

Tietosuojavastaavana julkisella sektorilla

Kokemuksia tietosuojavastaavan työstä ja UEF tietosuoja-asetus projekti

Juhta/Vahti, osoitusvelvollisuutta edistävä työpaja 12.2.2018

Helena Eronen, tietosuojavastaava

Kuka puhuu?

Helena Eronen:

- pätkätöitä Joensuun maakunta-arkistossa 1988-1989
- **arkistosihteeri** PKSHP/Asiakirjahallinto 1989-2003 (hallituksen nimeämä tietosuojasta vastaava viranhaltija 2000 – 2003)
- **arkistotoimen johtaja, tietosuojavastaava** PPSHP/Asiakirjahallinto 2003 – 2012
- **kehittämispäällikkö, tietosuojavastaava**, PSSHP/Tietohallinto 1.10.2012 – 28.2.2017
- **tietosuojavastaava** Itä-Suomen yliopisto/ Yliopistopalvelut, 1.3.2017 alkaen
- asiantuntijana Kanta-palveluiden määrittelytyössä ja käyttöönotossa
- Terveystietojen tietosuojan ohjausryhmän (TELLU) sihteeri
- Suomen Tietosuojavastaavat (TIEVA) puheenjohtaja 2013-2017
- STTY (Sosiaali- ja terveydenhuollon tietojenkäsittely-yhdistys) hallituksen jäsen 2015 - 2016
- asiakastietolain (159/2007) muutostyöryhmän jäsen 2015 - 2016

Kokemuksia tietosuojavastaavan työstä

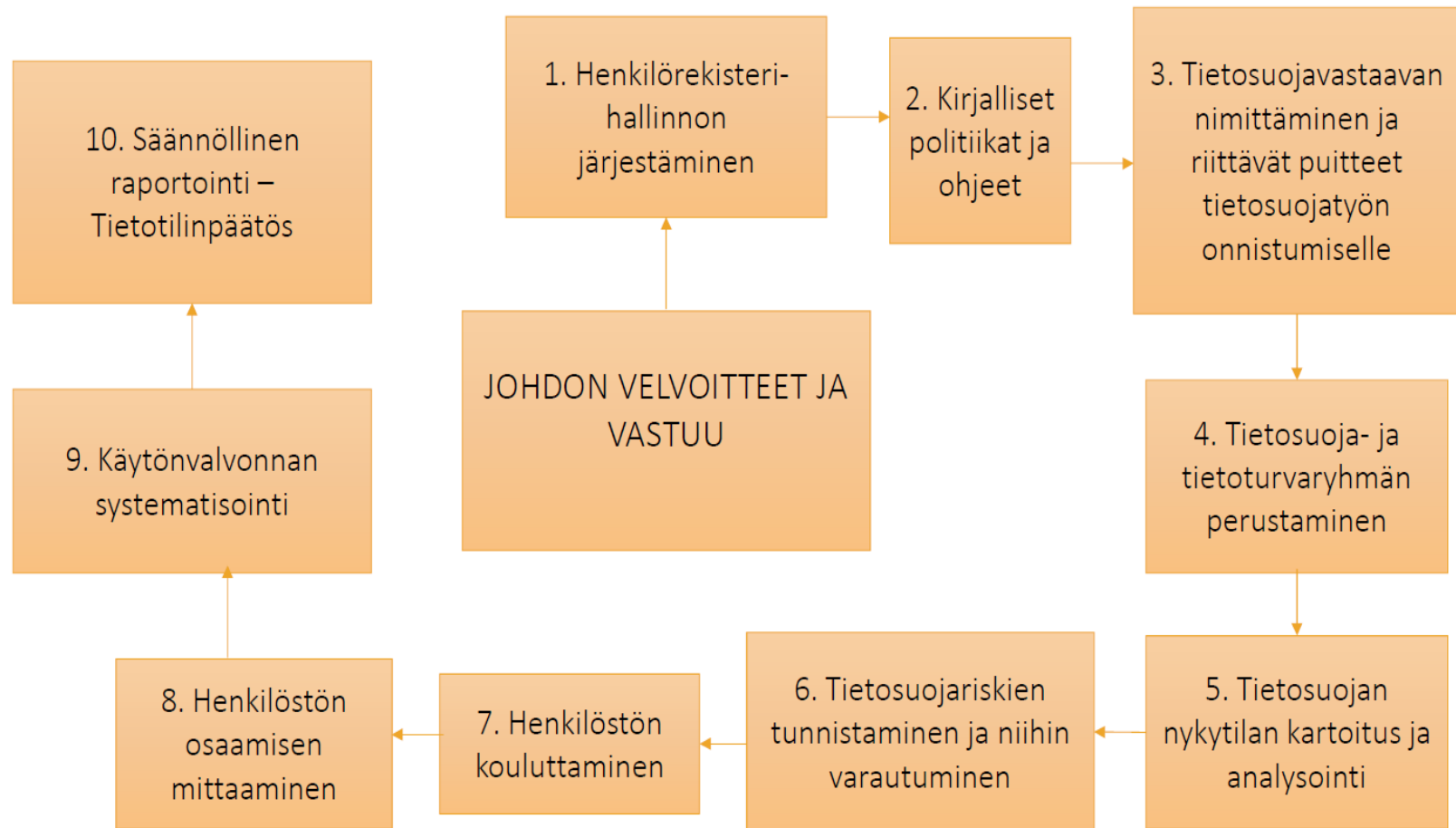
Tietosuojaavastaavan rooli ja asema

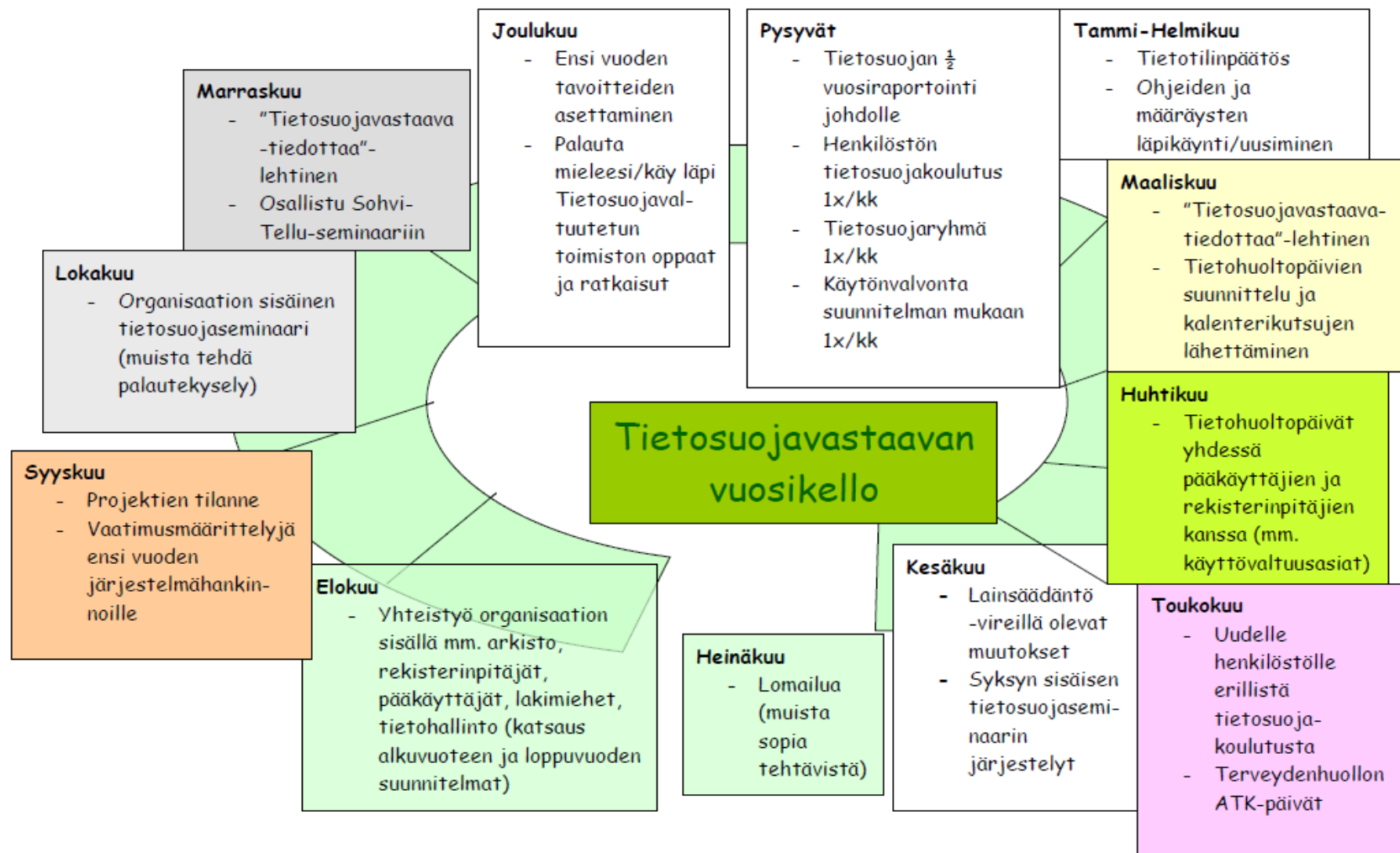


Tietosuojavastaava asiantuntijana

- Tietosuojavastaavan nimeäminen organisaatioon ei poista rekisterinpitäjänä olevan organisaation vastuuta
 - Tietosuojan taso ja sitä koskevat linjaukset ovat johdon vastuulla
- Ts –vastaava antaa asiantuntija-apua sekä henkilöstölle että ennen kaikkea johdolle, jolla on viimekätinen vastuu rekisterinpitäjänä henkilötietojen käsittelystä
 - Raportointi suoraan johdolle, riippumaton asema, johdon tuki
- Tietosuojavastaavan tehtävät, asema ja vastuu on syytä kuvata ja sopia ennen kuin ketään nimitetään tehtävään
 - Vrt. Kop, kop – ovi auki ja tyly ilmoitus: Sinä olet sitten tietosuojavastaava

Tietosuojatyön organisointi ja hallinta





Tiedon elinkaari

- Ajanjakso henkilötietojen keräämisestä niiden arkistointiin, hävittämiseen tai anonymisointiin



Haasteita

- Johdon tuki
 - Viestintä niin, että saat asiasi perille
- Henkilöstön saaminen mukaan tietosuojatyöhön
 - Organisaation ”virallinen mörkö” vai ”suurin hitler”
- Vuorovaikutustaidot rekisteröityihin päin
 - Viestintä kimpaantuneen asiakkaan kanssa on haasteellista

Perehdytys ja ohjeistus rekisterinpitäjän vastuulla

- Tietosuoja-asetus 25 artikla
 - Toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että käsitellään vain käyttötarkoituksen kannalta tarpeellisia henkilötietoja eikä niitä saateta rajoittamattoman henkilömäärän saataville
- Tietosuoja-asetus 32 artikla 4 kohta
 - Toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän ja henkilötietojen käsittelijän alaisuudessa toimiva käsittelee henkilötietoja ainoastaan rekisterinpitäjän ohjeiden mukaisesti
- Julkisuuslaki 18.1 § 5 kohta
 - Viranomaisen tulee huolehtia siitä, että sen palveluksessa olevilla on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta sekä tietojen antamisessa, käsittelyssä ja suojaamisessa noudatettavista menettelyistä, tietoturvallisuusjärjestelyistä ja tehtävänjaosta

Ohjeiden laatiminen tietosuojavastaavan tehtävänä

- Henkilötietojen käsittelyyn liittyvän ohjeistuksen suunnittelu ja laatiminen on keskeinen tietosuojavastaavan tehtävä
- Ohjeet laadittava tai päivitettävä aiemmat ohjeet
- Ohjeiden hallinta on jatkuva prosessi, ei kertaprojekti
- Yhteistyö kollegojen kanssa - yhtenäiset ohjeet saman alan toimijoilla

UEF Tietoturvallisuussäntöjä

Sääntö	Sisältö	Kohderyhmä
Tietoturvapolitiikka	Tietoturvallisuuden päämäärät, tavoitteet ja toteutus	Henkilöstö, opiskelijat
Tietoturvavastuut	Yleiset vastuut ja erityisvastuut	Henkilöstö, opiskelijat
IT-palvelujen käytäntösäännöt	IT-palvelujen käyttöä ja käyttäjätunnuksia koskevat yleiset periaatteet	Kaikki UEFin IT-palveluiden käyttäjät
Sähköpostisäännöt	Sähköpostin käytön periaatteet	Henkilöstö, opiskelijat
Seuraamuskäytäntö	Toimenpiteet rikkomusepäilyissä	Kaikki UEFin IT-palveluiden käyttäjät
IT-palveluiden ylläpitösäännöt	Ylläpitäjiä koskevat periaatteet	Tietojärjestelmien ylläpitäjät
Lokisääntö	Lokienhallinnan periaatteet	Omistajayksiköt, ylläpitäjät, tietotekniikkapalvelut
Työntekijän sähköpostin hakeminen ja avaaminen	Toimintaohje	Henkilöstö

Turvallisuussääntöjä täydentävät ohjeet

- Tietoaineistojen suojaaminen ja käsittely IT-järjestelmissä
- Tietoaineistojen käsittelyohje
- Sähköpostin suodatusohje
- Luettelo suodatettavista tiedostotyypeistä
- Toimenpiteet tietojärjestelmien käyttöoikeuden loputtua
- Ohjeet tietoaineistojen käsittelystä tietojärjestelmien käyttöoikeudenhaltijan kuoltua
- Tietoturvapoikkeamiin reagoiminen
- Tiedottaminen poikkeamatilanteissa

UEF henkilöstön ja opiskelijoiden oppaat

- [Henkilöstön tietoturvaopas](#)
 - [Henkilöstön tietoturvan pikaohje](#)
 - [Opiskelijan tietoturvaopas](#)
 - [Opiskelijan tietoturvan pikaohje](#)
 - [Mobiiliturvaohje](#)
- Lisäksi Tietotekniikkapalveluiden intra-sivuilla sisäisiä ohjeita ja koulutusaineistoa

UEF tietoaineistojen käsittelyohjeita

- Arkistonmuodostussuunnitelma
- Tietoaineistojen käsittelyohje

Itä-Suomen yliopiston tietoaineistojen käsittelyohje 14.11.2016

toimenpide	julkinen aineisto	perussuojaustaso	korkea suojastaso	rajaukset ja huomautukset
Aineiston tallennus työasemaan, verkkolevyille tai muistitikulle				
tallennus yliopiston työasemaan	sallittu	sallittu	sallittu, suositellaan salausta	käyttäjän huolehdittava itse varmuuskopiointista
tallennus henkilökohtaiselle X-verkkolevyille *)	sallittu	sallittu	sallittu	ei rajoituksia
tallennus henkilökoht. LocalDrive-tallennustilaan	sallittu	sallittu	sallittu	ei rajoituksia
tallennus henkilökohtaiseen MyPlace-tallennustilaan *)	sallittu	sallittu, rajauksin	sallittu, rajauksin	rajaus: on varmistettava ettei tiedostoja jaeta tai jaetaan vain määritellyille
tallennus henkilökohtaiseen OneDrive for Business-tallennustilaan (UEF hallinnoima O365-palvelu)	sallittu	sallittu, rajauksin	ei sallittu	rajaus: on varmistettava ettei tiedostoja jaeta / jaetaan vain määritellyille, huolehdittava varmuuskopiointista
aineiston tallennus (kopiointi) muistitikulle tai ulkoiselle kovalevyille	sallittu	sallittu, suositellaan salausta	sallittu vain salattuna	salauk: käytettävä salaavaa muistitikku/levyä tai aineisto suojataan salauksella
Aineistojen tallennus tai jakaminen julkisissa pilvipalveluissa				
tallennus julkiseen pilvipalveluun (esim. Dropbox, GoogleDrive, kuluttaja-OneDrive)	sallittu	ei sallittu	ei sallittu	käyttäjän huolehdittava itse varmuuskopiointista
Aineiston lähettäminen sähköpostilla				
lähetyt sähköpostina yliopiston sisällä	sallittu	sallittu	sallittu vain salattuna	suositellaan aineistojen toimittamista muiden palvelujen avulla
lähetyt sähköpostina yliopiston ulkopuolelle	sallittu	sallittu, rajauksin	sallittu vain salattuna	rajaus: käytettävä harkiten, suositellaan salausta tai aineistojen toimittamista muiden palveluiden avulla
Yhteisten verkkolevyjen ja verkkopalveluiden käyttö				
tallennus yksikön tai projektin yhteiselle verkkolevyille *)	sallittu	sallittu, rajauksin	sallittu, rajauksin	käyttöoikeudet vain niille joilla oikeus aineistoihin, yliopiston ulkopuolisilta salassapitositoumukset
tallennus yksikön tai projektin LocalDrive -työtilaan	sallittu	sallittu, rajauksin	sallittu, rajauksin	käyttöoikeudet vain niille joilla oikeus aineistoihin, yliopiston ulkopuolisilta salassapitositoumukset
tallennus yksikön tai projektin Sharepoint -työtilaan (UEF hallinnoima O365-palvelu)	sallittu	sallittu, rajauksin	ei sallittu	samat rajoitukset kuin yksikön/projektin localdrive-työtiloissa, lisäksi huolehdittava varmuuskopiointista
tallennus yksikön tai projektin TeamPlace-työtilaan *)	sallittu	sallittu, rajauksin	sallittu, rajauksin	samat rajoitukset kuin localdrive-työtilassa
tallennus yliopiston sisäisen ryhmän käyttöön rajattuun työtilaan (esim. UEF intranet työtila)	sallittu	sallittu, rajauksin	ei sallittu	rajaus: alueen käyttöoikeudet tulee rajata vain niille joilla oikeus käsitellä aineistoa
tallennus koko yliopistoyhteisölle avoimeen intranet -työtilaan (esim. UEF intra)	sallittu	sallittu, rajauksin	ei sallittu	rajaus: jaettavien aineistojen tulee olla sellaisia, joita voidaan jakaa koko yliopistoyhteisölle
aineiston jako yliopiston sisäisissä Yammer- viestiryhmissä (EU:n ulkopuolella sijaitseva palvelu)	sallittu	sallittu, rajauksin	ei sallittu	rajaus: jaettavien aineistojen ei tule sisältää luottamuksellisia henkilö- tai muita tietoja
Tallennus mobiililaitteisiin, tukostaminen				
tiedon säilytys matkapuhelimessa tai mobiililaitteissa	sallittu	sallittu, rajauksin	sallittu, rajauksin	rajaus: laite suojattava PIN-koodin lisäksi lukituskoodilla (numerokoodi tai salasala)
tukostaminen	ei rajoituksia	sallittu, rajauksin	sallittu, rajauksin	rajaus: käytettävä turvatulostuslupa (tai oheistulostinta)

*) poistuva palvelu, korvataan muilla palveluilla

Korkeakoulujen yhteinen ohjeistus

- Valmistunut
 - Korkeakoulujen opintotietojen tietosuojan käytäntesäännöt
 - Ohje ammattikorkeakoulujen ja yliopistojen opintohallinnon työn tueksi
 - Tietosuojavaltuutetun 2.5.2017 tarkastamat käytäntesäännöt
- Suunnitteilla
 - Korkeakoulujen yhteinen tietosuojapolitiikka
 - Yhteiset tieteellisen tutkimuksen tietosuojan käytäntesäännöt (hanke alkaa yhteisellä kokouksella 7.9.2017)
 - Sopimukseen tulevat tietosuojaliitteet (Helsingin yliopiston laatiman luonnoksen pohjalta valmistellaan yhteistyönä)

Ohjeiden laatiminen ja niiden sisällön kouluttaminen

- Pitää ensin selvittää, mitä ohjeita sekä minkälaista koulutusta henkilöstö kaipaa
- Esimiehet keskeisessä roolissa vaikuttamassa mm. uuden työntekijän perehdyttämisprosessin onnistumiseen
 - Pitää muistaa hyvän esimerkin tärkeys!
- Kannattaa osallistaa koko organisaatio jo ohjeistuksen laatimisen aikana
- Koulutuksen pitää olla käytännönläheistä eli kouluttajan pitää pystyä tunnistamaan substanssin erityispiirteet
- Pitää muistuttaa aina, että oikeaoppiset käytännöt tuovat oikeusturvaa organisaatiolle, työntekijälle ja asiakkaalle
- Koulutetaan tietoturvan ja tietosuojan yhteyshenkilöitä yksiköihin, joilta saa neuvoja ja jotka voivat myös suodattaa keskeisimmät ongelmat ohjeiden tulkinnassa tai muutostarpeissa esim. tietosuojavastaavalle tai tietoturva- ja tietosuojaryhmälle ratkaistavaksi

Malli seuraamustaulukosta

TAHALLISUUDEN ASTE RIKKOMUKSEN VAKAVUUS	Tietämättömyys, osaamattomuus, erehdys, vahinko, huolimattomuus	Piittaamattomuus, tahallisuus, toistuvuus
<u>Vakava rikkomus</u> (lain mukaan rikkomuksena tai rikoksena ttava teko)	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään	- tehdään rikosilmoitus - palvelusuhteen päättämismenettelyn käynnistys
<u>Rikkomus</u> (vakava väärinkäyttö tai turvallisuuden rikkominen)	- puheeksi ottaminen ja opastus - suullinen huomautus - kirjallinen varoitus	- kirjallinen varoitus - rikosilmoitusta harkitaan tai tehdään - palvelussuhteen päättämismenettelyn käynnistys
<u>Lievä rikkomus</u> (asiaton toiminta tai väärinkäytös)	- puheeksi ottaminen ja opastus - suullinen huomautus	- suullinen huomautus - kirjallinen varoitus - palvelussuhteen päättämismenettelyn käynnistys

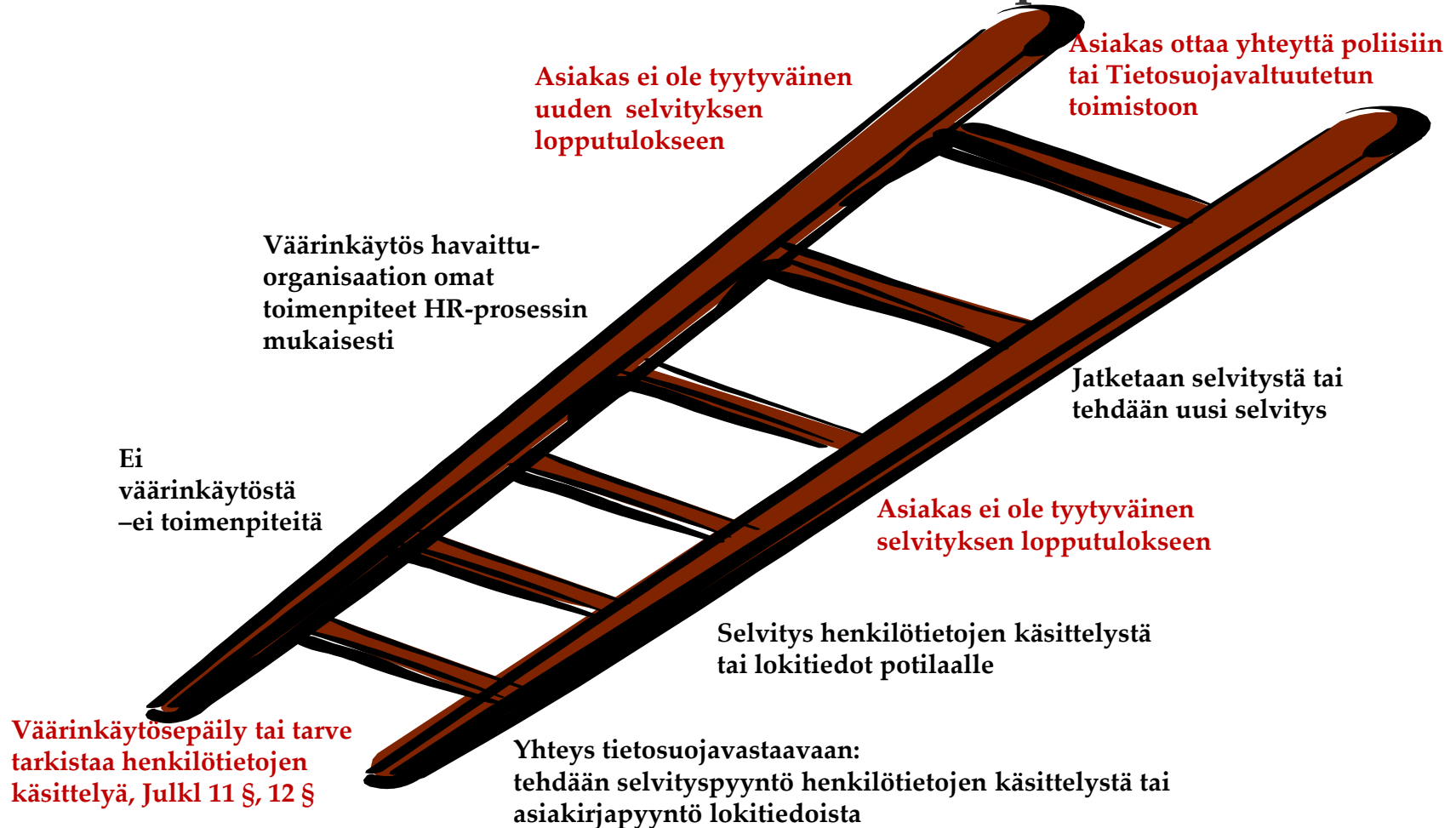
Koulutuskokemuksia

- Sisäisiin koulutuksiin osallistuminen vaihtelee
 - Ne, jotka eniten koulutusta tarvitsevat eivät aina tule koulutukseen tai käyvät kuittaamassa mahdollisen pakollisen läsnäolon ja poistuvat pian
- Miten saat koulutuksen sisällön kiinnostavaksi?
 - Käytännön esimerkit auttavat
- Tietosuojaavastaavan oma kouluttautuminen
 - Et voi kouluttaa toisia, jos et itse saa riittävää täydennyskoulutusta
 - Koulutusten hinta

Käytönvalvonnan prosessit

- Asiakaslähtöinen käytönvalvonta
 - ulkoinen asiakas epäilee väärinkäytöstä tai haluaa tarkistaa asiakastietojensa käsittelyn oikeellisuuden
- Harkinnallinen sisäinen valvonta
 - epäillään väärinkäytöstä ja tuodaan asia tietosuojavastaavalle toimenpiteitä varten
- Systemaattinen valvonta
 - etukäteissuunnitelmaan perustuva systemaattinen valvonta
 - esim. tietyin väliajoin, tietyn yksikön henkilökunta tai satunnaisotannat

Asiakaslähtöisen lokivalvonnan tikapuut



Hajautettu lokienhallinta

- **Lokit haettava jokaisesta järjestelmästä erikseen**
 - Tuottavatko kaikki henkilötietoja käsittelevät järjestelmät lokia?
- **SaaS –palvelut**
 - Lokit tilataan järjestelmätoimittajalta, maksu?
- **Eri järjestelmät lokittavat toisistaan poikkeavia asioita ja tuottavat erilaisia lokitulosteita**
 - Käyttäjähallinnan kautta voi lokille tulostua outoa tietoa
- **Ihmisen analysoitava**
 - tunnettava organisaation prosessit ja tietojärjestelmien toiminta sekä tiedettävä versionvaihdot

Keskitetty lokienhallinta

- Lokit haetaan yhdestä järjestelmästä, joka tuottaa kaikkien siihen liitettyjen järjestelmien lokit
 - onko kaikki henkilötietoja käsittelevät järjestelmät liitetty keskitettyyn hallintaan ja tuottavatko kaikki järjestelmät tarvittavan lokin?
 - voidaanko saas-palveluna tuotettujen järjestelmien lokit liittää keskitettyyn lokienhallintaan?
- Tuloste samanlainen kaikkien keskitettyyn hallintaan liitettyjen järjestelmien osalta?
 - lokikuvaukset ja määrittely lokitettavista tiedoista ennen käyttöönottoa
 - kaikki järjestelmät pystyvät tuottamaan samat lokitiedot
- Yleensä ihmisen analysoitava

Potilastietojärjestelmien lokitulosteista

- Acute: tilattava toimittajalta, tulostuu excel-muotoon (muokattavissa), sisältää outoja lyhenteitä ja termejä
- Effica: excel muotoinen (muokattavissa), sisältää outoja termejä ja lyhenteitä sekä asiakkaalle kuulumatonta tietoa (käyttäjätunnukset, tietokoneen numerot)
- Esko: ei muokattavissa, helppolukuinen, mutta sisältää asiakkaalle outoja termejä
- Mediatri: erilliset tulosteet tietosuojavastaavalle ja potilaalle, selkokielen ja ymmärrettävä
- Pegasos: tulostus hankalaa, eri osiota, joista voi tulostua eri tietoja, termit täysin vieraita asiakkaille
- Uranus: hidas haettava, tulostuu valtavasti rivejä, sisältää käyttäjätunnukset ja koneen numerot, jotka poistettava,
- Logmonitor, keskitetty järjestelmä: monen järjestelmän lokit kerralla, excel-muotoinen, sisältää automatiikkaa, mutta silti ihmisen analysoitava

Yhteistyö johdon ja henkilökunnan kanssa

- Tapaamiset johdon kanssa
 - Tietosuoja-asioiden säännölliset käsittelyt johtoryhmien kokouksissa
 - Vuosittainen raportointi johdolle + ad hoc –raportit tarvittaessa
- Henkilökunnan tukena tietosuoja-asioissa
 - Tavoitettavuus
 - Neuvonta, opastus ja tuki
- Erilaiset työryhmät

Rekisteröityjen tukena tietosuoja-asioissa

- Yhteystiedot julkisesti saataville
 - Organisaatioiden nettisivujen kautta hakusana tietosuojavastaava tuottaa aika usein tuloksen ”hakuehtojasi vastaavia tietueita ei löytynyt”
- Mahdollisuus asiointiin tietosuojavastaavan kanssa ainakin terveydenhuollossa tarpeellinen
 - Joskus haasteellisia asiakkaita
- Opastus, neuvonta ja asioiden selvittäminen sekä pyyntöihin vastaaminen

Tietosuojavastaavan verkosto

- Omassa organisaatiossa, mm.
 - Ylin johto, tietosuoja-/tietoturvaryhmä
 - Tietoturva-, turvallisuus-, potilasturvallisuushenkilöt, asiakirjahallinto ja arkistotoimi
 - Yksiköiden tietosuojayhdyshenkilöt
- Muut tietosuojavastaavat
 - Yhteistyö tietosuojavastaavien kesken
 - Korkeakoulujen tietosuojavastaavilla sähköpostilista ja yhteisiä kokouksia 4 – 5 krt/v
- Viranomaiset

EU:n tietosuoja-asetuksen toimeenpano UEFissa

4 tiedekuntaa

Filosofinen tiedekunta
JOENSUU | SAVONLINNA

Luonnontieteiden ja
metsätieteiden tiedekunta
JOENSUU | KUOPIO

Terveystieteiden tiedekunta
KUOPIO

Yhteiskuntatieteiden ja
kauppätieteiden tiedekunta
JOENSUU | KUOPIO | SAVONLINNA

24. Maailman parhaiden
nuorten yliopistojen
listalla QS Top 50
Under 50 -vertailussa

15 000

TUTKINTO-OPISKELIJAA

20 000

AIKUISOPISKELIJAA

2700

HENKILÖSTÖÄ

300

Maailman parhaan
yliopiston joukossa
useissa kansainvälisissä
vertailuissa

13 koulutusala

100

PÄÄAINETTA /
KOULUTUSOHJELMAA

2500

TUTKINTOA, joista
160 tohtoritutkintoja (2014)

1000

ULKOMAISTA VAIHTO-/ TUTKINTO-
OPISKELIJAA VUOSITTAIN

uef.fi

Tietosuoja-asetus -projekti

- Projektin ohjausryhmä:
 - Petri Rintamäki, lakiasiaainjohtaja
 - Juha Eskelinen, tietohallintojohtaja
 - Olavi Manninen, tietoturvapäällikkö
 - Helena Eronen, tietosuojavastaava
- Ohjausryhmä kokoontuu kuukausittain ja seuraa valmistautumisprojektin etenemistä, hallintojohtaja on mukana kokouksissa tarvittaessa.
- Sovittu osa-alueet ja niiden vastuuhenkilöt

1. Hallinnolliset tehtävät

- Tietosuojaavastaava nimitetty
- Projektilla on ohjausryhmä
- Johdon ja hallituksen informointi ja seurannasta sopiminen:
 - tilannekatsaus UEF-joryssa 23.1.2018
 - säännöllinen tilanneseuranta joryssa
 - tilannekatsaus yliopiston hallitukselle 18.4.2018
 - tutkimus ja tietosuoja aiheena johdon päivillä 8.2.2018
- Tilanneseuranta myös yliopiston turvaryhmässä
- Tiedottaminen yt-toimikunnassa 19.2.2018

2. Tietosuojaselosteiden/ilmoitusten uusiminen

- Tietosuojapolitiikka
 - Korkeakouluyhteistyössä kaikkien käyttöön pohjadokumentti, valmisteluvastuu Aalto-yliopistolla.
- Tietosuojaselosteet/-ilmoitukset
 - Nykyiset rekisteriselosteet päivitetään
 - Uudet selosteet/ilmoitukset eivät rekisterikohtaisia vaan laajempia käyttötarkoitukskohtaisia, esim. henkilöstöasiat, rekrytointi, opiskelijoiden tietojen käsittely, oppilaiden tietojen käsittely, oppimisympäristöt, talousasiat, käyttäjähallinta, tekniset alustat, kiinteistöhuolto jne.

3. *Tietojärjestelmäkuvaukset*

- IT-järjestelmäluetteloon kootaan nykyistä tarkemmat kuvaukset tietojärjestelmistä -> toimii jatkossa niin Tipan kuin tietosuojavastaavan työvälineenä.
- Henkilötietojen käsittely tietojärjestelmissä kuvataan erilliselle lomakkeelle (eLomake)
 - Tipan lomakkeella tekniset tiedot
 - Omistajayksikön lomakkeella toiminnalliset tiedot

4. *Henkilötietoaineistojen kartoitus*

- Kartoitettu tietojärjestelmät
- Tutkimusaineistokyselyllä kartoitettu tutkimuaineistot. Vuoden 2017 loppuun mennessä on saatu eLomake – järjestelmään 429 vastausta sekä muutamia vastauksia sähköpostilla.
 - Aineistojen omistajuus ja henkilötietojen käsittely
- Arkistossa olevat henkilötiedot: selvitys menossa
- Yksiköissä olevat henkilötiedot: selvitys alkamassa

5. Tietojärjestelmäsopimukset

- Laadittu tietosuojasopimus ja valmistelussa siihen kaksi liitettä
 - Liite 1: tietojenkäsittelyn kuvaus
 - Liite 2: organisatoriset ja tekniset toimenpiteet
- Tietosuojasopimus liitetään olemassa oleviin sopimuksiin, läpikäynti aloitetaan muutamasta toimittajasta ja saatujen kokemusten perusteella loput.
- Uusien järjestelmien hankinnassa huomioidaan tietosuoja-asetus.

6. Tietotilinpäätös

- Antaa kokonaiskuvan tietojenkäsittelyn nykytilasta ja kuvaa hyvän tietojenkäsittelytavan noudattamista.
- Tapa hoitaa tietosuoja-asetuksen osoitusvelvollisuutta.
- Ensimmäinen tietotilinpäätös tehdään vuodesta 2018.
- Valmistelu aloitetaan syksyllä 2018.

7. Rekiserinpitäjän velvollisuuksiin liittyvät prosessit

- Vaikutustenarviointi ja ennakkokuuleminen
- Tietoturvaloukkaukset ja niistä ilmoittaminen
- Aktiivinen informointi
- Tietosuoja-asiat mukaan tutkimuksen prosesseihin

8. Rekisteröidyn oikeuksiin liittyvät prosessit

- Informointi henkilötietojen käsittelystä
- Tieto-, korjaus-, poisto-, siirto- ja vastustamispyynnöt
 - Kuka ottaa vastaan pyynnöt ja huolehtii vastauksen antamisesta
 - Kuinka saadaan tuotettua pyydetyt tiedot
- Valmis toukokuussa 2018

9. Tietosuoja – ja tietoturvariskit

- Kartoitetaan henkilötietojen käsittelyyn liittyvät tietosuoja- ja tietoturvariskit sekä korkean riskin omaavat järjestelmät ja aineistot.
- Organisaation omat toimet riskin minimoimiseksi.
- Yliopistotason riskikartoitus on tehty aiemmin, tehtävänä sen päivittäminen – joudutaan todennäköisesti siirtämään syksyyn 2018

10. Tietoaineistojen käsittelyn ohjeistus

- Päivitetään olemassa oleva ohjeistus ja saatetaan se henkilöstön tietoon.
- Huomioidaan pseudonymisointi ja anonymisointi.
- Aloitetaan syksyllä 2018.

11. Ohjeet ja säännöt

- Tietosuojapolitiikka
 - Yhteistyössä korkeakoulujen kanssa
- Tietosuojasivuston laajentaminen uuf.fi –sivustolle sekä Heimoon ja Kamuun
- Käytännesäännöt henkilötietojen käsittelystä yhteistyössä korkeakoulujen kanssa
- Tietoturvasäännösten osalta päivitettävä lokisääntöä.

12a. Laitosten ja tutkimusryhmien palvelimet ja järjestelmät: tietoturvaasteita

- Pienet ylläpitoresurssit, usein 1 henkilö.
- Pitkä käyttöikä -> tietoturvapäivitysten loppuminen.
- Varmuuskopiointijärjestelyt kevyet/puutteelliset.
- Tipalla ei tietoja palvelimista eikä niillä toteutetuista ratkaisuksista.

12b. Laitosten ja tutkimusryhmien palvelimet ja järjestelmät: ratkaisut

- Kootaan palvelinrekisteri.
- Yksikkökohtaiset konsultoivat auditoinnit.
- Erilliset palaverit ja koulutus yksiköille.
- Lisätään myös yksiköiden omat järjestelmät IT-järjestelmärekisteriin.

13. Muutokset järjestelmiin/uudet järjestelmät

- Loki/SIEM –järjestelmän hankinta (menossa).
- IDM –järjestelmän uusiminen (kytketään Mepco-projektiin).
- O365 –varmistusjärjestelmä (2018).
- O365 –suojausominaisuuksien hyödyntäminen (pilotti).
- Turvaposti (käytön laajentaminen).
- MDM –järjestelmä: mobiililaitehallinta.
- Järjestelmien hallinnoinnin tietoturvakäytännöt.
- Salauksen käyttö järjestelmissä.

14. Omistajayksiköiden roolin selkiyttäminen

- Omistajayksikön rooli ja vastuu omasta kokonaisuudestaan.
- Rekisterinpitäjän ja henkilötietojen käsittelijän roolit.
- Tutkimusaineistojen omistajuus.

15. Tietosuojakoulutukset ja -testit

- Johdon perehdytys
 - Tilannekatsaukset säännöllisesti hallituksessa ja johtoryhmissä
 - Johdon päivät tarvittaessa (aihe esillä Johdon päivillä 2018)
- Yleiskoulutukset koko henkilöstölle
 - Pidetään lukukausittain, kevät 2018 kaksi kertaa, jatkossa kerran lukukaudessa vuoroin Joensuussa ja Kuopiossa, videointi toiselle kampukselle
- Kohdennetut koulutukset tutkimus- ja opetushenkilöstölle
 - Pidetään säännöllisesti luentosalikoulutuksia lukukausittain, kevät 2018 kaksi koulutusta, jatkossa kerran lukukaudessa
 - Tarvittaessa erillisiä koulutuksia tiedekunta-/laitos-/yksikkötasolla
- Verkkokoulutusympäristö ja tietosuoja-/tietoturvatestit
 - Asia valmistelussa tietosuojavastaavalla ja tietoturvapäälliköllä
- Tehdään henkilökunnalle jaettava esite tietosuoja-asetuksesta

Seuraavat koulutustilaisuudet

- **Tietosuoja tutkimustyössä**

- Kaksi saman sisältöistä koulutusta Kuopiossa 16.2. ja Joensuussa 20.3., videointi kaikille kampuksille ja Joensuun tilaisuus tallennetaan
- Koulutuksen sisältö:
 - Tietosuojalainsäädännön soveltaminen tieteellisessä tutkimuksessa ja henkilötietojen käsittelyn perusteet, Tietojensaantiin liittyvät kysymykset, Tutkimussuunnitelma ja aineistohallinta
 - Henkilötietojen käsittely tutkimustyössä (tunnisteelliset henkilötiedot, rekisterinpitäisyys, suostumus, informointi, arkistointi, tietojen hävittäminen, pseudonymisointi, anonymisointi)
 - Tietojen säilyttämien ja suojaaminen tutkimuksen aikana - mitä välineitä ja keinoja UEF tarjoaa

16. Tietosuoja- ja tietoturvayhteistyö

- Tietosuojayhteistyö
 - Korkeakoulujen tietosuojavastaavien yhteistyöryhmä
 - Tietosuojavaikuttetun toimiston johtamat yhteistyöryhmät
- Tietoturvayhteistyö
 - Yliopistojen Sec-työvaliokunnan kautta
- Juhta/Vahti yhteistyö

Mitä toivotaan yliopiston johtoryhmältä?

- Tehtäväkenttä todella laaja ja siirtymäaika päättyy 25. toukokuuta.
- Toivotaan yliopiston johtoryhmän, rehtoraatin, yliopistopalvelujen ja tiedekuntien johdon tukea projektin eri osa-alueiden läpiviemiseen.

Toiveet yliopistopalveluille

- Tietosuojaselosteet/-ilmoitukset:
tietosuojavastaava laatii luonnokset, yksiköistä tarvitaan täydentämistä ja kommentointia.
- Tietojärjestelmäkuvaukset:
pääkäyttäjien täytettäväksi eLomake –järjestelmässä henkilötietojen käsittelyn kuvaukset

Toiveet tiedekunnille ja laitoksille

- Järjestetään auditointikeskustelut yksiköiden ja tutkimusryhmien kanssa: kemia, soveltava fysiikka, tietojenkäsittelytiede, bioinformatiikka, A. I. Virtanen-instituutti, farmasia, normaalikoulu ym.
- Kootaan tiedot yksiköiden palvelimista ja järjestelmistä.
- Tipalla on jatkossa tiedot laitosten järjestelmistä ja pystytään paremmin tukemaan yksiköiden ratkaisuja sekä tietoturvan ja tietosuojan toteutumista
- Laitosten tietosuojayhdyshenkilöt?

SMART SCIENCE BY *SMART* PEOPLE