Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet

#tuki2018 #stöd2018

Työpaja #7 – 8.12.2017

- **Rekisteröidyn oikeuksien toteuttaminen, lasten erityisaseman huomioiminen**
- **Tietoturvapoikkeama- ja tietosuojaloukkaustilanteiden hallinta, osa 2 – tarvittavien prosessien ja kyvykkyyksien kehittäminen sekä ohjeistus ja koulutus, tarvittava yhteistyö eri toimijoiden kesken. 17.11. annetun harjoituskotitehtävän purku**

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 Mitä tulee huomioida tietoturvapoikkeama- ja tietosuojaloukkaustilanteessa – Poliisin näkökulma, *Rikosylikomisario Tero Muurman, Keskusrikospoliisi*

10.00 Rekisteröidyn oikeuksien toteuttaminen; lasten erityisaseman huomioiminen

10.45 Biotauko

11.00 Rekisteröidyn oikeuksien toteuttaminen; lasten erityisaseman huomioiminen jatkuu

12.00 Lounastauko (omakustanne)

13.00 Viestintäviraston Kyberturvallisuuskeskuksen palvelut tietoturvaloukkaustapauksissa, *johtava asiantuntija Kauto Huopio, Viestintäviraston kyberturvallisuuskeskus*

14:00 Tietoturvapoikkeama- ja tietosuojaloukkaustilanteiden hallinta, osa 2 – tarvittavien prosessien ja kyvykkyyksien kehittäminen sekä ohjeistus ja koulutus, tarvittava yhteistyö eri toimijoiden kesken

15.00 Kahvitauko

15.15 Edellisen kerran kotitehtävän purku

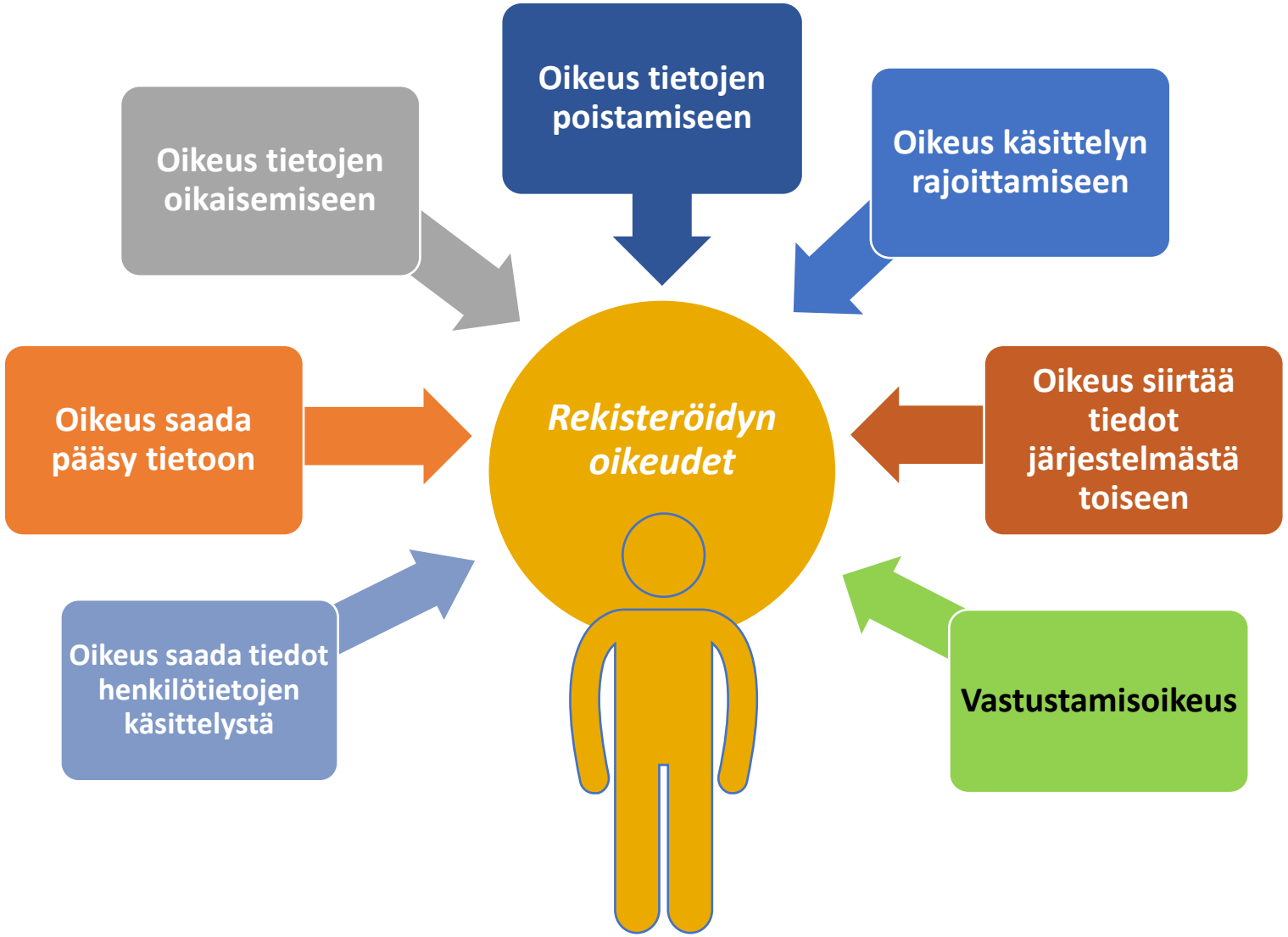
16.00 Kotitehtävän esittely ja yhteenveto

16.15 Työpaja päättyy

Rekisteröidyn oikeudet ja niiden toteuttaminen

Rekisteröidyn oikeudet (12-21 art.)

#tuki2018 #stöd2018



Oikeudet polveutuvat henkilötietojen käsittelyn periaatteista (5 art.)

Rekisterinpitäjän tiedonantovelvollisuus (13 art.)

#tuki2018 #stöd2018

- Kerättäessä rekisteröidyltä häntä koskevia henkilötietoja rekisterinpitäjän on silloin, kun henkilötietoja saadaan, toimitettava rekisteröidylle kaikki seuraavat tiedot:

  a) rekisterinpitäjän ja tapauksen mukaan tämän mahdollisen edustajan identiteetti ja yhteystiedot;

  b) tapauksen mukaan tietosuojavastaavan yhteystiedot;

  c) henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;

  d) rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu 6 artiklan 1 kohdan f alakohtaan;

  e) henkilötietojen vastaanottajat tai vastaanottajaryhmät;

  f) tapauksen mukaan tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle, ja tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, []

Ei sovelleta, jos ja niiltä osin kun rekisteröity on jo saanut tiedot

Rekisterinpitäjän tiedonantovelvollisuus (13 art.) jatkuu

- Edellä tarkoitettujen tietojen lisäksi rekisterinpitäjän on silloin, kun henkilötietoja saadaan, toimitettava rekisteröidylle seuraavat lisätiedot, jotka ovat tarpeen asianmukaisen ja läpinäkyvän käsittelyn takaamiseksi:

  a) henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit;

  b) rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista tai vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen;

  c) oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen, jos käsittely perustuu 6 artiklan 1 kohdan a alakohtaan tai 9 artiklan 2 kohdan a alakohtaan;

Ei sovelleta, jos ja niiltä osin kun rekisteröity on jo saanut tiedot

Rekisterinpitäjän tiedonantovelvollisuus (13 art.) jatkuu

#tuki2018 #stöd2018

d) oikeus tehdä valitus valvontaviranomaiselle;

e) onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset;

f) automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.

Ei sovelleta, jos ja niiltä osin kun rekisteröity on jo saanut tiedot

Rekisterinpitäjän tiedonantovelvollisuus (14 art.)

#tuki2018 #stöd2018

- Kun tietoja ei ole saatu rekisteröidyltä, rekisterinpitäjän on toimitettava rekisteröidylle seuraavat tiedot:

  a) rekisterinpitäjän ja tämän mahdollisen edustajan identiteetti ja yhteystiedot;

  b) tapauksen mukaan mahdollisen tietosuojavastaavan yhteystiedot;

  c) henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste;

  d) kyseessä olevat henkilötietoryhmät;

  e) mahdolliset henkilötietojen vastaanottajat tai vastaanottajaryhmät;

  f) tarvittaessa tieto siitä, että rekisterinpitäjä aikoo siirtää henkilötietoja kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle, ja tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, tai jos kyseessä on 46 tai 47 artiklassa tai 49 artiklan 1 kohdan toisessa alakohdassa tarkoitettu siirto, tieto sopivista tai asianmukaisista suojatoimista ja siitä, miten niistä saa jäljennöksen tai minne ne on asetettu saataville.

Rekisterinpitäjän tiedonantovelvollisuus (14 art.) jatkuu

- Edellä tarkoitettujen tietojen lisäksi rekisterinpitäjän on toimitettava rekisteröidylle seuraavat tiedot, jotka ovat tarpeen rekisteröidyn kannalta asianmukaisen ja läpinäkyvän käsittelyn takaamiseksi:

  a) henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit;

  b) rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu 6 artiklan 1 kohdan f alakohtaan;

  c) rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista ja vastustaa käsittelyä sekä oikeutta siirtää tiedot järjestelmästä toiseen;

  d) oikeus peruuttaa suostumus milloin tahansa tämän vaikuttamatta suostumuksen perusteella ennen sen peruuttamista suoritetun käsittelyn lainmukaisuuteen, jos käsittely perustuu 6 artiklan 1 kohdan a alakohtaan tai 9 artiklan 2 kohdan a alakohtaan;

Rekisterinpitäjän tiedonantovelvollisuus (14 art.) jatkuu

e) oikeus tehdä valitus valvontaviranomaiselle;

f) mistä henkilötiedot on saatu sekä tarvittaessa se, onko tiedot saatu yleisesti saatavilla olevista lähteistä;

g) automaattisen päätöksenteon, muun muassa 22 artiklan 1 ja 4 kohdassa tarkoitetun profiloinnin olemassaolo, sekä ainakin näissä tapauksissa merkitykselliset tiedot käsittelyyn liittyvästä logiikasta samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle.

Rekisterinpitäjän tiedonantovelvollisuus 14 art. – aikarajat

#tuki2018 #stöd2018

- Rekisterinpitäjän on toimitettava tiedot:
  a) kohtuullisen ajan kuluttua mutta viimeistään kuukauden kuluessa henkilötietojen saamisesta ottaen huomioon tietojen käsittelyyn liittyvät erityiset olosuhteet;
  b) jos henkilötietoja käytetään viestintään asianomaisen rekisteröidyn kanssa, viimeistään silloin kun rekisteröityyn ollaan yhteydessä ensimmäisen kerran; tai
  c) jos henkilötietoja on tarkoitus luovuttaa toiselle vastaanottajalle, viimeistään silloin kun näitä tietoja luovutetaan ensimmäisen kerran.

Rekisterinpitäjän tiedonantovelvollisuus 14 art. – poikkeukset

#tuki2018 #stöd2018

- 14 artiklan tiedonantovelvoitetta ei ole, jos ja siltä osin kuin
  a) rekisteröity on jo saanut tiedot;
  b) kyseisten tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa […];
  c) tietojen hankinnasta tai luovuttamisesta säädetään nimenomaisesti rekisterinpitäjään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa vahvistetaan asianmukaiset toimenpiteet rekisteröidyn oikeutettujen etujen suojaamiseksi; tai
  d) tiedot on pidettävä luottamuksellisina, koska niitä koskee unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuva vaitiolovelvollisuus, kuten lakisääteinen salassapitovelvollisuus.

Oikeus saada pääsy tietoihin (15 art.)

#tuki2018 #stöd2018

- Rekisteröidyllä on asetuksen art. 15 mukaisesti oikeus saada pääsy häntä koskeviin henkilötietoihin, eli nk. tarkastusoikeus. Tämä tarkoittaa sitä, että rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä.
- Tarkastusoikeuden toteuttaminen ei saa vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin.
- Sellainen henkilötiedoksi luokiteltava tieto, jota ei vielä ole kytketty yksittäiseen rekisteröityyn, ei kuulu tarkastusoikeuden piiriin.

Oikeus saada pääsy tietoihin (15 art.)

#tuki2018 #stöd2018

- Mikäli rekisteröityä koskevia tietoja käsitellään, rekisterinpitäjän on toimitettava **jäljennös** käsitellyistä henkilötiedoista sekä seuraavat tiedot:

  a) käsittelyn tarkoitukset;

  b) kyseessä olevat henkilötietoryhmät;

  c) vastaanottajat tai vastaanottajaryhmät, erityisesti kolmansissa maissa olevat vastaanottajat tai kansainväliset järjestöt, joille henkilötietoja on luovutettu tai on tarkoitus luovuttaa;

  d) mahdollisuuksien mukaan henkilötietojen suunniteltu säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit;

  e) rekisteröidyn oikeus pyytää rekisterinpitäjältä häntä itseään koskevien henkilötietojen oikaisemista tai poistamista taikka henkilötietojen käsittelyn rajoittamista tai vastustaa tällaista käsittelyä;

  f) oikeus tehdä valitus valvontaviranomaiselle; ja

  g) jos henkilötietoja ei kerätä rekisteröidyltä, kaikki tietojen alkuperästä käytettävissä olevat tiedot.

Oikeus tietojen oikaisemiseen (16 art.)

#tuki2018 #stöd2018

- Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot.
- Ottaen huomioon tarkoitukset, joihin tietoja käsiteltiin, rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, muun muassa toimittamalla lisäselvitys.
- Rekisterinpitäjän on ryhdyttävä korjaaviin toimenpiteisiin myös silloin, kun luotettava tieto henkilötiedon virheellisyydestä on saatu jostain muusta lähteestä kuin rekisteröidyltä itseltään.

Koskee myös rekisterinpitäjän itsensä havaitsemia virheitä tiedoissa

Oikeus tietojen poistamiseen (17 art.)

#tuki2018 #stöd2018

- Rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä, ja rekisterinpitäjällä on velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä, edellyttäen että jokin seuraavista perusteista täyttyy:
  a) henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin;
  b) rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut 6 artiklan 1 kohdan a alakohdan tai 9 artiklan 2 kohdan a alakohdan mukaisesti, eikä käsittelyyn ole muuta laillista perustetta;
  c) rekisteröity vastustaa käsittelyä 21 artiklan 1 kohdan nojalla eikä käsittelyyn ole olemassa perusteltua syytä tai rekisteröity vastustaa käsittelyä 21 artiklan 2 kohdan nojalla;
  d) henkilötietoja on käsitelty lainvastaisesti;
  e) henkilötiedot on poistettava unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi;
  f) henkilötiedot on kerätty 8 artiklan 1 kohdassa tarkoitetun tietoyhteiskunnan palvelujen tarjoamisen yhteydessä.

Rajoitukset!

Oikeus tietojen poistamiseen (17 art.)

#tuki2018 #stöd2018

- Jos rekisterinpitäjä on julkistanut henkilötiedot ja sillä on 1 kohdan mukaisesti velvollisuus poistaa tiedot, sen on käytettävissä oleva teknologia ja toteuttamiskustannukset huomioon ottaen toteutettava kohtuulliset toimenpiteet, muun muassa tekniset toimet, ilmoittaakseen henkilötietoja käsitteleville rekisterinpitäjille, että rekisteröity on pyytänyt kyseisiä rekisterinpitäjiä poistamaan näihin henkilötietoihin liittyvät linkit tai näiden henkilötietojen jäljennökset tai kopiot.

Oikeus käsittelyn rajoittamiseen (18 art.)

#tuki2018 #stöd2018

- Rekisteröidyllä on oikeus siihen, että organisaatio rajoittaa käsittelyä, jos kyseessä on yksi seuraavista tilanteista:
  a) rekisteröity kiistää henkilötietojen paikkansapitävyyden, jolloin käsittelyä rajoitetaan ajaksi, jonka kuluessa rekisterinpitäjä voi varmistaa niiden paikkansapitävyyden;
  b) käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista;
  c) rekisterinpitäjä ei enää tarvitse kyseisiä henkilötietoja käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi; tai
  d) rekisteröity on vastustanut henkilötietojen käsittelyä odotettaessa sen todentamista, syrjäyttävätkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteet.

Oikeus käsittelyn rajoittamiseen (18 art.)

#tuki2018 #stöd2018

- Jos käsittelyä on rajoitettu edellä mainitun nojalla, näitä henkilötietoja saa, säilyttämistä lukuun ottamatta, käsitellä ainoastaan rekisteröidyn suostumuksella taikka oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi tahi toisen luonnollisen henkilön tai oikeushenkilön oikeuksien suojaamiseksi tai tärkeää unionin tai jäsenvaltion yleistä etua koskevista syistä.
- Ennen kuin käsittelyn rajoitus poistetaan, rekisterinpitäjän on ilmoitettava siitä rekisteröidylle.

”Henkilötietojen käsittelyn rajoittamista koskevia menetelmiä voivat olla esimerkiksi valittujen tietojen siirtäminen toiseen käsittelyjärjestelmään tai käyttäjien pääsyn estäminen valittuihin henkilötietoihin.”c

Lähde: TSV ohje ” Miten valmistautua EU:n tietosuoja-asetukseen?”

Oikeus saada siirrettyä tiedot järjestelmästä toiseen (19 art.)

#tuki2018 #stöd2018

”Oikeus on luonteeltaan sellainen, ettei sitä olisi käytettävä niitä rekisterinpitäjiä vastaan, joiden julkisiin velvollisuuksiin henkilötietojen käsittely kuuluu. Siksi ***sitä ei pitäisi soveltaa*** **silloin, kun henkilötietojen käsittely on tarpeen rekisterinpitäjää koskevan lakisääteisen velvoitteen noudattamiseksi tai yleisen edun vuoksi toteutettavan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi**.”

Vastustamisoikeus (21 art.)

#tuki2018 #stöd2018

- Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, joka perustuu 6 artiklan 1 kohdan e tai f alakohtaan (julkisen vallan käyttö tai oikeutettu etu).
- Tällöin rekisterinpitäjä ei saa enää käsitellä henkilötietoja, paitsi jos rekisterinpitäjä voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet tai jos se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.
- Jos henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä on oikeus milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä tällaista markkinointia varten, mukaan lukien profilointia silloin kun se liittyy tällaiseen suoramarkkinointiin.

Muotovaatimukset rekisteröidyille annettavia tietoja koskien

#tuki2018 #stöd2018

- Rekisteröidyille annettavat tiedot on annettava rekisteröidylle tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä varsinkin silloin, kun tiedot on tarkoitettu erityisesti lapselle.
- Tiedot on toimitettava kirjallisesti tai muulla tavoin ja tapauksen mukaan sähköisessä muodossa.
- Jos rekisteröity sitä pyytää, tiedot voidaan antaa suullisesti edellyttäen, että rekisteröidyn henkilöllisyys on vahvistettu muulla tavoin.
- 13 ja 14 artiklassa tarkoitetut tiedot voidaan antaa rekisteröidyille yhdistettynä vakiomuotoisiin kuvakkeisiin, jotta suunnitellusta käsittelystä voidaan antaa mielekäs yleiskuva helposti erottuvalla, ymmärrettävällä ja selvästi luettavissa olevalla tavalla. Jos kuvakkeet esitetään sähköisessä muodossa, niiden on oltava koneellisesti luettavissa.

TIETOSUOJASELOSTE!

Jos rekisteröity esittää pyynnön sähköisesti, tiedot on toimitettava sähköisesti mahdollisuuksien mukaan, paitsi jos rekisteröity toisin pyytää.

Määräajat

#tuki2018 #stöd2018

- Rekisterinpitäjän on toimitettava rekisteröidylle tiedot toimenpiteistä, joihin on ryhdytty 15–22 artiklan nojalla tehdyn pyynnön johdosta ilman aiheetonta viivytystä ja joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta.
- Määräaikaa voidaan tarvittaessa jatkaa enintään kahdella kuukaudella ottaen huomioon pyyntöjen monimutkaisuus ja määrä. Rekisterinpitäjän on ilmoitettava rekisteröidylle tällaisesta mahdollisesta jatkamisesta kuukauden kuluessa pyynnön vastaanottamisesta sekä viivästymisen syyt.
- Jos rekisterinpitäjä ei toteuta toimenpiteitä rekisteröidyn pyynnön perusteella, rekisterinpitäjän on ilmoitettava viipymättä ja viimeistään kuukauden kuluessa pyynnön vastaanottamisesta rekisteröidylle syyt siihen ja kerrottava mahdollisuudesta tehdä valitus valvontaviranomaiselle ja käyttää muita oikeussuojakeinoja.

Kustannukset ja henkilöllisyyden todentaminen

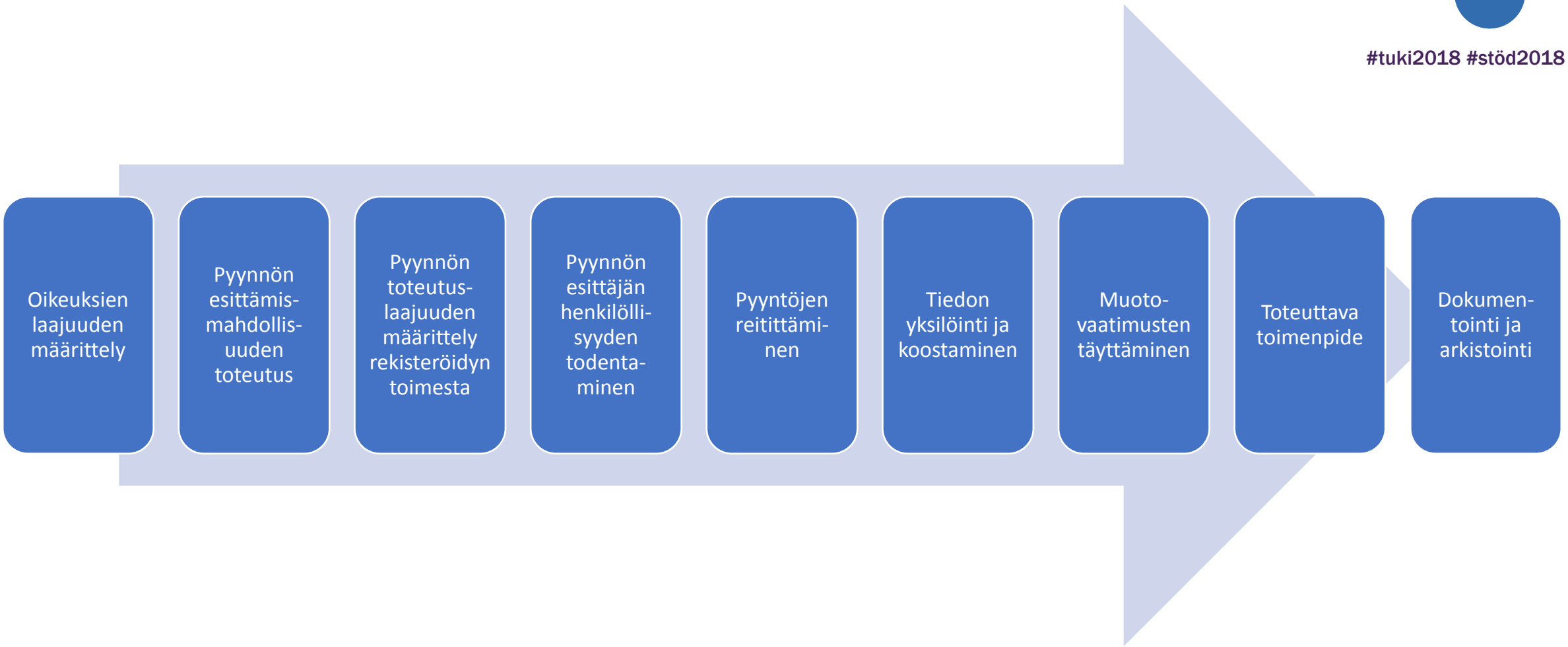
#tuki2018 #stöd2018

- 13 ja 14 artiklan nojalla toimitetut tiedot ja kaikki 15–22 ja 34 artiklaan perustuvat tiedot ja toimenpiteet ovat maksuttomia. Jos rekisteröidyn pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, erityisesti jos niitä esitetään toistuvasti, rekisterinpitäjä voi joko
  - periä kohtuullisen maksun ottaen huomioon tietojen tai viestien toimittamisesta tai pyydetyn toimenpiteen toteuttamisesta aiheutuvat hallinnolliset kustannukset; tai
  - kieltäytyä suorittamasta pyydettyä toimea.

  Näissä tapauksissa rekisterinpitäjän on osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus.
- Jos rekisterinpitäjällä on perusteltua syytä epäillä 15–21 artiklan mukaisen pyynnön tehneen luonnollisen henkilön henkilöllisyyttä, rekisterinpitäjä voi pyytää toimittamaan lisätiedot, jotka ovat tarpeen rekisteröidyn henkilöllisyyden vahvistamiseksi.

Rekisteröidyn oikeuksien toteuttamisen prosessi

#tuki2018 #stöd2018



Muut rekisteröidyn oikeudet

#tuki2018 #stöd2018

- Oikeus saada rekisterinpitäjä ilmoittamaan oikaisusta, poistosta ja käsittelyn rajoittamisesta tietojen vastaanottajille (art. 19)
- Oikeus olla joutumatta automatisoitujen päätösten kohteeksi (art. 22)
- Oikeus saada tieto rekisterinpitäjään kohdistuneesta tietoturvaloukkauksesta (art. 34)
- Oikeus tehdä valitus valvontaviranomaiselle (art. 77)
- Oikeus tehokkaisiin oikeussuojakeinoihin rekisterinpitäjää vastaan (art. 79)
- Oikeus saada korvaus aiheutuneista vahingoista (art. 82)

Tietoyhteiskunnan palveluihin liittyvään lapsen suostumukseen sovellettavat ehdot (8 art.)

#tuki2018 #stöd2018

- Jos henkilötietojen käsittelyn peruste on rekisteröidyn suostumus, katsotaan, että kun kyseessä on tietoyhteiskunnan palvelujen tarjoaminen suoraan lapselle, lapsen henkilötietojen käsittely on lainmukaista, jos lapsi on vähintään 16-vuotias.
- Jos lapsi on alle 16 vuotta, tällainen käsittely on lainmukaista vain siinä tapauksessa ja siltä osin kuin lapsen vanhempainvastuunkantaja on antanut siihen suostumuksen tai valtuutuksen.
- Jäsenvaltiot voivat lainsäädännössään säätää tätä tarkoitusta koskevasta alemmasta iästä, joka ei saa olla alle 13 vuotta.
- Rekisterinpitäjän on toteutettava kohtuulliset toimenpiteet tarkistaakseen tällaisissa tapauksissa, että lapsen vanhempainvastuunkantaja on antanut suostumuksen tai valtuutuksen, käytettävissä oleva teknologia huomioon ottaen.

Taustamateriaalia

#tuki2018 #stöd2018

- WP 29-työryhmän mietintö oikeudesta siirtää tiedot rekisterinpitäjältä toiselle
- Tietosuojavaltuutetun opas "Miten valmistautua EU:n tietosuoja-asetukseen?”
- Euroopan tietosuojavaltuutetun (EDPS) ohjeet rekisteröidyn oikeuksien toteuttamisesta (osin vanhentunut)

Tietoturvapoikkeama- ja tietosuojaloukkaustilanteiden hallinta, osa 2 – tarvittavien prosessien ja kyvykkyyksien kehittäminen sekä ohjeistus ja koulutus, tarvittava yhteistyö eri toimijoiden kesken.

17.11.2017 kotitehtävän purku

Kotitehtävän 17.11. purku

#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

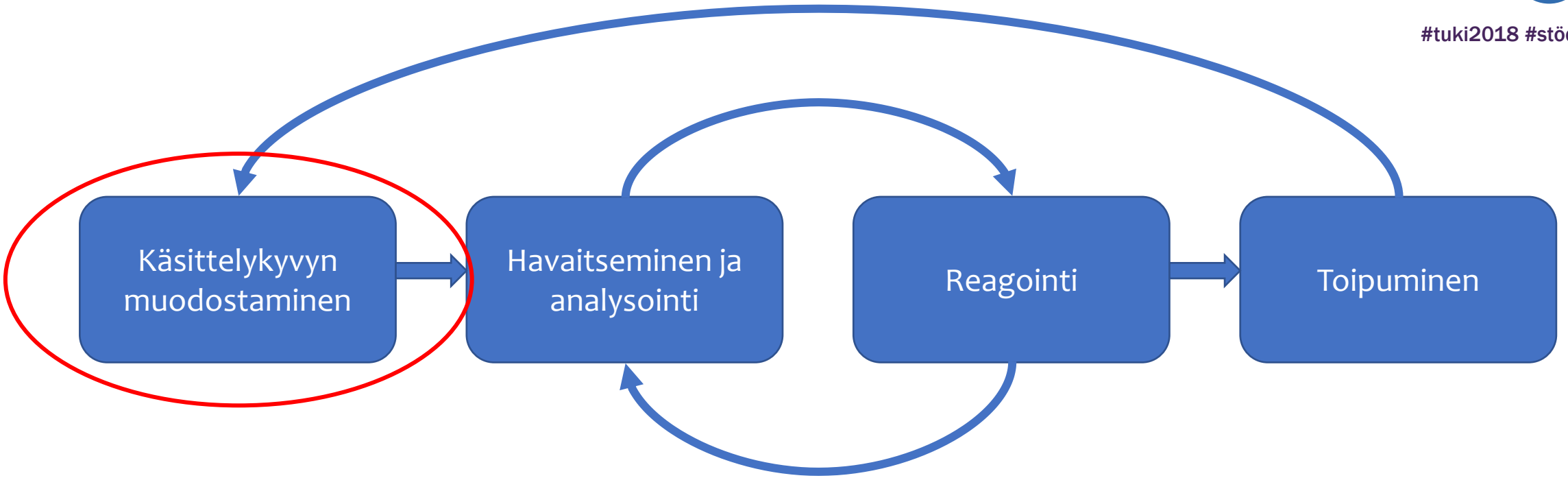
Kuinka monen osallistujan organisaatiossa on määritelty tietoturvaloukkausten hallinta?
Mitä standardia tai ohjetta olette hyödyntäneet?

VAHTI 8/2017

#tuki2018 #stöd2018

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

Hallintaprosessi



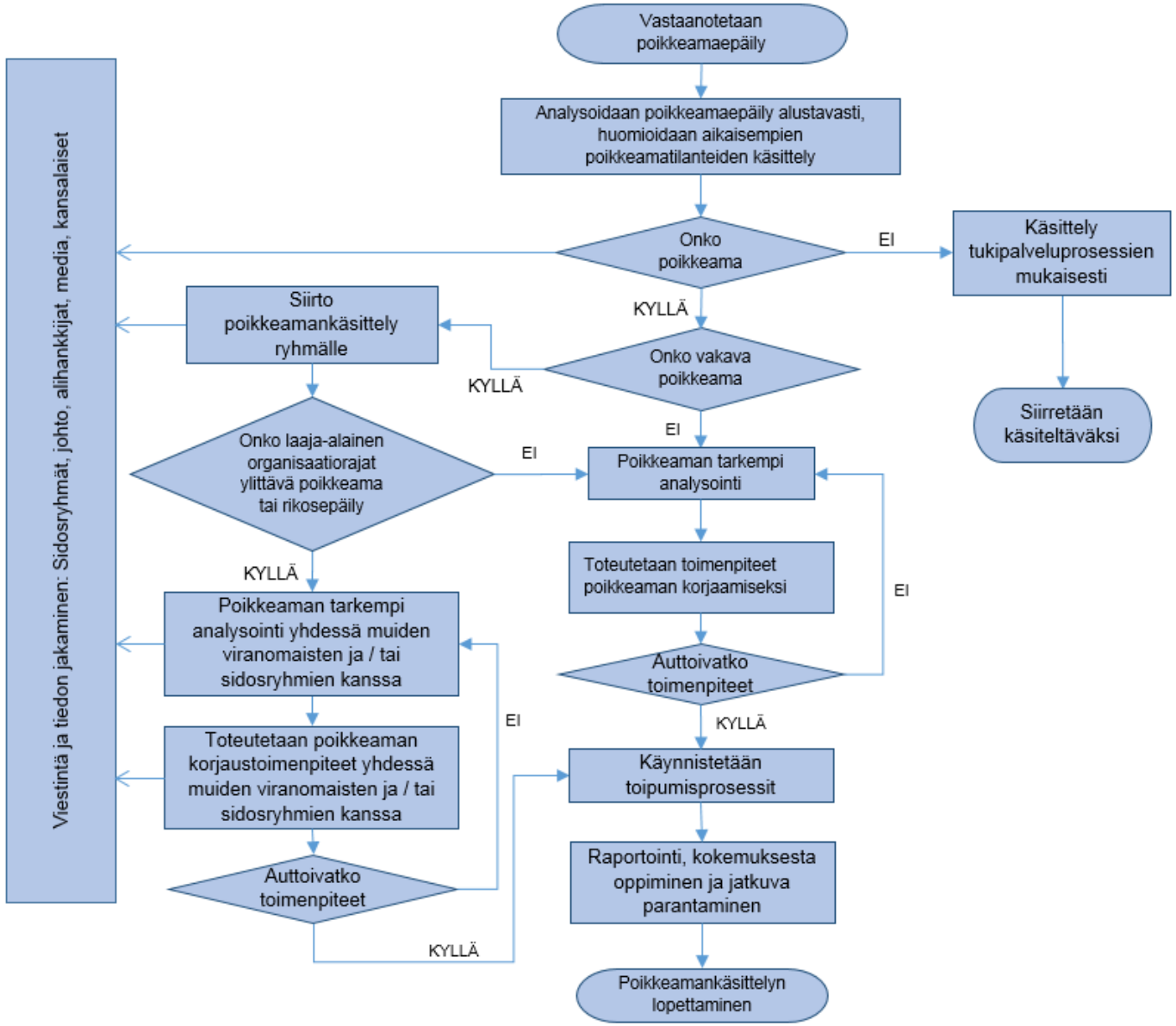
Käsittelykyvyn muodostaminen

#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

Prosessin määritys

#tuki2018 #stöd2018



Vastuut

#tuki2018 #stöd2018

- Tietoturvapäällikkö
- Tietosuojavastaava
- Verkon ylläpitäjä
- Palveluntarjoajan tietoturvavastaava

Poikkeamatyyppien luokittelu

- Luokitellaan tyypillisimmät poikkeamat valmiiksi
- Esimerkkejä
  - Palvelunestohyökkäys
  - Haittaohjelma
  - Luvaton käyttö
  - Varkaus
  - Tietovuoto (tahaton tai tahallinen)
  - Tiedon tuhoutuminen
  - …

Ohjeet eri tilanteille

#tuki2018 #stöd2018

- Hyvä malli VAHTI-ohjeessa
- Ohjeessa on käytävä läpi tyypillisimmät toimenpiteet
  - Käsittelyryhmän kokoonpano
  - Sidosryhmät
  - Viestintä
  - Käsittelylokin ylläpito
  - Step-by-step ohje havaitsemisesta toipumiseen
- Ohjetta ei kuitenkaan pidä noudattaa orjallisesti

Poikkeamanhallintaryhmä

- Koostumus vaihtelee havaitun poikkeaman ja sen vakavuuden mukaisesti
- Tyypillisesti kokoontuu käsittelemään vain vakavia poikkeamia

Koulutus ja harjoittelu

Koulutus

#tuki2018 #stöd2018

- Yleinen koulutus koko henkilöstölle
  - Poikkeamien havaitseminen
  - Oikea reagointi ja ilmoittaminen
- Poikkeamanhallintaryhmän koulutus
  - Osallistuu harjoituksiin
  - Tekniset koulutukset poikkeamien selvittäjille

Tekniset koulutukset

#tuki2018 #stöd2018

- Teknisessä roolissa toimivien on hyvä osata perusteet tietoturvaloukkausten tutkinnasta
  - Verkko, haittaohjelmat, palvelunesto, forensiikka
- Kaupallisten toimijoiden kurssit
  - SANS, GIAC, etc.

Harjoittelu

- Vaatii huolellista suunnittelua
- Tyypillisesti pitäisi harjoitella vuosittain
  - Haastavaa löytää aikaa harjoitteluun
- Harjoituksessa tyypillisesti yksi tai muutama skenaario
  - Haastavuus organisaation kypsyyden mukaan
  - Keskittyy yleensä todennäköisiin tapahtumiin
- Paperiharjoitus vs. rajattu simulointi

Yhteistyö eri toimijoiden kesken

Kyberturvallisuuskeskus

#tuki2018 #stöd2018

- Entinen CERT-FI
- Viestintäverkkojen ja –palveluiden toimintavarmuus ja turvallisuus
  - Erityisesti teleyritykset ja huoltovarmuuskriittiset toimijat
- Tietoturvaloukkausten ja uhkien selvitys
  - Erityisesti laajempien loukkausten koordinointi
  - Jakaa tietoa anonyymisti esimerkiksi uhreille
- Tiedon kerääminen ja jakaminen
  - Postituslistat

VIRT

#tuki2018 #stöd2018

- Virtual Incident Reponse Team
- SecIT hankkeessa kehitetty malli
- Valtion yleinen toimintamalli laajempiin häiriöihin – ei ainoastaan tietoturvaloukkauksiin
- Vakavassa loukkaustapauksessa yhteys KTK:hon, joka käynnistää VIRT-työskentelyn
- Tyypillisessä kokoonpanossa ViVi/KTK, Valtori sekä ministeriöt ja virastot
- Ei vielä tue kuntakenttää

Tietosuojavaltuutetun toimisto

#tuki2018 #stöd2018

- Yleinen ohjeistus ja neuvonta
  - Lait ja niiden soveltaminen
- Ohjeet rekisterinpitäjille
- Lausunnot

Muut

#tuki2018 #stöd2018

- Oma palveluntarjoaja
  - Usein monia palveluntarjoajia
- Internet-operaattori
- Ministeriöt ja virastot
  - Vertaistuki
- Poliisi
  - KRP

Harjoitustehtävä

Harjoitustehtävä 8.12.

- Täyttäkää ryhmissä oheinen poikkeamatilanneohje henkilötietojen tietoturvaloukkaukselle
  - Ranskalaiset viiva riittävät
  - Kohdassa ”Toimet” pitää kattaa koko ketju havaitsemisesta toipumiseen – panostakaa tähän
  - Voitte hyödyntää myös prosessikuvausta sivulla 36

Yhteenveto

Yhteenveto

#tuki2018 #stöd2018

- Huolellisella valmistautumisella lasketaan loukkausten käsittely- ja toipumisaikaa
- Erilaisiin tapauksiin valmistautuminen mahdollistaa todellisissa tilanteissa oikean reagoinnin
- Pelkät prosessikuvaukset ja suunnitelmat eivät riitä – harjoittelulla oppii enemmän
- Yhteistyö eri toimijoiden kanssa tärkeää

Kotitehtävä

Kotitehtävä 8.12.2017

#tuki2018 #stöd2018

- Laadi vastaava kuvaus kuin harjoitustehtävässä, mutta omaa organisaatiotasi varten
  - Sovella työpajassa ja harjoituksessa opittua
  - Muista sopeuttaa omaan organisaatiosi

#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