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 henkilö-tietoja sisältävästä arkistosta USB-muistitikulle. Muistitikku varastetaan tiloihin tehdyn murron yhteydessä.	Ei.	Ei.	Mikäli tiedot on salattu uusimman tekniikan mukaisella algoritmilla, tiedoista on varmuuskopioita, yksilöllinen salaus-avain ei vaarannu ja tiedot voidaan palauttaa ajoissa, tästä tietoturva-loukkauksesta ei välttämättä tarvitse ilmoittaa. Jos tiedot kuitenkin myöhem-min 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 henkilötietojen luonteesta riippuen ja jos henkilöille todennäköisesti aiheutuvien seurausten vakavuus on suuri.	

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

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 tietoturvaloukkauksen kohteena oleville henkilöille ilmoitetaan, jos on olemassa korkea riski ja on selvää, ettei tietoturvaloukkaus vaikuta muihin henkilöihin.	Jos lisätutkinnan jälkeen havaitaan, että tietoturvaloukkaus vaikuttaa useampiin henkilöihin, ilmoitus valvontaviranomaiselle on päivitettävä ja rekisterinpitäjän on ilmoitettava myös kyseisille muille henkilöille, jos näihin kohdistuu korkea riski.

vi. Rekisterinpitäjä ylläpitää sähköistä markkinapaikkaa, ja sillä on asiakkaita useissa jäsenvaltioissa. Markkinapaikkaan tehdään verkkohyökkäys, ja hyökkäyksen tekijä julkaisee verkossa käyttäjänimiä, salasanoja ja ostohistorioita.	Kyllä, ilmoitetaan johtavalle valvontaviranomaiselle, jos asiaan liittyy rajatylittävää tietojenkäsittelyä.	Kyllä, sillä voi aiheutua korkea riski.	Rekisterinpitäjän olisi toteutettava toimia, esimerkiksi vaadittava käyttäjiä uusimaan kohteena olleiden tilien salasanat sekä toteutettava muita toimenpiteitä riskin lieventämiseksi. Rekisterinpitäjän olisi otettava huomioon myös mahdolliset muut ilmoittamisvelvollisuudet, jotka perustuvat esimerkiksi verkko- ja tietoturvadirektiiviin, koska se on digitaalisen palvelun tarjoaja.
vii. Henkilötietojen käsittelijänä toimiva verkkosäilytyspalveluja tarjoava yritys havaitsee virheen koodissa, jolla hallitaan käyttövaltuuksia. Vian vaikutuksesta kuka tahansa käyttäjä voi päästä kenen tahansa muun käyttäjän tilin tietoihin.	Henkilötietojen käsittelijänä verkkosäilytyspalveluja tarjoavan yrityksen on ilmoitettava viipymättä asiakkailleen (rekisterinpitäjille), joihin vika vaikuttaa. Olettaen, että verkkosäilytyspalveluja tarjoava yritys on suorittanut oman tutkintansa, kohteena olevilla rekisterinpitäjillä pitäisi olla kohtuullinen varmuus siitä, kohdistuiko tietoturvaloukkaus juuri niihin. Tietoturvaloukkauksen katsotaan todennäköisesti tulleen niiden tietoon, kun verkkosäilytyspalveluja tarjoava yritys (henkilötietojen käsittelijä) on ilmoittanut niille loukkauksista. Tämän jälkeen rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta	Jos henkilöille ei todennäköisesti aiheudu korkeaa riskiä, heille ei tarvitse ilmoittaa.	Verkkosäilytyspalvelu ja tarjoavan yrityksen (henkilötietojen käsittelijän) on otettava huomioon mahdolliset muut ilmoittamisvelvollisuudet (esimerkiksi verkko- ja tietoturvadirektiivin nojalla, koska se on digitaalisen palvelun tarjoaja). Jos ei ole näyttöä siitä, että jokin rekisterinpitäjistä olisi käyttänyt hyväkseen tätä järjestelmän heikkoutta, ei ehkä ole tapahtunut ilmoitettavaa tietoturvaloukkausta, mutta kyseessä on todennäköisesti rekisteröitävä tietoturvaloukkaus tai 32 artiklan noudattamatta jättäminen.

	valvontaviran-omaiselle.		
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 henkilötietojen laajuudesta ja tyypistä sekä mahdollisten seurausten vakavuudesta riippuen.	
x. Suoramarkkinointisähköposti-viesti lähetetään ”vastaanottaja”- tai ”kopio”-kentissä oleville vastaanottajille, jolloin kaikki vastaanottajat voivat nähdä muiden vastaanottajien sähköpostiosoitteet.	Kyllä, valvontaviran-omaiselle ilmoittami-nen saattaa olla pakollista, jos tämä vaikuttaa suureen määrään henkilöitä, jos paljastetaan arkaluonteisia tietoja (esimerkiksi psyko-terapeutin postitus-lista) tai jos jotkin muut tekijät aiheut-tavat korkeita riskejä (sähköpostiviesti sisältää esimerkiksi kirjautumisessa käytettäviä sala-sanoja).	Kyllä, ilmoitetaan henkilöille, asianomaisten henkilötietojen laajuudesta ja tyypistä sekä mahdollisten seurausten vakavuudesta riippuen.	Ilmoittaminen ei ehkä ole tarpeen, jos arkaluonteisia tietoja ei paljastu ja jos paljastuneita sähkö-postiosoitteita on vain vähän.