Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet

#tuki2018 #stöd2018

Työpaja #6 – 17.11.2017

- Tietosuojavastaavan rooli sekä vastuut
- Tietoturvapoikkeama- ja tietosuojaloukkaustilanteiden hallinta, osa 1 – taustaa, havainnointikyky sekä reagointi – kuinka tietosuojaloukkaukset voidaan tunnistaa? Tiedonannot ja viranomaisille ja rekisteröidyille.

Kuntaliitto Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintäteknikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto

Tilaisuuden ohjelma

#tuki2018 #stöd2018

- 8.30 Kahvi
- 9.00 Tilaisuuden avaus – Tuula Seppo, Kuntaliitto & Kimmo Rousku, valtiovarainministeriö
- 9.15 Ari Andreasson, Tampereen kaupungin tietosuojavastaava, käytännön kokemuksia ja havaintoja tietosuojavastaavan elämässä
- 10.15 Bio- ja jaloittelutauko
- 10.30 Tietosuojavastaavan rooli sekä vastuut
- 12.00 Lounastauko (omakustanne)
- 13.00 MMKT –toimintamallin ja videon esittely
- 13.10 Tietoturvapoikkeama- ja tietosuojaloukkaustilanteiden hallinta – taustaa, havainnointikyky sekä reagointi – kuinka tietosuojaloukkaukset voidaan tunnistaa?
- 14.30 Kahvitauko
- 14.45 Ryhmätehtävä; tiedonannot ja viranomaisille ja rekisteröidyille
- 15.30 Kotitehtävän esittely
- 16.00 Yhteenveto
- 16.15 Työpaja päättyy

Tietosuojavastaavan rooli sekä vastuut (GDPR 37-39 artiklat)

Velvollisuus nimittää tietosuojavastaava (1/2)

#tuki2018 #stöd2018

— Tiettyjen rekisterinpitäjien sekä käsittelijöiden on nimitettävä tietosuojavastaava suoraan asetuksen perusteella.

— Rekisterinpitäjän ja henkilötietojen käsittelijän on nimitettävä tietosuojavastaava aina kun

a) tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin; tai

b) rekisterinpitäjän tai henkilötietojen käsittelijän keskeiset tehtävät muodostuvat käsittelytoimista, jotka luonteensa, laajuutensa ja/tai tarkoitustensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa; tai

c) rekisterinpitäjän tai henkilötietojen käsittelijän keskeiset tehtävät muodostuvat käsittelystä, joka kohdistuu laajamittaisesti 9 artiklan 1 kohdan mukaisiin erityisiin tietoryhmiin ja 9 a artiklassa tarkoitettuihin rikostuomioita tai rikoksia koskeviin tietoihin.

Velvollisuus nimittää tietosuojavastaava (2/2)

#tuki2018 #stöd2018

—Ellei ole ilmeistä, että organisaatiolla ei ole velvollisuutta nimetä tietosuojavastaavaa, suosittelee EU:n WP29 tietosuojatyöryhmä, että harkitaan sisäisesti tulisiko tietosuojavastaava nimetä, ja että päätöksen perusteet dokumentoidaan osoitusvelvollisuuden periaatteen mukaisesti.

—Lisäksi on mahdollista, että kansallinen lainsäädäntö velvoittaa nimittämään tietosuojavastaavan joillakin toimialoilla (esim. terveydenhuoltoalalla pakollinen).

Rekisterinpitäjän tai henkilötietojen käsittelijän on julkistettava tietosuojavastaavan yhteystiedot ja ilmoitettava ne valvontaviranomaiselle.

Tietosuojavastaavan asema

#tuki2018 #stöd2018

— Tietosuojavastaava ei ole vastuussa vaatimuksenmukaisuudesta rekisterinpitäjän tai käsittelijän puolesta – viimekäteinen vastuu on aina organisatiolla ja sen johdolla.

— Tietosuojavastaavan tehtävänä on auttaa rekisterinpitäjää tietosuojavelvoitteiden toteuttamisessa ja toimia erityisasiantuntijana organisaatiossa.

— Asetuksen artiklat tietosuojavastaavan toimintaa koskien pätevät riippumatta siitä onko tämä lakisääteinen vai vapaaehtoisesti nimetty rooli.

— Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että tietosuojavastaava otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn.

— Rekisterinpitäjän ja henkilötietojen käsittelijän on tuettava tietosuojavastaavaa tämän suorittaessa 39 artiklassa tarkoitettuja tehtäviä antamalla tälle resurssit, jotka ovat tarpeen näiden tehtävien täyttämisessä, samoin kuin pääsyn henkilötietoihin ja käsittelytoimiin, sekä tämän asiantuntemuksen ylläpitämiseksi.

Tietosuojavastaavan riippumattomuus

#tuki2018 #stöd2018

- Tietosuojavastaavaa koskee 38 artiklan mukaan riippumattomuusvaatimus.
  - Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, ettei tietosuojavastaava ota vastaan ohjeita näiden tehtävien hoitamisen yhteydessä.
  - Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuojavastaavaa sen vuoksi, että hän on hoitanut tehtäviään.
  - Tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle.
  - Tietosuojavastaavaa koskee salassapitovelvollisuus tehtäviä suorittaessa.
  - Tietosuojavastaava voi suorittaa muita tehtäviä ja velvollisuuksia. Rekisterinpitäjän tai henkilötietojen käsittelijän on varmistettava, että tällaiset tehtävät ja velvollisuudet eivät aiheuta eturistiriitoja.

Tietosuojavastaavan pätevyysvaatimukset (1/2)

#tuki2018 #stöd2018

- Vaatimuksia ei ole tyhjentävästi määritelty asetuksessa, mutta Artikla 37(5) antaa osviittaa pätevyysvaatimuksille.
  - Vaadittu osaamistaso riippuu henkilötietojen käsittelystä, esimerkiksi jos käsittely sisältää erityisiin tietoryhmiin sisältyvää henkilötietoa, voidaan edellyttää korkeampaa osaamistasoa.
- Tietosuojavastaavaa nimitettäessä on otettava huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä sekä valmiudet suorittaa 39 artiklassa tarkoitetut tehtävät.

Tietosuojavastaavan pätevyysvaatimukset (2/2)

#tuki2018 #stöd2018

- Vähimmäisvaatimukset asetuksen ja WP29-työryhmän lausuntojen perusteella ovat:
  - Riittävä asiantuntemus kansallisesta ja EU-tason tietosuojalainsäädännöstä ja käytänteistä, sekä syvällinen ymmärrys GDPR:n vaatimuksista (artiklat 37.1, 37.5, johdantokappale 97)
  - Ymmärrys rekisterinpitäjän liiketoiminnasta ja liiketoimintasektorista.
  - Hyvä ymmärrys rekisterinpitäjän tai henkilötietojen käsittelijän toiminnasta, käsittelytoimista, tietojärjestelmistä ja tietojenkäsittelyprosesseista sekä tietoturvallisuuden ja riskien hallinnasta (artiklat 39.2, 35.2, johdantokappale 77)
  - Valmius edistää tietosuojakulttuuria organisaatiossa

Tietosuojavastaavan tehtävät

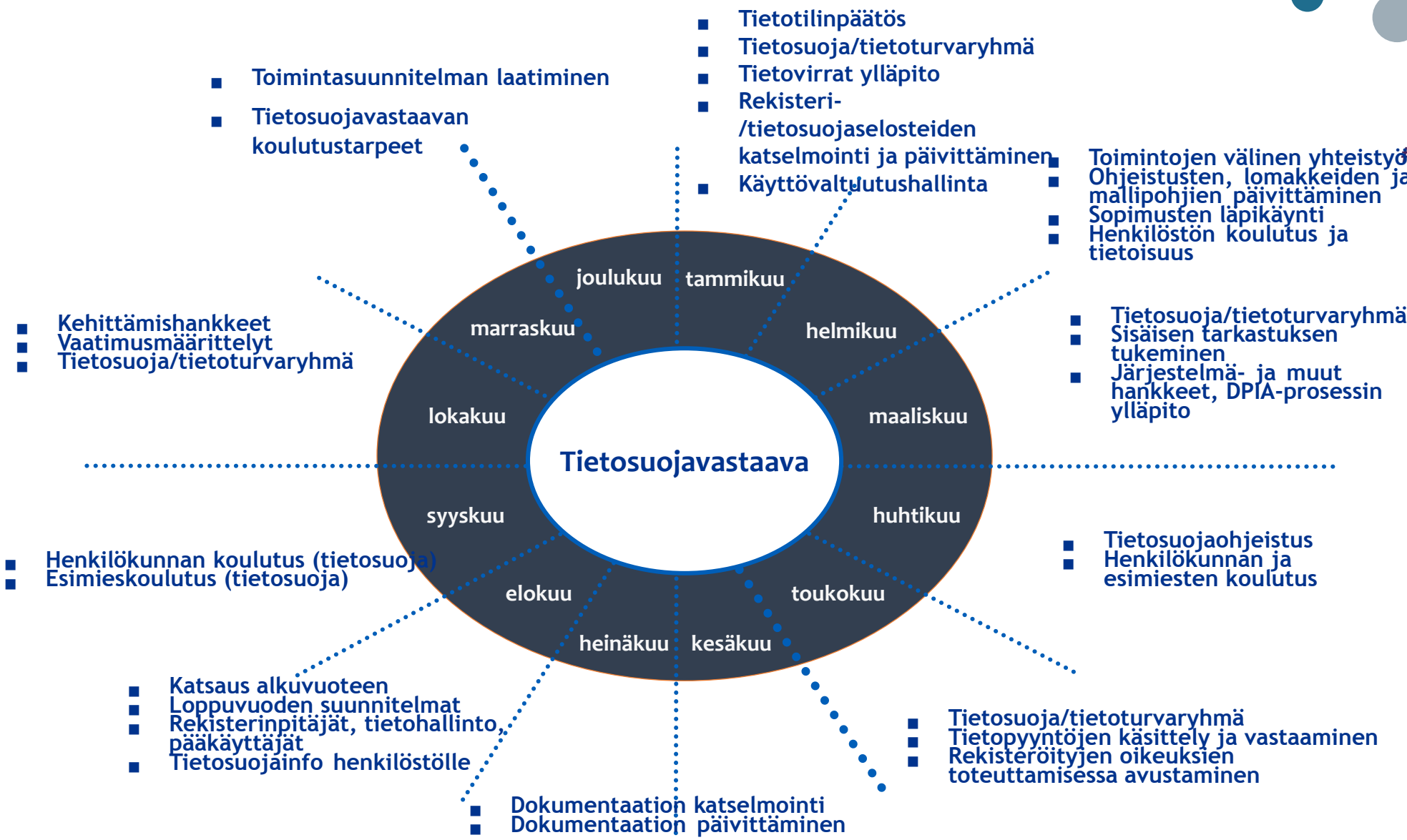
#tuki2018 #stöd2018

- Tietosuojavastaavalla on oltava ainakin seuraavat tehtävät (39 artikla)
  - antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat niiden tämän asetuksen ja muiden unionin tai jäsenvaltioiden tietosuojasäännösten mukaisia velvollisuuksia;
  - seurata, että noudatetaan tätä asetusta, muita unionin tai jäsenvaltion tietosuojalainsäännöksiä ja rekisterinpitäjän tai henkilötietojen käsittelijän toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan, mukaan lukien vastuunjako, tiedon lisääminen ja käsittelyyn osallistuvan henkilöstön koulutus ja tähän liittyvät tarkastukset;
  - antaa pyydettäessä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta 35 artiklan mukaisesti;
  - tehdä yhteistyötä valvontaviranomaisen kanssa;
  - toimia valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, mukaan lukien 36 artiklan mukainen ennakkokuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä.

Tietosuojavastaavan rooli organisaatiossa

#tuki2018 #stöd2018

Tietosuojavastaavan tehtävät – vuosikello (esimerkki)



Vaihtoehtoisia ratkaisumalleja tietosuojavastaavan nimittämiselle

#tuki2018 #stöd2018

- Jos rekisterinpitäjä tai henkilötietojen käsittelijä on viranomainen tai julkishallinnon elin, yksi ainoa tietosuojavastaava voidaan nimittää useampaa tällaista viranomaista tai julkishallinnon elintä varten niiden organisaatiorakenne ja koko huomioon ottaen.
- Tietosuojavastaava voi myös olla hankittu asiantuntijapalveluna ulkopuoliselta palveluntarjoajalta
  - Ulkoistusorganisaation työntekijöiden täytettävä asetuksen vaatimukset: ammattipätevyys, ei intressiristiriitoja

Esim. yhteinen tietosuojavastaava sairaanhoitopiirin organisaatioille

Ryhmätehtävä

#tuki2018 #stöd2018

1. Määrittele organisaatiosi tietosuojavastaavan asemassa tietosuoja-asetukseen liittyvä arviointi- ja kehityshanke:

   ✓ Minkälaisia resursseja hankkeeseen tarvitaan?

   ✓ Mitä tietoja organisaation henkilötietojen käsittelystä tarvitaan, jotta arviointi ja kehitys voi onnistua?

   ✓ Miten hanke vaiheistetaan?

   ✓ Mitkä ovat tietosuojan aihealueet, joita hankkeessa arvioidaan ja kehitetään?

Yhteenveto

#tuki2018 #stöd2018

- Tietosuojavastaava (Data Protection Officer, DPO) on laissa määritelty rooli, jolla on tietyt tehtävät, asema ja vaatimukset, ja jonka nimittäminen on joissain tapauksissa organisaatiolla pakollista.
  - Rekisterinpitäjien ja henkilötietojen käsittelijöiden on varmistuttava siitä, onko organisaatioon asetuksen mukaan nimettävä tietosuojavastaava.
  - Konserni, samoin kuin useampi viranomainen tai julkishallinnon elin, voi tietyin edellytyksin nimittää vain yhden tietosuojavastaavan.
  - Tietosuojavastaava voi olla organisaation henkilöstön jäsen tai hoitaa tehtäviään palvelusopimuksen perusteella (= ulkoistettu asiantuntija).
- Nimitettäessä tietosuojavastaavaa tulee ottaa huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä.
- Tietosuojavastaavan tehtävänä on muun muassa seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet.
  - Tietosuojavastaavan tehtävänä on myös toimia valvontaviranomaisen sekä rekisteröityjen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä kysymyksissä.
  - Tietosuojavastaava ei kuitenkaan ole vastuussa henkilötietojen käsittelyn lainmukaisuudesta vaan vastuu kuuluu edelleen organisaation johdolle.
- Tietosuojavastaavan on oltava riippumaton eikä hän saa ottaa vastaan ohjeita tehtäviensä hoitamisen yhteydessä.
- Tietosuojavastaavan yhteystiedot on julkaistava ja lisäksi ilmoitettava valvontaviranomaisille.

Taustamateriaalia

#tuki2018 #stöd2018

– Artikla 29 WP 243/rev.01: Tietosuojavastaavia koskevat ohjeet

– Usein kysytyt kysymykset / tietosuojavastaavat

– EU-tietosuojan kokonaisuudistus. VAHTI-raportti 1/2016.

Tietoturvapoikkeama- ja tietosuojaloukkaustilanteiden hallinta, osa 1 – taustaa, havainnointikyky sekä reagointi – kuinka tietosuojaloukkaukset voidaan tunnistaa? Tiedonannot ja viranomaisille ja rekisteröidyille.

#tuki2018 #stöd2018

Kuinka monen osallistujan organisaatiossa on tapahtunut tietoturvaloukkaus? Entä henkilötietoihin kohdistunut tietoturvaloukkaus?

#tuki2018 #stöd2018

Joku julkaisi 16 000 suomalaisen henkilötunnukset netissä kuusi vuotta sitten – nyt niillä tehtaillaan tuhansia rikoksia vuodessa

yle.fi

THL pyytää anteeksi: 6000 suomalaisen luottamuksellisia henkilötietoja levisi verkkoon

EU:n perusoikeusviraston raportti tiedustelupalvelujen tarkkailutoiminnasta: tietosuojan ja yksityisyydensuojan suojatoimia vahvistettava

Julkaistu 27.10.2017

VAHTI 8/2017

#tuki2018 #stöd2018

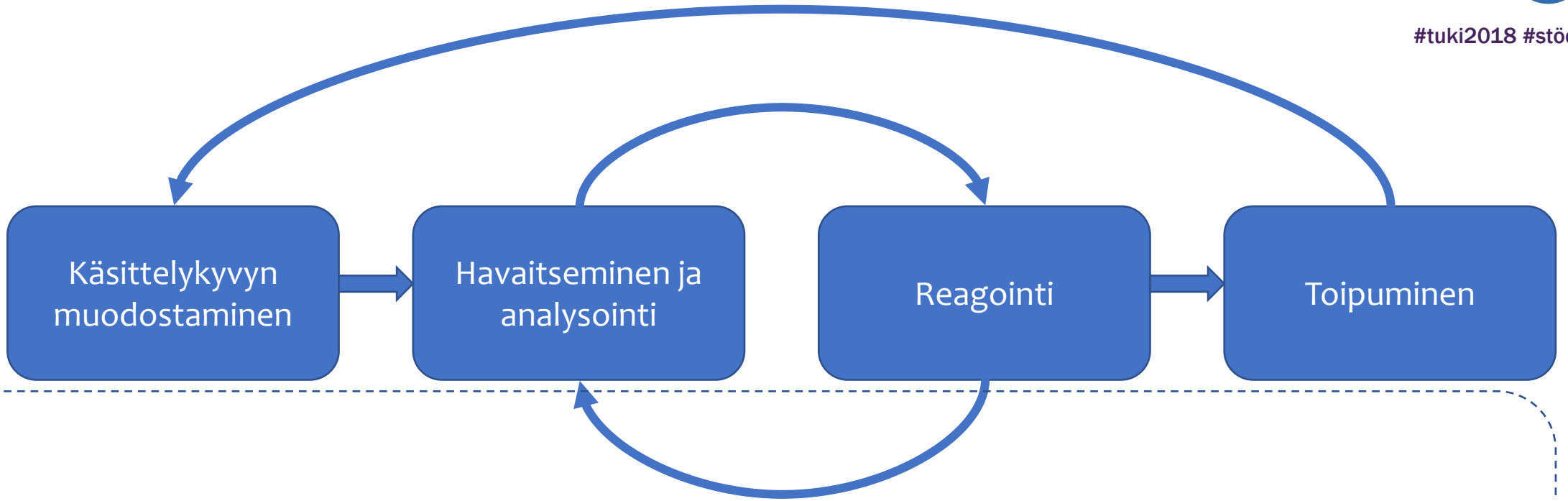
- Tietoturvapoikkeamatilanteiden hallinta
  - Prosessi
  - Käsittelykyvyn muodostaminen
  - Havaitseminen ja analysointi
  - Reagointi
  - Toipuminen
- Liitteet
  - Käytännön ohjeita eri tilanteisiin
  - Dokumenttipohjia

VAHTI 8/2017

#tuki2018 #stöd2018

- Tarkoitettu erityisesti julkishallinnolle
  - Myös julkishallinnon palveluntarjoajille
- Ottaa huomioon Suomen lainsäädännön
- Muut ohjeet (NIST, ISO 27035 jne.) ovat sisällöltään suurin piirtein vastaavia

Hallintaprosessi



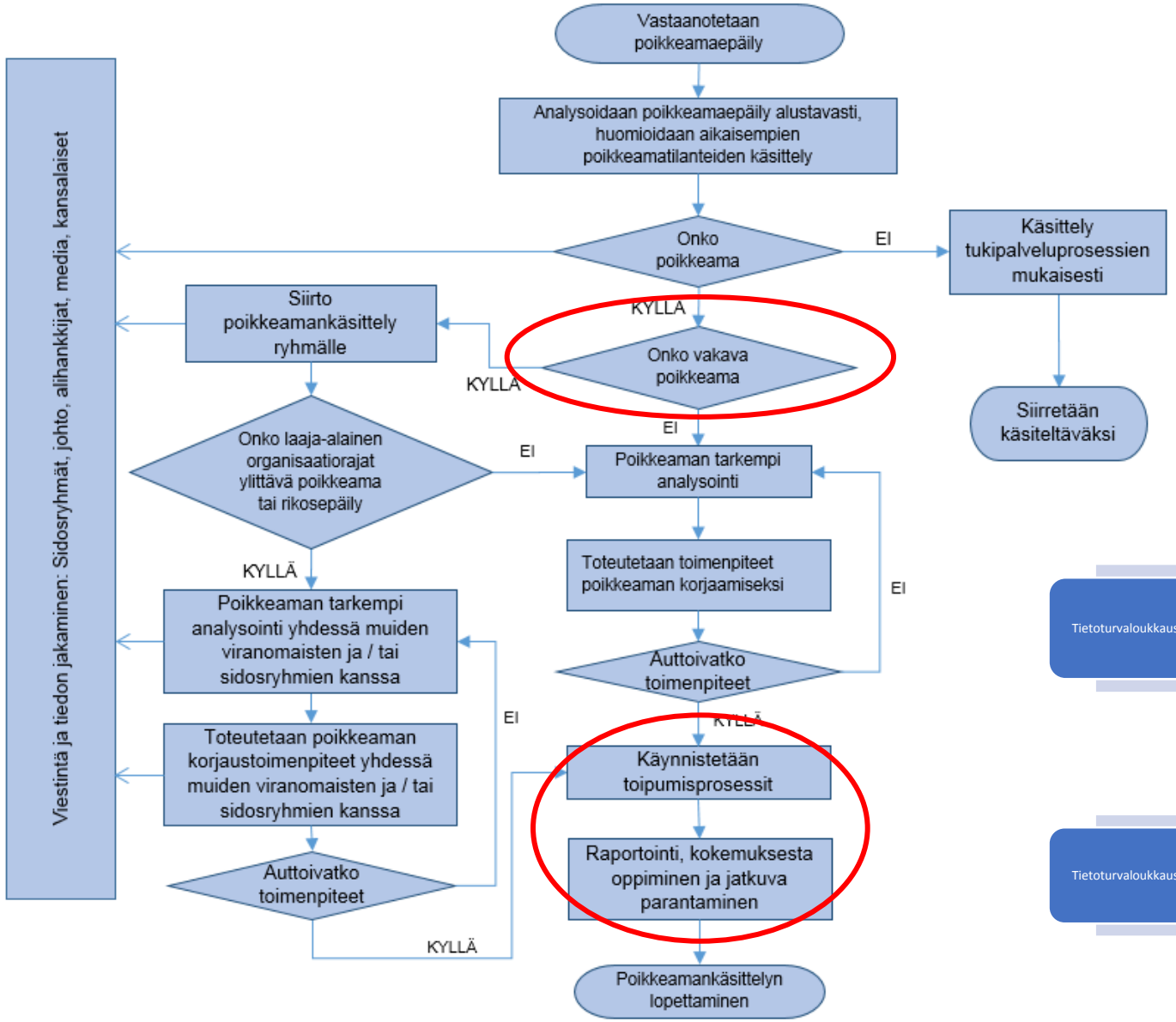
Muissa ohjeissa myös

Valmistautuminen	Monitorointi	Rajoittaminen, poistaminen toipuminen	Tapahtumasta oppiminen
Suunnittelu	Havaitseminen ja raportointi		

Henkilötietojen tietoturvaloukkaus

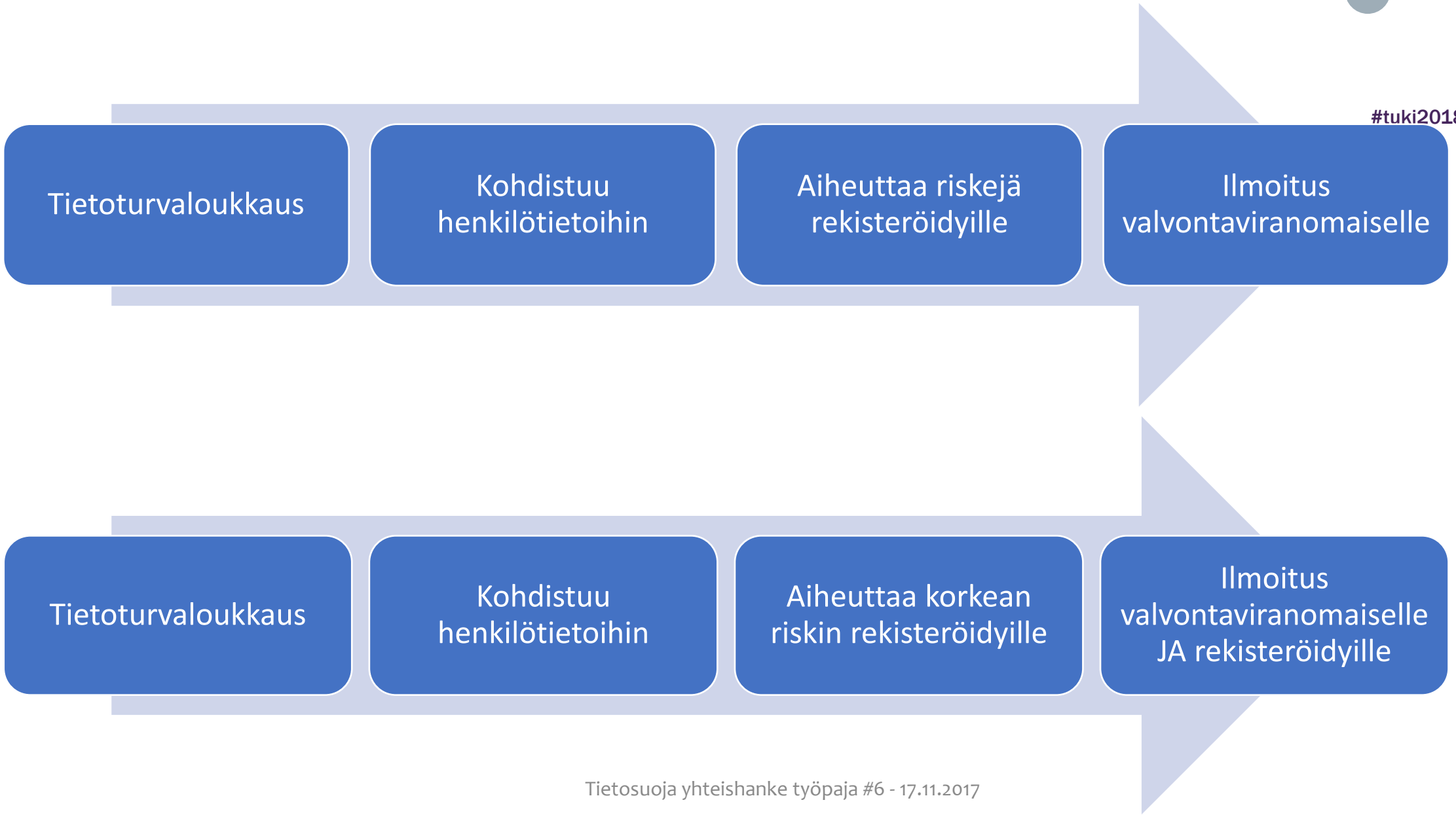
- Voi tulla kyseeseen lähes aina tietoturvaloukkauksen yhteydessä
  - Myös tiedon tuhoutuminen
- Henkilötietojen tietoturvaloukkauksen vakavuus on aina arvioitava ennen toimenpiteisiin ryhtymistä
  - Tietosuoja-asetus luo lisää painetta selvittää loukkaukset nopeasti
  - Henkilötietojen käsittelijöiden rooli ja tehtävät merkittäviä

#tuki2018 #stöd2018



Ilmoitusvelvollisuus – päätöksentekoketju

#tuki2018 #stöd2018



Käsittelykyvyn muodostaminen

#tuki2018 #stöd2018

- Osaaminen
  - Tekninen osaaminen
  - Oman ympäristön tunteminen
- Valmistautuminen
  - Prosessit ja vastuut
  - Viestinnän ja yhteistyön suunnittelu
  - Koulutus ja harjoittelu
- Torjunnan ja valvonnan suunnittelu
  - Mahdollistaa havainnoinnin
  - Lokijärjestelmät

Poikkeaman havaitseminen ja analysointi

#tuki2018 #stöd2018

- Oman ympäristön tunteminen
  - Tekniset havainnointikeinot
- Organisaatiosta tulevat signaalit
- Ulkopuolelta tulevat ilmoitukset
- Sisäiset loukkaukset
- Kaikki ilmoitukset otettava vakavasti

Poikkeamaan reagointi

#tuki2018 #stöd2018

- Suunnittelu mahdollistaa oikean reagoinnin
- Tapahtumien luokittelu
- Eristäminen
- Tapahtumapäiväkirja
- Todisteiden säilytys
- Tiedon jakaminen
  - Tietosuoja-asetuksen vaatimat ilmoitukset
  - Muille mahdollisille uhreille

Toipuminen

#tuki2018 #stöd2018

- Jatkuvuus- ja toipumissuunnittelu
  - VAHTI 2/2016 – Toiminnan jatkuvuuden hallinta
- Viestintä
- Normaalitilaan paluu
- Raportointi
  - Tapahtumista oppiminen

Henkilötietojen tietoturvaloukkausten tunnistaminen

Henkilötietojen tietoturvaloukkauksen tunnistaminen

- Tärkeintä on tietää, missä järjestelmissä tai tallennuspaikoissa on henkilötietoa
  - Tietoinventaari, järjestelmäsalkku tai muu vastaava
  - Seloste käsittelytoimista; rekisteri- tai tietosuojaselosteet
- Jos henkilötietoa sisältävän järjestelmän tietoturvaa on loukattu, ota aina huomioon tietosuojavaatimukset
  - Selvitys
  - Dokumentointi
  - Tiedonannot
- Tunnistaminen voi tapahtua myös valvontajärjestelmissä
  - Selkokielinen tiedonsiirto
  - Lokit ja niiden valvonta

Henkilötietojen tietoturvaloukkausten ilmoitusvelvollisuus

Henkilötietojen tietoturvaloukkaus – määritelmä

#tuki2018 #stöd2018

- Henkilötietojen tietoturvaloukkauksen (4 art 12 kohta) seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.
  - Esimerkiksi hävinnyt USB-tikku, varastettu läppäri tai CD-levy, tietokoneen hakkerointi, haittaohjelmatartunta, tulipalo datakeskuksessa, henkilötietoja viety kyberhyökkäyksen seurauksena, kiristysohjelmahyökkäys, postitettu väärän henkilön tiliote jne.

- Hakkerointi
- Muistivälineen tai laitteen menetys
- Salauksen purun mahdottomuus
- Luvaton salaus
- Tiedon tuhoutuminen
- Tiedon turvaton käsittely
- Järjestelmäviat
- ...

Lähde: Niina Heikman, Tietosuojavaltuutetun toimisto

Henkilötietojen tietoturvaloukkaus – määritelmä

#tuki2018 #stöd2018

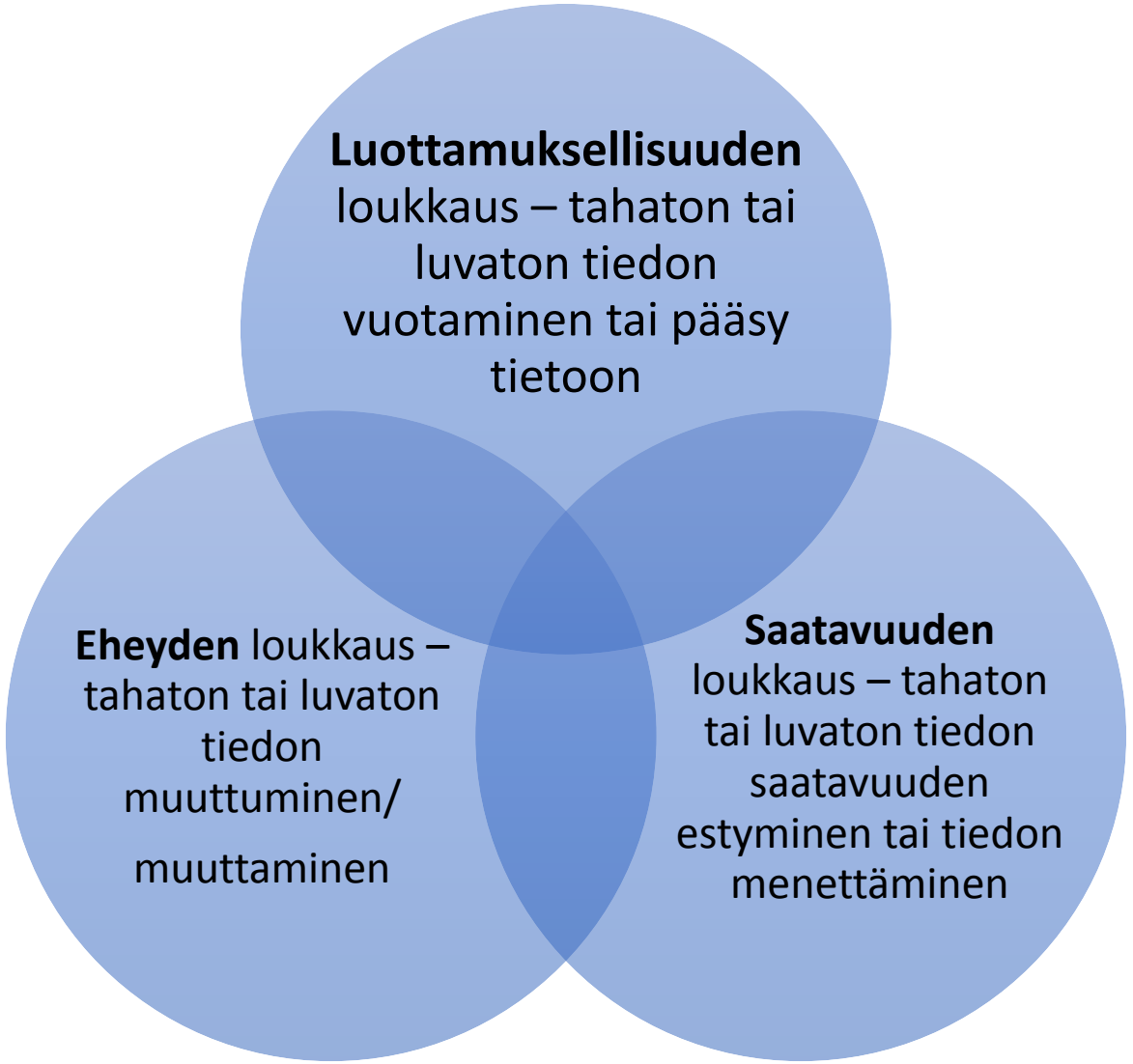
- WP29 on antanut näkemyksensä henkilötietojen tietoturvaloukkauksen määritelmästä jo aiemmin lausunnossaan 03/2014 (e-privacy)
  - Seuraukset ilmenevät perinteisissä tietoturvan oikeushyvissä eli luottamuksellisuuden, käytettävyyden/saatavuuden tai eheyden puutteina tai rikkoutumisena.
  - Käytettävyyden/saatavuuden loukkaus ei aina yksiselitteistä, mutta ainakin silloin, kun henkilötiedot on pysyvästi menetetty tai ne ovat tuhoutuneet
    - Kryptattu data, jonka salausavain on kadotettu eikä tietoja pystytä palauttaman esim. varmuuskopion avulla
    - Myös pidempiaikainen sähkökatkos, palvelunestohyökkäys

- Hakkerointi
- Muistivälineen tai laitteen menetys
- Salauksen purun mahdottomuus
- Luvaton salaus
- Tiedon tuhoutuminen
- Tiedon turvaton käsittely
- Järjestelmäviat
- …

Lähde: Niina Heikman, Tietosuojavaltuutetun toimisto

Henkilötietojen tietoturvaloukkauksen luokat

#tuki2018 #stöd2018



Lähde: WP 29 / 248

Ilmoitusvelvollisuus valvontaviranomaisille (33 art.)

#tuki2018 #stöd2018

- Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä valvontaviranomaiselle
- Ilmoitus on tehtävä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta
- Jos ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys
- Jos tietoja ei ole mahdollista toimittaa samanaikaisesti, ne voidaan toimittaa vaiheittain

”Kohtuullinen varmuus”

Ilmoitusvelvollisuus valvontaviranomaisille (33 art.)

#tuki2018 #stöd2018

- Ilmoituksessa on vähintään
  - kuvattava henkilötietojen tietoturvaloukkaus, ml. mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien
  - ryhmät ja arvioidut lukumäärät;
  - ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;
  - kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;
  - kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Ilmoitusvelvollisuus rekisteröidyille (34 art.)

#tuki2018 #stöd2018

- Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä
- Rekisteröidylle annettavassa ilmoituksessa on kuvattava selkeällä kielellä henkilötietojen tietoturvaloukkauksen luonne ja annettava tiettyjen tietojen lisäksi suosituksia siitä, miten loukkauksen mahdollisia haittavaikutuksia voi lieventää

WP 29 / 248:
”Ilmoitus tulisi tehdä rekisteröidyille henkilökohtaisella viestillä johon ei tule liittää muuta informaatiota, ellei tällainen ilmoitus vaatisi suhteetonta vaivannäköä.”

Ilmoitusvelvollisuus rekisteröidyille (34 art.)

#tuki2018 #stöd2018

- Ilmoitusta rekisteröidylle ei kuitenkaan tarvitse tehdä, jos
  - rekisterinpitäjä on soveltanut loukkauksen kohteena oleviin henkilötietoihin asianmukaisia teknisiä ja organisatorisia suojatoimenpiteitä (erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta);
  - rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu; tai
  - se vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla.
- Jos rekisterinpitäjä ei ole vielä ilmoittanut loukkauksesta rekisteröidylle, viranomainen voi vaatia ilmoituksen tekemistä tai päättää, että ilmoitusta ei tarvitse tehdä.

WP 29 / 248:
”Ilmoitus tulisi tehdä rekisteröidyille henkilökohtaisella viestillä johon ei tule liittää muuta informaatiota, ellei tällainen ilmoitus vaatisi suhteetonta vaivannäköä.”

Korkea riski

#tuki2018 #stöd2018

- Tietoturvaloukkauksen tyyppi
- Henkilötiedon luonne, arkaluonteisuus tai määrä
- Rekisteröityjen tunnistamisen helppous
- Negatiivisten seurausten vakavuus rekisteröidyille
- Rekisteröidyn erityiset ominaisuudet
- Rekisterinpitäjän erityiset ominaisuudet
- Rekisteröityjen määrä

Lähde: WP 29 / 248

Poikkeus ilmoitusvelvollisuuteen

#tuki2018 #stöd2018

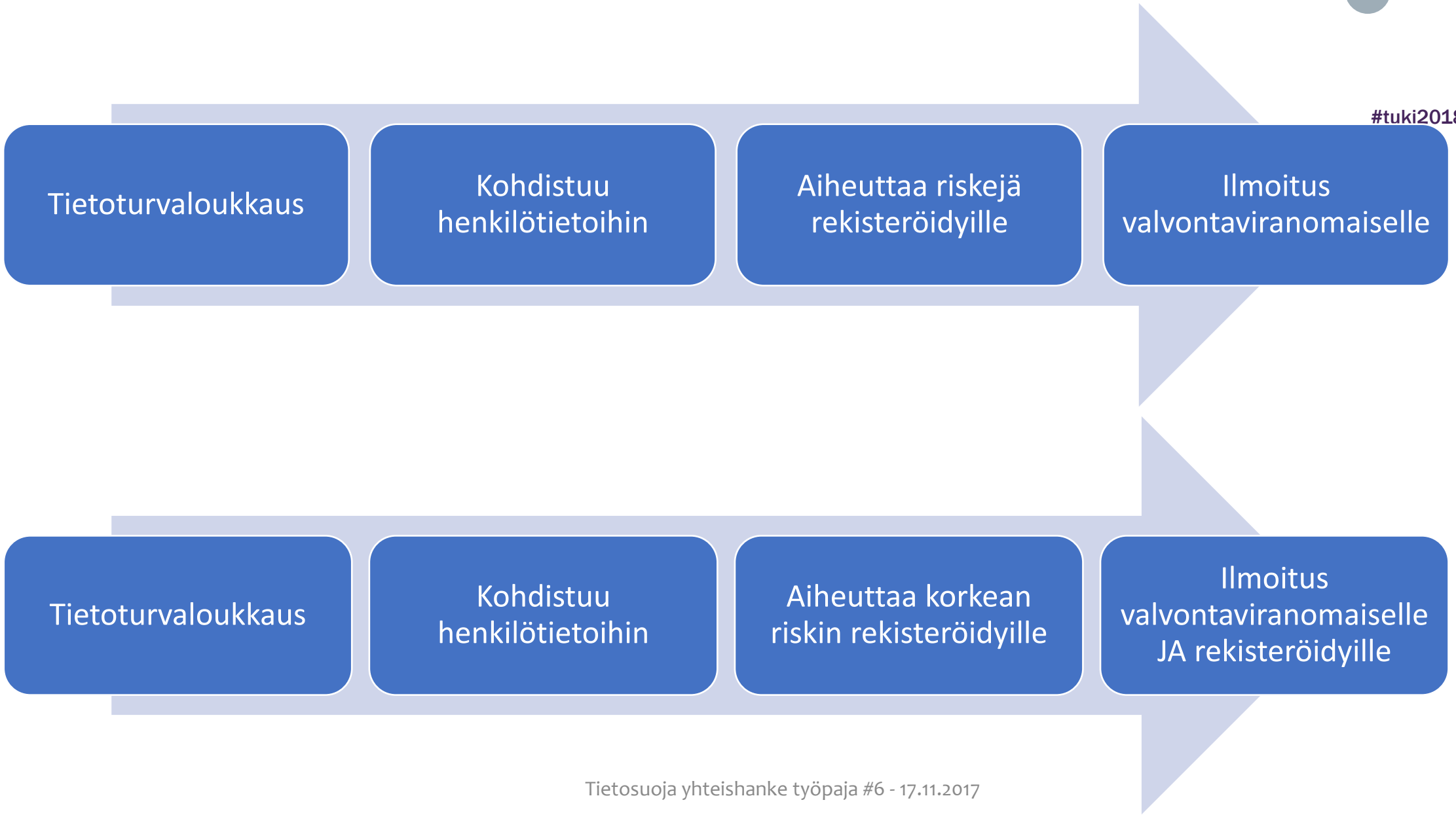
- Jos henkilötietojen tietoturvaloukkaus on tapahtunut, siitä ei tarvitse ilmoittaa valvontaviranomaiselle (eikä rekisteröidyille), jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä
- Riippumatta siitä, tuleeko loukkauksesta ilmoittaa viranomaiselle vai ei, rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset (33 art 5 kohta)
  - Tämä koskee henkilötietojen tietoturvaloukkaukseen liittyviä seikkoja, sen vaikutuksia ja toteutettuja korjaavia toimia
  - Valvontaviranomaisen on voitava tämän dokumentoinnin avulla tarkistaa, että rekisterinpitäjä on noudattanut 33 artiklaa

Esimerkki:
- (Mobiili)laite joka on kryptattu
- Salausavaimet ovat tallessa ja suojattu
- Tiedosta on olemassa myös rekisterinpitäjän hallussa ja saatavilla olevia kopioita

Lähde: Niina Heikman, Tietosuojavaltuutetun toimisto

Ilmoitusvelvollisuus – päätöksentekoketju

#tuki2018 #stöd2018



Harjoitustehtävä

Kuvaus tietoturvatapahtumasta

- Tietomurto web-pohjaiseen järjestelmään
  - Järjestelmässä liikkui rahaa
  - Järjestelmässä henkilötietoja, tietokannan koko n. 5 gigatavua
- Murto havaittiin nopeasti, sillä Google laittoi sivuston Chromen varoituslistalle
- Lokit suhteellisen hyvällä tasolla
- Löydökset:
  - Havaittu järjestelmään asennettu haittaohjelmia levittävä komponentti
  - Löydetty palvelimelle pudotettu RAT (remote access tool)
  - RATin osoite: www.example.com/openx/plugins/backdoor.php
  - Löydetty 2. piilotettu takaovi
  - Löydetty lokeista jälki asennetun RATin käytöstä

Tehtävä

1. Kenelle tietoturvallisuuteen liittyvästä poikkeamaepäilystä on hyvä ilmoittaa välittömästi?
2. Onko tapahtunut henkilötietojen tietoturvaloukkausta?
   - Onko rekisteröityjä tiedotettava?
   - Onko tietosuojavaltuutetulle ilmoitettava?
   - Tekisitkö rikosilmoitusta?
3. Miten hoitaisit ilmoitusten tekemisen?

Web-palvelimen loki: https://pastebin.com/FfT0MHXn

Yhteenveto

Yhteenveto

#tuki2018 #stöd2018

- Valmistautuminen on kaiken A ja O
- Huolehdi riittävistä kyvykkyyksistä tietoturvaloukkausten tunnistamiseen ja selvittämiseen
- Tiedä, missä henkilötieto sijaitsee
- Selvitä aina mahdolliset henkilötietojen tietoturvaloukkaukset huolellisesti
- Tiedota ja ilmoita, kun siihen on tarvetta (rekisterinpitäjä aina vastuussa tästä)
  - Tietosuojavaltuutettu
  - Kyberturvallisuuskeskus
  - Poliisi
  - Rekisteröidyt

Kotitehtävä 17.11.2017

Kotitehtävä

#tuki2018 #stöd2018

1. Selvitä onko organisaatioissasi nimetty tietosuojavastaavaa ja hänen tehtävänsä määritelty tietosuoja-asetuksen edellyttämällä tavalla?
2. Selvitä miten tietoturvapoikkeamien selvitys on järjestetty omassa organisaatiossasi
   - Ottaako se huomioon henkilötietojen tietoturvaloukkauksen erityistapauksena?
   - Onko tietosuoja-asetuksen tuoma ilmoitusvelvollisuus huomioitu?
3. Mikäli havaitsit edellisessä tehtävässä puutteita, käynnistä prosessien parannus
   - Nivoa henkilötietojen tietoturvaloukkausten käsittely osaksi tietoturvapoikkeamien käsittelyprosessia.
   - Laadi kaavake omalle organisaatiollesi henkilötietojen tietoturvaloukkauksen ilmoittamisesta. Voit hyödyntää oheista pohjaa.

#tuki2018 #stöd2018

Kysymykset materiaaliin liittyen voi osoittaa:

Mikko Viemerö (CIPP/E, CIPM, CIPT, CISA, CISM)
KPMG Cyber Security Services
+358 20 760 3530
mikko.viemero@kpmg.fi

Antti Alestalo (CISSP, CISA, CPTE)
KPMG Cyber Security Services
+358 40 5822 399
antti.alestalo@kpmg.fi

Kuntaliitto Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintätekniikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto