ASETUKSET

KOMISSION ASETUS (EU) N:o 611/2013,

annettu 24 päivänä kesäkuuta 2013,

henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY mukaisten henkilötietojen tietoturvaloukkausten ilmoittamiseen sovellettavista toimenpiteistä

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12 päivänä heinäkuuta 2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY ([1]) (sähköisen viestinnän tietosuojadirektiivi)ja erityisesti sen 4 artiklan 5 kohdan,

on kuullut Euroopan verkko- ja tietoturvavirastoa (ENISA),

on kuullut yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY ([2]) 29 artiklalla perustettua tietosuojatyöryhmää (artikla 29 -työryhmä),

on kuullut Euroopan tietosuojavaltuutettua,

sekä katsoo seuraavaa:

(1) Direktiivissä 2002/58/EY säädetään sellaisten kansallisten säännösten yhdenmukaistamisesta, joita tarvitaan samantasoisen perusoikeuksien ja -vapauksien, erityisesti yksityisyyttä ja luottamuksellisuutta koskevan oikeuden, suojan varmistamiseksi henkilötietojen käsittelyssä sähköisen viestinnän alalla sekä tällaisten tietojen ja sähköisten viestintälaitteiden ja -palvelujen vapaan liikkuvuuden varmistamiseksi unionissa.

(2) Direktiivin 2002/58/EY 4 artiklan mukaan yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien on ilmoitettava henkilötietojen tietoturvaloukkauksista toimivaltaisille kansallisille viranomaisille ja eräissä tapauksissa myös niiden kohteeksi joutuneille tilaajille ja henkilöille. Henkilötietojen tietoturvaloukkaukset määritellään direktiivin 2002/58/EY 2 artiklan i alakohdassa tietoturvaloukkauksiksi, jotka johtavat yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamisen yhteydessä unionissa siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvaan tai laittomaan tuhoamiseen, häviämiseen, muuttamiseen, luvattomaan luovuttamiseen tai käyttöön antamiseen.

(3) Direktiivin 2002/58/EY 4 artiklan 2, 3 ja 4 kohdassa tarkoitettujen toimenpiteiden yhdenmukaisen toteuttamisen varmistamiseksi komissio valtuutetaan sen 4 artiklan 5 kohdassa hyväksymään teknisiä täytäntöönpanotoimenpiteitä, jotka koskevat kyseisessä artiklassa tarkoitettuihin tiedotus- ja ilmoitusvaatimuksiin sovellettavia olosuhteita, muotoa ja menettelyjä.

(4) Toisistaan poikkeavat kansalliset vaatimukset voivat tässä yhteydessä aiheuttaa oikeudellista epävarmuutta, monimutkaisempia ja raskaampia menettelyjä ja huomattavia hallinnollisia kustannuksia rajojen yli toimiville palveluntarjoajille. Näistä syistä komissio katsoo tarpeelliseksi hyväksyä tällaisia teknisiä täytäntöönpanotoimenpiteitä.

(5) Tämä asetus rajoittuu henkilötietojen tietoturvaloukkauksista ilmoittamiseen, eikä siinä näin ollen vahvisteta direktiivin 2002/58/EY 4 artiklan 2 kohtaan liittyviä teknisiä täytäntöönpanotoimenpiteitä, jotka koskevat tilaajille ilmoittamista verkon turvallisuuteen kohdistuvista erityisistä riskeistä.

(6) Direktiivin 2002/58/EY 4 artiklan 3 kohdan ensimmäisestä alakohdasta seuraa, että palveluntarjoajien olisi ilmoitettava toimivaltaiselle kansalliselle viranomaiselle kaikista henkilötietojen tietoturvaloukkauksista. Näin ollen päätöstä siitä, ilmoitetaanko henkilötietojen tietoturvaloukkauksesta toimivaltaiselle kansalliselle viranomaiselle, ei saisi jättää palveluntarjoajan omaan harkintavaltaan. Tämä ei kuitenkaan saisi estää kyseistä toimivaltaista kansallista viranomaista priorisoimasta tiettyjen tietoturvaloukkausten tutkintaa tarpeelliseksi katsomallaan tavalla sovellettavan lainsäädännön mukaisesti ja toteuttamasta tarvittavia toimia henkilötietojen tietoturvaloukkauksien ylitai aliraportoinnin välttämiseksi.

(7) Henkilötietojen tietoturvaloukkauksista toimivaltaiselle kansalliselle viranomaiselle tehtäviä ilmoituksia varten on tarkoituksenmukaista säätää järjestelmästä, joka muodostuu tietyin edellytyksin eri vaiheista, joista kullakin on tietty aikaraja. Tämän järjestelmän tarkoituksena on varmistaa, että toimivaltaiselle kansalliselle viranomaiselle ilmoitetaan tietoturvaloukkauksesta mahdollisimman aikaisin ja mahdollisimman tyhjentävästi estämättä kuitenkaan tarpeettomasti palveluntarjoajaa tutkimasta tietoturvaloukkausta ja toteuttamasta tarpeellisia toimenpiteitä tietoturvaloukkauksen rajoittamiseksi ja sen seurausten korjaamiseksi.

([1]) EYVL L 201, 31.7.2002, s. 37.
([2]) EYVL L 281, 23.11.1995, s. 31.

(8) Pelkkä epäily henkilötietojen tietoturvaloukkauksen tapahtumisesta tai pelkkä tietoturvapoikkeaman havaitseminen ilman, että palveluntarjoajan yrityksistä huolimatta käytettävissä on riittäviä tietoja, ei ole riittävä syy katsoa, että tässä asetuksessa tarkoitettu tietoturvaloukkaus on havaittu. Erityistä huomiota olisi tässä yhteydessä kiinnitettävä liitteessä I tarkoitettujen tietojen saatavuuteen.

(9) Asianomaisten toimivaltaisten kansallisten viranomaisten olisi tämän asetuksen soveltamisen yhteydessä tehtävä yhteistyötä sellaisissa tapauksissa, joissa henkilötietojen tietoturvaloukkauksella on rajat ylittävä ulottuvuus.

(10) Tässä asetuksessa ei määritellä tarkemmin henkilötietojen tietoturvaloukkauksien luetteloa, jota palveluntarjoajien on pidettävä yllä, koska sen sisältö määritellään tyhjentävästi direktiivin 2002/58/EY 4 artiklassa. Palveluntarjoajat voivat kuitenkin käyttää tätä asetusta määritellessään luettelon muotoa.

(11) Kaikkien toimivaltaisten kansallisten viranomaisten olisi annettava palveluntarjoajien käyttöön suojattu sähköinen menetelmä henkilötietojen tietoturvaloukkauksista ilmoittamiseen noudattaen yhteistä muotoa, joka perustuu standardiin, kuten XML:ään, ja joka sisältää liitteessä I mainitut tiedot asianomaisilla kielillä, jotta kaikki palveluntarjoajat unionissa voivat noudattaa samanlaista ilmoitusmenettelyä riippumatta siitä, minne ne ovat sijoittautuneet tai missä henkilötietojen tietoturvaloukkaus on tapahtunut. Tähän liittyen komission olisi helpotettava suojatun sähköisen menetelmän käyttöönottoa järjestämällä tarvittaessa kokouksia toimivaltaisten kansallisten viranomaisten kanssa.

(12) Arvioitaessa, onko henkilötietojen tietoturvaloukkauksella todennäköisesti haittavaikutuksia tilaajan tai henkilön henkilötiedoille tai yksityisyydelle, olisi otettava huomioon erityisesti kyseisten henkilötietojen luonne ja sisältö, varsinkin jos tiedot sisältävät taloudellista informaatiota, kuten luottokortti- ja pankkitilitietoja, direktiivin 95/46/EY 8 artiklan 1 kohdassa tarkoitettuihin erityisiin luokkiin kuuluvia tietoja ja tiettyjä tietoja, jotka liittyvät erityisesti puhelin- tai internetpalvelujen tarjoamiseen, kuten sähköpostitiedot, paikannustiedot, internetin lokitiedostot, www-selaushistoriat ja puheluerittelyt.

(13) Poikkeuksellisissa olosuhteissa palveluntarjoajan olisi voitava lykätä tilaajalle tai henkilölle annettavaa ilmoitusta, jos tilaajalle tai yksityishenkilölle ilmoittaminen voi vaarantaa henkilötietojen tietoturvaloukkauksen asianmukaisen tutkimisen. Tässä yhteydessä poikkeuksellisiin olosuhteisiin voivat kuulua myös rikostutkinta sekä muut sellaiset henkilötietojen tietoturvaloukkaukset, jotka eivät ole vakavia rikoksia mutta joiden osalta voi olla tarkoituksenmukaista lykätä ilmoittamista. Toimivaltaisen kansallisen viranomaisen olisi joka tapauksessa arvioitava kunkin tapauksen olosuhteet huomioon ottaen, hyväksytäänkö lykkääminen vai vaaditaanko ilmoitusta.

(14) Palveluntarjoajilla olisi oltava tilaajiensa yhteystiedot suoran sopimussuhteen vuoksi, mutta palveluntarjoajilla ei välttämättä ole näitä tietoja muista henkilöistä, joihin henkilötietojen tietoturvaloukkaus on vaikuttanut haitallisesti. Tällöin palveluntarjoajan olisi voitava aluksi ilmoittaa näille henkilöille suurimmissa kansallisissa tai alueellisissa tiedotusvälineissä, kuten sanomalehdissä, julkaistavilla ilmoituksilla, minkä jälkeen sen olisi annettava mahdollisimman pian henkilökohtainen ilmoitus siten kuin tässä asetuksessa säädetään. Palveluntarjoajalla ei siis ole velvollisuutta julkaista ilmoitusta tiedotusvälineissä, mutta sillä on halutessaan lupa toimia näin, kunnes se on yksilöinyt kaikki henkilöt, joihin tietoturvaloukkaus on vaikuttanut.

(15) Tietoturvaloukkausta koskevat tiedot olisi liitettävä pelkästään tietoturvaloukkauksen asiayhteyteen eikä muita aiheita koskevien tietojen yhteyteen. Esimerkiksi henkilötietojen tietoturvaloukkausta koskevien tietojen antamista tavanomaisen laskun yhteydessä ei saisi pitää asianmukaisena keinona ilmoittaa henkilötietojen tietoturvaloukkauksesta.

(16) Tässä asetuksessa ei säädetä erityisistä teknisistä suojatoimenpiteistä, joiden vuoksi voidaan poiketa velvoitteesta ilmoittaa henkilötietojen tietoturvaloukkauksista tilaajille tai henkilöille, sillä nämä suojatoimenpiteet voivat muuttua ajan myötä teknologian kehityksen myötä. Komission olisi kuitenkin voitava julkaista ohjeellinen luettelo nykykäytännön mukaisista tällaisista erityisistä teknisistä suojatoimenpiteistä.

(17) Salauksen tai tiivistämisen toteuttamista ei saisi pitää itsessään riittävänä, jotta palveluntarjoajat voisivat yleisemmin väittää täyttäneensä direktiivin 95/46/EY 17 artiklassa asetetun yleisen tietoturvavelvoitteen. Palveluntarjoajien olisi tältä osin toteutettava myös riittävät organisatoriset ja tekniset toimenpiteet henkilötietojen tietoturvaloukkausten torjumiseksi, havaitsemiseksi ja estämiseksi. Palveluntarjoajien olisi otettava huomioon mahdollinen suojakeinojen toteuttamisen jälkeinen jäännösriski, jotta voidaan ymmärtää, missä henkilötietojen tietoturvaloukkauksia voi potentiaalisesti esiintyä.

(18) Jos palveluntarjoaja käyttää toista palveluntarjoajaa suorittamaan osan palvelusta esimerkiksi laskutuksessa tai

hallinnossa, tätä toista palveluntarjoajaa, joka ei ole suorassa sopimussuhteessa loppukäyttäjään, ei saisi velvoittaa antamaan ilmoituksia henkilötietojen tietoturvaloukkauksista. Sen sijaan sen olisi varoitettava ja informoitava palveluntarjoajaa, jonka kanssa sillä on suora sopimussuhde. Tämän olisi koskettava myös sähköisten viestintäpalvelujen tukkutarjontaa, jossa tukkupalveluntarjoaja ei yleensä ole suorassa sopimussuhteessa loppukäyttäjään.

(19) Direktiivissä 95/46/EY määritellään yleiset puitteet henkilötietojen suojalle Euroopan unionissa. Komissio on antanut ehdotuksen direktiivin 95/46/EY korvaavasta Euroopan parlamentin ja neuvoston asetuksesta (tietosuoja-asetus). Ehdotetussa tietosuoja-asetuksessa kaikki rekisterinpitäjät velvoitettaisiin ilmoittamaan henkilötietojen tietoturvaloukkauksista direktiivin 2002/58/EY 4 artiklan 3 kohtaan perustuvalla tavalla. Tämä komission asetus on täysin johdonmukainen kyseisen ehdotetun säädöksen kanssa.

(20) Ehdotetussa tietosuoja-asetuksessa direktiiviin 2002/58/EY tehdään myös joitain teknisiä mukautuksia, jotta voidaan ottaa huomioon direktiivin 95/46/EY muuttaminen asetukseksi. Komissio tekee arvioinnin uuden asetuksen aineellisoikeudellisista seurauksista direktiivin 2002/58/EY kannalta.

(21) Tämän asetuksen täytäntöönpanoa olisi tarkasteltava kolme vuotta sen voimaantulon jälkeen, jolloin myös sen sisältöä olisi tarkasteltava uudelleen tuolloin voimassa olevan oikeudellisen kehyksen, muun muassa ehdotetun tietosuoja-asetuksen, perusteella. Tämän asetuksen uudelleentarkastelu olisi mahdollisuuksien mukaan kytkettävä direktiivin 2002/58/EY tuleviin uudelleentarkasteluihin.

(22) Tämän asetuksen täytäntöönpanoa voidaan arvioida muun muassa toimivaltaisten kansallisten viranomaisten niille ilmoitetuista henkilötietojen tietoturvaloukkauksista mahdollisesti pitämien tilastojen pohjalta. Näitä tilastoja voidaan pitää esimerkiksi toimivaltaiselle kansalliselle viranomaiselle ilmoitettujen henkilötietojen tietoturvaloukkauksien määrästä, tilaajalle tai henkilölle ilmoitettujen henkilötietojen tietoturvaloukkauksien määrästä, henkilötietojen tietoturvaloukkauksen ratkaisemiseen kuluneesta ajasta ja siitä, onko käytössä teknisiä suojatoimenpiteitä. Näiden tilastojen olisi annettava komissiolle ja jäsenvaltioille johdonmukaiset ja vertailukelpoiset tilastotiedot nimeämättä ilmoituksen tekevää palveluntarjoajaa ja kyseisiä tilaajia ja yksityishenkilöitä. Komissio voi tätä tarkoitusta varten myös järjestää säännöllisiä kokouksia toimivaltaisten kansallisten viranomaisten ja muiden asiaankuuluvien sidosryhmien kanssa.

(23) Tässä asetuksessa säädetyt toimenpiteet ovat viestintäkomitean lausunnon mukaiset,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

1 artikla

Soveltamisala

Tätä asetusta sovelletaan yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien, jäljempänä 'palveluntarjoaja', suorittamaan henkilötietojen tietoturvaloukkauksista ilmoittamiseen.

2 artikla

Ilmoittaminen toimivaltaiselle kansalliselle viranomaiselle

1. Palveluntarjoajan on ilmoitettava kaikista henkilötietojen tietoturvaloukkauksista toimivaltaiselle kansalliselle viranomaiselle.

2. Palveluntarjoajan on ilmoitettava henkilötietojen tietoturvaloukkauksesta toimivaltaiselle kansalliselle viranomaiselle 24 tunnin kuluessa sen havaitsemisesta, kun tämä on käytännössä mahdollista.

Palveluntarjoajan on annettava toimivaltaiselle kansalliselle viranomaiselle tekemässään ilmoituksessa liitteessä I mainitut tiedot.

Jotta ilmoituksen antaminen tämän asetuksen nojalla olisi mielekästä, henkilötietojen tietoturvaloukkauksen on katsottava tapahtuneen, jos palveluntarjoaja on saanut riittävän tiedon siitä, että on ilmennyt henkilötietojen vaarantumiseen johtanut tietoturvapoikkeama.

3. Jos kaikkia liitteessä I esitettyjä tietoja ei ole saatavilla ja henkilötietojen tietoturvaloukkausta on tutkittava tarkemmin, palveluntarjoaja voi antaa toimivaltaiselle kansalliselle viranomaiselle alustavan ilmoituksen 24 tunnin kuluessa henkilötietojen tietoturvaloukkauksen havaitsemisesta. Tässä toimivaltaiselle kansalliselle viranomaiselle annettavassa alustavassa ilmoituksessa on oltava liitteessä I olevassa 1 jaksossa esitetyt tiedot. Palveluntarjoajan on annettava toimivaltaiselle kansalliselle viranomaiselle täydentävä ilmoitus mahdollisimman pian ja viimeistään kolmen päivän kuluttua alustavasta ilmoituksesta. Tässä täydentävässä ilmoituksessa on oltava liitteessä I olevassa 2 jaksossa esitetyt tiedot, ja siinä on tarpeen mukaan päivitettävä jo annetut tiedot.

Jos palveluntarjoaja ei tutkimuksistaan huolimatta pysty antamaan kaikkia tietoja kolmen päivän kuluessa alustavasta ilmoituksesta, palveluntarjoajan on annettava kyseisessä määräajassa käyttöön saamansa tiedot ja perusteltava toimivaltaiselle kansalliselle viranomaiselle, miksi loput tiedot ilmoitetaan määräajan jälkeen. Palveluntarjoajan on ilmoitettava loput tiedot kansalliselle toimivaltaiselle viranomaiselle ja tarpeen mukaan päivitettävä jo annetut tiedot mahdollisimman pian.

4. Toimivaltaisen kansallisen viranomaisen on annettava kaikkien kyseiseen jäsenvaltioon sijoittautuneiden palveluntarjoajien käyttöön suojattu sähköinen menetelmä, jonka avulla henkilötietojen tietoturvaloukkauksista on ilmoitettava, sekä tiedot sen käyttöönoton ja käytön menettelyistä. Komissio järjestää tarvittaessa toimivaltaisten kansallisten viranomaisten kanssa kokouksia tämän säännöksen täytäntöönpanon helpottamiseksi.

5. Jos henkilötietojen tietoturvaloukkaus vaikuttaa tilaajiin tai henkilöihin muissa jäsenvaltioissa kuin sen toimivaltaisen kansallisen viranomaisen jäsenvaltiossa, jolle henkilötietojen tietoturvaloukkauksesta on ilmoitettu, toimivaltaisen kansallisen viranomaisen on ilmoitettava tästä asianomaisille muille kansallisille viranomaisille.

Tämän säännöksen täytäntöönpanon helpottamiseksi komissio laatii luettelon toimivaltaisista kansallisista viranomaisista ja tarvittavista yhteyspisteistä ja pitää sitä yllä.

3 artikla

Ilmoittaminen tilaajalle tai henkilölle

1. 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.

2. Arvioitaessa sitä, onko henkilötietojen tietoturvaloukkauksella todennäköisesti haittavaikutuksia tilaajan tai henkilön henkilötiedoille tai yksityisyydelle, on otettava huomioon erityisesti seuraavat tekijät:

a) kyseisten henkilötietojen luonne ja sisältö, erityisesti jos tiedot sisältävät taloudellista informaatiota, kuuluvat direktiivin 95/46/EY 8 artiklan 1 kohdassa tarkoitettuihin erityisiin luokkiin tai ovat paikannustietoja, internetin lokitiedostoja, www-selaushistorioita, sähköpostitietoja ja puheluerittelyjä;

b) henkilötietojen tietoturvaloukkauksesta sen kohteeksi joutuneelle tilaajalle tai henkilölle todennäköisesti aiheutuvat seuraukset, erityisesti jos tietoturvaloukkaus voi johtaa henkilöllisyysvarkauteen tai -petokseen, ruumiilliseen tai henkiseen kärsimykseen, nöyryytykseen tai maineen vahingoittumiseen; ja

c) henkilötietojen tietoturvaloukkauksen olosuhteet, erityisesti jos tiedot on varastettu tai jos palveluntarjoaja tietää, että tiedot ovat luvattomasti kolmannen osapuolen hallussa.

3. Ilmoitus on annettava tilaajalle tai yksityishenkilölle ilman aiheetonta viivytystä henkilötietojen tietoturvaloukkauksen havaitsemisen jälkeen siten kuin 2 artiklan 2 kohdan kolmannessa alakohdassa esitetään. Se ei saa olla riippuvainen 2 artiklassa tarkoitetusta henkilötietojen tietoturvaloukkauksen ilmoittamisesta toimivaltaiselle kansalliselle viranomaiselle.

4. Palveluntarjoajan on annettava tilaajalle tai henkilölle tekemässään ilmoituksessa liitteessä II esitetyt tiedot. Tilaajalle tai henkilölle annettava ilmoitus on laadittava selkeällä ja helposti ymmärrettävällä kielellä. Palveluntarjoaja ei saa käyttää ilmoitusta tilaisuutena uusien tai lisäpalvelujen mainontaan tai myynninedistämiseen.

5. Jos tilaajalle tai henkilölle ilmoittaminen voi poikkeuksellisten olosuhteiden vuoksi vaarantaa henkilötietojen tietoturvaloukkauksen asianmukaisen tutkinnan, palveluntarjoaja voi kansallisen toimivaltaisen viranomaisen suostumuksen saatuaan lykätä tilaajalle tai henkilölle annettavaa ilmoitusta, kunnes toimivaltainen kansallinen viranomainen katsoo, että henkilötietojen tietoturvaloukkauksesta voidaan ilmoittaa tämän artiklan mukaisesti.

6. Palveluntarjoajan on ilmoitettava henkilötietojen tietoturvaloukkauksesta tilaajalle tai henkilölle viestintämenetelmillä, jotka takaavat tiedon nopean vastaanottamisen ja jotka on asianmukaisesti suojattu tekniikan nykytason mukaisesti. Tietoturvaloukkausta koskevat tiedot on liitettävä pelkästään tietoturvaloukkauksen asiayhteyteen eikä muita aiheita koskevien tietojen yhteyteen.

7. Jos palveluntarjoaja, joka on suorassa sopimussuhteessa loppukäyttäjään, 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. Näissä ilmoituksissa on oltava liitteessä II esitetyt tiedot, tarvittaessa tiivistetysti esitettyinä. Tässä tapauksessa palveluntarjoajan on jatkettava kaikkia kohtuullisia toimia voidakseen yksilöidä kyseiset henkilöt ja ilmoittaa heille liitteessä II esitetyt tiedot mahdollisimman pian.

4 artikla

Tekniset suojatoimenpiteet

1. Poiketen siitä, mitä 3 artiklan 1 kohdassa säädetään, ilmoitusta henkilötietojen tietoturvaloukkauksesta sen kohteeksi joutuneelle tilaajalle tai henkilölle ei vaadita, jos palveluntarjoaja on osoittanut toimivaltaista kansallista viranomaista tyydyttävällä tavalla, että se on toteuttanut asianmukaiset tekniset suojatoimenpiteet ja että kyseisiä toimenpiteitä sovellettiin tietoturvaloukkauksen kohteena olevaan tietoon. Tällaisten teknisten suojatoimenpiteiden avulla tiedot muutetaan sellaiseen muotoon, että ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin.

2. 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.

3. Kuultuaan toimivaltaisia viranomaisia artikla 29 -työryhmän kautta, Euroopan verkko- ja tietoturvavirastoa ja Euroopan tietosuojavaltuutettua komissio voi julkaista ohjeellisen luettelon 1 kohdassa tarkoitetuista nykyisiin käytäntöihin perustuvista asianmukaisista teknisistä suojatoimenpiteistä.

5 artikla

Toisen palveluntarjoajan käyttö

Jos sähköisen viestintäpalvelun tarjonnassa käytetään alihankkijana toista palveluntarjoajaa, joka ei ole suorassa sopimussuhteessa tilaajiin, tämän toisen palveluntarjoajan on ilmoitettava henkilötietojen tietoturvaloukkauksesta välittömästi sitä alihankkijana käyttävälle palveluntarjoajalle.

6 artikla

Raportointi ja uudelleentarkastelu

Komissio antaa kolmen vuoden kuluessa tämän asetuksen voimaantulosta kertomuksen sen täytäntöönpanosta, tuloksellisuudesta ja vaikutuksesta palveluntarjoajiin, tilaajiin ja yksityishenkilöihin. Komissio tarkastelee tätä asetusta uudelleen kyseisen kertomuksen perusteella.

7 artikla

Voimaantulo

Tämä asetus tulee voimaan 25 päivänä elokuuta 2013.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 24 päivänä kesäkuuta 2013.

Komission puolesta
Puheenjohtaja
José Manuel BARROSO

LIITE I

Toimivaltaiselle kansalliselle viranomaiselle annettavan ilmoituksen sisältö

1 jakso

Palveluntarjoajan tunnistetiedot

1. Palveluntarjoajan nimi

2. Tietosuojavastaavan henkilöllisyys ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa

3. Tieto siitä, onko kyseessä alustava vai täydentävä ilmoitus.

Alustavat tiedot henkilötietojen tietoturvaloukkauksesta (täydennetään tarvittaessa myöhemmillä ilmoituksilla)

4. Tietoturvapoikkeaman (arvioidun, ellei tiedossa) tapahtumisen ja havaitsemisen päivämäärä ja kellonaika

5. Henkilötietojen tietoturvaloukkauksen olosuhteet (esim. tietojen menetys, varkaus tai jäljentäminen)

6. Kyseisten henkilötietojen luonne ja sisältö

7. Tekniset ja organisatoriset toimenpiteet, joita palveluntarjoaja soveltaa (tai aikoo soveltaa) tietoturvaloukkauksen kohteena oleviin henkilötietoihin

8. Toisten palveluntarjoajien osallisuus (soveltuvin osin)

2 jakso

Lisätiedot henkilötietojen tietoturvaloukkauksesta

9. Tiivistelmä henkilötietojen tietoturvaloukkauksen aiheuttaneesta tietoturvapoikkeamasta (ml. tietoturvaloukkauksen fyysinen tapahtumapaikka ja kyseessä olleet tallennusvälineet)

10. Tietoturvaloukkauksen kohteeksi joutuneiden tilaajien tai henkilöiden lukumäärä

11. Mahdolliset tilaajille tai henkilöille aiheutuvat seuraukset ja haittavaikutukset

12. Tekniset ja organisatoriset toimenpiteet, jotka palveluntarjoaja toteuttaa mahdollisten haittavaikutusten lieventämiseksi

Mahdollinen tilaajille tai henkilöille annettu lisäilmoitus

13. Ilmoituksen sisältö

14. Käytetyt viestintämenetelmät

15. Ilmoituksen saaneiden tilaajien tai henkilöiden lukumäärä

Mahdolliset rajatylittävät kysymykset

16. Tilaajia tai henkilöitä muissa jäsenvaltioissa koskeva henkilötietojen tietoturvaloukkaus

17. Ilmoittaminen muille toimivaltaisille kansallisille viranomaisille

LIITE II

Tilaajalle tai henkilölle annettavan ilmoituksen sisältö

1. Palveluntarjoajan nimi

2. Tietosuojavastaavan henkilöllisyys ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa

3. Tiivistelmä henkilötietojen tietoturvaloukkauksen aiheuttaneesta tietoturvapoikkeamasta

4. Tietoturvapoikkeaman arvioitu päivämäärä

5. Kyseisten henkilötietojen luonne ja sisältö 3 artiklan 2 kohdassa tarkoitetussa mielessä

6. Henkilötietojen tietoturvaloukkauksesta sen kohteeksi joutuneelle tilaajalle tai henkilölle todennäköisesti aiheutuvat seuraukset 3 artiklan 2 kohdassa tarkoitetussa mielessä

7. Henkilötietojen tietoturvaloukkauksen olosuhteet 3 artiklan 2 kohdassa tarkoitetussa mielessä

8. Toimenpiteet, jotka palveluntarjoaja on toteuttanut henkilötietojen tietoturvaloukkauksen vuoksi

9. Palveluntarjoajan suosittelemat toimenpiteet, joilla voidaan lieventää mahdollisia haittavaikutuksia