TIETOSUOJA

KUMPPANUUSTALO HILMA 16.10.2024

KUKA OLEN?

- Heidi Ilmonen
- Yrittäjä, kouluttaja ja yritysneuvoja Salus Qualitas Consulting Oy / SoteTraining
- Projektipäällikkö CyberCare Kymi- hanke (XAMK)
- MBA, Tradenomi (Ympäristö –ja laatujohtaminen), Kyberturva Insinööri (YAMK)- opiskelija.
- Suunnitellut oman Kanta-yhteensopivan asiakastietojärjestelmän ja pohtinut siitä lähtien tietosuojaan, kyberturvaan ja tietoturvaan liittyviä kysymyksiä
- SoteTraining portaalin perustaja.

VAHINKOJEN VÄLTTÄMINEN

- Tietosuojalakien tavoitteen voi tiivistää ajatukseen, jossa vahinkojen ei enää sallita tapahtuvan, tai ainakin organisaation hallussa olevat henkilötiedot eivät tässä yhteydessä vaarannu.
- Miksi näin on? Laki velvoittaa turvallisuuteen ja huolellisuuteen, tällöin kaikki henkilötiedoille sattuvat vahingot ovat osoituksia siitä, että lain vaatimusta tältä osin ei ole täytetty.
- Mitä tämä käytännössä sitten tarkoittaa?

  Esimerkiksi henkilötietoja sisältävä muistitikku on suojattava niin, etteivät tiedot paljastu, vaikka tikku katoaisi.
  Kannettavassa tietokoneessa olevat tiedot suojataan niin, etteivät ne paljastu vaikka kone varastettaisiinkin.
  Yrityksen verkko on eristettävä niin hyvin, ettei hakkeri pääse sisään ja pääse verkon kautta kiinni verkossa oleviin laitteisiin.

TIETOSUOJAAN LIITTYVIÄ YLEISIÄ PERIAATTEITA

- Henkilötietoja tulee käsitellä laillisesti ja niiden käsittelyssä tulee olla huolellinen
- Yksityisyyden suojaa turvaavia perusoikeuksia ei saa rajoittaa ilman asiaan liittyvää laillista perustetta
- Henkilötietojen käsittely pitää olla aina suunnitelmallista (rekisterit ja riittävät kuvaukset)
- Määritellystä henkilörekisteristä saa käyttää vain tehtävän hoitoon liittyviä rajattuja tietoja
- Asiakkaalla on tiedonsaantioikeus häneen liittyvien henkilötietojen käsittelystä ja käsittelyn tarkoituksesta
- Henkilöllä on oikeus tarkistaa itseään koskevat tiedot ja hänellä on oikeus myös pyytää niiden korjaamista tarvittaessa. Pyynnöt tehtyine toimenpiteineen kirjataan.

KATSAUS TIETOSUOJALAINSÄÄDÄNTÖÖN

EU:n alueella tietosuojaa sääntelee tietosuoja-asetus eli GDPR (General Data Protection Regulation), joka astui voimaan toukokuussa 2018. Sitä edeltävä tietosuojadirektiivi (95/46/EC) oli peräisin vuodelta 1995.

Tietosuoja-asetus on suoraan sovellettavaa oikeutta, joten suomalainen tuomioistuin noudattaa sitä sellaisenaan. Asetus on sama kaikissa EU-maissa, mikä takaa yhtenäiset oikeudet EU-kansalaisille.

Henkilötietojen käsittelystä säädettiin Suomessa vuonna 1987 hyväksytyssä henkilörekisterilaissa (471/1987), joka tuli vuomaa vuoden 1988 alusta. Se korvattiin vuonna 1999 henkilötietolailla (523/1999).

EU:n tietosuoja-asetuksen jälkeen monet henkilötietolain asetukset kävivät tarpeettomiksi, koska niistä säädetään asetuksessa, mutta asetus ei yksin riitä.

Suomessa vuoden 2019 alusta voimaan tullut tietosuojalaki (1050/2018) säätää niistä tietosuoja-asioista, jotka on jätetty GDPR:n ulkopuolelle. Esimerkiksi henkilötunnus on kansallinen asia, joten sen käytöstä maat päättävät itse.

Tietosuojan lisäksi henkilötietojen käsittelyä säädetään monissa muissakin suomalaisissa laeissa. Sosiaali- ja terveysalaa koskevissa laissa erityisesti, mutta myös perustuslaissa (yksityisyydensuoja) (Järvinen, P. 2022)

TIETOSUOJA-ASETUKSEN KESKEISET PERIAATTEET

Tietosuoja-asetuksen perimmäinen tarkoitus on tietosuoja käytäntöjen juurruttaminen osaksi organisaation ja sen henkilöstön toimintaa

Tietosuoja-asetuksessa ajatuksena on toisaalta lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä, mutta myös vahvistaa rekisterissä olevien asiakkaiden oikeutta valvoa omien henkilötietojensa käsittelyä

Asetukseen sisältyy osoittamisvelvollisuus. Mikäli organisaatio ei pysty osoittamaan tietosuojaan ja tietoturvaan liittyviä toimintoja asiakirjoin ja käytännöin seuraamuksena voi olla liikevaihtoon perustuva sakkorangaistus tai toiminnan keskeyttäminen

Tietosuoja-asetus koskee kaikkia sen soveltamisalaan kuuluvia henkilötietoja käsitteleviä organisaatioita mukaan lukien rekisterinpitäjät ja henkilötietojen käsittelijät

Tietosuoja asetusta sovelletaan automaattiseen henkilötietojen käsittelyyn ja sellaiseen henkilötietojen käsittelyyn, joka muodostaa rekisterin tai osan rekisteriä

KÄSITTELYPERUSTE

Henkilötietojen käsittelyyn tulee olla aina perusteltu syy, ilman syytä se on lainvastaista.

Käsittelyperusteita ovat:

- Suostumus (ei pelkkä pään nyökkäys, vaan selkeä, kiistaton, siitä pitää jäädä jälki ja rekisteröidyn on ymmärrettävä, mihin lupa liittyy)
- Sopimuksen toteuttamiseen liittyvä tarve (yrityksen asiakkuuden tai jäsenyyden kannalta tarpeellisten tehtävien hoitamista) esimerkiksi Googlen tai Facebookin oikeus käsitellä tietojamme
- Lakisääteinen velvoite (viranomaisen oikeus käsitellä kansalaisen henkilötietoja laissa määriteltyjen tehtävien toteuttamiseksi)
- Elintärkeiden etujen suojaaminen (poliisi tai pelastustoimi suojatessaan elintärkeitä etuja tilanteissa joissa, muiden henkilöiden terveys tai turvallisuus on vaarassa)
- Yleinen etu tai julkiseen valtaan liittyvä peruste (luottotietoja myyvät yritykset, terveydenhuollon hallinto, kansanterveyteen liittyvät palvelut)
- Oikeutettu etu (uusi, rekisterinpitäjän mahdollisuuksia laajentava käsite) tarkoittaa tilannetta, jossa yrityksellä on tarve käsitellä toiminnassaan henkilötietoja ilman, että sillä on henkilöön asiakassuhdetta tai häneltä saatua suostumusta. (esim. markkinointi, tilastointi, tieteellinen tutkimus, lokitiedostojen käsittely)

MITÄ TEHDÄ AINAKIN?
1. KARTOITA HENKILÖTIEDOT

- Tietosuoja-asetus määrittelee henkilötiedon käsitteen kohtalaisen laajasti, siksi henkilötietojen kartoittaminen kannattaakin tehdä ajatuksella.
- Käytännössä kaikki tiedot, jotka ovat kohtuullisella tavalla liitettävissä kohonkin ihmiseen, ovat henkilötietoja.
- Huomiona se, että henkilötietojen ei tarvitse olla välttämättä missään rekisterissä, vaan kaikki esimerkiksi digitaalisessa muodossa olevat henkilötiedot ovat asetuksen soveltamisalan piirissä.
- Kartoitus on toki järkevintä aloittaa ”suurimmista” käytössä olevista järjestelmistä, kuten jäsenhallinta, asiakastietokanta… Ja tästä edetään sitten yksittäisiin tietoihin.
- Tietoja voi olla tallessa yllättävinkin monissa paikoissa, selvitä siis mitä kaikkia eri henkilötietoja organisaatio kerää ja nämä tulisi ryhmitellä järkeviksi kokonaisuuksiksi, kuten työntekijöiden tiedot, asiakkaiden yhteyshenkilöt, uutiskirjeen tilaajat, verkkopalvelun käyttäjät…

MITEN TARTUN TOIMEEN HENKILÖTIETOJEN OSALTA: ESIMERKKI

Henkilötietoryhmä?	Tiedon sijainti?	Mitä tietoa?
Asiakkaat	• Yrityksen OneDrive (Kansioissa olevia tiedostoja) • Teams (tiimien projektiryhmät) • Asiakastietojärjestelmä • Työkoneet • Sähköposti • Kirjanpito-ohjelma (Laskutus) • Manuaaliset arkistot	• Asiakassuunnitelmat word tiedosto • Postituslistat excel tiedosto • Osallistujalistat • Asiakkaiden ja omaisten yhteydenottoja ja viestintää sähköpostissa • Asiakkaiden laskut ja maksuhistoria • Sopimukset • Lääkelistat
Työntekijät	• Yrityksen OneDrive • Kirjanpito-ohjelma (Palkanlaskenta) • Manuaaliset arkistot • Internet-sivut • Some-kanavat	• Työsopimukset • Työhakemukset • Palkanmaksutiedot • Palkkahistoria • Sairauslomatodistukset • Todistukset • Yhteystiedot ja valokuvat
Yhteistyökumppanit	• Yrityksen OneDrive • Kirjanpito-ohjelma (laskutus)	• Sopimukset • Laskut ja laskuhistoria

MITÄ TEHDÄ AINAKIN? 2. SELVITÄ KÄYTTÖTARKOITUS JA SIIVOA TIETOVARANNOT

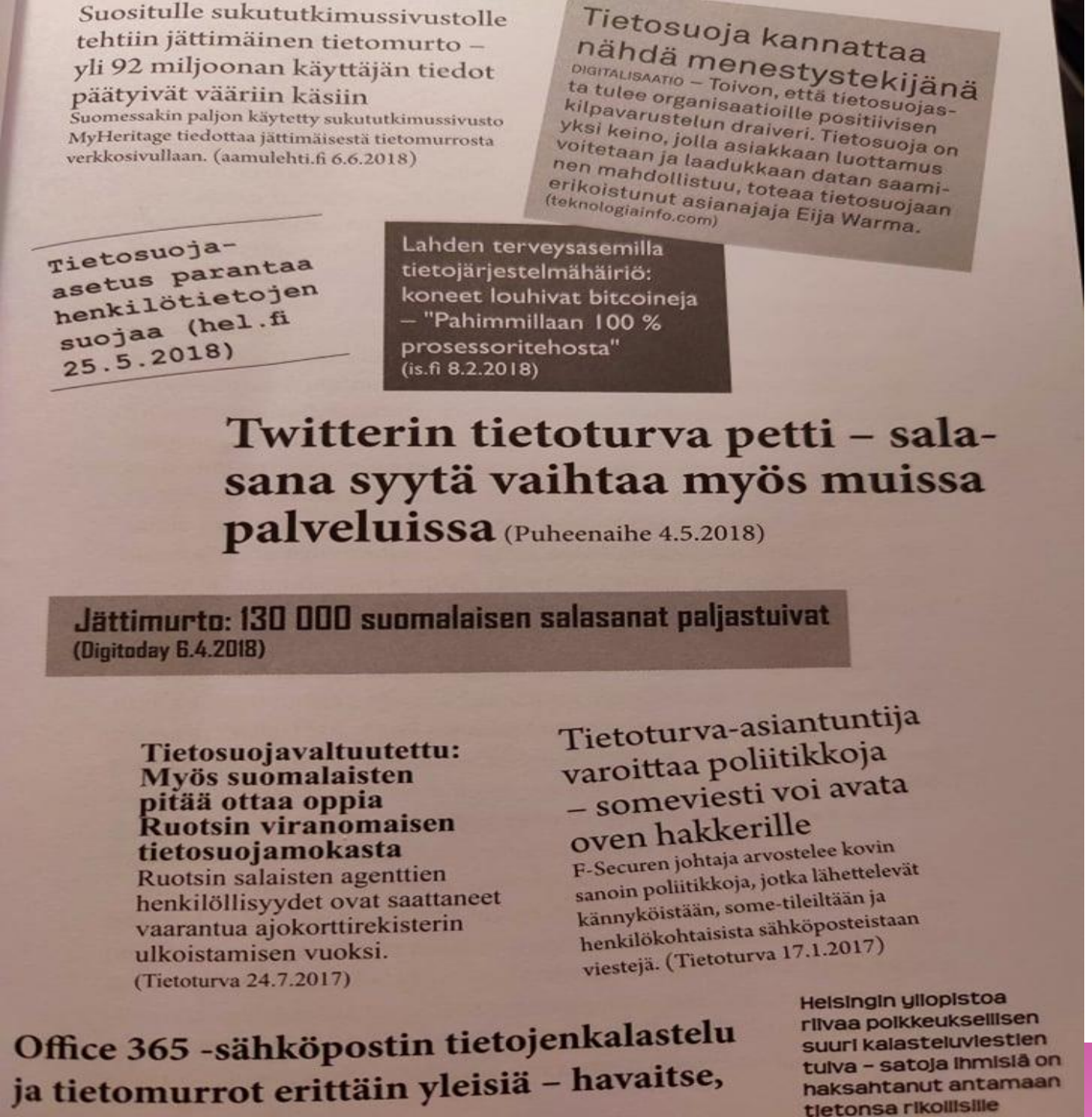
- Halussa olevien henkilötietojen listaamisen ja siivoamisen jälkeen määritellään jokaisen kokonaisuuden osalta miksi näitä tietoja tarvitaan, eli mikä on tarve ja toisaalta myös laillinen käsittelyperuste.
- Mikäli henkilötietojen kartoituksen yhteydessä havaitaan, että käytössä on vanhentunutta ja / tai tarpeetonta tietoa tulee nämä poistaa saman tien, erityisesti virheelliset ja vanhat tiedot tulee poistaa viipymättä.

TIETOVARANTOJEN SIIVOUSPÄIVÄ

- Järjestele mahdollisesti sekaisin olevat tiedostot ja kuvat oikeisiin kansioihin, joihin puolestaan jaat tarvittaessa käyttöoikeudet työtehtävien mukaan.
- Pohdi samassa yhteydessä, kenellä organisaatiosi jäsenillä tulee olla oikeuksia käytössä oleviin eri järjestelmiin ja minkä tasoisia käyttöoikeuksia he tarvitsevat.
- Jatka siivousurakkaasi myös paperiarkiston puolelle. Järjestele ja mapita paperiset arkistot ja hävitä asianmukaisesti kaikki tarpeeton tieto.
- Turhan tiedon poistaminen täyttää myös tietosuojalainsäädännön henkilötiedon minimoinnin ja säilytyksen rajoittamisen velvoitteet.
- Siivousurakka kannattaa tehdä sekä tietosuojan että liiketoiminnan tehokkuuden vuoksi.

MITÄ TEHDÄ AINAKIN?
3. RISKIARVIOT

- Tietosuoja-asetus perustuu riskiperusteisuus ajattelutapaan
- Tämän vuoksi kannattaakin käydä ajatuksella läpi, mitä ihmisille, joiden tiedoista on kysymys, voisi tapahtua, jos heidän tiedot vaikkapa tuhoutuisivat, häviäisivät tai päätyisivät vääriin käsiin.
- Toisaalta tätä ajattelua kannattaa tehdä myös sen osalta, mitä tämä tarkoittaa yhdistykselle, onko vaarana jopa mainehaitta ja lehtikirjoittelu? Miten tähän on varauduttu?
- Samoin kannattaa pohtia millaisia kykyjä organisaatiolla on reagoida mahdollisiin tietomurtoihin tai siitä, että henkilötietoihin ei pääse enää käsiksi.
- Tunnistetut riskit tulee aina luokitella sen mukaan miten todennäköisiä ne ovat ja miten suuri vahinko niiden toteutumisesta voisi organisaatiolle koitua.
- Laadi toimenpiteet joilla ainakin vakavimmat riskit saadaan torjuttua ja vahingot pienennettyä.



TIETOSUOJAAN (JA TIETOTURVAAN) LIITTYVIÄ UUTISOTSIKOITA VIIMEVUOSILTA

- Tietosuojan hyvä hallinta kannattaa nähdä kokonaisuutena, johon oleellisesti liittyy myös tietoturva ja some!
- Mitä enemmän viestimme ja käytämme verkkoa sitä laajemmin meidän tulee huomioida myös erilaiset tietosuojaan liittyvät näkökulmat toiminnassamme.
- Käytännössä mikä tahansa verkonyli toimiva laite, järjestelmä tai ohjelma on potentiaalinen hyökkäyksen kohde.

KIITOS!