

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.

[22] Ks. tietosuojatyöryhmän ohjeet tietosuojaa koskevasta vaikutustenarvioinnista, jotka ovat saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

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 katsotaan 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.

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[23]. On tärkeää, että kun tietoturvaloukkaus havaitaan, siitä raportoidaan ylöspäin asianmukaiselle johdon tasolle, jotta siihen voidaan puuttua ja siitä voidaan ilmoittaa 33 artiklan mukaisesti ja tarvittaessa 34 artiklan mukaisesti. Tällaiset toimenpiteet ja raportointimekanismit voitaisiin kuvailla yksityiskohtaisesti rekisterinpitäjän turvapoikkeamia koskevissa valmiussuunnitelmissa ja/tai hallinnointijärjestelyissä. Nämä auttavat rekisterinpitäjää suunnittelussa ja sen määrittämisessä, kenellä organisaatiossa on operatiivinen vastuu tietoturvaloukkauksen hallinnoinnista ja ilmoitetaanko turvapoikkeamasta hierarkiassa ylöspäin, ja jos ilmoitetaan, miten.

Rekisterinpitäjällä olisi myös oltava järjestelyjä käyttämiensä henkilötietojen käsittelijöiden kanssa, joilla on velvollisuus ilmoittaa rekisterinpitäjälle tietoturvaloukkauksista (ks. jäljempänä).

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.

- 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 (onko todennäköistä, että riskiä ei ole, että riski on tai että riski on suuri) 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 se etenee.

Näin ollen pitäisi olla selvää, että rekisterinpitäjällä on velvollisuus reagoida alustavaan hälytykseen ja selvittää, onko tietoturvaloukkaus todella tapahtunut. Rekisterinpitäjä voi vähän aikaa tutkia asiaa ja kerätä näyttöä ja muuta merkityksellistä tietoa. Kun rekisterinpitäjä on todennut kohtuullisen varmasti, että tietoturvaloukkaus on tapahtunut, sen on ilmoitettava siitä valvontaviranomaiselle ilman aiheetonta

[23] 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.

viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa, mikäli 33 artiklan 1 kohdan ehdot täyttyvät[24]. Jos rekisterinpitäjä ei toimi nopeasti ja käy ilmi, että tietoturvaloukkaus on tapahtunut, tätä voidaan pitää 33 artiklassa säädetyn ilmoittamisvelvollisuuden laiminlyöntinä.

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

Yleisen tietosuoja-asetuksen 26 artikla koskee yhteisrekisterinpitäjiä, ja sen mukaan yhteisrekisterinpitäjien on määritettävä kunkin vastuualueet yleisen tietosuoja-asetuksen noudattamiseksi[25]. Tähän sisältyy sen määrittäminen, mikä osapuoli vastaa 33 ja 34 artiklan velvoitteiden noudattamisesta. Tietosuojatyöryhmä 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

Rekisterinpitäjällä on kokonaisvastuu henkilötietojen suojaamisesta, mutta henkilötietojen käsittelijällä on merkittävä rooli, jotta rekisterinpitäjä voi noudattaa velvoitteitaan. Tämä koskee myös tietoturvaloukkauksesta ilmoittamista. 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”.

Asetuksen 33 artiklan 2 kohdassa todetaan selvästi, että jos rekisterinpitäjä käyttää henkilötietojen käsittelijää, tämän on ilmoitettava sen rekisterinpitäjän puolesta käsittelemien henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa. On syytä huomauttaa, ettei henkilötietojen käsittelijän tarvitse ensin arvioida 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 siitä 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, esimerkiksi sitä, onko rekisterinpitäjän hallussa yhä kopio tai varmuuskopio henkilötietojen käsittelijän tuhoamista tai kadottamista henkilötiedoista. Tämä saattaa vaikuttaa siihen, onko rekisterinpitäjän ilmoitettava tietoturvaloukkauksesta.

[24] 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=EN

[25] Ks. myös johdanto-osan 79 kappale.

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 tietosuojatyöryhmä suosittaa, että henkilötietojen käsittelijä ilmoittaa tietoturvaloukkauksesta rekisterinpitäjälle välittömästi ja toimittaa lisätietoja siitä sitä mukaa, kun tarkempia tietoja saadaan. Tämä on tärkeää, jotta rekisterinpitäjän on helpompi noudattaa vaatimusta ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa.

Kuten edellä mainittiin, rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa olisi täsmennettävä, miten 33 artiklan 2 kohdassa säädetyt vaatimukset ja muut yleisen tietosuoja-asetuksen säännöksen olisi täytettävä. Sopimuksessa voidaan vaatia, että henkilötietojen käsittelijä tekee ilmoituksen varhaisesta vaiheessa, mikä puolestaan tukee rekisterinpitäjän velvollisuuksia ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa.

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

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 33 ja 34 artiklan mukaisesti. On kuitenkin tärkeää muistaa, että oikeudellinen vastuu ilmoittamisesta säilyy rekisterinpitäjällä.

B. Tietojen toimittaminen valvontaviranomaiselle

1. Toimitettavat tiedot

Kun rekisterinpitäjä ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle, sen olisi 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.”

Yleisessä tietosuoja-asetuksessa ei määritellä rekisteröityjen tai henkilötietotyyppien ryhmiä. Tietosuojatyöryhmä ehdottaa kuitenkin, että rekisteröityjen ryhmät perustuvat niiden rekisteröityjen eri tyyppeihin, 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 henkilötietotyypit voivat viitata rekisterinpitäjän hallussa mahdollisesti oleviin eri tyyppisiin tietoihin, kuten terveystietoihin, koulutustietoihin, sosiaalihuoltotietoihin, taloudellisiin tietoihin, pankkitilien numeroihin ja passinumeroihin.

Johdanto-osan 85 kappaleessa todetaan selvästi, että ilmoittamisen yhtenä tarkoituksena on rajoittaa henkilöille aiheutuvia vahinkoja. Näin ollen jos rekisteröityjen tyypit tai henkilötietotyypit viittaavat ovat sellaisia, että tietoturvaloukkauksen seurauksena voi aiheutua vahinkoa (esimerkiksi identiteettivarkaus, petos, taloudelliset menetykset, salassapitovelvollisuuden vaarantuminen), on

tärkeää, että ilmoituksessa mainitaan nämä kategoriat. Tällä tavoin ilmoittaminen on yhteydessä vaatimukseen kuvata tietoturvaloukkauksen todennäköiset seuraukset.

Sen, että tarkkoja tietoja (esimerkiksi tietoturvaloukkauksen kohteeksi joutuneiden rekisteröityjen tarkkaa määrää) ei ole saatavilla, ei pitäisi estää ilmoituksen tekemistä ajoissa. Yleisessä tietosuoja-asetuksessa sallitaan arvioiden tekeminen asianomaisten rekisteröityjen ja henkilötietojen lukumäärästä. Painopisteen pitäisi olla tietoturvaloukkauksen haittavaikutusten torjumisessa pikemmin kuin tarkkojen lukujen toimittamisessa. Kun on käynyt selväksi, että tietoturvaloukkaus on tapahtunut, mutta sen laajuus ei vielä ole tiedossa, vaiheittain tehtävä ilmoitus (ks. jäljempänä) on näin ollen turvallinen tapa täyttää ilmoittamisvelvollisuudet.

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 voidaan selittää kattavasti.

Esimerkki

Rekisterinpitäjä voi katsoa hyödylliseksi mainita valvontaviranomaiselle tehtävässä ilmoituksessa henkilötietojen käsittelijänsä nimeltä, jos se on tietoturvaloukkauksen perimmäinen aiheuttaja ja varsinkin jos on aiheutunut turvapoikkeama, joka vaikuttaa monien muiden samaa henkilötietojen käsittelijää käyttävien rekisterinpitäjien henkilötietoihin.

Valvontaviranomainen voi joka tapauksessa pyytää lisätietoja osana tietoturvaloukkausta koskevaa tutkintaansa.

2. Vaiheittain tapahtuva ilmoittaminen

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

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

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 asetuksessa sallitaan vaiheittain tapahtuva ilmoittaminen. Tätä sovelletaan todennäköisemmin monimutkaisemmissa tietoturvaloukkauksissa, kuten tietyntyyppisissä kyberturvallisuuspoikkeamissa, jotka saattavat edellyttää esimerkiksi perusteellista rikosteknistä tutkimusta, jotta voidaan määrittää kattavasti tietoturvaloukkauksen luonne ja se, missä määrin henkilötiedot ovat vaarantuneet. Näin ollen rekisterinpitäjän on monissa tapauksissa suoritettava lisätutkimuksia ja toimitettava täydentäviä tietoja myöhemmin. Tämä on sallittua, mikäli rekisterinpitäjä toimittaa viivästyksestä perustellun selityksen 33 artiklan 1 kohdan mukaisesti. Tietosuojatyöryhmä 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 se saa tietoturvaloukkauksesta tietoonsa muita merkityksellisiä tietoja, jotka on toimitettava valvontaviranomaiselle.

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

Valvontaviranomaiselle ilmoittamisen tarkoituksena ei kuitenkaan ole ainoastaan neuvojen 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[26] 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. Yleisemmin ottaen valvontaviranomaiselle ilmoittaminen ei voi olla peruste jättää ilmoittamatta tietoturvaloukkauksesta rekisteröidylle tapauksissa, joissa tätä edellytetään.

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 aiheudu seuraamuksia.

Esimerkki

Rekisterinpitäjä ilmoittaa valvontaviranomaiselle tietoturvaloukkauksesta 72 tunnin kuluessa siitä, kun se on havainnut kadottaneensa USB-muistitikun, joka sisältää kopion joidenkin sen asiakkaiden henkilötiedoista. USB-muistitikku löydetään myöhemmin rekisterinpitäjän tiloista ja se palautetaan. Rekisterinpitäjä ilmoittaa tästä valvontaviranomaiselle ja pyytää ilmoituksen muuttamista.

On syytä huomauttaa, että vaiheittainen ilmoittaminen on jo käytössä direktiivin 2002/58/EY ja asetuksen (EU) N:o 611/2013 voimassa olevien vaatimusten nojalla ja muiden omatoimisesti ilmoitettavien turvapoikkeamien ollessa kyseessä.

3. Ilmoittamisen viivästyminen

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

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 sen aloittaessa tutkintaansa ja ennen ilmoittamista se havaitsee 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 asiallisen ilmoituksen, joka koskee useita hyvin samanlaisia tietoturvaloukkauksia, jotka johtuvat mahdollisesti eri syistä. Tämä saattaa aiheuttaa sen, että

[26] Ks. 9 artikla.

ilmoittaminen valvontaviranomaiselle kestää yli 72 tuntia siitä, kun nämä tietoturvaloukkaukset tulevat ensimmäisen kerran rekisterinpitäjän tietoon.

Tiukasti ottaen jokainen yksittäinen tietoturvaloukkaus on turvapoikkeama, josta on ilmoitettava. Välttääkseen liiallista vaivaa 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.

Vaikka yleisessä tietosuoja-asetuksessa jossakin määrin sallitaan ilmoittamisen viivästyminen, tätä ei tulisi pitää säännöllisenä käytäntönä. On syytä huomauttaa, että niputettuja ilmoituksia voidaan tehdä myös useista samanlaisista tietoturvaloukkauksista, joista on ilmoitettu 72 tunnin kuluessa.

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

1. Rajatylittävät tietoturvaloukkaukset

Jos henkilötietoja käsitellään rajatylittävästi[27], 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[28]. Yleisen tietosuoja-asetuksen 55 artiklan 1 kohdassa säädetään seuraavaa:

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

56 artiklan 1 kohdassa säädetään 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.”

Lisäksi 56 artiklan 6 kohdassa säädetään seuraavaa:

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

Tämä tarkoittaa, että jos tietoturvaloukkaus tapahtuu rajatylittävän käsittelyn yhteydessä ja siitä on ilmoitettava, rekisterinpitäjän on ilmoitettava siitä johtavalle valvontaviranomaiselle[29]. Laatiessaan tietoturvaloukkauksia koskevaa valmiussuunnitelmaansa rekisterinpitäjän on tästä syystä arvioitava, mikä valvontaviranomainen on johtava valvontaviranomainen, jolle sen on ilmoitettava

[27] Ks. 4 artiklan 23 kohta.

[28] Ks. myös johdanto-osan 122 kappale.

[29] Ks. tietosuojatyöryhmän ohjeet rekisterinpitäjän tai henkilötietojen käsittelijän johtavan valvontaviranomaisen määrittämiseen, saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235

tietoturvaloukkauksista[30]. Näin 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 jäsenvaltiossa tietoturvaloukkaus on todennäköisesti vaikuttanut rekisteröityihin. Jos rekisterinpitäjällä on epäselvyyttä siitä, mikä on johtava valvontaviranomainen, sen olisi ilmoitettava ainakin sen paikan paikalliselle valvontaviranomaiselle, jossa tietoturvaloukkaus on tapahtunut.

2. EU:n ulkopuolisissa toimipaikoissa tapahtuvat tietoturvaloukkaukset

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. Asetuksen 3 artiklan 2 kohdassa säädetään seuraavaa[31]:

> ”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.”

Myös 3 artiklan 3 kohta on merkityksellinen, ja siinä säädetään seuraavaa[32]:

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

Jos rekisterinpitäjään, joka ei ole sijoittautunut unioniin, sovelletaan 3 artiklan 2 tai 3 kohtaa ja siihen kohdistuu tietoturvaloukkaus, 33 ja 34 artiklan mukaiset ilmoittamisvelvoitteet sitovat sitä näin ollen tästä huolimatta. Yleisen tietosuoja-asetuksen 27 artiklassa edellytetään rekisterinpitäjän (ja henkilötietojen käsittelijän) nimittävän edustajan unionin aluetta varten sovellettaessa 3 artiklan 2 kohtaa. Tällaisissa tapauksissa tietosuojatyöryhmä suosittaa, että ilmoitus tehdään sen jäsenvaltion valvontaviranomaiselle, johon rekisterinpitäjän edustaja EU:ssa on sijoittautunut[33]. Vastaavasti jos henkilötietojen käsittelijään sovelletaan 3 artiklan 2 kohtaa, sitä sitovat henkilötietojen käsittelijöille asetetut velvoitteet, joista tässä yhteydessä erityisen merkittävä on 33 artiklan 2 kohdassa säädetty velvollisuus ilmoittaa tietoturvaloukkauksesta rekisterinpitäjälle.

D. Tilanteet, joissa ilmoittamista ei edellytetä

---

[30] Kaikkien kansallisten tietosuojaviranomaisten yhteystiedot ovat saatavilla seuraavassa verkko-osoitteessa: http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm

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

[32] Ks. myös johdanto-osan 25 kappale.

[33] Ks. johdanto-osan 80 kappale ja 27 artikla.

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 tarjoajien voimassa olevien tietoturvaloukkausten ilmoittamista koskevien vaatimusten kanssa, joista säädetään direktiivissä 2009/136/EY ja joiden mukaan kaikki merkitykselliset tietoturvaloukkaukset on ilmoitettava toimivaltaiselle viranomaiselle.

Lausunnossaan 3/2014 henkilötietojen tietoturvaloukkauksen ilmoittamisesta[34] 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 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[35]. Vaikka tiedot olisi salattu, niiden häviäminen tai muuttaminen voi aiheuttaa rekisteröidyille kielteisiä seurauksia, jos rekisterinpitäjällä ei ole riittäviä varmuuskopioita. Tällaisessa tapauksessa rekisteröidyille olisi ilmoitettava, vaikka tiedot olisi suojattu asianmukaisella salauksella.

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.

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

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 32 artiklan 1 kohdan c alakohdassa todetaan, ”kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa” on merkittävä turvallisuustekijä.

[34] Tietosuojatyöryhmän lausunto 3/2014 henkilötietojen tietoturvaloukkauksen ilmoittamisesta http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_fi.pdf

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

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.

Jos rekisterinpitäjä ei tee ilmoitusta valvontaviranomaiselle tilanteessa, jossa tietoja ei tosiasiallisesti ole salattu turvallisesti, tämä merkitsee 33 artiklan noudattamatta jättämistä. Tästä syystä rekisterinpitäjien olisi salausohjelmistoja valitessaan huolellisesti tarkasteltava tarjotun salauksen laatua ja asianmukaista toteutusta sekä ymmärrettävä sen antaman suojan taso ja asianmukaisuus suhteessa riskeihin. Rekisterinpitäjien olisi myös tunnettava salaustuotteensa toiminta. Laite saattaa esimerkiksi olla salattu, kun siitä on sammutettu virta, mutta salaamaton valmiustilassa. Joissain salausta käyttävissä tuotteissa on ”oletusarvoisia salausavaimia”, jotka kunkin asiakkaan on muutettava, jotta ne olisivat toimivia. 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 suojelun tason.

III. 34 artikla – Ilmoittaminen rekisteröidylle

A. Ilmoittaminen yksittäisille henkilöille

Tietyissä tapauksissa rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta valvontaviranomaisen lisäksi myös henkilöille, joihin se vaikuttaa.

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.”

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 tarvitse ilmoittaa henkilöille, mikä suojelee heitä tarpeettomien ilmoitusten aiheuttamalta väsymykseltä.

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[36]. Kuten edellä todettiin, nopealla ilmoittamisella autetaan – tietoturvaloukkauksen luonteesta ja sen aiheuttamasta riskistä

[36] Ks. myös johdanto-osan 86 kappale.

riippuen – henkilöitä toteuttamaan toimia suojellakseen itseään sen mahdollisilta kielteisiltä seurauksilta.

Näiden suuntaviivojen liitteessä B on luettelo esimerkkitapauksista, joissa tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin henkilöille ja rekisterinpitäjän täytyy ilmoittaa siitä niille, joihin se vaikuttaa.

B. Toimitettavat tiedot

Henkilöille tehtävän ilmoituksen suhteen 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.”

Tämän säännöksen mukaan rekisterinpitäjän on annettava ainakin seuraavat tiedot:

- kuvaus tietoturvaloukkauksen 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 ja joihin tarvittaessa kuuluu myös toimenpiteitä mahdollisten haittavaikutusten lieventämiseksi.

Esimerkkinä toimenpiteistä, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut tietoturvaloukkauksen johdosta, se voi mainita ilmoittaneensa tietoturvaloukkauksesta valvontaviranomaiselle ja saaneensa tämän jälkeen neuvoja tietoturvaloukkauksen hoidosta 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 pääsytietonsa ovat vaarantuneet. Tässäkin yhteydessä rekisterinpitäjä voi päättää toimittaa myös muita tietoja tässä edellytettyjen tietojen lisäksi.

C. Yhteydenotto henkilöihin

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

Kun tietoturvaloukkauksesta ilmoitetaan rekisteröidyille, olisi käytettävä nimenomaisesti tähän tarkoitukseen laadittuja viestejä, joita ei tule lähettää yhdessä muiden tietojen, kuten säännöllisten päivitysten, uutiskirjeiden tai vakiomuotoisten viestien, kanssa. Tämän avulla ilmoitus tietoturvaloukkauksesta on selkeä ja läpinäkyvä.

Esimerkkejä läpinäkyvistä ilmoitusmenetelmistä ovat muun muassa suorat viestit (esimerkiksi sähköposti, tekstiviesti, suora viesti), näkyvät palkit tai ilmoitukset verkkosivustoilla, postilähetykset ja näkyvät ilmoitukset painetuissa viestimissä. Pelkästään lehdistötiedotteessa tai yrityksen blogissa annettava ilmoitus ei ole tehokas keino ilmoittaa tietoturvaloukkauksesta yksittäiselle henkilölle. Tietosuojatyöryhmä 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 vain yhden viestintäkanavan sijasta.

Rekisterinpitäjien on ehkä myös varmistettava, että ilmoitus on saatavilla asianmukaisissa vaihtoehtoisissa muodoissa ja tarvittavilla kielillä, jotta varmistetaan, että henkilöt voivat ymmärtää saamansa tiedon. On esimerkiksi asianmukaista ilmoittaa tietoturvaloukkauksesta henkilölle kielellä,

jota on aiemmin käytetty asioitaessa vastaanottajan kanssa. 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, paikallisella kielellä annettava ilmoitus voi olla hyväksyttävä vaadittavat resurssit huomioon ottaen. Keskeistä on auttaa rekisteröityjä ymmärtämään tietoturvaloukkauksen luonne ja toimenpiteet, joita he voivat toteuttaa suojautuakseen siltä.

Rekisterinpitäjät voivat parhaiten määrittää, mikä on asianmukaisin viestintäkanava tietoturvaloukkauksesta ilmoittamiseksi henkilöille, varsinkin jos niiden kanssakäyminen asiakkaidensa kanssa on tiivistä. Rekisterinpitäjän on kuitenkin luonnollisesti varottava käyttämästä tietoturvaloukkauksen vaarantamaa viestintäkanavaa, sillä sitä voivat käyttää myös rekisterinpitäjäksi tekeytyvät hyökkäyksen tekijät.

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.”

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.

Tähän liittyy 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 tietoturvaloukkauksen tutkintaa. Tämän jälkeen rekisteröidyille on kuitenkin ilmoitettava tietoturvaloukkauksesta nopeasti.

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 pääsy henkilötietoihinsa ja toimittaa rekisterinpitäjälle tarvittavat lisätiedot yhteyden ottamiseksi).

D. Tilanteet, joissa ilmoittamista ei edellytetä

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

- Rekisterinpitäjä on soveltanut asianmukaisia teknisiä ja organisatorisia toimenpiteitä suojatakseen henkilötiedot ennen tietoturvaloukkausta, 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 tunnistevälineellä.
- 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 tunnistaa välittömästi henkilötietoihin päässeen henkilön ja toteuttaa toimia tätä vastaan ennen kuin tämä pystyi tekemään tiedoilla mitään. On kuitenkin edelleen otettava asianmukaisesti

huomioon luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset kyseisten tietojen luonteesta riippuen.

- Yhteyden ottaminen henkilöihin vaatisi kohtuutonta vaivaa[37] esimerkiksi jos näiden yhteystiedot 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 voidaan tiedottaa yhtä tehokkaalla tavalla. Jos ilmoittaminen aiheuttaisi kohtuutonta vaivaa, voidaan myös harkita teknisiä järjestelyjä, joilla tiedot tietoturvaloukkauksesta asetetaan saataville pyynnöstä. Tästä saattaa olla hyötyä henkilöille, joihin tietoturvaloukkaus saattaa vaikuttaa, mutta joihin rekisterinpitäjä ei muulla tavoin saa yhteyttä.

Osoitusvelvollisuusperiaatteen mukaisesti rekisterinpitäjien olisi pystyttävä osoittamaan valvontaviranomaiselle täyttävänsä yhden tai useamman näistä ehdoista [38]. On 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.

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

IV. **Riskin ja korkean riskin arviointi**

A. Riski ilmoittamisen käynnistäjänä

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.

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.

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*

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

[38] Ks. 5 artiklan 2 kohta.

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[39].

B. Riskiä arvioitaessa huomioon otettavat tekijät

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 niiden mukaan riski olisi arvioitava objektiivisen arvioinnin perusteella.

On syytä huomauttaa, että arvioitaessa tietoturvaloukkauksen aiheuttamaa riskiä henkilöiden oikeuksille ja vapauksille keskitytään eri asioihin kuin tietosuojaa koskevassa vaikutustenarvioinnissa[40]. Tietosuojaa koskevassa vaikutustenarvioinnissa otetaan huomioon sekä riskit, jotka aiheutuvat, kun tiedonkäsittely suoritetaan suunnitellusti, että tietoturvaloukkauksen aiheuttamat riskit. Mahdollisen tietoturvaloukkauksen yhteydessä siinä tarkastellaan yleisesti tietoturvaloukkauksen todennäköisyyttä ja siitä rekisteröidylle mahdollisesti aiheutuvia vahinkoja; toisin sanoen siinä arvioidaan hypoteettista tapahtumaa. Todellisen tietoturvaloukkauksen kohdalla tapahtuma on jo tapahtunut, ja näin ollen painopiste on siitä aiheutuvassa henkilöihin kohdistuvien vaikutusten riskissä.

Esimerkki

Tietosuojaa koskevassa vaikutustenarvioinnissa todetaan, että ehdotettu tietyn suojausohjelmiston käyttö henkilötietojen suojaamiseksi on asianmukainen toimenpide, jolla varmistetaan tietojenkäsittelystä muutoin henkilöille aiheutuvaa riskiä vastaava turvallisuuden taso. Jos kuitenkin myöhemmin saadaan tietää, että ohjelmistossa on heikkous, tämä muuttaa ohjelmiston soveltuvuutta suojeltuihin henkilötietoihin kohdistuvan riskin torjumiseen ja se olisi arvioitava uudelleen osana tietosuojaa koskevaa jatkuvaa 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.

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 tietosuojatyöryhmä suosittaa, että arvioinnissa olisi otettava huomioon seuraavat kriteerit[41]:

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

[40] Ks. tietosuojatyöryhmän ohjeet tietosuojaa koskevasta vaikutustenarvioinnista, jotka ovat saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[41] Asetuksen (EU) N:o 611/2013 3 artiklan 2 kohdassa annetaan ohjeita tekijöistä, jotka olisi otettava huomioon ilmoitettaessa tietoturvaloukkauksista sähköisten viestintäpalvelujen alalla, ja niistä voi olla hyötyä yleisen

- Tietoturvaloukkausten tyypit

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

- Henkilötietojen luonne, arkaluonteisuus ja määrä

Riskiä arvioitaessa keskeinen tekijä on luonnollisesti tietoturvaloukkauksen vaarantamien 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.

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

Jotkin henkilötietotyypit saattavat ensi näkemältä vaikuttaa suhteellisen harmittomilta, mutta olisi pohdittava huolellisesti, mitä tällaiset tiedot saattavat paljastaa asianomaisesta henkilöstä. Luettelo säännöllisiä toimituksia vastaanottavista asiakkaista ei ehkä ole erityisen arkaluonteinen, mutta samat tiedot asiakkaista, jotka ovat keskeyttäneet toimitukset lomansa ajaksi, voivat olla hyödyllisiä rikollisille.

Vastaavasti pienellä määrällä erittäin arkaluonteisia henkilötietoja voi olla suuri vaikutus henkilöön, ja suuri määrä yksityiskohtaisia tietoja voi paljastaa suuremman määrän tietoja kyseisestä henkilöstä. Samoin tietoturvaloukkaus, joka vaikuttaa suureen määrään monien rekisteröityjen henkilötietoja, voi vaikuttaa vastaavan suureen määrään henkilöitä.

- Henkilöiden tunnistamisen helppous

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 erityistä henkilöllisyyden selvittämistä tai henkilötietojen yhdistäminen tiettyyn henkilöön saattaa olla äärimmäisen vaikeaa, mutta kuitenkin mahdollista tietyissä olosuhteissa. Tunnistaminen vaarantuneista tiedoista voi olla mahdollista suorasti tai epäsuorasti, mutta se voi myös riippua tietoturvaloukkauksen asiayhteydestä ja henkilötietoihin liittyvien tietojen julkisesta saatavuudesta. Tämä koskee erityisesti luottamuksellisuuteen ja käytettävyyteen vaikuttavia tietoturvaloukkauksia.

Kuten edellä todettiin, riittävän tasoisella salauksella suojatut henkilötiedot eivät ole sivullisten ymmärrettävissä ilman salausavainta. Lisäksi asianmukaisesti toteutettu pseudonymisoiminen (jolla 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

tietosuoja-asetuksen mukaisen ilmoittamisen yhteydessä. Ks. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fi:PDF

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

Tietoturvaloukkaukseen liittyvien henkilötietojen luonteesta, esimerkiksi tietoryhmistä, riippuen henkilöille mahdollisesti aiheutuva vahinko voi olla erityisen vakava, etenkin jos tietoturvaloukkaus voi johtaa identiteettivarkauteen tai petokseen, fyysisiin vahinkoihin, ahdistukseen, nöyryyttämiseen tai maineen vahingoittumiseen. Jos tietoturvaloukkaus koskee heikossa asemassa olevien henkilöiden henkilötietoja, vahinkoriski saattaa olla suurempi.

Rekisterinpitäjän tieto 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 turvallisesti tuhoamaan saamansa tiedot. Molemmissa tapauksissa vastaanottajaa voidaan pitää ”luotettavana”, koska rekisterinpitäjällä on jatkuva suhde tähän ja se saattaa olla tietoinen vastaanottajan menettelyistä, aiemmasta toiminnasta 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 rekisterinpitäjän tietoturvaloukkauksen jälkeen tekemässä riskinarvioinnissa – 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).

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

- Henkilön erityiset ominaisuudet

Tietoturvaloukkaus voi vaikuttaa henkilötietoihin, jotka koskevat lapsia tai muita heikossa asemassa olevia henkilöitä, jotka saattavat tämän seurauksena olla suuremmassa vaarassa. Saattaa olla myös muita henkilöön liittyviä tekijöitä, jotka voivat vaikuttaa siihen, kuinka suuri tietoturvaloukkauksen vaikutus näihin henkilöihin on.

- Rekisterinpitäjän erityiset ominaisuudet

Rekisterinpitäjän ja sen toiminnan luonne ja rooli saattavat vaikuttaa siihen, kuinka suuri tietoturvaloukkauksen henkilöille aiheuttama riski on. Jos esimerkiksi terveydenhoidon organisaatio käsittelee henkilötietoja, tämä tarkoittaa, että henkilöihin kohdistuu heidän henkilötietojensa vaarantuessa suurempi uhka kuin jos kyseessä olisi jonkin sanomalehden postituslista.

- Niiden henkilöiden määrä, joihin tietoturvaloukkaus vaikuttaa

Tietoturvaloukkaus saattaa koskea vain yhtä tai vain muutamaa henkilöä tai useita tuhansia henkilöitä tai vielä suurempaa joukkoa. Yleisesti voidaan todeta, että mitä useampaa henkilöä tietoturvaloukkaus

koskee, 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 henkilöihin kohdistuvan vaikutuksen todennäköisyys ja vakavuus.

- Yleisiä seikkoja

Arvioidessaan tietoturvaloukkauksesta todennäköisesti aiheutuvaa riskiä rekisterinpitäjän olisi siis 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 esimerkkejä eri tyyppisistä tietoturvaloukkauksista, joihin liittyy korkea riski henkilöille.

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[42].

V. Osoitusvelvollisuus ja rekisterin pitäminen

A. Tietoturvaloukkausten dokumentointi

Riippumatta siitä, onko tietoturvaloukkauksesta ilmoitettava valvontaviranomaiselle, rekisterinpitäjän on dokumentoitava kaikki tietoturvaloukkaukset, sillä 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.”

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 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[43].

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 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.

---

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

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

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 mukaisesti[44] ja käsittelyn lainmukaisuuden täyttämiseksi[45]. Sen on säilytettävä dokumentaatio 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[46] ei sovelleta.

Tietosuojatyöryhmä 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[47]. Jos rekisterinpitäjä taas katsoo, että jokin 34 artiklan 3 kohdan ehdoista täyttyy, sen olisi voitava toimittaa tätä tukeva asianmukainen näyttö.

Jos rekisterinpitäjä ei ilmoita tietoturvaloukkauksesta valvontaviranomaiselle, vaan ilmoittaminen viivästyy, rekisterinpitäjän on voitava esittää viivästymisen perustelut; tätä koskeva dokumentaatio voi auttaa osoittamaan, että ilmoittamisen viivästyminen on perusteltu ja oikeasuhteinen.

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

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

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

B. Tietosuojavastaavan rooli

Rekisterinpitäjällä tai henkilötietojen käsittelijällä voi olla tietosuojavastaava[48] joko 37 artiklan vaatimusten perusteella tai vapaaehtoisesti hyvän käytännön mukaisesti. Yleisen tietosuoja-asetuksen

[44] Ks. 5 artikla.

[45] Ks. 6 artikla ja myös 9 artikla.

[46] Ks. 5 artiklan 1 kohdan e alakohta

[47] Ks. johdanto-osan 85 kappale.

[48] Ks. tietosuojavastaavia koskevat tietosuojatyöryhmän ohjeet, jotka ovat saatavilla verkko-osoitteessa http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

39 artiklassa säädetään useista tietosuojavastaavan pakollisista tehtävistä, mutta sillä ei estetä rekisterinpitäjää osoittamasta tietosuojavastaavalle tarvittaessa muita tehtäviä.

Erityisen merkittävää tietoturvaloukkauksesta ilmoittamisen kannalta on, että tietosuojavastaavan pakollisiin tehtäviin sisältyy 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 33 artiklan 3 kohdan b alakohdassa edellytetään, että rekisterinpitäjä ilmoittaa tietosuojavastaavan nimen ja yhteystiedot tai muun yhteyspisteen.

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.

Näiden seikkojen vuoksi tietosuojavastaavalla olisi oltava keskeinen avustava rooli pyrittäessä ehkäisemään tietoturvaloukkauksia tai niiden valmistelua. Se antaa neuvoja ja valvoo säännösten noudattamista sekä tietoturvaloukkauksen aikana (eli ilmoitettaessa valvontaviranomaiselle) samoin kuin valvontaviranomaisen mahdollisesti myöhemmin suorittaman tutkinnan aikana. Tästä syystä tietosuojatyöryhmä suosittaa, että tietosuojavastaavalle ilmoitetaan viipymättä tietoturvaloukkauksesta ja että se on mukana hallinta- ja ilmoittamisprosessissa koko tietoturvaloukkauksen ajan.

VI. **Muihin säädöksiin perustuvat ilmoittamisvelvollisuudet**

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 vaihdella eri jäsenvaltioissa, mutta seuraavassa on esimerkkejä muihin säädöksiin sisältyvistä ilmoittamisvaatimuksista ja niiden suhteesta yleiseen tietosuoja-asetukseen.

- Asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla (eIDAS-asetus)[49].

eIDAS-asetuksen 19 artiklan 2 kohdassa edellytetään luottamuspalvelujen tarjoajien ilmoittavan valvontaelimelleen tietoturvaloukkauksista ja eheyden häviämisestä, joilla on huomattavia vaikutuksia tarjottuun luottamuspalveluun tai sen puitteissa ylläpidettyihin henkilötietoihin. Jos tällainen tietoturvaloukkaus tai eheyden häviäminen 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)[50].

Verkko- ja tietoturvadirektiivin 14 ja 16 artiklassa edellytetään keskeisten palvelujen tarjoajien ja digitaalisen palvelun tarjoajien ilmoittavan turvapoikkeamista toimivaltaiselle viranomaiselleen. Kuten

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

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

verkko- ja tietoturvadirektiivin johdanto-osan 63 kappaleessa[51] 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 silti ilmoitettava poikkeamista valvontaviranomaiselle, jos ne ovat tai niistä tulee yleisen tietosuoja-asetuksen mukaisia henkilötietojen tietoturvaloukkauksia, poikkeamien ilmoittamista koskevien verkko- ja tietoturvadirektiivin vaatimusten lisäksi.

Esimerkki

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

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

Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien on direktiivin 2002/58/EY puitteissa[52] ilmoitettava tietoturvaloukkauksista toimivaltaisille kansallisille viranomaisille.

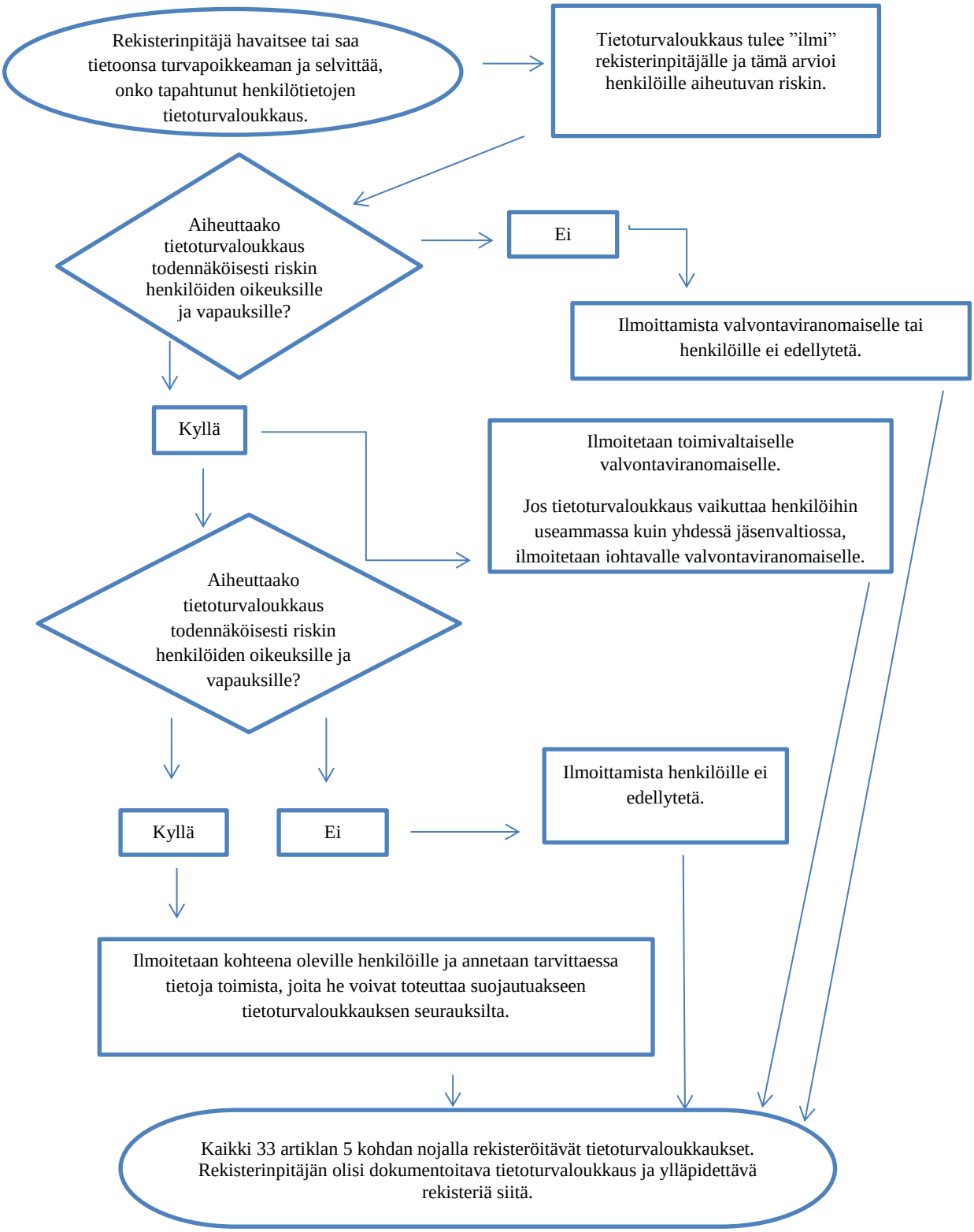
Rekisterinpitäjien olisi oltava tietoisia myös muihin sovellettaviin järjestelmiin perustuvista muista mahdollisista oikeudellisista, lääketieteellisistä tai ammatillisista ilmoittamisvelvollisuuksista.

51 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.”*

52 Euroopan komissio julkaisi 10. tammikuuta 2017 ehdotuksen sähköisen viestinnän tietosuoja-asetukseksi, jolla korvataan direktiivi 2009/136/EY ja poistetaan ilmoittamista koskevat vaatimukset. Nykyiset ilmoittamisvaatimukset pysyvät kuitenkin voimassa, kunnes Euroopan parlamentti on hyväksynyt tämän ehdotuksen, ks. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

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 vai korkea riski.

Esimerkki	**Ilmoitetaanko valvontaviran-omaiselle?**	**Ilmoitetaanko rekisteröi-dylle?**	**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 valvontaviranomai-selle, jos henkilöille todennäköisesti aiheutuu seurauksia.	Kyllä, ilmoitetaan henkilöille kohteena olleiden henkilötietoje n luonteesta riippuen ja jos henkilöille todennäköises ti 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 mahdollisesta tietojen käytettävyyden häviämisestä sekä muista todennäköisistä seurauksista riippuen.	Jos saatavilla oli varmuuskopio ja tiedot pystyttiin palauttamaan nopeasti, turvapoikkeamasta ei tarvitse ilmoittaa valvontaviranomaiselle tai henkilöille, koska käytettävyys tai luottamuksellisuus ei hävinnyt pysyvästi. Jos valvontaviranomainen kuitenkin saa 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 toisen henkilön kuukausittaisen tiliotteen. Rekisterinpitäjä suorittaa lyhyen tutkinnan (joka saatetaan päätökseen 24 tunnin kuluessa) ja selvittää kohtuullisen varmasti, 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 tietoturvalouk kaus 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	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

hyökkäyksen tekijä julkaisee verkossa käyttäjänimiä, salasanoja ja ostohistorioita.			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 verkkosäilytyspalveluja tarjoava yritys havaitsee virheen koodissa, jolla hallitaan käyttövaltuuksia. Vian vaikutuksesta kuka tahansa käyttäjä voi päästä kenen tahansa muun käyttäjän tilin tietoihin.	Henkilötietojen käsittelijänä verkkosäilytyspalvelu ja tarjoavan yrityksen on ilmoitettava viipymättä asiakkailleen (rekisterinpitäjille), joihin vika vaikuttaa. Olettaen, että verkkosäilytyspalve-luja tarjoava yritys on suorittanut oman tutkintansa, kohteena olevilla rekisterinpitäjillä pitäisi olla kohtuullinen varmuus siitä, kohdistuiko tietoturvaloukkaus juuri niihin. Tietoturvaloukkauksen katsotaan todennäköisesti tulleen niiden tietoon, kun verkkosäilytyspalve-luja tarjoava yritys (henkilötietojen käsittelijä) on ilmoittanut niille loukkauksista. Tämän jälkeen rekisterinpitäjän on ilmoitettava	Jos henkilöille ei todennäköi-sesti aiheudu korkeaa riskiä, heille ei tarvitse ilmoittaa.	Verkkosäilytyspalvelu ja tarjoavan yrityksen (henkilötietojen käsittelijän) on otettava huomioon mahdolliset muut ilmoittamis-velvollisuudet (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.

	tietoturvaloukkauk-sesta valvonta-viranomaiselle.		
viii. Sairaalan potilastiedot ovat poissa käytöstä 30 tunnin ajan verkkohyökkäyksen vuoksi.	Kyllä, sairaalalla on velvollisuus ilmoittaa tästä, koska potilaiden hyvinvoinnille ja yksityisyydensuojalle saattaa aiheutua korkea riski.	Kyllä, kohteena oleville henkilöille ilmoitetaan.	
ix. Suuren opiskelijamäärän henkilötiedot lähetetään erehdyksessä väärälle postituslistalle, jolla on yli tuhat vastaanottajaa.	Kyllä, ilmoitetaan valvontaviranomai-selle.	Kyllä, ilmoitetaan henkilöille, asianomaisten henkilötieto-jen laajuudesta ja tyypistä sekä mahdollisten seurausten vakavuudesta riippuen.	
x. Suoramarkkinointisähköpostivie sti lähetetään ”vastaanottaja”- tai ”kopio”-kentissä oleville vastaanottajille, jolloin kaikki vastaanottajat voivat nähdä muiden vastaanottajien sähköpostiosoitteet.	Kyllä, valvontaviranomaisel le 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 henkilötieto-jen laajuudesta ja tyypistä sekä mahdollisten seurausten vakavuudesta riippuen.	Ilmoittaminen ei ehkä ole tarpeen, jos arkaluonteisia tietoja ei paljastu ja jos paljastuneita sähköpostiosoitteita on vain vähän.