LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

EU-tietosuoja-asetus
Vaikutukset korkeakoulun IT:n näkökulmasta
Case Laurea

FUASin etiikkaseminaari 4.4.2017 – Laurea

Kimmo Pettinen

Sisältö

- Tieto - henkilötieto
- GDPR:n vaikutukset
  - Pääasiallinen lähde: *Miten valmistautua EU:n tietosuoja-asetukseen / Tietosuojavaltuutetun toimisto + OM*
- Mitä on tehty/tekeillä?
- Mitä seuraavaksi?

- CSC:n palvelut avoin data

Tieto - henkilötieto

- Tiedolla on kolme ominaisuutta, joita haluamme/täytyy suojata:
  - Luottamuksellisuus (confidentiality)
    - Vain ne keillä on tehtävänsä mukaisesti oikeus käsitellä tietoa
  - Eheys (integrity)
    - Tieto pysyy muuttumattomana, oikeana ja täydellisenä
  - Käytettävyys (availability)
    - Tieto (tietojärjestelmä) on silloin saatavissa kun valtuutetut niitä tarvitsevat
- ”*Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.*”

GDPR:n vaikutukset

- Tietosuoja-asetus
  - Velvoittaa jäsenmaissa toimivia yrityksiä ja julkisia toimijoita
  - Tietosuoja-asetus voimaan 24.5.2016, sovelletaan 25.5.2018 alkaen
    - Silloin henkilötietojen käsittelyn on oltava tietosuoja-asetuksen mukaista!
  - OM:n asettama työryhmä:
    - Selvittää mm. onko tarvetta erilliselle henkilötietolaille
    - Valmistelee tarvittavan lainsäädännön tietosuojaviranomaisesta
    - Jäsenvaltioiden kansallisen liikkumavaran
    - Mietintö 31.5.2017 mennessä

GDPR:n vaikutukset

- Rekisteröidyn nykyiset oikeudet säilyvät
  - oikeus tarkastaa ja oikaista itseään koskevat tiedot
  - oikeus tulla unohdetuksi
- Rekisteröidyn uusia oikeuksia
  - Tietojen saaminen sähköisesti
  - Siirto toiseen järjestelmään
  - Lasten henkilötietojen käsittelyyn vanhempien lupa
  - Oikeus tietojenkäsittelyn vastustamiseen

GDPR:n vaikutukset

- Yrityksille velvollisuus
  - Nimittää tietosuojavastaava mikäli ehdot täyttyvät
  - Ilmoittaa tietoturvaloukkauksista valvontaviranomaiselle ja rekisteröidylle
    - Kaikille niille joita tietoturvaloukkaus koskee!!

GDPR:n vaikutukset

- Rikkeistä valtavat sakot (4% tai 20 M€)
- Organisaatiolla on oltava kyky osoittaa noudattavansa
  - asetusta henkilötietoja käsiteltäessä sekä
  - toteuttavansa tietosuojaperiaatteita myös käytännössä
- Riskiperusteinen lähestymistapa – riskit arvioitava

GDPR:n vaikutukset

- Osoitusvelvollisuus edellyttää käsittelyyn liittyvien prosessien sekä tietosuojaperiaatteiden käytännön toteuttamisen **dokumentointia**.
- … rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan **varmistaa ja osoittaa**, että asetusta noudatetaan.

Mitä on tehty/tekeillä

- AMK-sektorilla:
  - ARENE:n työryhmä http://www.arene.fi/fi/arene/ajankohtaista/tyoryhma-tukemaan-tietosuoja-asetuksen-soveltamista-ammattikorkeakouluissa
    - Tavoitteet:
      - Kartoittaa, mitä tietosuoja-asetus merkitsee ammattikorkeakouluille
      - Tukea yhteistyön organisoitumista koko korkeakoulusektorilla
      - Tukea tietosuojavastaavien verkostoitumista
      - Valmistella yhteisiä linjauksia, toimintamalleja, ohjeita yms. yhteiseen käyttöön

Mitä on tehty/tekeillä

- AMK-sektorilla:
  - Korkeakoulujen välinen IT yhteistyö
    - Eduuni – yhteinen työtila, johon kerätään tietoja kypsyystasosta
  - Yhteistyötä Euroopan korkeakoulujen kanssa (EUNIS)

Mitä on tehty/tekeillä

- Laureassa
  - Tietosuojavastaava nimitetty
    - Tietosuojavastaavan koulutuksessa
    - Tiivis työpari tietoturvavastaavan kanssa
  - Huomiointi sopimuksissa
    - Perustietotekniikka kilpailutus – ***tietosuojaliite***
    - Kuvattu rekisterinpitäjän ja käsittelijän vastuut ja velvollisuudet
  - Tietoturvan systemaattiseen hallintaan järjestelmä
    - Käyttöönottokoulutus tänään 4.4.2017
  - Tietojärjestelmien kriittisyysluokitus
  - Menossa oppimis- ja tiedonhankintavaihe

Mitä seuraavaksi

- Tietotilinpäätöksen suunnittelu
  - Käsiteltävien henkilötietojen inventaario toiminnoittain
    - Henkilötietojen käsittelijät (myös kolmannet osapuolet)
  - Tietovirtakaaviot
  - Tietosuojan edellytysten arvioinnit ja mahdolliset tietosuojan vaikutusten arvioinnit
  - Rekisteriselosteiden ajantasaisuuden ja viestinnän tarkastus
  - Sopimusten tietosuoja- ja tietoturvavaatimukset
  - Koonti ja tulokset tietotilinpäätökseen
  - Arkkitehtuurikuvausten ylläpito

Haasteita

- Koulutus/tiedonjako
  - IT-Porukat oppiin
  - Myös koko organisaation tasolla
- Tietojärjestelmiin kohdistuvat vaatimukset
- Datan poistoprosessi jos käyttäjä haluaa tulla unohdetuksi
  - Mitä tietoa pitää/voi poistaa
  - Mitä lain mukaan on säilytettävä
  - Mitä tarkoittaa muutostöinä?