Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet

#tuki2018 #stöd2018

Työpaja #5 – 25.10.2017

- **Vaatimusten huomioiminen uusia palveluita ja tietojärjestelmiä kehittäessä; vaikutustenarvioinnit**
- **Tietosuojan ja tietoturvallisuuden huomioiminen hankinnoissa ja sopimuksissa**

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 Vaatimusten huomioiminen uusia palveluita ja tietojärjestelmiä kehittäessä; vaikutustenarvioinnit
- 10.30 Bio- ja jaloittelutauko
- 10.45 Työpaja jatkuu; ryhmätehtävä 1
- 12.00 Lounastauko (omakustanne)
- 13.00 – 13:30 Outi Jousi (Hannes Snellman): Vanhat sopimukset & yleisimmät sudenkuopat
- 13:30 – 13:45 Ryhmätehtävä 2
- 13:45 Työpaja jatkuu - Tietosuojan ja tietoturvallisuuden huomioiminen hankinnoissa ja sopimuksissa
- 14.30 Kahvitauko
- 14:45 Työpaja jatkuu
- 15:30 Julkishallinnon GDPR-itsearviointityökalun esittely
- 16.00 Yhteenveto ja kotitehtävä
- 16.15 Työpaja päättyy

Tietosuojan vaikutustenarvioinnit (”Data Protection Impact Assessment” / ”DPIA”)

Sisäänrakennettu tietosuoja (”Privacy by Design”)(25 art.)

#tuki2018 #stöd2018

Tietosuojan sekä tietoturvan huomiointi ja sisäänrakentaminen prosessien sekä järjestelmien suunnittelussa

- ✓ Henkilötiedon keruun ja käsittelyn minimointi
- ✓ Käyttäjäpiirin tehokas rajaaminen (käyttövaltuudet ja pääsynvalvonta)
- ✓ Säilytysaikojen määrittely ja vanhentuneen tiedon poistaminen
- ✓ Pseudonymisointi & anonymisointi
- ✓ Tiedon salakirjoittaminen (kryptaus)
- ✓ Tietoturva
- ✓ Käyttäjäystävälliset asetukset (”oletusarvoinen tietosuoja”)
- ✓ Tietosuojavastaavan rooli
- ✓ Vaikutustenarvioinnit
- ✓ Sovelluskehitys

Vaikutustenarvioinnin tavoite on sisäänrakennetun tietosuojan toteutuminen sekä prosesseissa, palveluissa että järjestelmissä

Tietosuojan vaikutustenarviointi (35 art.)

#tuki2018 #stöd2018

- Jos tietyntyyppinen henkilötietojen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa – käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen – luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin, rekisterinpitäjän on ennen käsittelyä toteutettava arviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle.
- Yhtä arviota voidaan käyttää samankaltaisiin vastaavia korkeita riskejä aiheuttaviin käsittelytoimiin.
- Tietosuojaa koskevaa vaikutustenarviointia tehdessään rekisterinpitäjän on pyydettävä neuvoja tietosuojavastaavalta, jos sellainen on nimitetty.

Kohteena suunnitellusta toiminnasta johtuvat riskit jotka kohdistuvat suoraan rekisteröityyn

Tietosuojan vaikutustenarviointi (35 art.)

#tuki2018 #stöd2018

- Tietosuojaa koskeva vaikutustenarviointi vaaditaan erityisesti tapauksissa joissa:
  a. luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmällinen ja kattava arviointi, joka perustuu automaattiseen käsittelyyn, kuten profilointiin, ja johtaa päätöksiin, joilla on luonnollista henkilöä koskevia oikeusvaikutuksia tai jotka vaikuttavat luonnolliseen henkilöön vastaavalla tavalla merkittävästi;
  b. laajamittainen käsittely, joka kohdistuu 9 artiklan 1 kohdassa tarkoitettuihin erityisiin henkilötietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin tietoihin; tai
  c. yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti.
- Valvontaviranomaisen on laadittava ja julkaistava luettelo käsittelytoimien tyypeistä, joiden yhteydessä vaaditaan 1 kohdan nojalla tietosuojaa koskeva vaikutustenarviointi.

Tietosuojan vaikutustenarviointi – korkea riski

#tuki2018 #stöd2018

Vaikutustenarviointi mahdollisesti suoritettava mm. seuraavissa tapauksissa:

- Profilointi ja pisteyttäminen
- Automatisoitu päätöksenteko
- Järjestelmällinen seuranta
- Arkaluonteisten tietojen käsittely
- Suurten tietomassojen käsittely
- Tietojen yhdistely eri lähteistä
- Heikossa asemassa olevien henkilötietojen käsittely (mm. lapset)
- Edistykselliset tietojenkäsittelytavat
- Jos tietojenkäsittely estää rekisteröityä käyttämästä oikeuksiaan tai tekemästä sopimusta

Jo yhden kriteerin täyttyminen voi tarkoittaa vaikutustenarvioinnin suorittamisen velvoitetta

Tietosuojan vaikutustenarviointi (35 art.)

#tuki2018 #stöd2018

- Arvioinnin on sisällettävä vähintään:

  a. järjestelmällinen kuvaus suunnitelluista käsittelytoimista, ja käsittelyn tarkoituksista, mukaan lukien tarvittaessa rekisterinpitäjän oikeutetut edut;

  b. arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden;

  c. arvio 35 art. 1 kohdassa tarkoitetuista rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä; ja

  d. suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että tietosuoja-asetusta on noudatettu ottaen huomioon rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut.

Ennakkokuuleminen (36 art.)

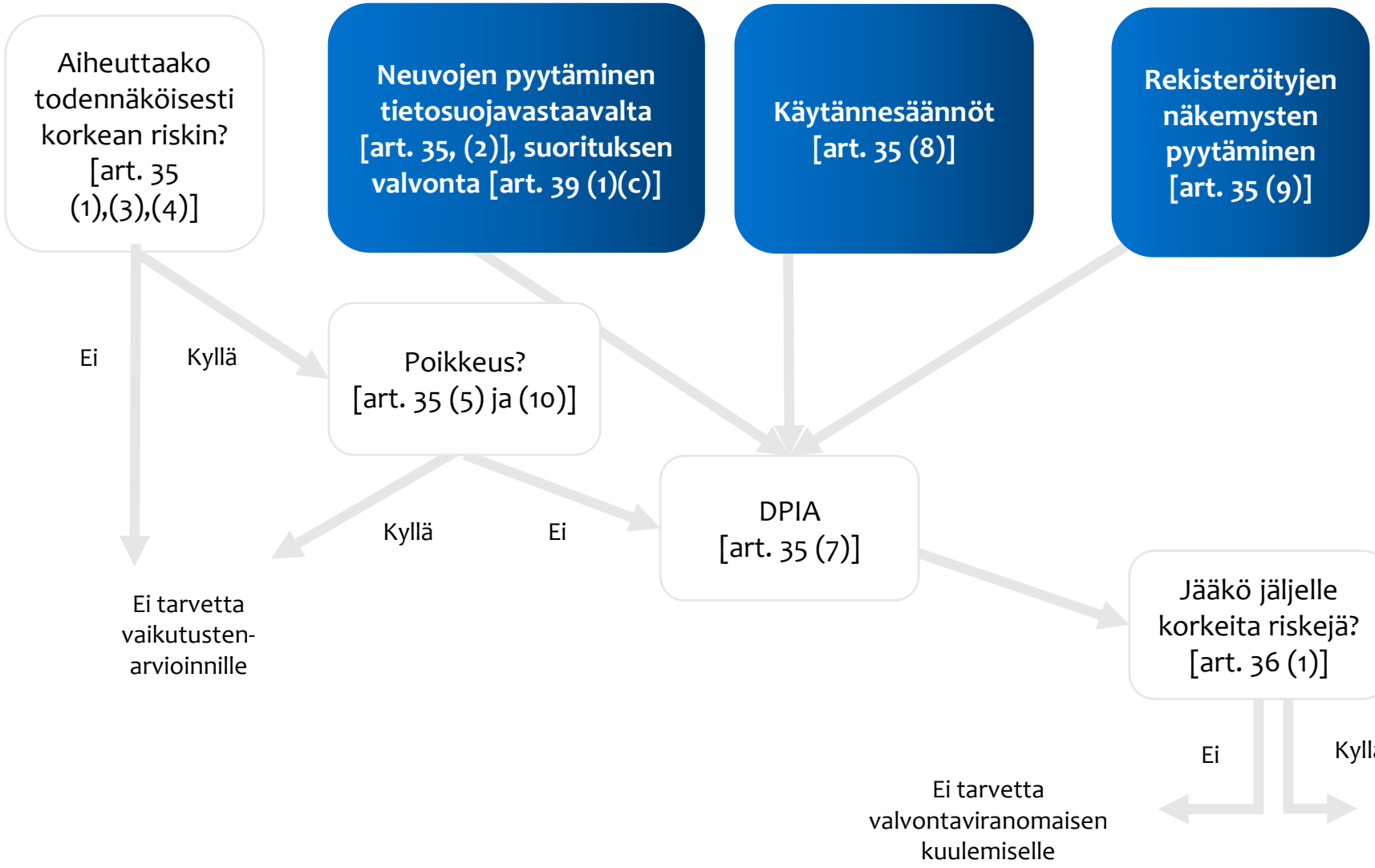
- Rekisterinpitäjän on ennen käsittelyä kuultava valvontaviranomaista, jos vaikutustenarviointi osoittaa, että riskejä ei ole pystytty laskemaan hyväksyttävälle tasolle (→ käsittely aiheuttaisi edelleen korkean riskin)
- Jos valvontaviranomainen katsoo, että suunniteltu käsittely rikkoisi tietosuoja-asetusta, erityisesti jos rekisterinpitäjä ei ole riittävästi tunnistanut tai pienentänyt riskiä, valvontaviranomaisen on enintään kahdeksan viikon kuluessa kuulemispyynnöstä annettava kirjallisesti ohjeet rekisterinpitäjälle tai tapauksen mukaan henkilötietojen käsittelijälle [].

Keinoja laskea riskitasoa, mm.:

- Tiedon suojaustoimet
- Prosessien uudelleenmäärittely
- Tiedon saatavuuden ajallinen, määrällinen tai käyttäjäperusteinen rajaaminen
- Autentikoinnin vahvistaminen
- Sopimusvaatimukset

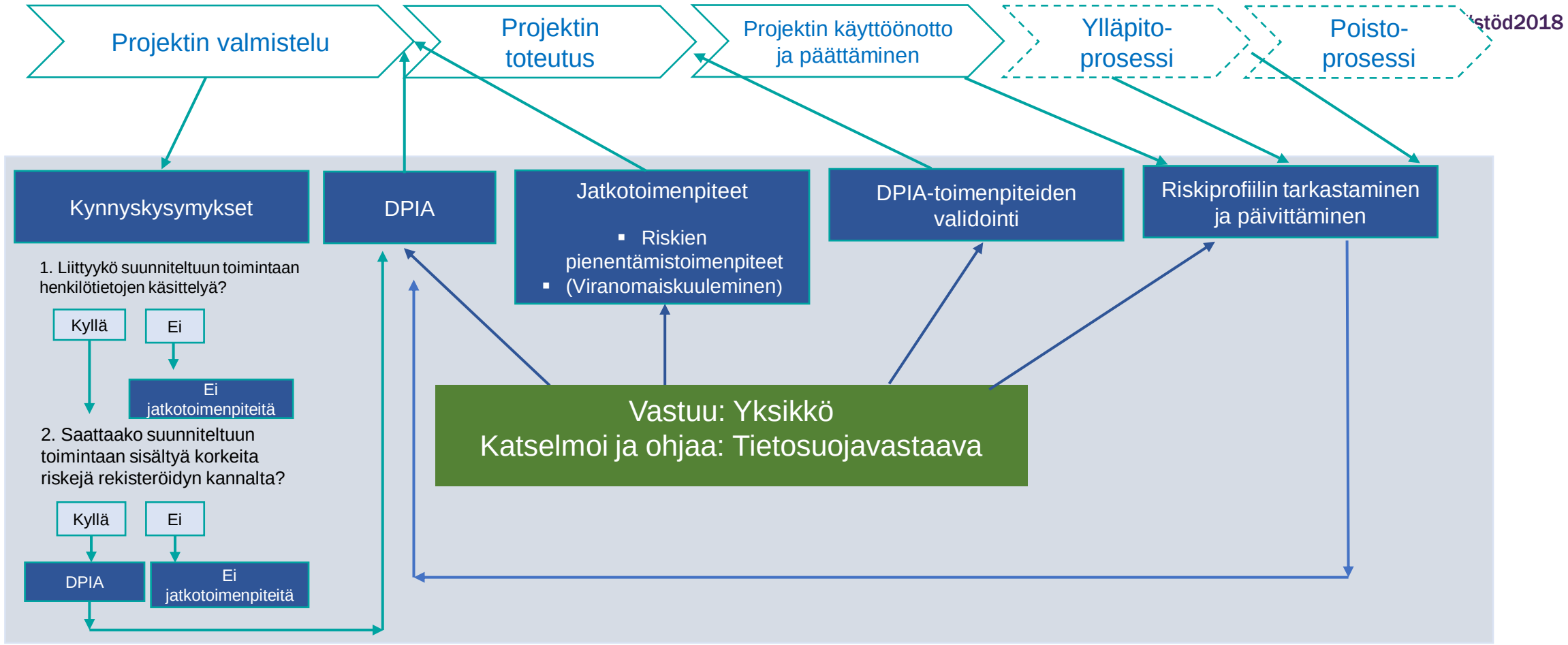
Tietosuojan vaikutustenarviointi – milloin?

#tuki2018 #stöd2018



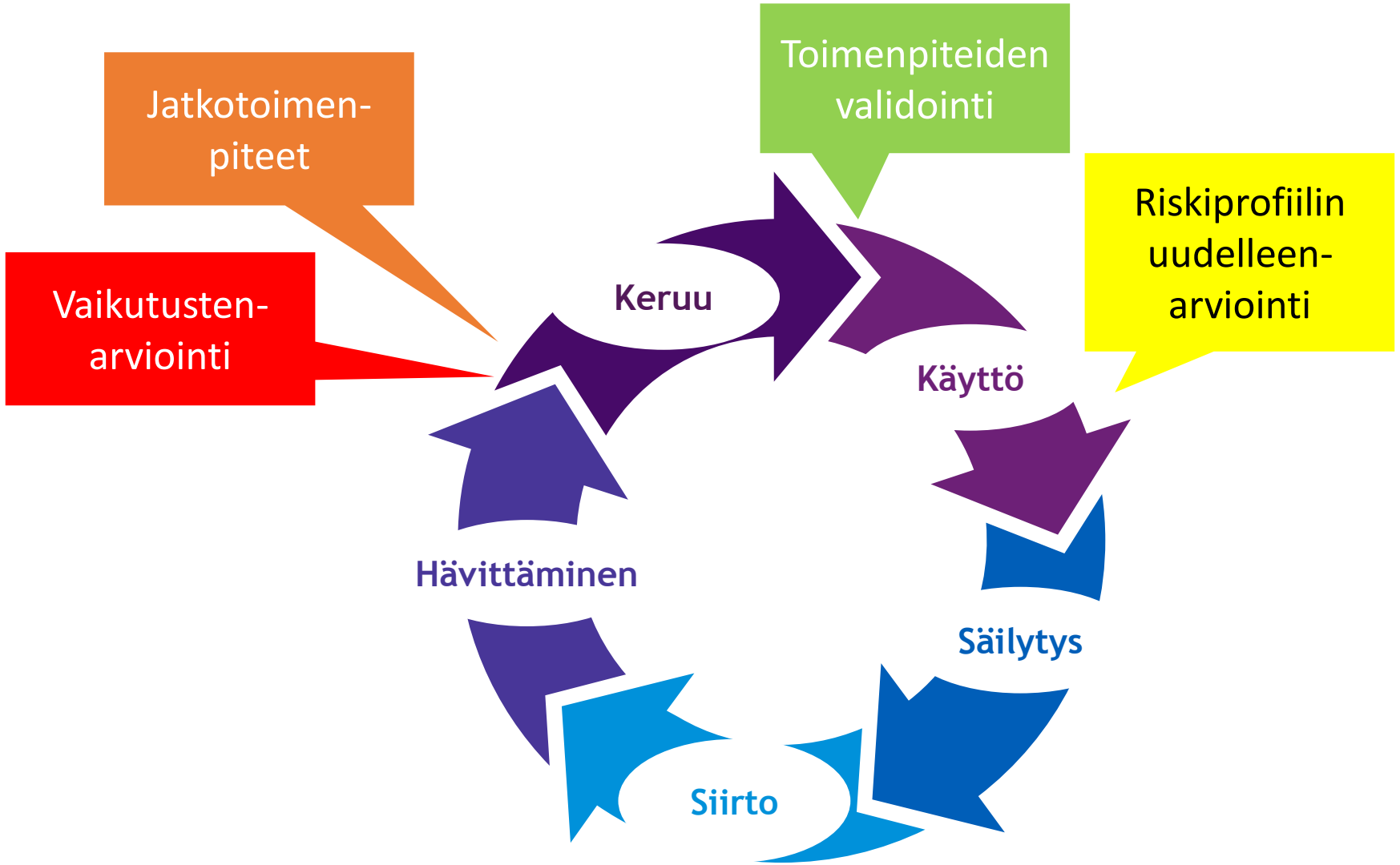
Lähde: Art. 29 tietosuojatyöryhmä WP248 rev. 01

Kehitystoiminta ja vaikutustenarviointi



Tiedon elinkaari ja vaikutustenarviointi

#tuki2018 #stöd2018



Ryhmätehtävä # 5.1

#tuki2018 #stöd2018

1. Arvioidaan kuvitteellista tapausta, joka on kuvattu jaettavassa monisteessa. Ryhmän tehtävä on
   a. arvioida kuvatuista seikoista johtuvia riskejä rekisteröidylle; sekä
   b. määritellä riskienhallintakeinoja havaituille riskeille.

Tietosuojan ja tietoturvallisuuden huomioiminen hankinnoissa ja sopimuksissa

Rekisterinpitäjän ja henkilötietojen käsittelijän välinen suhde

Rekisterinpitäjällä tarkoitetaan organisaatiotasi silloin, kun se määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Palvelutuottaja voi toisaalta myös olla rekisterinpitäjä

Rekisterinpitäjä

- Päätösvalta henkilötietojen käyttämisen ja säilytyksen suhteen
- Vastaa käsittelyn oikeellisuudesta ja lainmukaisuudesta, myös ulkoistustapauksissa
- Vastaa rekisteröidyn oikeuksien toteutumisesta
- Suunnittelee tietojen käsittelyn ja luovutukset sekä näihin liittyvät yksityiskohdat
- Vastaa käsittelijän ohjeistamisesta

Henkilötietojen käsittelijällä tarkoitetaan organisaatiota, joka käsittelee henkilötietoja rekisterinpitäjän lukuun

Henkilötietojen käsittelijä voi olla esim. palveluyritys tai ICT-palvelujen tarjoaja

Henkilötietojen käsittelijä (ks. myös artikla 29)

- Ei itsenäistä päätösvaltaa henkilötietojen käyttämisen ja säilytyksen suhteen
- Käsittelee tietoja vain sovitussa käyttötarkoituksessa
- Noudattaa rekisterinpitäjän ohjeita
- Henkilötietojen käsittelijä on vastuussa käsittelystä aiheutuneesta vahingosta vain, jos se ei ole noudattanut nimenomaisesti henkilötietojen käsittelijöille osoitettuja tämän asetuksen velvoitteita tai jos se on toiminut rekisterinpitäjän lainmukaisen ohjeistuksen ulkopuolella tai sen vastaisesti.

Lähde: Karoliina Lehto, Hansel Oy (mukaillen)

Henkilötietojen käsittelijä ja alihankinnan ketjutus

#tuki2018 #stöd2018

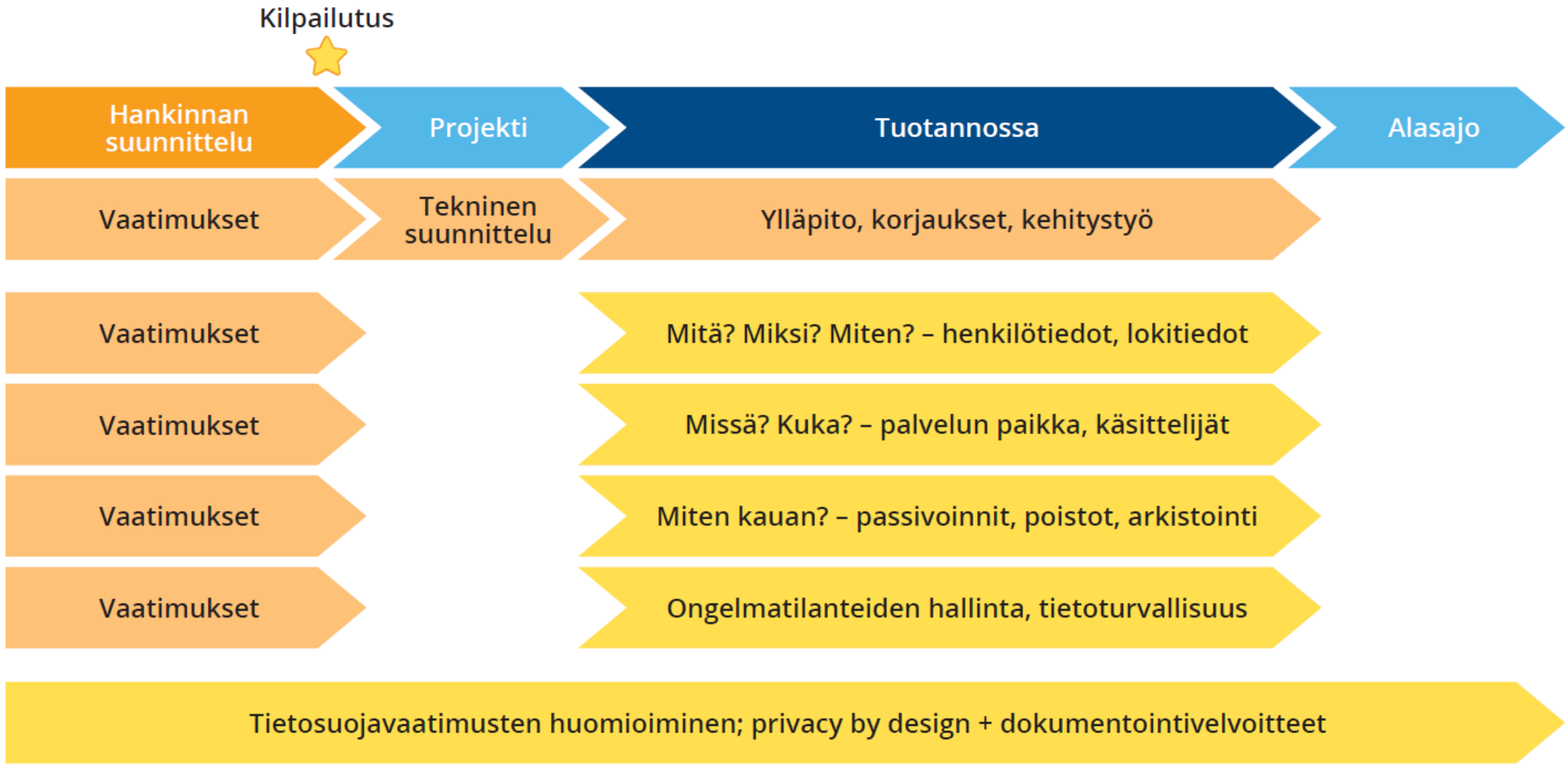
- Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tämän asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu.
- Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa.
- Kun kyse on (yleisestä) kirjallisesta ennakkoluvasta, henkilötietojen käsittelijän on tiedotettava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, ja annettava siten rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia.

Henkilötietojen käsittelijä ja alihankinnan ketjutus

#tuki2018 #stöd2018

- Kun henkilötietojen käsittelijä käyttää toisen henkilötietojen käsittelijän palveluksia erityisten käsittelytoimintojen suorittamiseksi rekisterinpitäjän puolesta, kyseiseen toiseen henkilötietojen käsittelijään sovelletaan sopimuksen [] mukaisesti samoja tietosuojavelvoitteita kuin ne, jotka on vahvistettu 28.3 kohdassa tarkoitetussa rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa [].
- Kun toinen henkilötietojen käsittelijä ei täytä tietosuojavelvoitteitaan, alkuperäinen henkilötietojen käsittelijä on edelleen täysimääräisesti vastuussa toisen henkilötietojen käsittelijän velvoitteiden suorittamisesta suhteessa rekisterinpitäjään.
- Jos käsittelijä ryhtyy käsittelemään henkilötietoja muussa kuin sovitussa käyttötarkoituksessa, sille voi syntyä tältä osin rekisterinpitäjän vastuu.

Tietojärjestelmän elinkaari



Lähde: Kuntaliiton tietosuojaohje sopimukset ja alihankkijat

Hankinnan elinkaari

- Tietoturvallisuusvaatimukset
- Tietosuojavaatimukset (mallilausekkeet tms. asetuksen vaatimat sopimusehdot)
- Henkilötietojen käsittelyn hallinnolliset ja toiminnalliset vaatimukset

Organisaation tarve käsitellä henkilötietoja

- Henkilötietojen käsittelyprosessien määrittely
- => Rekisterinpitäjyys, suunnitteluvelvoite (osoitusvelvollisuus), henkilötietojen ja –virtojen kartoitus, käsittelytarkoitukset, tietosisältö, oikeudellinen käsittelyperuste, tietojen lähteet ja luovutukset, tietovirrat, EU/ETA näkökulma, säilytysaikojen määrittely
- Suojaustarpeen ja –keinojen määrittely (tekniset vaatimukset, käyttöoikeudet, toimintatavat

Hankintaprosessi

- Tarvekartoitus
- Tietopyyntö
- Tarjouspyyntö
- Tarjous
- Tarjousten vertailu ja neuvottelu
- Hankintasopimus
- Tilaus

Tarjouspyyntövaatimusten lisäksi: henkilötietojen käsittelyä koskevat rekisterinpitäjän prosessikohtaiset ohjeet käsittelijälle

Käyttöönotto

- Hankinnan kohteen käyttöönotto vaatimusten mukaisena (ml. henkilötietojen käsittelyn koko elinkaari)
- Tietosuojaan ja tietoturvallisuuteen liittyvien hallinnollisten yhteistyöelinten ja raportoinnin perustaminen, ml. vastuutukset
- Tietosuojaan ja tietoturvallisuuteen liittyvien prosessien perustaminen, vastuutus ja resursointi

Tuotanto

- Tietosuojan ja tietoturvallisuuden jatkuva ylläpito, seuranta, raportointi ja kehittäminen sopimuksissa määriteltyjen sekä lainsäädännön vaatimusten mukaisesti
- Säännölliset tietosuojan ja tietoturvallisuuden auditoinnit (riskiperusteisuus) => raportointi, kehittäminen, tietotilinpäätös

Käsittelytoimien alasajo

- Tietojen luovuttaminen rekisterinpitäjälle (tietojen hävittäminen palveluntuottajalta)
- Säilytysaika- ym. säilytysvaatimukset huomioitava, käsittelijällä myös velvoitteita tietojen säilyttämiseen
- Tietoturvallisuusvaatimusten (mm. tietovälineiden hävittäminen) toteutus

Tietosuojan sopimusvaatimukset (28 art.)

#tuki2018 #stöd2018

Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä [kirjallisella] sopimuksella tai muulla unionin oikeuden tai jäsenvaltion lainsäädännön mukaisella oikeudellisella asiakirjalla, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Tässä sopimuksessa tai muussa oikeudellisessa asiakirjassa on säädettävä erityisesti, että henkilötietojen käsittelijä

a. käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti, mikä koskee myös henkilötietojen siirtoja kolmanteen maahan tai kansainväliselle järjestölle [];

b. varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus;

c. toteuttaa kaikki 32 artiklassa vaaditut toimenpiteet;

d. noudattaa [] toisen henkilötietojen käsittelijän käytön edellytyksiä (ks. s. 17);

Soveltuvin osin!

Tietosuojan sopimusvaatimukset (jatkuu)

d. ottaen huomioon käsittelytoimen luonteen auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat III luvussa säädettyjen rekisteröidyn oikeuksien käyttämistä;

e. auttaa rekisterinpitäjää varmistamaan, että 32–36 (*henkilötietojen tietoturvaloukkausten ilmoitusvelvollisuus; tietosuojan vaikutustenarvioinnit*) artiklassa säädettyjä velvollisuuksia noudatetaan ottaen huomioon käsittelyn luonteen ja henkilötietojen käsittelijän saatavilla olevat tiedot;

f. rekisterinpitäjän valinnan mukaan poistaa tai palauttaa käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset, paitsi jos unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan säilyttämään henkilötiedot;

g. saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen 28 artiklassa säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja sallii rekisterinpitäjän tai muun rekisterinpitäjän valtuuttaman auditoijan suorittamat auditoinnit, kuten tarkastukset, sekä osallistuu niihin.

Lisäksi rekisterinpitäjän tulee osana turvallisuussopimusta harkita henkilötietojen käsittelijän sitouttamista siihen, että henkilötietojen käsittelyä suorittavat vain sellaiset henkilöt, jotka ovat saaneet hyväksyttävän tuloksen turvallisuusselvityksessä, jos rekisterinpitäjällä on lainmukainen oikeus teettää turvallisuusselvityksiä.

Henkilötietojen siirto EU:n/ETA:n ulkopuolelle

#tuki2018 #stöd2018

Henkilötietojen siirto EU:n tai Euroopan talousalueen ulkopuolelle on luvallista seuraavin järjestelyin:

1. Komission päätös siirron kohdevaltion tietosuojan tason riittävyydestä
2. Yhdysvaltalaisia organisaatiota koskeva ”Privacy Shield”-järjestelmä
3. Rekisteröityjen yksiselitteisen suostumuksen perusteella tai kun siirto on tarpeen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen valmistelemiseksi tai täytäntöön panemiseksi
4. Sopimuslausekkein annettavat takeet
5. EU-komission hyväksymät mallisopimuslausekkeet

- Rekisterinpitäjä on velvollinen hankkimaan riittävät siirtoperusteet
- Henkilötietojen käsittelijä on velvollinen hankkimaan vastaavat siirtoperusteet, mikäli siirtää tietoja itse EU:n/ETA:n ulkopuolelle

Käsittelyn turvallisuus

Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

a) henkilötietojen pseudonymisointi ja salaus;

b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;

c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;

d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Konkreettiset tietoturvavaatimukset → turvallisuussopimus tms.

#tuki2018 #stöd2018

Toisin sanoen

- Vastaako palvelun turvallisuustaso tiedon vaatimaa suojausvelvoitetta?
- Toiminnalliset vaatimukset
- Tietoturvatoimenpiteet
- Valvonta- ja raportointikäytännöt
- Säännöllinen testaus

Turvallisuustason mitoittaminen

#tuki2018 #stöd2018

Käytännössä turvallisuustason arvioinnissa voidaan huomioida mm.

- hankinnan kohteena olevassa palvelussa tai järjestelmässä käsiteltävien tietojen suojaustasoluokittelu, sekä
- hankinnan kohteena olevan palvelun tai järjestelmän oma luokittelu, jolloin arvioidaan mm.
  - millaisia tietoja käsitellään;
  - onko luottamuksellisuus, käytettävyys vai eheys keskeisenä vaatimuksena;
  - käsittelyn, palvelun tai järjestelmän merkitys organisaation ydintoiminnalle;
  - käsittelyn, palvelun tai järjestelmän merkitys asiakkaille tai muulle toimintaverkostolle; ja
  - käsittelyn, palvelun tai järjestelmän merkitys yhteiskunnalle ja välillisille asiakkaille.

RISKILÄHTÖISYYS!

Lähde: Kuntaliiton tietosuojaohje sopimukset ja alihankkijat

Tietosuojasopimuksen tehtävä – yhteenveto

#tuki2018 #stöd2018

Sopimuksessa on vahvistettava:

- Osapuolten roolit ja vastuut
- Henkilötietojen käsittelyn kohde ja kesto
- Käsittelyn luonne ja tarkoitus
- Henkilötietojen tyypit ja rekisteröityjen ryhmät
- Rekisterinpitäjän velvollisuudet ja oikeudet
- Henkilötietojen käsittelijän velvollisuudet ja oikeudet

Lähde: Karoliina Lehto, Hansel Oy (mukaillen)

Henkilötietojen käsittelijän avustamisvelvollisuus

#tuki2018 #stöd2018

- Rekisteröidyn oikeuksien toteuttaminen ml. tiedonantovelvoitteet
- Henkilötietojen tietoturvaloukkausten havainnointi, dokumentointi ja ilmoittaminen
- Tietosuojan vaikutustenarviointien tekeminen
- Sisäänrakennettu ja oletusarvoinen tietosuoja
- Yleinen tiedonantovelvollisuus osoitusvelvollisuuden toteuttamisen tueksi
- Auditointien salliminen

Yhteenveto – muistilista

#tuki2018 #stöd2018

- Selvitä tietojenkäsittelyn roolit
- Selvitä, mitä velvollisuuksia sinuun rekisterinpitäjänä kohdistuu
- Selvitä, mitä velvollisuuksia asetus asettaa käsittelyn ulkoistajalle
- Selvitä ja määrittele, mitä henkilötietoja hankittavassa järjestelmässä tullaan käsittelemään ja miten
- Pohdi, mitkä tehtävät hoidat itse ja mitä palveluntarjoaja tekee – roolit ja vastuut
- Listaa ja laadi tarvittavat politiikat, ohjeistukset, prosessit, kuvaukset ja käytännesäännöt
- Liitä tarjouspyyntöön vaatimusmäärittely ja varmista, että siinä on otettu huomioon myös tietosuoja
- Liitä tarjouspyyntöön sopimusehdot, joissa vyörytät palveluntarjoajalle ne velvollisuudet ja tehtävät, jotka sen tulee hoitaa, jotta käsittely on laillista ja jotta rekisterinpitäjän velvollisuudet voidaan täyttää ja rekisteröidyn oikeudet toteutuvat – vakioehtojen käyttö ei riitä täyttämään tätä vaatimusta.

Lähde: Karoliina Lehto, Hansel Oy (mukaillen)

Tietosuojan itsearviointityökalu

Tietosuojan arviointityökalu – esittely

#tuki2018 #stöd2018

Osa-alue #	Tietosuojan osa-alue	Vaatimus #	Pvm	Tekijä	Aihe-alue	Ylemmän tason vaatimus	Tarkemmat vaatimukset	Dokumentaatio / vaad todiste
1	Tietosuojan hallinta							
		1.1			Tietosuojan hallintamalli	Organisaation hallinnolliset rakenteet, roolit ja vastuut henkilötietojen keräämisen, käytön, luovuttamisen, poistamisen sekä suojaamisen, käsittelytoimien suunnittelun, valvonnan ja rekisteröityjen oikeuksien toteuttamisen osalta.	Tietosuojan hallintamalli on muodostettu (dokumentoitu, kommunikoitu ja implementoitu). Tietosuojaan liittyvät roolit ja vastuut ovat selkeästi määritelty organisaatiossa, ja tietosuojaroolit ovat osa keskeisten henkilöiden tehtävänkuvauksia. Tietosuoja-asetuksen tarkoittama riittävän ammattipätevyyden ja tietosuojalainsäädännön tuntemuksen omaava tietosuojavastaava on nimetty, ja on luotu prosessit ja käytänteet, jotka tukevat tietosuojavastaavan toimintaa ja raportoimista ylimmälle johdolle. Tietosuojavastaavaan liittyvä ilmoitus on tehty tietosuojavaltuutetulle.	Kuvaukset hallintarakenteista, raportointiketjuista ja määritetyistä Kuvaukset vastuista työnkuvauksi todisteet tietosuojavastaavan nimit Tietosuojavastaavan työnkuvaus j riittävästä resursoinnista Osoitus tietosuojavaltuutetulle teh tietosuojavastaavaa koskevasta iln
		1.2			Tietosuojaorganisaatio	Tehtävät liittyen tietosuojan jatkuvan kehittämisen ja ylläpidon ohjelman hallinnointiin, kuten tietosuojatyön budjetointi, resursointi (ml. tietosuojavastaava tai tietosuojan vastuuhenkilö), strateginen tavoiteasetanta sekä toiminnan jatkuva kehittäminen, arviointi ja mittaaminen.	Tietosuojaorganisaation tehtävienjako on määritetty, dokumentoitu ja osoitettu tarkoituksenmukaisille henkilöille. On olemassa dokumentoidut prosessit, jotka mahdollistavat ja varmistavat tietosuojaorganisaation asianmukaisen toiminnan, mukaan lukien: - Tarvittavien resurssien tunnistaminen vähintään seuraavalle vuodelle - Budjettitarpeiden tunnistaminen ja seuranta sisäisen henkilöstön ja teknologiaratkaisujen osalta - Tietosuojatoiminnon tavoitteiden asettaminen ja seuranta On olemassa prosessi sen varmistamiseksi, että tietosuojaorganisaation resurssitarpeet tunnistetaan vähintään vuodeksi eteenpäin.	Dokumentoidut tietosuojaorganisa tehtävät Dokumentoidut budjettiluvut Dokumentoidut tavoitteet ja mittari Tietosuojan kehittämissuunnitelm
2	Henkilötieto-inventaario							
		2.1			Henkilötietoinventaari	Organisaation kuvauskanta henkilötietojen käsittelytoimista, sisältäen kuvauksen mm. siitä mitä henkilötietoja organisaation eri prosesseissa käsitellään, mihin käyttötarkoituksiin, missä tietoa säilytetään ja kenelle mitäkin tietoa luovutetaan tai jaetaan.	Organisaatio on määritellyt keskitetyn, ajantasaisen ja kattavan luettelo henkilötietojen käsittelyn kokonaisuudesta. Henkilötietojen käsittelyyn liittyvät liiketoimintaprosessit, järjestelmät ja kumppanit kartoitetaan, dokumentoidaan ja katselmoidaan määräajoin näissä tapahtuneiden muutosten tunnistamiseksi. Näiden muutosten mukaisten vaikutusten päivittäminen luetteloon on vastuutettu ja tähän on olemassa prosessi.	Osoitus keskeisten käsittelytoimiir asioiden tunnistamisesta: - Henkilötietojen ja niiden luokituk tunnistaminen - Henkilötietoja käsittelevien prose kartoitus - Henkilötietojen käsittelyyn liittyvi tietojärjestelmien kartoitus - Prosesseihin liittyvien henkilötie käsittelytarkoitusten kartoitus - Käsittelyn oikeusperusteiden kar

Kotitehtävä 25.10.2017

Kotitehtävä – työpaja #5

#tuki2018 #stöd2018

1. Mikäli tällainen selvitystyö ei ole organisaatiossasi vielä käynnissä, varmista että sellainen työ käynnistetään, jossa arvioidaan olemassa olevat ulkoistussopimukset ja arvioidaan niiden vaatimusten riittävyyttä tietosuoja-asetuksen vaatimuksiin.

2. a) Tutustu itsearviointityökaluun ja valmistaudu työkalun lopullisen version julkaisun jälkeen hyödyntämään sitä omassa organisaatioosi, kehittämiskohteiden selvittämiseksi suhteessa tietosuoja-asetuksen vaatimuksiin.

   b) Anna palautetta työkalun toiminnasta sekä kehittämisideoita sen parantamista.

Kertaus

#tuki2018 #stöd2018

1. Toimitamme linkin tilaisuuden palautekyselyyn ja materiaaleihin
2. Tee kotitehtävät – varmista että työpajassa käsitellyt asiat etenevät organisaatiossasi
3. Ilmoittaudu seuraavaan työpajaan kun laitamme sinulle linkin
4. Vastaa viikkoa ennen seuraavaa työpajaa toimittamaamme kyselyyn koskien kotitehtävien suorittamista
5. Katso Arjen tietosuoja-videot ja suorita nettitesti – huolehdi, että organisaatiosi huolehtii sen levittämisestä henkilöstölle viimeistään syksyn aikana – sekä kerää tiedot ja varmistaa, että henkilöstö katsoo sen ja suorittaa nettitestin hyväksytysti

Hyödyllisiä linkkejä

#tuki2018 #stöd2018

- Art. 29 työryhmän linjaus tietosuojan vaikutustenarvioinnista ja ”korkeasta” riskistä

- Laki julkisista hankinnoista ja käyttöoikeussopimuksista
- Kuntaliiton ym.: Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja
- Hankinnat.fi
- Vahti tietoturvallisuussopimusmalli

Lähde: Karoliina Lehto, Hansel Oy (mukaillen)

#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

Kuntaliitto
Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori
Valtion tieto- ja viestintäteknikkakeskus

OIKEUSMINISTERIÖ
JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto