

Tietosuojaverkosto on aloittanut toimintansa

3

Selviytymisopas EU:n tietosuoja-asetuksen pykäläviidakkoon

4-5

Tiukentuva tietosuoja - etua vai haittaa?

6-7

1 000 euron jäsenedut!

PÄÄKIRJOITUS



Mika Helenius, TIVIAN toiminnojohtaja

Halvatus GDPR meni pieleen!

► Kun vuonna 2011 Maximilian "Max" Schrems nosti kanteen Facebookia vastaan henkilökohtaisten tietojen tallentamisesta, alkoi ennen kuulumaton yksityisyyden lakien ja tietopolitiikan uudelleen kirjoittaminen. Yhdysvalloissa opiskellut Schrems katsoi, ettei saanut EU-kansalaisena toisessa EU-maassa itselleen kuuluvaa oikeutta. Hän haastoi Irlannin tietosuojaviranomaiset EU-oikeuteen. Samalla suuri osa Euroopan orastavasta ohjelmistoteollisuudesta hurrasi ja toivoi uuden mahdollisuuden alkavan. Guardian-lehti uutisoi 2012, että kyseessä voisi olla jopa lähes 50 miljardin euron liiketoiminnan uudelleenjako. Mitä tapahtui? Syntyikö Eurooppaan uutta ohjelmisto- ja alustalousteollisuutta? Edistikö tietosuojalainsäädännön kirjoittaminen eurooppalaista osaamista ja innovaatiota? Paraniko eurooppalaisten yritysten kilpailukyky ja liiketoiminnan kehittämisen edellytykset? Ei.

Yhä useammassa omaa alustatalouden liiketoimintaa kehittävässä yhtiössä on tuskailtu halvaannuttavan ja häjyn GDPR-lainsäädännön edessä. Vuosien ja vuosien kehittämispanokset, jotka olisi Euroopassa pitänyt saada oman osaamisen ja oman liiketoiminnan kehittämiseen ovat valuneet hallintoon ja kontrollin rakentamiseen. GDPR onkin ollut suurta lakimiesten juhlaa liiketoimintaedellytysten ja -kehityksen kustannuksella. Miksi näin pääsi

tapahtumaan? Miksi eurooppalaiset haluavat estää kaupan, markkinoinnin ja myynnin toisilleen Euroopassa? Miksi luovutamme digitaalisen kehityksen, alustatalouden vallan ja ohjelmistotalouden infrastruktuurin kehityksen ulkopuolelle?

Euroopassa ja Suomessa ollaan edelleen ns. *"software crisis"* / *"software gap"* -tilassa tasan viisikymmentä vuotta 1968 Saksan Garmischissa pidetyn ensimmäisen eurooppalaisen NATO Software Engineering Conferencen jälkeen. Tuoreen EU-selvityksen mukaan EU-maissa on kasvava yli 500 000 ohjelmistosuunnittelua ymmärtävän johtajan ja asiantuntijan vaje – vaikka EU on panostanut miljardeja ICT-alan yliopistokoulutukseen ja -tieteeseen.

GDPR on hyvä esimerkki osaamisvajeen ja yksipuolisen valmistelun seurauksista koko EU:n talousalueella. GDPR luo tilanteen, joissa voimme helposti tehdä ja jatkaa B2B-liiketoimintaa, mutta henkilökohtainen B2C-myynti tulee moninkertaisesti hankaloitumaan. Onko kilpailuneutraalia, että sallimme henkilökohtaisen myynnin tapahtuvan luokattomien ehtojen puitteissa, ekosysteemeissä, alustoissa ja laitteissa, joiden liiketoiminta tapahtuu kokonaan mantereemme ulkopuolelta? Saimme ehkä pelastettua osan yksityisyydestä – tosin oman talouden, liiketoiminnan ja kulttuurin kustannuksella.



Tietosuojaverkosto on aloittanut toimintansa

Teksti: Jasmina Heinonen

Tietoturva ry on perustanut yhteistyössä HR Legal Services Oy:n tietosuojalakimies Jasmina Heinosen kanssa Tietosuojaverkoston. Tietosuojaverkoston tavoitteena on jakaa tietoa tietosuojasta, herättää keskustelua ja tukea tietosuojaa työkseen tekeviä. Tietosuojaverkosto halutaan pitää matalan kynnyksen yhteistyöfoorumina.

► Tietosuojaverkosto sai alkunsa Heinosen LinkedIniin kirjoittamasta viestistä: *”Tietoturva ry:n Ursula Koski otti minuun yhteyttä, kun LinkedIniin spontaanisti kirjoittamani ajatus oli levinnyt ympäri verkkoa. Siitä se sitten lähti. Aloitimme yhdessä toteuttaa verkostoa. Verkostoa ei olisi voinut perustaa ilman Tietoturva ry:n panostusta. Siitä syntyy väkisinkin erilaisia kuluja”*, kertoo Heinonen.

Tietosuojaverkosto saikin useita satoja suoria ilmoituksia kiinnostuksesta toimintaan. Ajatus levisi verkossa nopeasti. *”Minusta kiinnostus Tietosuojaverkosta kohtaan kuvastaa erityisesti, kuinka monelle on epäselvää, mitä tuleva uusi yleinen tietosuoja-asetus oikein tarkoittaakaan”*, kertoo Heinonen. Tietosuojaverkoston ideana, että osallistujat jakaisivat tietoa keskenään sekä kysyisivät kysymyksiä vaikeista teemoista. Heinonen työskentelee itse tietosuojavastaavana, valmentaa tietosuojasta sekä johtaa GDPR-projekteja. Tietosuoja-asetus on tullut hänelle tutuksi työssä, mutta hän kokee silti usein kaipaavansa mm. tarkempia linjauksia. *”Epätietoisuudessa eläminen on kuormittavaa, kun haluaisi tehdä työnsä hyvin ja oikein. Huomaan kuitenkin, etten ole ainoa, jolla on sama ongelma”*, kuvailee Heinonen.

Tiistaina 16.1.2018 pidettiin Tietosuojaverkoston perustamistilaisuus. Tilaisuuteen osallistui myös tietosuojavaltuutettu **Reijo Aarnio** kertoen tietosuoja-asetukseen liittyvät ajankohtaiset kuulumiset. Muita puhujia olivat **Krista Venhomaa**. Muita Tietosuojaverkoston tapahtumia on ollut Tietosuojaan kyselytunti 15.2.2018.

Osallistuminen verkoston toimintaan on täysin maksutonta.

MITEN TIETOSUOJAVERKOSTON TOIMINTAAN PÄÄSEE MUKAAN?

Jos olet mukana LinkedInissä tai Facebookissa, Tietosuojaverkoston ryhmä löytyy sieltä. Ryhmän nimi on *Tietosuojaverkosto*. Ryhmää ylläpitää Tietoturva ry:n puheenjohtaja Ursula Koski.

Tietosuojaverkoston lisäksi kehitteillä oma nettisivusto. Väliaikainen sivusto löytyy: <https://tietosuojaverkosto.wordpress.com>.

Sivusto on julkinen, joten tapahtumien materiaalit jaetaan sosiaalisen median ryhmissä. Sivuston kautta on myös mahdollista kommentoida ja kehittää Tietosuojaverkoston toimintaa.

Jasmina Heinonen

Tietosuojalakimies ja tietosuojavastaava
HR Legal Services Oy

Työskennellyt aiemmin Finnet-liitolla, jossa perehtyi tietosuoja-asioihin. Tehnyt työkseen myös työsuohdejuridiikkaa. Nykyään tekee työkseen tietosujaa sekä erityisesti yleisen tietosuoja-asetuksen täytäntöönpanoa eri organisaatioissa, kuten työttömyyskassoissa, eri yrityksissä ja kouluissa.

Selviytymisopas

EU:n tietosuoja-asetuksen pykäläviidakkoon

Teksti: Paula Miinala ja Minna Oksanen

► EU:n tietosuoja-asetus (GDPR = General Data Protection Regulation) vaikuttaa liiketoimintaprosesseihin ja tulevaan lainsäädäntöön. Se koskee jokaista organisaatiota, joka käsittelee eurooppalaisen henkilötietoja. Viisas johto näkee vahvan tietosuojan lisäävän organisaation luotettavuutta ja panostaa asetuksen toteuttamiseen. Hyvä tietosuoja kannattaa tuoda esiin osana yrityskuvaa, sitä ei kannata jättää vain juristien ja tietohallinnon asiaksi vaan se on koko organisaation asia. Organisaation johto on tarvittavien toimenpiteiden mahdollistaja sekä jalkauttaja koko organisaatiossa.

Organisaatiolla on näyttövelvollisuus asetuksen noudattamisesta. Tätä varten on hyvä laatia omavalvontasuunnitelma. Tässä artikkelissa esitämme yksinkertaisen perusrungon siitä, millainen tämä omavalvontasuunnitelma voisi olla.



Paula Miinalainen on pitkän linjan ICT-ammattilainen, jolla on vuosikymmenien aikana kertynyt ammattitaito järjestelmien rakentamisesta erityisesti taloushallinnon ja vakuutusten hoidon alueilla. Nyt Paulan mielestä on tärkeää yhdenmukaistaa vastaavia järjestelmiä ja tietosuoja EU:n alueella.



Minna Oksanen on tiedon hallinnan ammattilainen Talent Basesta, jolla on kokemusta sekä BI-alueesta että master datan jalkauttamisesta ja liiketoiminnan käsite- ja tietomallinnuksesta. Hän on ollut asiantuntijana useassa regulaatiohankkeessa mm. viimeisimpänä ison organisaation GDPR-hankkeesta. Minna on TIVIAN hallituksen jäsen ja vastuussa viestintätoimikunnasta.

TEE NÄMÄ:

1. Mieti tietosuojalupaus

Tietosuojalupaus: Pidämme henkilötietojen turvallisuudesta huolta tietosuojalainsäädännön mukaisesti. Järjestelmämme ovat suojattuja, emmekä anna tietoja kolmannelle osapuolelle ilman henkilön lupaa.

2. Tunnista henkilötietorekisterit ja niissä olevat tiedot.

- Huomaa, että myös paperiset asiakirjat mapissa voivat muodostaa henkilötietorekisterin.
- Määrittele, mihin tietoa käytetään ja kauanko sitä tarvitaan. Jos tiedon säilyttämiselle ei ole perusteita, se tulee poistaa.

3. Tee jokaisesta rekisteristä tietosuojaseloste. Valmiin täytettävän lomakkeen saat osoitteesta www.tietosuoja.fi, josta edelleen polku Etusivu » Materiaalia » Lomakkeet » Rekisteri- ja tietosuojaselosteet. Kirjoita pohjaan heti kaikki sillä hetkellä tiedossa olevat asiat ja täydennä sitä mukaa kuin asiat selviävät. Näin pohja ohjaa työn etenemistä. Kun suunnittelet uutta henkilörekisteriä, niin pohja toimii heti suunnittelun alusta lähtien muistilistana asioista, jotka tulee huomioida.

4. Tee kustakin rekisteristä henkilötietojen käsittelyn prosessikuvaus, jossa kuvaat, kuka tekee, mitä tekee, miksi tekee ja missä tekee. Kuvaa millaiset oikeudet tekijällä on henkilötietojen käsittelyyn.

5. Käy läpi kumppanit, jotka ovat henkilötietojen käsittelijöitä.

It-palvelujen toimittajat, it-tuki, rekrytointikumppanit, arkistojen tuhoajat. Tarkista ja tarvittaessa tarkenna kumppanin kanssa tehdyt sopimukset. Sopimusten tulee aina olla kirjallisia ja kattaa kokonaan mahdollinen alihankkijaketju. Rekisterinpitäjällä on ensisijainen vastuu koko käsittelyketjusta.

6. Ohjeista kriisitilanteen toiminta esimerkiksi näin:

Kriisitilanteen toiminta

- Jos ilmenee, että on tapahtunut tietovuoto, niin asiasta ilmoitetaan välittömästi tietosuojavaltuutetun toimistoon.
- Tämä tulee tehdä mahdollisuuksien mukaan 72 tunnin kuluessa tietovuodon ilmitulosta.

Käyntiosoite: Ratapihantie 9, 6. krs, 00520 Helsinki

Postiosoite: PL 800, 00521 Helsinki

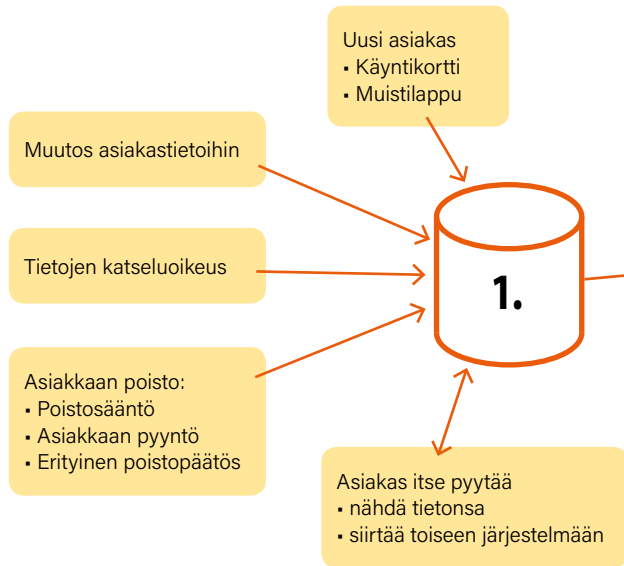
Sähköposti: tietosuoja@om.fi Vaihde: 029 56 66700

Jos on syytä epäillä, että vuodosta on haittaa henkilötiedon henkilölle itselleen, myös häntä tulee informoida!

Firma oy
rekisterinpitäjä (controller)

Asiakasrekisteriin liittyvä aineisto säilytetään toimistossa lukitussa kaapissa.

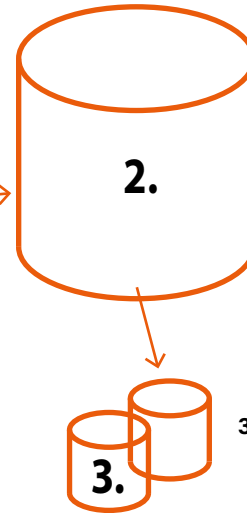
Postittaja oy:n ohjelmistoa käyttävät nimetyt henkilöt, joilla on henkilökohtaiset käyttäjätunnukset ja salasانات.



1. Firma Oy:n excel-tiedostoja omalla tietokoneella, johon pääsee vain käyttäjän salasanalla. Tiedostoissa on markkinointiryhmäkohtaisia osoitteistoja.

Postittaja oy
käsittelijä (processor)

Sähköpostiosoitteet ovat Postittaja oy:n järjestelmässä, josta on erillinen kuvaus (Liite1).



2. Markkinointirekisterin osoitedata on Postittaja Oy:n järjestelmässä Liite 1.

3. Asiakkaille lähtevät sähköpostit.

Rekisterinpitäjä (controller) on organisaatio, joka yksin tai yhdessä toisen tahon kanssa määrää henkilötietojen käsittelyn tarkoitukset ja keinot.

Käsittelijä (processor) on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Henkilötieto (personal data) on kaikkea tunnistettua ja tunnistettavissa olevaa luonnollista henkilöä koskevaa tietoa (myös esim. IP-osoite tai auton rekisterinumero).

Rekisteröity (data subject) on luonnollinen henkilö.

Rekisteri (filing system) on mikä tahansa jäsenneilty henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein (voi olla hajautettu, keskitetty tai jaettu).

Suostumus (consent) on mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojen käsittelyn.

ESIMERKKI OMAVALVONTASUUNNITELMAN SISÄLLYSLUETTELOSTA:

1. Tietosuojalupaus
2. Kriisitilanteen toiminta
3. Henkilörekisterit
 - 3.1. Marrek, Firma Oy:n markkinointirekisteri
 - Marrekin prosessikuvaus
 - Marrekin tietosuojaseloste
 - Marrekin sopimus Käsittelijä Osoite Oy päivältä pp.kk.vvvv liite 1.1
 - Marrekin tietosuojalupaus Käsittelijä Osoite Oy päivältä pp.kk.vvvv liite 1.2
 - 3.2. Henrek, Firma Oy:n henkilökuntarekisteri
 - Henrekin prosessikuvaus
 - Henrekin tietosuoja seloste
 - Henrekin sopimus Käsittelijä Palkat Oy päivältä pp.kk.vvvv liite 2.1
 - Henrekin tietosuojalupaus Käsittelijä Palkat Oy päivältä pp.kk.vvvv liite 2.2
4. Henkilökunnan koulutus ja jatkuva perehdyttäminen
5. Omavalvontasuunnitelman ylläpito



Tiukentuva tietosuoja – etua vai haittaa?

Teksti: Lea Virtanen

► Tietosuoja-asetusta lähestytään monessa organisaatiossa juristilähtöisesti, koska kysymys on lainsäädännöstä ja sen soveltamisesta käytäntöön. Myös Helsingin kaupungin tietosuojavastaava on juristi. Meillä Työterveys Helsingissä GDPR:n käytännön toimet ovat tietohallinnon vastuulla. Tietosuojan työryhmässä on mukana hallintohenkilöstöä mm. sopimushallinnosta, henkilöstöhallinnosta, terveydenhoidosta ja tietohallinnosta.

Henkilöasiakkaita meillä on yli 40 000 eli lähes koko kaupungin ja sen tytäryhtiöiden henkilöstö. Juridiikkaan on tarvittaessa saatavissa apua Kaupungin oikeuspalveluilta. Päävastuun kantaa johtokunta ja sen delegoimana toimitusjohtajamme.

Sopimushallinnossa työtä teettävät henkilötietoja sisältävät tietojärjestelmät, joita koskevat sopimukset tulee saattaa nykyisen asetuksen mukaisiksi. Myös hankinnoissa on huomioitava tietosuoja-asetus. Henkilöstöhallinto analysoi oman henkilörekisterimme. Meidän tapauksessamme tämä työ tehdään pääosin Kaupungin kanslian toimesta, koska kaupungilla on yksi yhteinen henkilötieto-

järjestelmä ja siihen liittyvä rekisteriseloste. Työterveydessä keskeinen rekisteri on potilastietorekisteri. Vaikka potilastietoja sisältäviä tietojärjestelmiä on useita, niin tarvitaan vain yksi rekisteriseloste, joka kattaa tietoja useista tietojärjestelmistä. Kaikki muutkin olemassa olevat rekisteriselosteet on sovittu uusittaviksi. Terveydenhuollossa on ollut tiukat vaatimukset tietosuojan suhteen jo vuosia, joten tehtävänä on lähinnä varmistaa tietojen kattavuus ja uusien rekisteriselosteiden muoto.

Tietoteknisesti isoimmat haasteet liittyvät lokitietoihin, niiden olemassaoloon, käsittelyyn ja säilyttämiseen. Näiltä osin meillä on kaupunkitasoinen projekti menossa, missä selvitetään jokaisen henkilötietoja sisältävän järjestelmän lokitietojen riittävyys suhteessa nykyisen tietosuoja-asetuksen vaatimuksiin. Järjestelmätoimittajat vastaavat omalta osaltaan näihin haasteisiin. Tässä kokonaisuudessa ei tulla välttymään tietojärjestelmäprojekteilta, sillä varmasti löytyy järjestelmiä, joihin lisälokistusta on rakennettava. Myös tietojen säilytys ja lokitietojen säilytysajat poikkeavat terveydenhuollos-



Lea Virtanen vastaa Työterveys Helsingin tietohallinnosta ja on johtoryhmän jäsen.

sa yleisistä säilytysajoista. Terveysthuollon omavalvontasuunnitelmat on tarkistettava ja dokumentoitava toteutetut toimenpiteet sekä havainnot tarkemmin kuin aikaisemmin.

Tietosuojaa ei ole ilman tietoturvasuutta, viittaa esimerkiksi fyysiseen tietoturvaan kuten ovien ja työasemien asianmukaiseen lukitukseen. Erityistä huomiota kiinnitetään potilastietojen tietoturvalle käsittelyyn. Tietoturvasuus on osana kevään aikana koko henkilöstölle pidettävää pakollista tietosuojakoulutusta.

Tietosuojaa-asetus on läpinäkyvyyden kannalta hyvä asia, koska kansalaisen oikeuksia omiin tietoihinsa selkeytetään. Toisaalta tietosuojaa-asetus tuo tiukennuksia käsittelyyn ja lisääntyvää valvontaa, joka puolestaan voi rajoittaa asioiden tekemistä. Tietojenkäsittelyssä on entistä tarkemmin pohdittava, mitä tietoja voidaan käyttää ja mitä ei. Myös tietopyyntöprosessien läpivienti on suunniteltava sujuvaksi, jotta vastaukset pystytään antamaan asetuksen vaatimissa ajassa.

Maaliskuussa 2018 on annettu hallituksen esitys uudeksi tie-

tusojalaki. Lailla täydennettäisiin ja täsmennettäisiin Euroopan unionin yleistä tietosuojaa-asetusta. Samalla kumottaisiin henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Jos lainsäädäntö selkiytyy ja osa laeista yhdistyy yhteen lakiin, niin kehitys on tervetullutta. Terveysthuoltoon jää kuitenkin runsaasti säädöksiä, joiden käytäntöön vieminen ja henkilöstölle kouluttaminen on erityisen tärkeää osana tietosuojakoulutusta sekä perehdyttämisprosessia. Asetuksen tuomat sanktiot ohjaavat myös toimijoita hoitamaan tietosuojan kokonaisuudessaan mahdollisimman hyvin.

Rajoittaako tiukentuva tietosuojaa Euroopan laajuisesti tietojen käyttöä ja saattaako se meidät eurooppalaisen huonompaan kilpailuasemaan Aasian ja Yhdysvaltojen kanssa, missä tiedon hyödyntäminen ei rajoiteta eurooppalaisen tietosuojan tapaan? Aika näyttää, miten riittävä avoimuus ja tiukentuvat tietosuojakäytännöt tulevat sopimaan yhteen.

SUURI SUOMALAINEN KODAUSTUTKIMUS 2018

TIVIA

#sskt18

Hyvä syy
liittyä TIViaan

#2.

Teemme oman osaamisen
kehittämisen helpoksi. Osallistu
TIVIAN lukuisiin seminaareihin,
koulutuksiin ja webinaareihin!

TIVIA kouluttaa:

- 17.4. Tietosuoja-asetus tietosuojavastaavalle
- 23.–24.4. Certified ScrumMaster
- 21.5. Business Transformation Architect -koulutus
- 30.–31.5. Koneoppiminen – johdanto data-analyysin menetelmiin ja sovelluksiin

tivia.fi/koulutukset

TIVIAssa tapahtuu:

- 13.–14.4. Tulevaisuuden verkostot
- 24.4. Finnish Internet Forum
- 26.4. EuroCIO dinner
- 8.5. Tekoäly ja robotiikka digitalisoituvassa yhteiskunnassa
- 5.6. ICT Ladies risteilee digiajassa
- 26.–28.9 Tekoäly työyhteisössä –huippuseminaari

tivia.fi/tiviassa-tapahtuu

65 vuotta

TIVIA

ICT-ammattilaisten valtakunnallisia verkostoja vuodesta -53
Lisätietoja www.tivia.fi