TIETOSUOJATYÖRYHMÄ

693/14/FI
WP 213

Lausunto 3/2014 henkilötietojen tietoturvaloukkauksen ilmoittamisesta

Annettu 25. maaliskuuta 2014

Tiivistelmä

Tietosuojatyöryhmä antaa tässä lausunnossa rekisterinpitäjille ohjeita, joiden avulla ne voivat päättää, ilmoittavatko rekisteröidyille ”henkilötietojen tietoturvaloukkauksesta”. Lausunnossa otetaan huomioon direktiiviin 2002/58/EY perustuvat sähköisen viestinnän palveluntarjoajien velvoitteet, mutta siinä annetaan tietosuoja-asetusehdotuksen hengessä esimerkkejä useilta eri aloilta ja esitellään kaikkia rekisterinpitäjiä koskevia hyviä käytäntöjä.

Direktiivin 2002/58/EY mukaan kaikista tietoturvaloukkauksista on ilmoitettava toimivaltaiselle viranomaiselle. Tässä lausunnossa tarkastellaan kuitenkin henkilötietojen tietoturvaloukkauksia, joista on ilmoitettava rekisteröidyille, ja kerrotaan, mitä rekisterinpitäjä olisi voinut järjestelmässään tehdä estääkseen henkilötietojen tietoturvaloukkauksen alun alkaenkin tai millä toimenpiteillä rekisterinpitäjä olisi voinut vapautua velvollisuudestaan ilmoittaa asiasta rekisteröidyille.

Lausunnossa vastataan myös keskeisimpiin henkilötietojen tietoturvaloukkauksia ja direktiivin 2002/58/EY soveltamista koskeviin kysymyksiin.

1. Johdanto

Direktiivin 2002/58/EY 2 artiklan i kohdan mukaan ’henkilötietojen tietoturvaloukkauksella’ tarkoitetaan ”tietoturvaloukkausta, joka johtaa yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamisen yhteydessä yhteisössä siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvaan tai laittomaan tuhoamiseen, häviämiseen, muuttamiseen, luvattomaan luovuttamiseen tai käyttöön antamiseen”.

Direktiivin 2002/58/EY (ja ehdotetun EU:n tietosuoja-asetuksen) mukaan henkilötietojen tietoturvaloukkauksesta on ilmoitettava toimivaltaiselle kansalliselle viranomaiselle. Ilmoituksessa annettavista tiedoista säädetään tarkemmin asetuksen (EU) N:o 611/2013 liitteessä I.

Kun henkilötietojen tietoturvaloukkauksella on todennäköisiä haittavaikutuksia rekisteröidyn[1] henkilötiedoille tai yksityisyydelle, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta myös rekisteröidylle ilman aiheetonta viivästystä[2].

Sekä direktiivissä 2002/58/EY että asetuksessa (EU) N:o 611/2013 säädetään ilmoitusvelvollisuutta koskevasta poikkeuksesta, jonka mukaan rekisteröidylle ei tarvitse ilmoittaa, jos tiedot on saatettu sellaiseen muotoon, että ne eivät ole ymmärrettävissä. Ilmoitusta henkilötietojen tietoturvaloukkauksesta rekisteröidylle ei vaadita[3], jos palveluntarjoaja on osoittanut toimivaltaista viranomaista tyydyttävällä tavalla, että se on toteuttanut asianmukaisia teknisiä toimenpiteitä tietojen muuttamiseksi sellaiseen muotoon, etteivät ne ole ymmärrettävissä henkilöille, joilla ei ole lupaa päästä tietoihin[4], ja jos kyseisiä toimenpiteitä sovellettiin tietoturvaloukkauksen kohteena olevaan tietoon.

Poikkeus velvollisuudesta ilmoittaa yksityishenkilöille perustuu siihen, että rekisteröidyn yksityisyyteen kohdistuva riski voidaan asianmukaisilla toimenpiteillä pienentää merkityksettömän alhaiseksi. Henkilötietojen luottamuksellisuuden vaarantava tietoturvaloukkaus on henkilötietojen tietoturvaloukkaus, vaikka tiedot olisi suojattu uusimman tekniikan mukaisella algoritmilla, ja se on ilmoitettava viranomaiselle. Jos salauksessa käytetyn avaimen luottamuksellisuus ei kuitenkaan ole vaarantunut, tiedot ovat periaatteessa sellaisessa muodossa, etteivät ne ole sellaisten henkilöiden ymmärrettävissä, jolla ei ole lupaa päästä tietoihin. Tällöin tietoturvaloukkaus ei todennäköisesti vaikuta rekisteröityyn haitallisesti, eikä sitä siksi tarvitse ilmoittaa rekisteröidylle itselleen.

Vaikka tiedot olisi salattu, niiden katoamisesta tai muuttamisesta voi aiheutua rekisteröidyille haittaa, jos rekisterinpitäjällä ei ole riittäviä varmuuskopioita. Tällaisissa tilanteissa

[1] Termiä ’rekisteröity’ käytetään tässä lausunnossa direktiivissä 95/46/EY annetun määritelmän mukaisesti. Määritelmä vastaa direktiivissä 2002/58/EY käytettyä ilmaisua ’tilaaja tai henkilö’.

[2] Direktiivin 2002/58/EY ja asetuksen (EU) N:o 611/2013 mukaan henkilötietojen tietoturvaloukkauksesta on ilmoitettava viranomaiselle 24 tunnin kuluessa sen havaitsemisesta, kun tämä on käytännössä mahdollista. Joissakin tapauksissa aikarajaa voidaan pidentää 72 tuntiin. Tilaajalle tai henkilölle ilmoitus on annettava ilman aiheetonta viivytystä (asetuksen (EU) N:o 611/2013 2 artiklan 2 kohdan mukaisesti) henkilötietojen tietoturvaloukkauksen havaitsemisen jälkeen. Rekisteröidylle tehtävä ilmoitus ei saa olla riippuvainen tietoturvaloukkauksen ilmoittamisesta toimivaltaiselle kansalliselle viranomaiselle.

[3] Huomaa, että jos salausavain myöhemmin vaarantuu, palveluntarjoajan on ilmoitettava kaikki aiemmat tietoturvaloukkaukset, jotka on jätetty ilmoittamatta kyseisen avaimen salassa pysymisen perusteella.

[4] Direktiivin 2002/58/EY 4 artiklan 3 kohta; asetuksen (EU) N:o 611/2013 4 artiklan 1 kohta; yleinen tietosuoja-asetus, esittelijän kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnan äänestyksen jälkeen toimittama epävirallinen konsolidoitu versio, 32 artiklan 3 kohta.

rekisteröidyille tehtävää ilmoitusta olisi vaadittava silloinkin, kun tiedot on suojattu salauksen avulla.

Edellä esitetyn vuoksi rekisterinpitäjien on hyvä toimia ennakoivasti ja suunnitella toimiaan tarkoituksenmukaisesti. Direktiivin 95/46/EY 17 artiklassa ja direktiivin 2002/58/EY 4 artiklan 1 ja 1 a kohdassa säädetään, että rekisterinpitäjien on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla on ”taattava asianmukainen turvallisuuden taso suhteessa käsittelyn riskeihin”. Tämän vuoksi on tärkeää luoda asianmukainen riskinhallinnan kehys, joka sisältää toimintatavan edellyttämät vähimmäisosatekijät ja vastaa rekisterinpitäjän määrittelemien asianmukaisten teknisten ja organisatoristen suojakeinojen vähimmäisvaatimuksia. Kehyksessä olisi keskityttävä erityisesti suojakeinoihin, joilla tiedot voidaan tarvittaessa muuttaa sellaiseen muotoon, etteivät ne ole ymmärrettävissä. Yritysten olisi myös etukäteen laadittava henkilötietojen tietoturvaloukkausten varalta asianmukaiset suunnitelmat, joiden avulla ne voivat reagoida henkilötietojen tietoturvaloukkauksiin nopeasti ja tehokkaasti.

Jos 17 artiklaa on noudatettu asianmukaisesti eli ennen tietojen käsittelyn aloittamista, henkilötietojen tietoturvaloukkaukseen liittyvät riskit on otettu huomioon ja niitä on vähennetty jo etukäteen. Tämä voi vähentää henkilötietojen tietoturvaloukkauksia ja niistä rekisteröidyille aiheutuvia seurauksia. Koska rekisteröidyille tehtäviä ilmoituksia ei vaadita tapauksissa, joissa tietoturvaloukkauksella ei ole haittavaikutuksia rekisteröityjen henkilötiedoille tai yksityisyydelle taikka joissa tietoturvaloukkauksen kohteena olevaan tietoon on sovellettu asianmukaisia teknisiä suojatoimenpiteitä, paras tapa välttää rekisteröidyille ilmoittaminen on toteuttaa henkilötietojen käsittelyä sisältävissä hankkeissa asianmukaiset toimenpiteet yksityisyyden suojaamiseksi.

Ilmoitukset on annettava rekisteröidyille ilman aiheetonta viivästystä[5], eikä ilmoituksen antaminen saa olla riippuvainen henkilötietojen tietoturvaloukkauksen ilmoittamisesta toimivaltaiselle kansalliselle viranomaiselle. Vaikkei se olekaan peruste rekisterinpitäjän päätökselle ilmoittaa henkilöille, rekisterinpitäjän on hyvä pitää mielessä, että yksi ilmoittamisen tärkeimmistä hyödyistä on, että rekisteröidyt saavat tarvitsemansa tiedot voidakseen ehkäistä tietoturvaloukkauksesta aiheutuvia haittavaikutuksia. Jos rekisterinpitäjä ei ole varma, onko todennäköistä, että rekisteröityjen henkilötiedoille tai yksityisyydelle aiheutuu haittavaikutuksia, asiasta kannattaa ilmoittaa varmuuden vuoksi. On myös syytä ottaa huomioon, että toimivaltaiset viranomaiset voivat ilmoitusta tarkemmin arvioituaan pyytää rekisterinpitäjää ilmoittamaan henkilöille.

Tässä lausunnossa esitetään **esimerkkejä tilanteista, joissa rekisteröidyille olisi annettava ilmoitus[6]**. Esimerkkiluettelo **ei ole tyhjentävä**. Kutakin henkilötietojen tietoturvaloukkausta tarkastellaan kolmen klassisen turvallisuuskriteerin perusteella: näin ollen ’tietojen käytettävyyteen vaikuttava tietoturvaloukkaus’ vastaa henkilötietojen tahatonta tai laitonta tuhoamista tai kadottamista, ’tietojen eheyteen vaikuttava tietoturvaloukkaus’ henkilötietojen muuttamista ja ’tietojen luottamuksellisuuteen vaikuttava tietoturvaloukkaus’ henkilötietojen

[5] Direktiivin 2002/58/EY ja asetuksen (EU) N:o 611/2013 mukaan henkilötietojen tietoturvaloukkauksesta on ilmoitettava viranomaiselle 24 tunnin kuluessa sen havaitsemisesta, kun tämä on käytännössä mahdollista. Joissakin tapauksissa aikarajaa voidaan pidentää 72 tuntiin. Tilaajalle tai henkilölle ilmoitus on annettava ilman aiheetonta viivästystä henkilötietojen tietoturvaloukkauksen havaitsemisen jälkeen.

[6] Koska tietosuojaa koskevassa asetusehdotuksessa ilmoitusvelvollisuus on yleistetty koskemaan kaikkia aloja ja koska useissa jäsenvaltioissa on jo voimassa lakisääteinen ilmoitusvelvollisuus, ei tässä lausunnossa käsiteltäviä esimerkkejä ole rajattu koskemaan yksinomaan sähköisen viestinnän alaa.

luvatonta luovuttamista tai käyttöön antamista. Tämän lisäksi lausunnossa annetaan **yleisiä ohjeita** tapauksista, joissa ilmoitusta ei tarvitse antaa. Lopuksi lausunnossa **käsitellään keskeisimpiä ongelmia**, joihin rekisterinpitäjät saattavat törmätä harkitessaan, ilmoittavatko rekisteröidyille vai eivät.

2. Tietoturvaloukkaukset, joista saattaa aiheutua rekisteröidyille haittavaikutuksia

Tietoturvaloukkauksista on ilmoitettava rekisteröidyille ilman aiheetonta viivästystä, jos niillä on todennäköisiä haittavaikutuksia henkilötiedoille tai yksityisyydelle. Tässä osiossa annetaan esimerkkejä tietoturvaloukkauksista, joissa ehto toteutuu. Osiossa annetaan myös esimerkkejä teknisistä toimenpiteistä, joiden avulla rekisteröidyille ilmoittaminen olisi voitu välttää, jos toimenpiteet olisi toteutettu ennen tapauksen sattumista.

Esimerkki 1. *Lastensairaalasta varastettiin neljä kannettavaa tietokonetta, joihin oli tallennettu 2 050 lapsen arkaluonteisia terveystietoja, sosiaalihuollon tietoja ja muita henkilötietoja.*

Tämä henkilötietojen tietoturvaloukkaus koskee tietojen luottamuksellisuutta sekä niiden käytettävyyttä ja eheyttä (jos rekisterinpitäjän käytettävissä ei ollut varmuuskopioita).

Tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Tietoturvaloukkauksen ensimmäinen vaikutus on terveydenhuollon vaitiolovelvollisuuden rikkoutuminen: tietokanta sisältää lasten henkilökohtaisia terveystietoja, jotka ovat nyt joutuneet sellaisten henkilöiden käsiin, joilla ei ole lupaa päästä tietoihin.
- Tietojen julkaiseminen voi vaikuttaa lasten koulu- ja/tai perheoloihin (esimerkiksi väkivaltaa, pitkäaikaissairauksia, mielenterveysongelmia taikka perheen sosiaalisia tai taloudellisia ongelmia koskevat tiedot).
- Tapaus voi vaikuttaa lapsiin ja heidän vanhempiinsa henkisesti.
- Tietoja voidaan käyttää vanhempien ja lasten kiristämiseen (riippuen lasten iästä).
- Vaikeasti sairaiden lasten vanhemmat voivat joutua sellaisten tahojen kohteiksi, jotka pyrkivät hyötymään heidän vaikeuksistaan (esimerkiksi huijarit ja lahkot).

Tietojen käytettävyyteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Tietoturvaloukkaus saattaa haitata lapsen hoidon jatkuvuutta ja johtaa sairauden pahentumiseen tai uusiutumiseen.
- Tietoturvaloukkaus voi johtaa lääkeaineallergiasta tai lääkkeiden yhteensopimattomuudesta johtuvaan tahattomaan myrkytykseen, joka voi aiheuttaa erilaisia terveysongelmia tai kuoleman.
- Tietoturvaloukkaus voi aiheuttaa aiheetonta viivästystä korvausten tai taloudellisen tuen maksamisessa rekisteröidyille, mikä vaikuttaisi kyseisten perheiden taloudelliseen tilanteeseen.

Tietojen eheyteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Tietojen katoaminen voi vaikuttaa potilastietojen eheyteen ja haitata lasten hoitamista. Jos esimerkiksi potilastiedoista on saatavilla vain vanha varmuuskopio, kaikki tietoihin varastetuilla tietokoneilla tehdyt muutokset menetetään ja tietojen eheys turmeltuu. Vanhentuneiden potilastietojen käyttö saattaa vaarantaa lasten hoidon jatkuvuuden, mikä voi johtaa sairauden pahentumiseen tai uusiutumiseen.

Mahdollisten vaikutusten vuoksi kyseisessä tapauksessa olisi annettava ilmoitus. Tilanteessa on kuitenkin otettava huomioon myös rekisteröityjen ikä ja kypsyysaste. Voisi olla sopivampaa ilmoittaa asiasta lapsen hoitoon aktiivisesti osallistuvalle vanhemmalle tai edunvalvojalle sen lisäksi, että asiasta ilmoitetaan lapselle itselleen, jos se on asianmukaista tai jos sitä edellytetään soveltuvassa lainsäädännössä.

Ilmoituksen saaneet vanhemmat voivat ilmoittaa poikkeavuuksista lapsen hoidossa, tarkistaa laitoksen tiedossa olevat allergiat tai pyytää uusia kokeita varmistaakseen, että lapset saavat oikeaa hoitoa. Vanhemmat voivat halutessaan kertoa lasten tilasta myös suoraan muille henkilöille hallitakseen lapsen ympäristöön kohdistuvia vaikutuksia.

Esimerkkejä etukäteen toteutettavista suojatoimenpiteistä, joilla riskejä olisi mahdollisesti voitu pienentää:

- Tietojen käytettävyyteen ja eheyteen vaikuttava tietoturvaloukkaus olisi voitu estää tai sen seurauksia ja haittavaikutuksia pienentää huolehtimalla, että käytettävissä on riittävän ajantasainen ja suojattu varmuuskopio.
- Tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdollisia seurauksia ja haittavaikutuksia olisi voitu pienentää suojaamalla tiedot soveltuvalla salausmenetelmällä, jossa on riittävän vahva ja salainen avain.

Jos nämä suojatoimenpiteet olisi toteutettu ja ne olisivat säilyneet turvattuina (eli avain olisi pysynyt salassa ja varmuuskopio käytettävissä), ei asianomaisille henkilöille olisi periaatteessa tarvinnut ilmoittaa asiasta. Suojatoimenpiteiden toteuttaminen olisi osoitettava toimivaltaista viranomaista tyydyttävällä tavalla.

Esimerkki 2. *Henkivakuutusyhtiön asiakkaiden henkilötietoihin päästiin luvatta käsiksi hyödyntämällä verkkosovelluksessa ollutta haavoittuvuutta. Tiedot sisälsivät rekisteröityjen nimet, osoitteet ja heidän täyttämänsä terveystietolomakkeet. Tietoturvaloukkaus koski 700:aa rekisteröityä.*

Tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Hyökkäyksen tekijän internetissä julkaisemat tiedot voivat vaikuttaa rekisteröityjen työnsaantimahdollisuuksiin (esimerkiksi terveysongelmia tai raskautta koskevat vastaukset).
- Tietoturvaloukkaus saattaa vaikuttaa rekisteröityjen työ- ja/tai perheoloihin.
- Tietoturvaloukkauksella saattaa olla myös henkisiä vaikutuksia, jos rekisteröidyt pyrkivät salaamaan diagnosoidun vaivansa.

- Tietoturvaloukkaus voi johtaa henkilötietopetoksiin.
- Tietoja (esimerkiksi asiakkuuksista tai tiettyjen palvelujen ostamisesta) voidaan hyödyntää verkkourkinnassa.

Koska tapauksesta todennäköisesti koituu rekisteröidyille haittavaikutuksia, siitä olisi ilmoitettava heille.

Esimerkkejä etukäteen toteutettavista suojatoimenpiteistä, joilla riskejä olisi mahdollisesti voitu pienentää:

- Tietoturvaloukkaus olisi voitu estää tai sen vaikutuksia pienentää seuraamalla säännöllisesti, onko käytettävässä tekniikassa haavoittuvuuksia, esimerkiksi tarkastamalla verkkosivusto säännöllisesti haavoittuvuuksien varalta ja päivittämällä ohjelmistot (tietoturvaohjelmisto mukaan lukien).

  Vaikka nollapäivän aukkoa hyödyntävistä haittakoodeista aiheutuvia tietoturvahaavoittuvuuksia on vaikea välttää, riskimarginaali voidaan saada hyväksyttävälle tasolle ehkäisemällä tietoturva-aukkojen hyödyntämistä riittävillä ja tehokkailla ennakoivilla toimilla, kuten koodin katselmoinnilla. Tietoturvaloukkauksesta aiheutuvia seurauksia voidaan vähentää myös hyvällä tietoturvaloukkausten hallintajärjestelmällä, jolla voidaan rajoittaa haittavaikutusten vaikutusaikaa ja laajuutta.
- Edellisen esimerkin tapaan tietojen luottamuksellisuutta koskevan tietoturvaloukkauksen mahdollisia seurauksia ja haittavaikutuksia olisi voitu pienentää suojaamalla asiakkaiden tiedot soveltuvalla salausmenetelmällä, jossa on riittävän vahva ja salainen avain. Tämä voisi olla tehokas suojatoimi erityisesti kiintolevyvarkauksien tai muiden vastaavien tilanteiden varalta.

- Vakuutusyhtiö olisi voinut käyttää erilaisia yksityisyyden suojaa parantavia menetelmiä minimoidakseen rekisteröityjä koskevien tietojen määrän ja/tai rekisteröityjen tunnistamismahdollisuudet. Yritys olisi esimerkiksi voinut lähettää asiakkailleen postitse satunnaiset tunnisteet verkossa olevan terveystietolomakkeen täyttämistä varten. Tällöin verkkolomakkeessa ei olisi tarvinnut kysyä nimeä, osoitetta, syntymäaikaa tai puhelinnumeroa.

Esimerkki 3. *Internetpalveluntarjoajan työntekijä on antanut sivulliselle sellaisen tilin käyttäjätunnuksen ja salasanan, jolla on käyttöoikeus koko asiakastietokantaan. Tilin avulla sivullinen voi päästä käsiksi kaikkiin asiakastietoihin täysin rajoituksetta. Tietokantaan on tallennettu asiakkaan nimi, osoite, sähköpostiosoite, puhelinnumerot ja muita tunnistetietoja (kuten käyttäjätunnus, salasanojen tiivisteet ja asiakastunnus) ja maksutiedot (esimerkiksi tilinumero ja luottokorttitiedot). Vaikka maksutiedot oli salattu uusimman tekniikan mukaisella algoritmilla, tietoturvaloukkauksessa hyödynnetyllä pääkäyttäjätilillä oli pääsy algoritmiin, joten niihin pääsi käsiksi myös sivullinen. Yrityksellä on yli 100 000 asiakasta.*

Tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Maksutietojen (etenkin luottokorttitietojen) väärinkäyttö aiheuttaisi asiakkaille taloudellisia seurauksia.

- Koska salasanojen tiivistämiseen käytetty menetelmä oli yksinkertainen, sivullinen voi helposti päätellä tiivistettä vastaavan selkokielisen tekstin. Tällöin kenen tahansa asiakkaan tiliä voitaisiin käyttää myös tietoturvaloukkauksessa käytetyn käyttäjätilin sulkemisen jälkeen.
- Sivullinen voisi helposti käyttää rekisteröityjen sähköpostiosoitteita ja salasanoja päästäkseen muihin verkkopalveluihin, sillä monet käyttävät samaa salasanaa useissa eri palveluissa.

Tietojen eheyteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Sivullisella oli pääsy koko tietokantaan, joten hän olisi voinut muokata, poistaa tai lisätä tileihin liittyviä tietoja.
    - Jos internetpalveluntarjoajan palveluun kuuluu sähköposti- tai verkkoisännöintipalvelu, sivullinen voisi päästä käsiksi sisältöön ja muokata tai poistaa sitä, muuttaa nimipalveluasetuksia tai lopettaa rekisteröidyn tilin.

Vaikka taloudelliset tiedot oli salattu, sivullinen pääsi käyttöliittymän kautta käsiksi salaamattomiin tietoihin. Tämän vuoksi ilmoittamisvelvollisuudesta ei voida poiketa.

Jos suojatut lokitiedostot ovat luotettavia (eli eivät ole vaarantuneet) ja jos lokitiedostoista voidaan nähdä, ettei kyseiseltä tililtä ole käytetty asiakastietokantaa, ei rekisteröidyille ilmoittamisen tulisi olla pakollista.

Kaikissa muissa tilanteissa tapauksesta olisi kuitenkin ilmoitettava asianomaisille asiakkaille, sillä kyseisellä tapauksella on todennäköisesti haittavaikutuksia rekisteröidyille eikä ilmoitusvelvollisuutta koskeva poikkeus siten päde.

Jos salasanat ovat vaarantuneet, rekisterinpitäjän olisi pakotettava rekisteröidyt suojatulla menetelmällä luomaan uusi salasana ja varmistettava, että kaikki uudet salasanat ovat oikeiden käyttäjien eikä heidän kirjautumistietonsa saaneiden sivullisten luomia. Käytännössä menettely voi vastata unohtuneen salasanan korvaamisessa käytettävää suojattua menetelmää, ja siinä olisi kerrottava myös salasanan uusimisen syy. Käyttäjälle lähetettävässä ilmoituksessa olisi myös suositeltava, ettei käyttäjä käytä uudelleen aiemmin käyttämäänsä salasanaa tai samankaltaista salasanaa ja että hän muuttaisi vaarantuneen salasanan myös kaikissa muissa käyttäjätileissään, joissa on käyttänyt samaa salasanaa.

Esimerkkejä etukäteen toteutettavista suojatoimenpiteistä, joilla riskejä olisi mahdollisesti voitu pienentää:

- Kullekin henkilölle on osoitettava oma tili, ja lupa henkilötietojen käsittelyyn olisi annettava ainoastaan tiedonsaantitarpeen ja pienimmän valtuuden periaatteen perusteella. Tämä koskee myös myyjiä, ulkopuolista huoltohenkilöstöä ja muita, joiden on väliaikaisesti päästävä käyttämään tietokantaa: heille tulisi antaa pääsy ainoastaan siihen toimintoon ja niihin tietoihin, joita he tarvitsevat tehtäviensä suorittamiseen, eikä luvan tulisi olla voimassa kauempaa kuin on tarpeen. Sellaisten tilien käyttöä, joilla on käyttöoikeus koko tietokantaan, olisi rajoitettava, ja käytössä olisi oltava menetelmiä, joilla kyseisten tilien käyttöä voidaan jäljittää ja rajoittaa. Tällaisilla suojatoimenpiteillä tietoturvaloukkaus olisi voitu ehkäistä tai sen vaikutuksia hillitä.

- Jos salasanat olisi tallennettu turvallisesti (esimerkiksi suolaamalla ja käyttämällä kryptografista tiivistefunktiota), olisi henkilöille aiheutuvia toissijaisia haittavaikutuksia voitu vähentää merkittävästi. Heikkojen salasanojen käyttäjät olisivat silti vaarassa etenkin, jos he käyttävät samoja kirjautumistunnuksia myös muissa verkkopalveluissa. Heidän altistumistaan olisi voitu pienentää kehottamalla heitä valitsemaan vahvempi salasana.

Esimerkki 4. *Luottokorttikuitteja sisältävä kirjekuori oli turvallisen tuhoamisen sijaan vahingossa heitetty tavalliseen roskakoriin. Roskakori tyhjennettiin ulkona olevaan suurempaan jäteastiaan. Joku poimi kirjekuoren suuresta jäteastiasta ja levitteli kuitteja ympäri läheistä asuinaluetta. Kuiteissa näkyivät täydet luottokorttitiedot[7] ja kortin haltijan nimi. Osassa kuiteista oli myös haltijan allekirjoitus. Tietoturvaloukkaus koski 800:aa rekisteröityä.*

Tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Tietoturvaloukkauksesta voi aiheutua rekisteröidyille taloudellisia vaikutuksia, jos heidän korttinsa ovat yhä voimassa ja niitä käytetään väärin[8].

Koska tapauksella on todennäköisiä haittavaikutuksia rekisteröidyille, siitä olisi ilmoitettava heille. Jos esimerkkitilanteessa tietoja ei ole rekisteröity muilla tavoin, asiasta voi olla vaikea ilmoittaa henkilökohtaisesti jokaiselle rekisteröidylle, sillä ei välttämättä ole tiedossa, kenen kuitteja kirjekuoressa oli. Kaupan tulisi ilmoittaa korttimaksupalvelun tarjoajalle, jotta se voi valvoa mahdollisia vilpillisiä maksutapahtumia. Asetuksessa (EU) N:o 611/2013[9] säädetään myös toisesta käytännöllisestä toimintatavasta. Siinä todetaan, että jos palveluntarjoaja ”ei kohtuullisin toimin kykene määrittämään 3 kohdassa tarkoitetussa määräajassa kaikkia henkilöitä, joihin henkilötietojen tietoturvaloukkaus todennäköisesti vaikuttaa haitallisesti, palveluntarjoaja voi tiedottaa siitä näille henkilöille suurimmissa kansallisissa tai alueellisissa tiedotusvälineissä kyseisessä määräajassa kyseisissä jäsenvaltioissa julkaistavilla ilmoituksilla”. Jos kaupan asiakaskunta koostuu pääasiassa paikallisesta väestöstä, alueellisessa sanomalehdessä julkaistavaa ilmoitusta voidaan pitää riittävänä toimena. Asiasta kannattaisi ilmoittaa myös luottokorttiyhtiöille, jotta ne voisivat paremmin suojella asiakkaitaan.

Jos rekisterinpitäjä olisi saanut pelastettua kirjekuoren jommastakummasta roska-astiasta tai jos kuorta ei jostakin muusta syystä olisi avattu, tapaus ei todennäköisesti olisi vaikuttanut rekisteröityihin haitallisesti eikä siitä siten olisi tarvinnut ilmoittaa heille.

Esimerkkejä etukäteen toteutettavista suojatoimenpiteistä, joilla riskejä olisi mahdollisesti voitu pienentää:

- Tietoturvaloukkauksen mahdollisuutta olisi voitu pienentää merkittävästi kertomalla työntekijöille kyseisenlaisten tietoturvaloukkausten mahdollisista

[7] Vaikka on hyvän käytännön mukaista jättää asiakkaan kuitista pois osa maksukortin tiedoista, se ei ole mahdollista kaikissa maksupäätteissä. Siksi tiedot saattavat näkyä kauppakuiteissa kokonaisuudessaan.
[8] Koska luottokorttitietoja voi yhä hyödyntää myös ilman CVV-turvakoodia (tai vastaavia tunnisteita), on tietoturvaloukkaus ilmoitettava, vaikka se ei koskisikaan CVV-koodeja.
[9] Vaikka tilanne ei kuulukaan asetuksen soveltamisalaan.

seurauksista ja käyttämällä luottokorttikuittien (ja muiden vastaavien henkilötietoja sisältävien asiakirjojen) tuhoamiseen asianmukaista toimistokäyttöön tarkoitettua silppuria[10] tai arkistojen tuhoamispalvelua ennen niiden viemistä roskiin.

- Sellaisen maksupäätteen käyttäminen, joka ei sisällytä kuittiin luottokorttitietoja kokonaisuudessaan.

Esimerkki 5. *Rahoitusneuvojan salausmenetelmällä suojattu kannettava tietokone on varastettu auton tavaratilasta. Tapaus koski 1 000 rekisteröidyn kaikkia esimerkiksi kiinnelainoja, palkkoja ja lainahakemuksia koskevien taloudellisten arviointien tietoja. Salausavain eli salalause ei ole vaarantunut, mutta tiedoista ei ole varmuuskopiota.*

Tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Tietoturvaloukkauksen kohteena olleiden tietojen tarkasta luonteesta riippuen tietojen väärinkäytöstä voi aiheutua rekisteröidyille monia haittavaikutuksia. Koska kannettavan tietokoneen koko kiintolevy oli salattu (uusimmalla tekniikalla) ja suojattu vahvalla salalauseella, joka ei vaarantunut, ei tilanteessa tapahtunut tietojen luvatonta luovuttamista.

Mahdolliset seuraukset ja haittavaikutukset:

- Koska tiedot eivät ole enää käytettävissä, rekisteröityjen on annettava tarvittavat tiedot uudelleen. Tästä aiheutuu rekisteröidyille lievää haittaa, sillä tietojen antaminen vie aikaa ja saattaa harmittaa.
- Joissakin tapauksissa tietojen menetys saattaa aiheuttaa sen, että rekisteröidyt eivät voi toimittaa tietoja tai hakemuksia määräaikaan mennessä, mistä voi tilanteesta riippuen aiheutua heille toissijaisia vaikutuksia, kuten sakot, tulojen tai odotettujen voittojen menettäminen, tilaisuuden hukkaaminen tai ostosopimuksen irtisanominen.

Koska tiedot katosivat ja tietojen käytettävyyttä koskevan tietoturvaloukkauksen vaikutuksia ei ollut ennaltaehkäisty, henkilötietojen tietoturvaloukkauksella on todennäköisiä haittavaikutuksia rekisteröidyille. Siksi asiasta olisi ilmoitettava kyseisille rekisteröidyille. Sen lisäksi, että ilmoituksessa kerrotaan, että rekisteröityjen on annettava tiedot uudelleen rahoitusneuvojalle, siinä tulisi kertoa myös rekisteröidyille tietoturvaloukkauksesta mahdollisesti aiheutuvista seurauksista ja haittavaikutuksista.

Esimerkkejä etukäteen toteutettavista suojatoimenpiteistä, joilla riskejä olisi mahdollisesti voitu pienentää:

- Tiedot olisi voitu palauttaa, jos käytössä olisi ollut tehokas ja turvallinen varmuuskopioratkaisu. Jos tiedoista olisi ollut ajantasainen varmuuskopio, ei tietoturvaloukkaus olisi vaikuttanut tietojen käytettävyyteen eikä asiasta olisi tarvinnut ilmoittaa.

[10] Esimerkiksi DIN 66399 -luokituksen turvaluokkaan 2 kuuluville paperiasiakirjoille tarkoitettu P-4-turvallisuustason silppuri.

Esimerkki 6. *Matkaviestinverkko-operaattorilla on verkkopalvelu, jossa palvelujen tilaajat voivat kirjautumisen jälkeen tarkastella laskutus- ja tilitietojaan. Operaattori on saanut tietää, että verkkosivuston salasanat sisältävään tietokantaan on tunkeuduttu laittomasti. Sivullinen on päässyt käsiksi käyttäjien tunnistetietoihin (käyttäjänimi ja suolaamattomat MD5-funktiolla tiivistetyt salasanat).*

Tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Sivullinen voi saada salasanat selville ja siten päästä käyttämään kenen tahansa asiakkaan tiliä, sillä hänellä on käytettävissään myös käyttäjätunnukset.
- Koska monet käyttävät samaa käyttäjätunnuksen ja salasanan yhdistelmää useissa eri verkkopalveluissa, sivullinen voi todennäköisesti käyttää myös joidenkin rekisteröityjen muita tilejä, kuten sähköpostitilejä.

Koska salasanojen tiivistämisessä oli käytetty yksinkertaista menetelmää, niiden ei voida katsoa olleen komission asetuksen (EU) N:o 611/2013 4 artiklan 2 kohdan[11] mukaisesti sellaisessa muodossa, etteivät ne ole ymmärrettävissä. Näin ollen rekisteröidyille tehtävää ilmoitusta koskevasta velvollisuudesta ei voida poiketa.

Koska tapauksella on todennäköisiä haittavaikutuksia rekisteröidyille eikä ilmoitusvelvollisuutta koskeva poikkeus päde tapaukseen, siitä olisi ilmoitettava asiakkaille, joihin tietoturvaloukkaus on vaikuttanut. Heitä olisi myös kehotettava selkeästi vaihtamaan salasanansa kaikissa niissä palveluissa, joissa he käyttävät samaa, vaarantunutta salasanaa. Kaikki käyttäjät olisi joka tapauksessa pakotettava vaihtamaan salasanansa palveluun kirjautumisen yhteydessä turvallista menetelmää käyttäen.

Esimerkkejä etukäteen toteutettavista suojatoimenpiteistä, joilla riskejä olisi mahdollisesti voitu pienentää:

- Jos salasanat olisi tallennettu turvallisesti (suolattuina ja kryptografisesti uusimman tekniikan mukaisella tiivistefunktiolla tiivistettyinä sekä salausavaimella tai suolamerkkijonolla suojattuina), olisi henkilöille aiheutuvia haittavaikutuksia voitu vähentää merkittävästi. Heikkojen salasanojen käyttäjät voisivat silti olla vaarassa etenkin, jos he käyttävät samoja kirjautumistunnuksia myös muissa verkkopalveluissa.

[11] Asetuksen 4 artiklan 2 kohdassa säädetään seuraavaa:

Tietojen katsotaan olevan sellaisessa muodossa, etteivät ne ole ymmärrettävissä, jos

a) ne on salattu turvallisesti käyttäen standardoitua algoritmia, salauksen purkamiseen käytetty avain ei ole vaarantunut missään tietoturvaloukkauksessa ja salauksen purkamiseen käytetty avain on muodostettu siten, etteivät henkilöt, joilla ei ole lupa käyttää avainta, voi saada sitä selville käytettävissä olevan teknologian avulla; tai

b) ne on korvattu niiden tiivistearvolla, joka on laskettu standardoitua 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.

Esimerkki 7. *Internetpalveluntarjoajalla on palvelu, jossa tilaajat voivat tarkastella tilitietojaan ja internetin käyttöhistoriaansa, kuten kuukausittaista kaistanleveyttään ja usein käyttämiänsä verkkosivustoja. Verkkosivuston koodausvirheen vuoksi käyttäjien kirjautumistunnuksia ei ollut vahvistettu ja tietoja pääsi käyttämään peukaloimalla URL-osoitteiden sisältämiä tilaajatunnusarvoa koskevia parametreja. Kaikkien asiakkaiden tilitietoihin pääsee käsiksi käymällä läpi peräkkäisiä tilaajatunnuksia.*

Tietojen luottamuksellisuuteen vaikuttavan tietoturvaloukkauksen mahdolliset seuraukset ja haittavaikutukset:

- Tietojen avulla rekisteröidyille voidaan lähettää roskapostia tai soittaa roskapuheluja.
- Tiedot voivat antaa kuvan tilaajan käyttäjäprofiilista ja kertoa yksityiskohtaisesti tämän käyttäytymisestä, mikä voi paljastaa tilaajasta arkaluonteisia tietoja. Tietoturvaloukkaus saattaa vaikuttaa rekisteröityjen työ- ja/tai perheoloihin.

Tietoturvaloukkauksella on asiakkaille todennäköisiä haittavaikutuksia, minkä vuoksi siitä olisi ilmoitettava heille.

Esimerkkejä etukäteen toteutettavista suojatoimenpiteistä, joilla riskejä olisi mahdollisesti voitu pienentää:

- Tietoturvaloukkaus olisi saatettu välttää, jos käytetyn tekniikan mahdollisia haavoittuvuuksia olisi seurattu esimerkissä 2 kuvatulla tavalla ja jos alustaa olisi testattu kehitysvaiheessa ennen sen käyttöönottoa ja koodille olisi tehty katselmointi.

3. Esimerkkitilanteita, joissa ei vaadita ilmoitusta rekisteröidyille

Vaikka henkilötietojen tietoturvaloukkauksesta aiheutuvat seuraukset on arvioitava tapauskohtaisesti, jotta kaikki tekijät voidaan ottaa asianmukaisesti huomioon arvioitaessa henkilöille todennäköisesti aiheutuvia haittavaikutuksia, rekisterinpitäjä voi yleisenä ohjeena ja edellisessä osiossa kuvattujen poikkeusten täydentämiseksi ottaa huomioon, ettei rekisteröidyille tehtävää ilmoitusta vaadita tietyissä erityistapauksissa.

Tällaisia tapauksia ovat esimerkiksi seuraavat:

- Henkilötietojen tietoturvaloukkaus vaikuttaa vain tietojen luottamuksellisuuteen, ja tiedot on salattu turvallisesti käyttäen uusimman tekniikan mukaista algoritmia, salauksen purkamiseen käytetty avain ei ole vaarantunut missään tietoturvaloukkauksessa ja salauksen purkamiseen käytetty avain on muodostettu siten, etteivät henkilöt, joilla ei ole lupa käyttää avainta, voi saada sitä selville käytettävissä olevan teknologian avulla. Kyseisillä toimilla tiedot on muutettu sellaiseen muotoon, että ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin.

- Tiedot, 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.

4. Kysymyksiä ja vastauksia

Milloin henkilöille ei ole pakko antaa ilmoitusta?

- Kun tietoturvaloukkaus ei ole henkilötietojen tietoturvaloukkaus (ks. seuraava kysymys).
- Kun henkilötietojen tietoturvaloukkauksella ei toimivaltaista viranomaista tyydyttävän, tilanteen vakavuutta koskevan arvioinnin perusteella ole todennäköisiä haittavaikutuksia rekisteröidyn henkilötiedoille tai yksityisyydelle.
- Kun palveluntarjoaja on osoittanut toimivaltaista viranomaista tyydyttävällä tavalla, että se on toteuttanut asianmukaisia teknisiä suojatoimenpiteitä ja että kyseisiä toimenpiteitä sovellettiin tietoturvaloukkauksen kohteena olevaan tietoon. Tällaisesta tilanteesta on kyse esimerkiksi silloin, kun (ainoastaan tietojen luottamuksellisuuteen vaikuttava) henkilötietojen tietoturvaloukkaus koskee vain uusimman tekniikan mukaisella algoritmilla salattua tietoa taikka suolauksella tai avaimella suojattua tiivistettyä tietoa, jonka tiivistämisessä on käytetty uusimman tekniikan mukaista tiivistefunktiota, ja kun salaiset avaimet ja suolat eivät ole vaarantuneet.
- Tässä lausunnossa kuvatuista tietoturvaloukkauksista ilmoittaminen on kaikille rekisterinpitäjille hyvä käytäntö, vaikkei ilmoituksen antaminen pakollista olisikaan.

Milloin tietoturvaloukkaus on henkilötietojen tietoturvaloukkaus?

Tietoturvaloukkaus katsotaan henkilötietojen tietoturvaloukkaukseksi, kun se kohdistuu henkilötietoihin, joilla tarkoitetaan direktiivin 95/46/EY 2 artiklan 1 kohdan a alakohdan mukaisesti ”*kaikenlaisia tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä (”rekisteröity”) koskevia tietoja; tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa, erityisesti henkilönumeron taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella*”.

Lausunnossa 4/2007 selitetään, että henkilötiedoilla tarkoitetaan henkilöön liittyviä tietoja: ”henkilö voidaan tunnistaa suoraan nimen perusteella tai epäsuorasti puhelinnumeron, auton rekisterinumeron, sosiaaliturvatunnuksen, passin numeron tai sellaisten merkityksellisten seikkojen yhdistelmän perusteella, joiden avulla hänet voidaan erottaa kaventamalla ryhmää, johon hän kuuluu (esimerkiksi ikä, ammatti tai asuinpaikka)”. Asiasta on saatavilla lisätietoa lausunnosta 4/2007.

Onko todennäköiset toissijaiset vaikutukset otettava huomioon?

Kyllä. Tietoturvaloukkauksesta on ilmoitettava rekisteröidyille, jos sillä on todennäköisiä haittavaikutuksia rekisteröityjen henkilötiedoille tai yksityisyydelle.
Näin ollen kaikki rekisteröidyille aiheutuvat mahdolliset seuraukset ja mahdolliset haittavaikutukset on otettava huomioon.

> ***Esimerkki 1:*** *Musiikkiviihdeyrityksen verkkosivustolle tehdään tietomurto, ja käyttäjätietokanta varastetaan ja julkaistaan internetissä. Vuodetut henkilötiedot sisältävät yrityksen verkkosivustolle rekisteröityneiden käyttäjien nimiä/sukunimiä, tietoja heidän musiikkimieltymyksistään sekä heidän käyttäjätunnuksiaan ja salasanojaan. Tietomurto koski 9 000:ta palvelun käyttäjää.*

Esimerkkitapauksessa tietomurrosta henkilöille aiheutuvat välittömät haittavaikutukset saattavat useimmissa tapauksissa vaikuttaa melko pieniltä (eli musiikkimakua koskevien tietojen vuotaminen) ja saattavat saada miettimään, tarvitseeko rekisteröidyille ilmoittaa. Koska myös salasanat vaarantuivat, rekisterinpitäjän on vaihdettava ne. Salasanojen vaihtamisen yhteydessä käyttäjille on kerrottava, miksi salasana pitää uusia. Koska monet käyttäjät käyttävät samaa salasanaa eri tileissä[12], on myös todennäköistä, että tietoturvaloukkauksen toissijaisena haittavaikutuksena on, että toisen tilin tietojen luottamuksellisuus vaarantuu. Rekisteröidyt voivat minimoida toissijaisia vahinkoja vaihtamalla kaikkien muidenkin tiliensä salasanat. Tämän vuoksi ilmoituksessa tulisi kertoa myös muita tilejä koskevista todennäköisistä haittavaikutuksista, ja siinä olisi siksi myös suositeltava, että rekisteröity käyttäisi eri verkkosivustoilla eri salasanoja ja vaihtaisi kaikkien niiden tilien salasanat, joissa on käyttänyt tietoturvaloukkauksessa vaarantunutta salasanaa.

> ***Esimerkki 2:*** *Toisena esimerkkinä voidaan mainita rikostapaus, jossa erästä henkilöä koskevia todisteita oli tallennettu CD-levylle, joka lähetettiin lakimiehelle kirjattuna kirjeenä. CD kuitenkin katosi matkalla.*

Esimerkkitapauksessa välitön tietoturvaloukkaus koskee tietojen käytettävyyttä. Sillä voi olla asianosaisille vähäinen tai hyvin suuri merkitys riippuen siitä, onko heillä mahdollisuus toteuttaa tarvittavat toimet ajoissa.
Myös toissijainen haittavaikutus on todennäköinen, jos CD on lähetetty ilman asianmukaista suojausta ja tietoihin päästään käsiksi. Henkilö, jolla on pääsy tietoihin, voi esimerkiksi myydä ne toimittajille. Toissijaisella vaikutuksella voi olla hyvinkin suuri merkitys asianosaiselle/asianosaisille.

Jos CD voitaisiin esimerkkitapauksessa lähettää ajoissa uudelleen, olisi henkilöön kohdistuva välitön vaikutus pieni eikä edellyttäisi ilmoitusta asianomaisille. Mahdollisen toissijaisen tietoturvaloukkauksen vaikutus voisi kuitenkin olla hyvin suuri, ja se edellyttäisi ehdottomasti, että kyseisille henkilöille ilmoitettaisiin asiasta.

Jos tapaus koskee vain yhtä henkilöä, onko hänelle ilmoitettava asiasta?

Kyllä. Direktiivissä 2002/58/EY ei säädetä rekisteröityjen vähimmäismäärästä, jota tietoturvaloukkauksen on koskettava, jotta ilmoitusmenettely on aloitettava. Televiestintädirektiivin 3 artiklan 1 kohdassa säädetään seuraavaa: ”*Jos henkilötietojen tietoturvaloukkauksella on todennäköisesti haittavaikutuksia tilaajan tai henkilön henkilötiedoille tai yksityisyydelle, palveluntarjoajan on 2 artiklassa tarkoitetun ilmoituksen lisäksi annettava tietoturvaloukkauksesta ilmoitus myös tilaajalle tai henkilölle.*”

Rekisterinpitäjän velvollisuus antaa ilmoitus riippuu siis todennäköisistä haittavaikutuksista eikä asianomaisten rekisteröityjen määrästä.

[12] Tuoreiden tutkimusten mukaan 55–80 prosenttia internetin käyttäjistä käyttää samaa salasanaa eri käyttäjätileissä.

Miten pitäisi käsitellä tietoja, jotka ovat todennäköisesti julkisia?

Tässä yhteydessä on otettava huomioon kaksi seikkaa:

1. ”Julkinen” voi tarkoittaa käytettävyyden ja saatavuuden eri asteita: tieto voi esimerkiksi olla vapaasti käytettävissä internetissä, vapaasti käytettävissä tilauspalvelussa tai pyynnöstä vapaasti käytettävissä reaalimaailmassa.
   Esimerkiksi Ranskassa vaaliluettelot ovat vaalien aikana esillä kaupungintalon seinällä, kaikkien äänestäjien tai puolueiden saatavilla, mutta laki ei salli luettelojen julkaisemista verkossa.
   Tällöin luettelon sähköisen version lähettäminen vahingossa väärälle äänestäjälle tai luettelon paperiversion hukkaaminen ei olisi tietojen luottamuksellisuuteen vaikuttava tietoturvaloukkaus, mutta luettelon julkaiseminen internetissä olisi, ja siitä pitäisi myös antaa ilmoitus.

2. Jotkin tiedot voivat olla julkisia tiettyjen rekisteröityjen osalta mutta eivät muiden.
   Esimerkiksi sukunimeen perustuva puhelinnumeroluettelo voi sisältää sekä julkisia, puhelinluetteloissa olevia numeroita että salaisia puhelinnumeroita.

Yhteenvetona todettakoon, että jos tietoturvaloukkaus muuttaa tiedon käytettävyyden, saatavuuden tai julkisuuden astetta, se olisi katsottava tietojen luottamuksellisuuteen vaikuttavaksi tietoturvaloukkaukseksi ja siitä olisi annettava ilmoitus (jos tietoturvaloukkauksella on todennäköisiä haittavaikutuksia sen kohteena oleville rekisteröidyille).

Miten ilmoitus tulisi antaa, jos tietoturvaloukkauksen vaikutuspiiriin kuuluvien henkilöiden yhteystiedot ovat puutteelliset tai niitä ei tiedetä?

On mahdollista, että loppukäyttäjään suorassa sopimussuhteessa olevalla palveluntarjoajalla ei ole riittävän yksityiskohtaisia yhteystietoja, jotta se voisi antaa tälle asianmukaisen ilmoituksen. Vaikka ilmoituksen voi antaa myös tiedotusvälineiden kautta, palveluntarjoajalla on silti velvollisuus pyrkiä kaikin kohtuullisin toimin ilmoittamaan asiasta rekisteröidyille henkilökohtaisesti[13].

On palveluntarjoajan velvollisuus jatkaa kohtuullisia toimia ja ottaa käyttöön kaikki kohtuudella vaaditut mekanismit varmistaakseen, että kaikki henkilöt, joihin tietoturvaloukkaus vaikuttaa, saavat tietää siitä. Tämä ei kuitenkaan sulje pois mahdollisuutta pyytää apua muilta palveluntarjoajilta tai rekisterinpitäjiltä, joilla on kyseiset yhteystiedot. Näin ollen neljännessä esimerkissä rekisterinpitäjä, jolla ei ole kaikkien asianosaisten kortinhaltijoiden yhteystietoja, voisi ilmoittaa asiasta maksupalvelujen tarjoajalle, joka voisi helposti ottaa yhteyttä kyseisiin henkilöihin. Muut tapaukset saattavat edellyttää toimivaltaisten viranomaisten yhteistyötä. Viranomaisille on joka tapauksessa ilmoitettava, jos palveluntarjoaja ei voi varmistaa henkilökohtaisten ilmoitusten antamista.

[13] Asetuksen (EU) N:o 611/2013 3 artiklan 7 kohdassa todetaan, että jos palveluntarjoaja ei kohtuullisin toimin kykene määrittämään kaikkia henkilöitä, joihin henkilötietojen tietoturvaloukkaus todennäköisesti vaikuttaa haitallisesti, palveluntarjoaja voi tiedottaa siitä näille henkilöille suurimmissa kansallisissa tai alueellisissa tiedotusvälineissä sovellettavassa määräajassa kyseisissä jäsenvaltioissa julkaistavilla ilmoituksilla. Samassa kohdassa säädetään, että palveluntarjoajan on jatkettava kaikkia kohtuullisia toimia voidakseen yksilöidä kyseiset henkilöt ja ilmoittaa heille mahdollisimman pian.

Tarvitseeko asiasta ilmoittaa myös niille rekisteröidyille, joihin tietoturvaloukkaus ei vaikuta?

Ei, jos voidaan luotettavasti määrittää, keneen tietoturvaloukkaus ei vaikuttanut. Jos esimerkiksi voidaan osoittaa, ettei tietoturvaloukkaus koskenut jotakin rekisteröityjen osajoukkoa, kyseisille rekisteröidyille ei tarvitse ilmoittaa asiasta. Tehdessään päätöstä rekisterinpitäjän on kuitenkin otettava huomioon kaikki todennäköiset haittavaikutukset. Tietoturvaloukkauksen luonteesta riippuen rekisteröidyille voi aiheuttaa huolta myös se, että he eivät saa ilmoitusta.