SoteNavi

- pienten ja keskisuurten yritysten ja järjestöjen valmennushanke

GDPR, EU:n tietosuoja-asetus / EPTEK ry Mustajärvi

15.5.2018

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

EPTEK

TAMK
TAMPEREEN AMMATTIKORKEAKOULU

Osaavaa kansalaistoimintaa
Opintokeskus Sivis

Elinkeino-, liikenne- ja ympäristökeskus

Kestävää kasvua ja työtä -ohjelma

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan sosiaalirahasto

Sisältö

- Mikä on GDPR?
- Oikeudet ja velvollisuudet
- Rekisterit
- Tietosuojaseloste
- Keneen GDPR vaikuttaa?

GDPR – Mikä?

- General Data Protection Regulation
- Tietosuoja-asetuksella tarkoitetaan Euroopan Unionin yleistä tietosuoja-asetusta, jonka EU:n parlamentti hyväksyi vuonna 2016.
- Asetus tulee sovellettavaksi 25.5.2018.
- Asetuksessa tarkennetaan ja tiukennetaan luonnollisen henkilön tietoturva-asemaa organisaatioissa.

GDPR – Oikeudet ja velvollisuudet

- Asetus yhtenäistää EU:n jäsenvaltioiden lainsäädäntöä luonnollisten henkilöiden tietosuojaa koskien.
- Luonnollisten henkilöiden oikeuksia selkeytetään / parannetaan
- Organisaatioille lisää velvollisuuksia
- Velvollisuuksien laiminlyönnistä mahdollisesti vakavia sanktioita organisaatioille

GDPR – Oikeudet ja velvollisuudet

- Rekisterissä olevalla henkilöllä on oikeus:
  - Päästä käsiksi omiin henkilötietoihinsa
  - Korjata niissä esiintyviä virheitä
  - Tulla unohdetuksi
  - Kieltää henkilötietojensa käsittely
  - Saada tiedot itselleen

GDPR – Oikeudet ja velvollisuudet

- Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.
- Tähän tulee GDPR:n myötä täydennystä
  - Mm. IP-osoitteet, evästeet saattavat olla jatkossa henkilötietoa
  - Vaikka yhdestä tietopalasesta ei voisi tunnistaa, kahdesta tai useammasta mahdollisesti voi?

(https://www.finlex.fi/fi/laki/ajantasa/1999/19990523)

GDPR – Oikeudet ja velvollisuudet

- Henkilöllä on oikeus päästä käsiksi henkilötietoihinsa, saada ne itselleen:
  - Voitte pyytää esimerkiksi Facebookilta henkilötietojanne tarkasteltavaksi
    - Testasin tätä jonkin aikaa sitten, saatu tietomäärä oli paljon suurempi, kuin osasin odottaa
    - Mukana oli kaikki lähettämäni chat-viestit, tilapäivitykset, aktiivisuudet, tykkäykset, jne.
    - Paketin sai ladattua sähköpostiin toimitetun linkin kautta
    - Kuvat eivät olleet tätä kautta saatavilla

GDPR – Oikeudet ja velvollisuudet

- Tarkastelun lisäksi luonnollisella henkilöllä on oikeus muokata henkilötietojaan virheiden varalta, sekä tulla unohdetuksi ja poistaa tietonsa.
  - Mikäli laki ei velvoita säilyttämään henkilötietoja, organisaatioilla on velvollisuus mahdollistaa henkilötietojen poistaminen sekä niiden käsittelyn kieltäminen, organisaatioiden täytyy mahdollistaa luonnollisen henkilön unohdetuksi tuleminen

GDPR – Oikeudet ja velvollisuudet

- Asetus koskee kaikkia organisaatioita, jotka käsittelevät EU:n kansalaisen henkilötietoja
- Organisaatioille koituu asetuksesta melkoisesti työtä:
  - Henkilötiedot suojattava asianmukaisesti
    - Kenellä on pääsy tietoihin? Fyysinen suojaus? Digitaalinen suojaus?
  - Ilmoitusvelvollisuus – tietomurroista ilmoitettava 72h kuluessa viranomaiselle
  - Hankittava suostumus henkilötietojen käsittelyyn
  - Henkilötietojen käsittely lokitietoihin

GDPR – Oikeudet ja velvollisuudet

- Rekisterinpitäjän täytyy ilmoittaa **selkokielellä** henkilötietojen keräämisestä
  - Ilmoitus on aiemmin mahdollisesti ängetty täyteen lakiteknisiä termejä, tehden siitä vaikealukuisen
  - Mitä tietoja kerätään?
- Rekisterinpitäjän täytyy ilmoittaa syy henkilötietojen käsittelyyn
  - Miksi henkilötietoja kerätään? Mitä niillä tehdään?
- Rekisterinpitäjän täytyy määritellä henkilötietojen säilyttämisen ja poistamisen käytännöt

GDPR – Rekisterit

- Henkilörekisteri syntyy, kun henkilötietoja kerätään ja tallennetaan. Rekisteri voi olla digitaalinen ja/tai paperilla.
- Henkilörekistereistä on laadittava tietosuojaselosteet
  - Tietosuojaseloste on laajennettu rekisteriseloste
- Esimerkkejä rekistereistä:
  - Asiakasrekisteri
    - Sisältää tarvittavat tiedot asiakkuuksista
  - Työntekijärekisteri
    - Sisältää tarvittavat tiedot työntekijöistä

(http://www.tietosuoja.fi/fi/index/materiaalia/lomakkeet/rekisteri-jatietosuojaselosteet.html)

GDPR – Tietosuojaseloste

- Tietosuojaseloste sisältää:
  1. Rekisterinpitäjän tiedot
     - Nimi, osoite, muut yhteystiedot
  2. Yhteyshenkilö rekisteriä koskevissa asioissa
     - Nimi, osoite, muut yhteystiedot
  3. Rekisterin nimi
     - Esim. Organisaation asiakasrekisteri
  4. Henkilötietojen käsittelyn tarkoitus ja peruste
     - Miksi tiedot kerätään, mitä niillä tehdään?
  5. Rekisterin tietosisältö
     - Esim. nimi, syntymäaika, yhteystiedot
  6. Säännönmukaiset tietolähteet
     - Mistä tieto saadaan?

GDPR – Tietosuojaseloste

- Tietosuojaseloste sisältää:
  7. Säännönmukaiset tietojen luovutukset ja tietojen siirto EU:n tai Euroopan talousalueen ulkopuolelle
     - Luovutetaanko tietoja? Kenelle, miksi?
  8. Rekisterin suojauksen periaatteet
     - Miten tiedot suojataan? Fyysisesti / digitaalisesti?
  9. Tietojen säilytys
     - Miten kauan tietoa säilytetään?
  10. Rekisteröidyn oikeudet
     - Oikeudet tarkastaa tietonsa, vaatia virheellisten tietojen oikaisua, poistoa, täydennystä, oikeus kieltää tietojensa käyttö

Keneen GDPR vaikuttaa?

- Tietosuoja-asetus vaikuttaa oikeastaan jokaiseen jossain määrin.
- Työntekijänä olette osaltanne velvollisia noudattamaan asetusta.
- Organisaatiot eivät voi sormia napsauttamalla päättää olevansa GDPR-yhteensopivia, vaan työntekijät täytyy kouluttaa toimimaan asetuksen vaatimusten mukaisesti.
- Toimintatapoihin on mahdollisesti tehtävä muutoksia, jotta asetusta voitaisiin noudattaa.

Pohdinta – mitä rekistereitä juuri sinulla on henkilökohtaisessa käytössäsi?

- Mitä henkilörekistereitä sinulla on käytössäsi työasioissa?
- Kuinka paljon turhaa henkilötietoa on jäänyt roikkumaan esimerkiksi tietokoneille, sähköpostiin, pilvipalveluihin?

Esimerkkejä yritysten rekistereistä

- https://www.hesburger.fi/kayttoehdot-ja-rekisteriselosteet/asiakaspalauterekisterin-tietosuojaseloste
- https://www.verkkokauppa.com/fi/ohjeet/tietosuojaseloste
- https://www.turkuamk.fi/media/filer_public/2016/11/03/tietosuojaseloste_2016.pdf

Vinkkejä

- Käykää aineisto läpi
  - Vuosien varrella kerääntyy valtavat määrät turhaa dataa, jonka seassa voi olla henkilötietojakin ripoteltuna
  - Esimerkiksi palaverimuistiot, muistiinpanot, jne. saattavat sisältää aivan turhaan henkilötietoja
  - Organisaation aineisto, esim. palvelimelta, yhteisiltä levyasemilta, arkistokaapeista
- Poistakaa turha data
  - Sentimentaalinen arvo kannattaa punnita tietosuojan kannalta
  - Henkilötietojen säilytys täytyy perustella, joten turhan datan säilytys sotii jopa asetusta vastaan
  - Olette vastuussa siitä, mitä säilötte järjestelmissänne
    - ”En minä tiennyt, että meillä on tällaista” on todella huono selitys
- Ei kannata unohtaa maalaisjärkeä
  - Tietosuoja-asetus ei tule voimaan tuhotakseen organisaatioita, vaan suojelemaan yksityisyyttä

Linkkejä:

https://www.eugdpr.org/

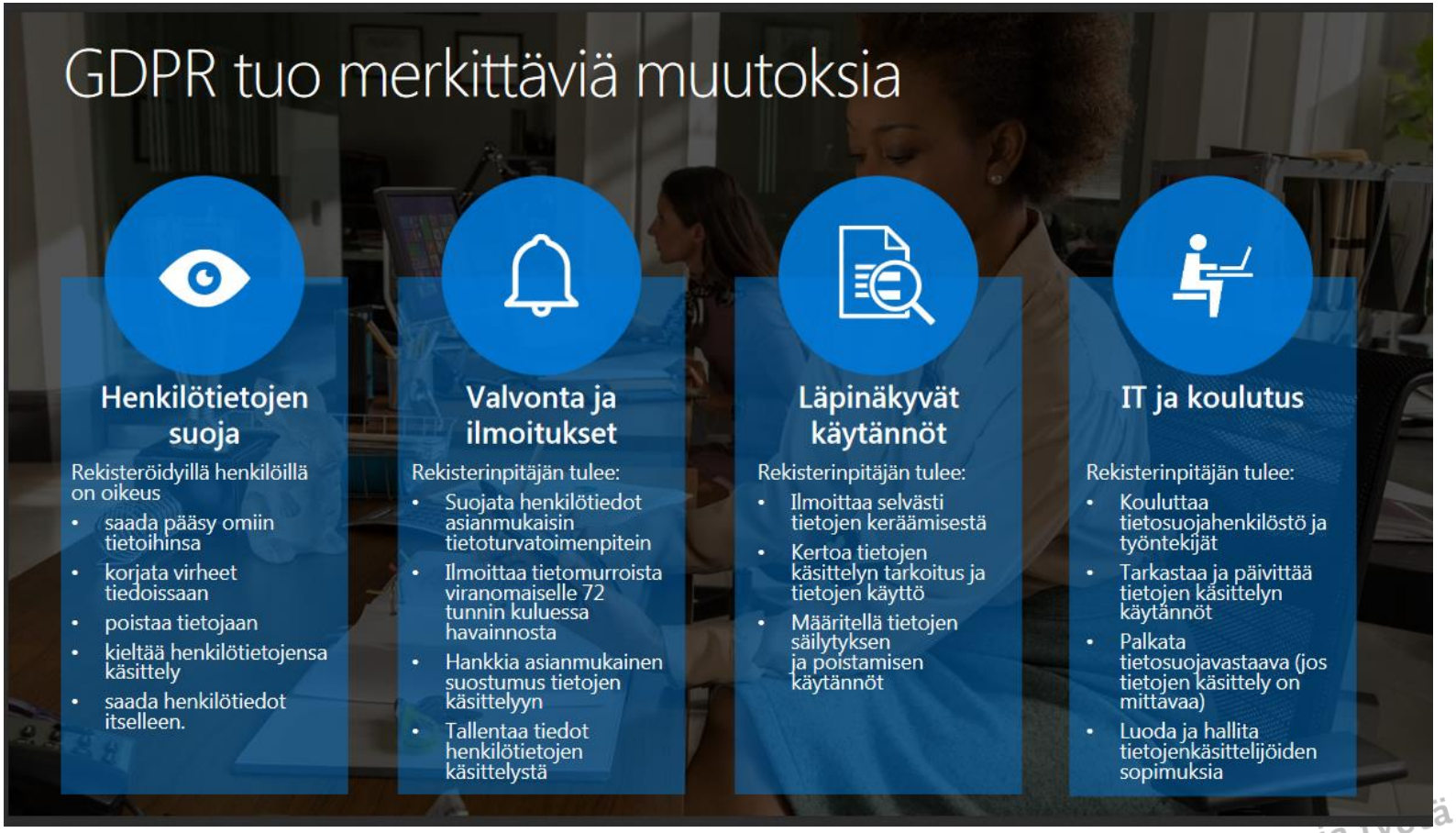
http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL

http://www.tietosuoja.fi

Muuta:

- Elisan webinaarit
- Muita webinaareja / Google -> GDPR webinaari

Ville Kankareen (Elisa) esitys Seinäjoen seminaarista



https://sotenavi.turkuamk.fi/seminaarit/seinajoen-valtakunnallinen-seminaari-21-3/

Kiitos!

Mustajärvi, Arttu

Arttu Mustajärvi
Teknologia-assistentti
Tekniikka

+358503823330 Matkapuhelin
arttu.mustajarvi@eptek.fi

Kestävää kasvua ja työtä -ohjelma

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan sosiaalirahasto