Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet

#tuki2018 #stöd2018

Työpaja #4 – 29.9.2017

- Rekisterinpitäjän velvollisuuksien toteuttaminen
- Riskienhallinta osa 4, tietosuojanäkökulma

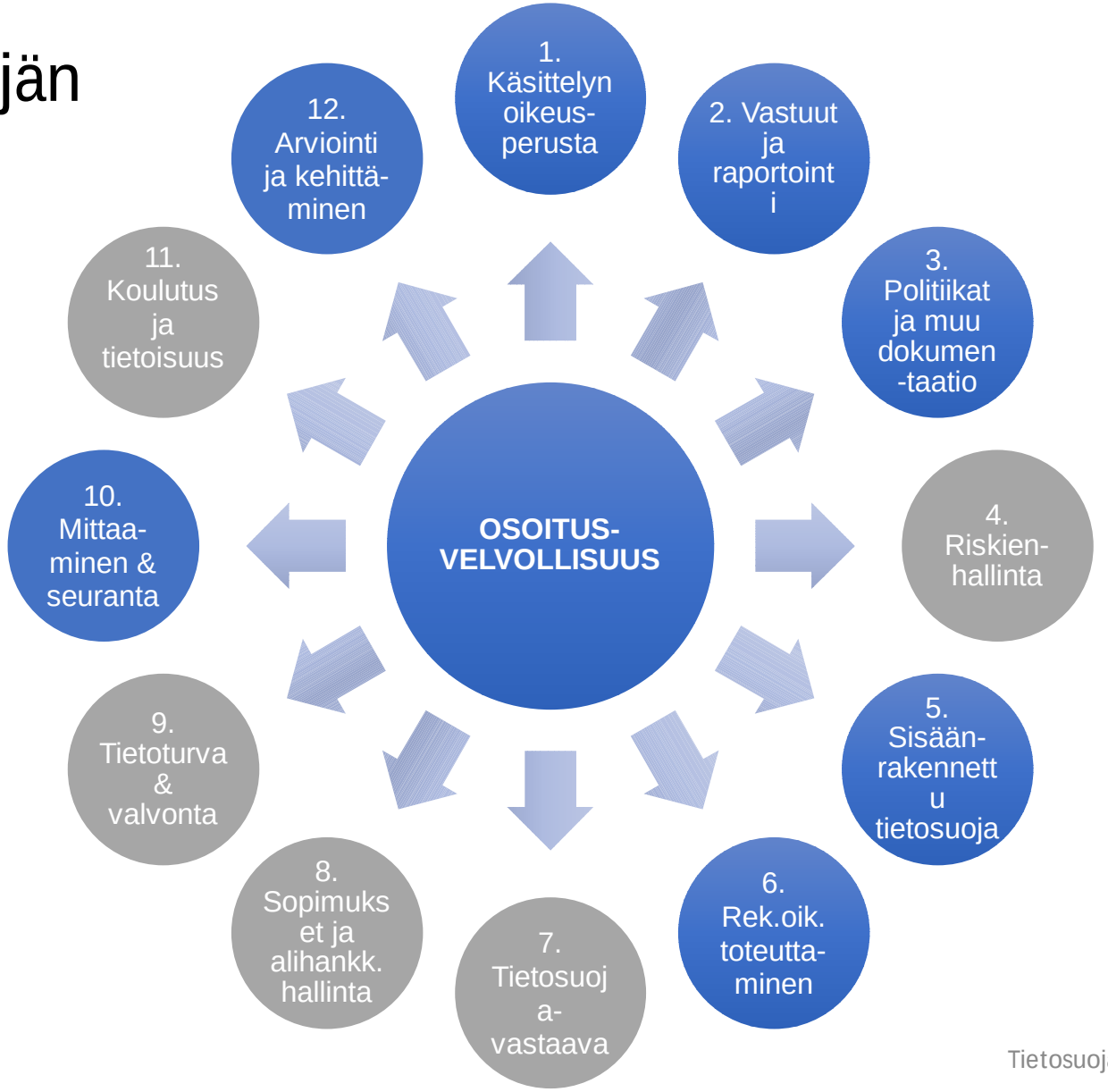
Tilaisuuden ohjelma

#tuki2018 #stöd2018

- 8.30 Kahvi
- 9.00 Tilaisuuden avaus – Tuula Seppo, Kuntaliitto & Kimmo Rousku, valtiovarainministeriö
- 9.15 Rekisterinpitäjän velvollisuuksien toteuttaminen
- 10.30 Bio- ja jaloittelutauko
- 10.45 Työpaja jatkuu + ryhmätyö ja sen purku
- 12.00 Lounastauko (omakustanne)
- 13.00 Poliisihallitus
- 13.30 Riskienhallinta osa 4, tietosuojanäkökulma
- 14.30 Kahvitauko
- 14.45 Työpaja jatkuu
- 16.00 Yhteenveto ja kotitehtävä
- 16.15 Työpaja päättyy

Rekisterinpitäjän velvollisuudet

Rekisterinpitäjän velvollisuudet



#tuki2018 #stöd2018

1. Käsittelyn oikeusperusta (6 art.)

#tuki2018 #stöd2018

- Laista johtuva velvoite
- Jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi
- Jos käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi
- Rekisteröidyn suostumus
- Sopimuksen valmistelu ja täytäntöönpano
- Rekisterinpitäjän oikeutettu etu
- ...

1. Käsittelyn oikeusperusta – henkilötietoinventaario

#tuki2018 #stöd2018

- Tärkeänä osana nykytila-analyysia on hyvä päivittää organisaation keräämien ja käsittelemien henkilötietojen kokonaiskuva.
- Tiedot avustavat yleisesti rekisterinpitäjän velvollisuuksien täyttämisessä sekä palvelevat suoraan osoitusvelvollisuuden täyttämistä.
- Myös 30 artikla antaa osviittaa kerättävien tietojen suhteen.

Kartoitettava mm.:

- Käsiteltävät henkilötietovarannot (→ henkilörekisterit)
- Henkilötietoluokat
- Henkilötietojen käsittelyperusteet
- Henkilötietojen käyttötarkoitukset
- Kytkennät prosesseihin
- Henkilötietojen säilytysajat
- Henkilötietovirrat
- Henkilötietojen käsittelyyn käytetyt järjestelmät
- Henkilötietojen maantieteellinen sijainti
- Palveluntoimittajat

2. Tietosuojavastuut – tyypilliset vastuunjaot

#tuki2018 #stöd2018

- Rekisterinpitäjä on oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjällä on vastuu henkilötietojen käsittelyn lainmukaisuudesta.
- Henkilötietojen käsittelijä on oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Myös henkilötietojen käsittelijällä on osaltaan vastuu henkilötietojen käsittelyn lainmukaisuudesta.
- Organisaation johdolla on kokonaisvastuu rekisterinpidosta sekä tietosuojan ja sen kehittämisen järjestämisestä ja resursoinnista. Nämä vastuut delegoituvat organisaation mukaisesti. Käytännön tason vastuut määrittää työjärjestys, hallintosääntö tai muu ohjeistus (esim. yksikön johtaja).

Henkilötietojen käsittelijän vastuu määräytyy lainsäädännön ja sopimusten perusteella

2. Tietosuojavastuut – tyypilliset vastuunjaot (jatkuu)

#tuki2018 #stöd2018

- Esimiehet vastaavat siitä, että heidän alaisillaan on riittävä osaaminen, mahdollisuus riittävään kouluttautumiseen, ohjeistus ja asianmukaiset työkalut henkilötietojen lainmukaiseen käsittelyyn. Heidän tehtävänään on valvoa tietosuojan toteutumista henkilöstön työssä ja raportoida tietosuojan vaarantumiset sekä poikkeamat periaatteista tai ohjeistuksesta organisaatiossa määrättävän toimintamallin mukaisesti.
- Henkilöstöllä on henkilötietoja käsitellessään velvollisuus toimia henkilötietolainsäädännön sekä tietosuojaperiaatteiden, tietoturvaperiaatteiden ja muun ohjeistuksen mukaisesti. Jokaisen vastuulla on raportoida havaitsemansa tietosuojan vaarantuminen tai poikkeamat periaatteista tai ohjeistuksesta organisaatiossa määrättävän toimintamallin mukaisesti.
- Tietosuojavastaava ei tittelistään huolimatta vastaa tietosuojasta kokonaisuutena vaan tehtävinä on neuvonta, kehittäminen ja seuranta → ks. työpajamateriaali 17.11.2017.

3. Politiikat ja muu dokumentaatio

#tuki2018 #stöd2018

Tietosuojaperiaatteet	Seloste henkilötietojen käsittelytoimista	Rekisteriselosteet / tietosuojaselosteet
Sopimukset	Henkilötietojen käsittelyn ohjeistus henkilöstölle sekä tietojenkäsittelijöille	Prosessien, analyysien ja toimenpiteiden dokumentointi
Riskienhallinta-periaatteet	Tietoturvapolitiikka	Käyttövaltuus- ja pääsynhallinta-periaatteet

3. Politiikat ja muu dokumentaatio

#tuki2018 #stöd2018

- Tietotilinpäätös
- Alihankkijoiden valintaa ohjaavat periaatteet
- Prosessikuvaukset rekisteröidyn oikeuksien toteuttamiseksi
- Kuvaus tietovirroista
- Tiedon luokittelun periaatteet
- Prosessikuvaus tietoturvaloukkausten ilmoittamiseksi
- Tiedonohjaus-suunnitelma
- Lokituksen periaatteet
- Tiedon varmistus-periaatteet
- Tietosuojan vuosikello

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

#tuki2018 #stöd2018

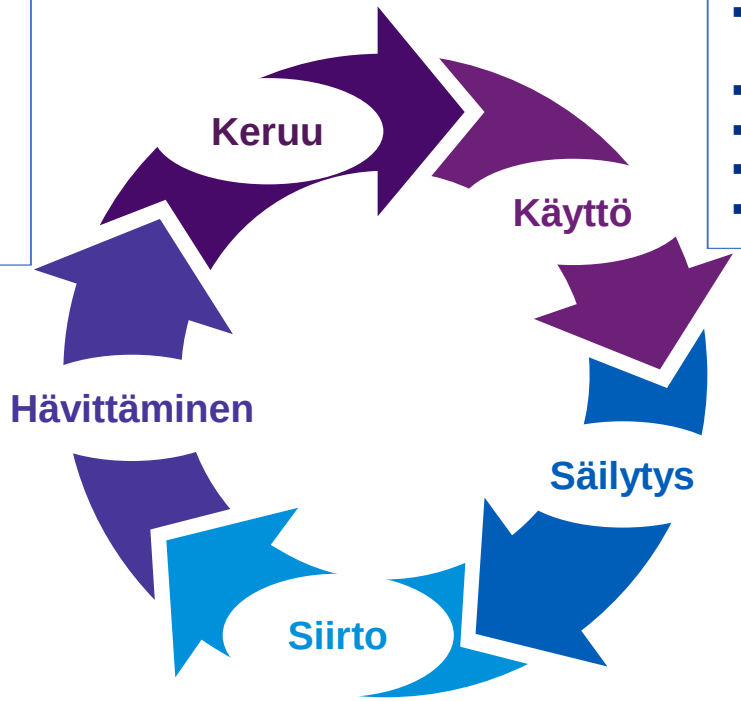
Tietosuojan sekä tietoturvan huomiointi ja sisäänrakentaminen prosessien sekä järjestelmien suunnittelussa

- ✓ 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

5. Sisäänrakennettu tietosuoja – tiedon elinkaari

#tuki2018 #stöd2018

- Oikeudellinen peruste
- Käyttötarkoitus
- Säilytysaikojen määrittely
- Tiedonannot
- Minimointi
- Luokittelu



- Käyttötarkoitus-sidonnaisuus
- Tarpeellisuus
- Tiedon laatu
- Jalostaminen
- Käyttäjienhallinta

- Säilytysaikojen noudattaminen
- Turvallisuus
- Tarpeettoman tiedon hävittäminen

- Pseudonymisointi
- Anonymisointi
- Tiedon salaaminen
- Arkistointi

- Siirtoperusteet
- Sopimukset
- Tiedonsiirtojen turvallisuus

5. Sisäänrakennettu tietosuoja – henkilötietojen käsittelyn periaatteet (5 art.)

#tuki2018 #stöd2018

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

- Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
  - → Laillinen käsittelyperuste
  - → Huolellisuus
  - → Tiedonannot

Käyttötarkoitussidonnaisuus

- Henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteen sopimattomalla tavalla
  - → Käyttötarkoitusten määrittely
  - → Tietoja ei voida kerätä ”varastoon” myöhemmin määriteltäviä käyttötarkoituksia varten
  - → Käyttötarkoitusten lisääminen vain rajatusti mahdollista

5. Sisäänrakennettu tietosuoja – henkilötietojen käsittelyn periaatteet (5 art.)

#tuki2018 #stöd2018

Tietojen minimointi

- Henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään
- → Tarpeellisuusvaatimus

Täsmällisyys

- Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä
- → Rekisteröidyn pyynnöstä tapahtuva korjaaminen
- → Muutoksenhaun yhteydessä tapahtuva korjaaminen
- → Viranomaisaloitteinen oikaisu
- → Omalähtöiset päivitykset, esim. yhteystiedot

5. Sisäänrakennettu tietosuoja – henkilötietojen käsittelyn periaatteet (5 art.)

#tuki2018 #stöd2018

Säilytyksen rajoittaminen

- Henkilötietoja on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten

→ Säilytysaikojen määrittely

→ Tiedon hävittäminen / anonymisointi

Eheys ja luottamuksellisuus

- Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia.

→ Tietoturva

→ Salakirjoitus / pseudonymisointi

5. Sisäänrakennettu tietosuoja – tietojen luokittelu

#tuki2018 #stöd2018

- Tietoturva-asetuksen (681/2010) mukaan salassa pidettävien asiakirjojen luokittelussa käytetään seuraavia luokkia (asetus koskee valtionhallinnon organisaatioita):

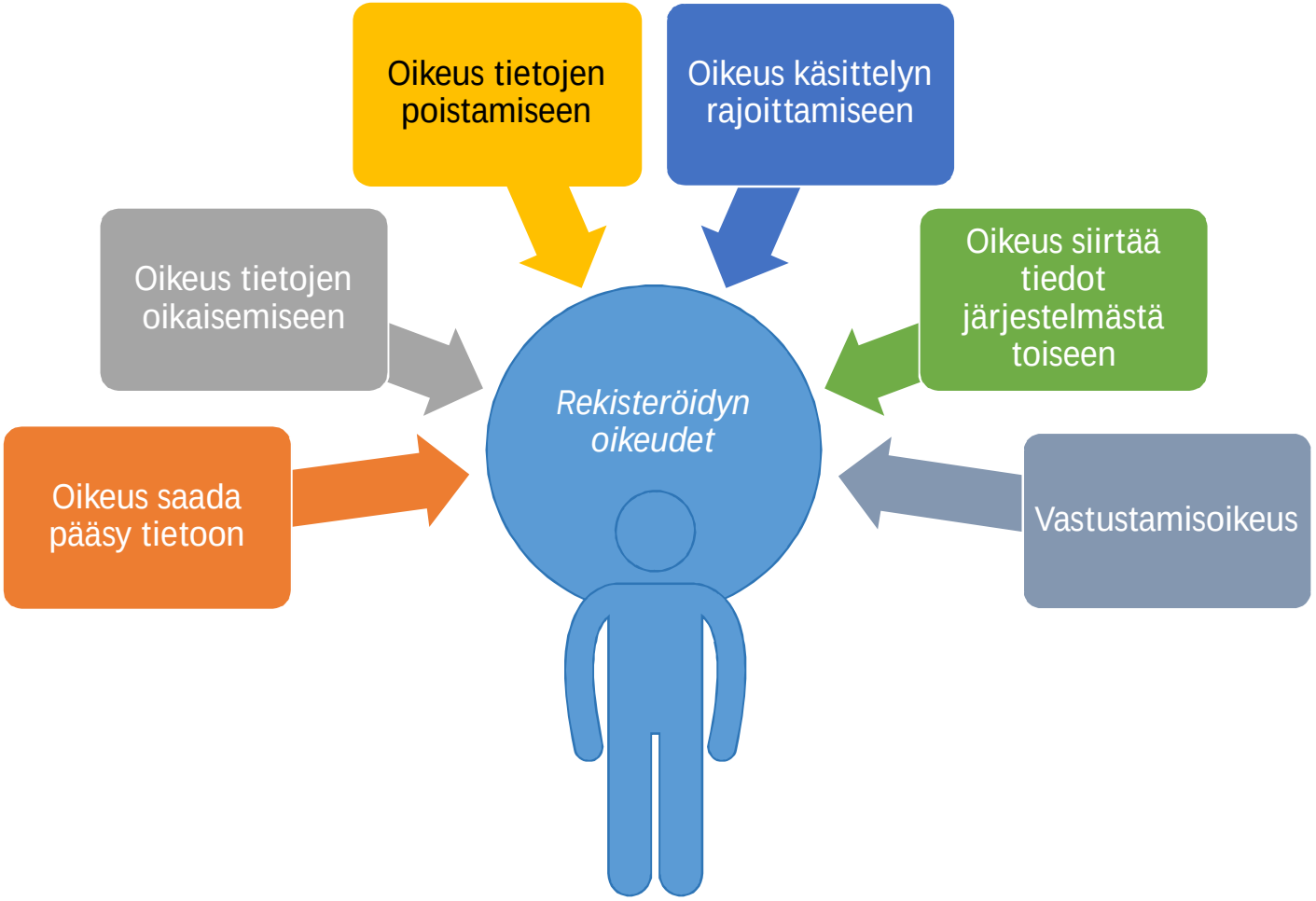
1. Suojaustaso I, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;
2. Suojaustaso II, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle;
3. Suojaustaso III, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle; (mm. potilastiedot, mahdollisesti arkaluonteiset henkilötiedot)
4. Suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle (mm. henkilötiedot, mahdollisesti arkaluonteiset henkilötiedot)

Kunnissa tiedot luokitellaan usein Julkisuuslain perusteella: Salassapidettävä – julkinen

Huom! Jatkossa: Tiedonhallintalaki

6. Rekisteröidyn oikeudet (15-21 artiklat)

#tuki2018 #stöd2018



6. Rekisteröidyn oikeudet – tiedonantovelvoite (13-14 art.)

- Rekisterinpitäjän tulee ilmoittaa rekisteröidyille helposti ymmärrettävässä muodossa, esim. tietosuojaselosteessa, seuraavat kohdat ennen kuin henkilötietoja kerätään:
  - Rekisterinpitäjän ja tietosuojavastaavan yhteystiedot (mikäli tietosuojavastaava on nimitetty);
  - Mihin tarkoituksiin henkilötietoja käsitellään ja mikä on käsittelyn oikeusperusta (esim. palvelun tarjoamiseksi rekisteröidyn suostumuksella);
  - Jos henkilötietoja luovutetaan kolmansille osapuolille, henkilötietojen vastaanottajat tai vastaanottajaryhmät;
  - Jos henkilötietoja siirretään kolmanteen maahan, miten tietosuojan riittävyydestä on huolehdittu ja mistä rekisteröity voi saada siitä lisätietoja;
  - Henkilötietojen säilytysaika tai kriteerit sille, miten säilytysaika määräytyy;

6. Rekisteröidyn oikeudet – tiedonantovelvoite (13-14 art.) (jatkuu)

#tuki2018 #stöd2018

- Rekisteröidyn oikeudet ja miten rekisteröidyt voivat niitä käyttää;
- Oikeus peruuttaa suostumus milloin tahansa;
- Oikeus tehdä valitus valvontaviranomaiselle;
- 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; sekä
- Liittyykö käsittelyyn automaattista päätöksentekoa tai profilointia, millainen käsittelylogiikka niihin liittyy, sekä niiden merkitys ja seuraukset rekisteröidyille.

- Mikäli rekisterinpitäjä ei kerää henkilötietoja rekisteröidyiltä suoraan vaan muista lähteistä, yllä mainittujen kohtien lisäksi on ilmoitettava:
  - Kerättävät tiedot; sekä
  - Mistä henkilötiedot on saatu ja onko tiedot saatu yleisesti saatavilla olevista lähteistä.

10. Mittaaminen ja seuranta

#tuki2018 #stöd2018

- Johdon tietoisuus organisaation tietosuojan nykytilasta on tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.
- Säännöllisen raportoinnin tulee sisältää tärkeimmät tietosuojaan ja henkilötietojen käsittelyyn liittyvät asiat.
- Niitä voivat olla esimerkiksi
  - tietosuojamittarit sisältäen niiden käytön raportointikauden aikana,
  - tietosuojan kehityshankkeet ja niiden tilanne,
  - havaitut puutteet ja tarpeet,
  - merkittävimmät tietoturvaloukkaukset, joilla on ollut tietosuojavaikutuksia, tehdyt riski- ja vaikutustenarvioinnit sekä niiden merkittävimmät löydökset hallintakeinoineen sekä
  - rekisteröityjen oikeuksiin ja yhteistyöhön valvontaviranomaisen kanssa liittyvät tarpeelliset tiedot.

12. Arviointi ja kehittäminen

- Teknisten ja organisatoristen toimenpiteiden tehokkuuden testaus ja arviointi
- Riskienhallinta
- Projektimalli & vaikutustenarvioinnit
- Käytännesäännöt ja standardit
- Automaatio
- Sovelluskehitys

Rekisterinpitäjän velvollisuuksien muut osa-alueet

- Seuraavista osa-alueista järjestetään JUHTA-hankkeen yhteydessä omat työpajat:
  - 4. Riskienhallinta (työpajat 12.6. – 29.9.2017)
  - 6. Rekisteröidyn oikeuksien toteuttaminen (8.12.2017)
  - 6. Tiedonantovelvoitteet (tammikuu 2018)
  - 7. Tietosuojavastaava (17.11.2017)
  - 8. Sopimukset ja alihankkijoiden hallinta (helmikuu 2018)
  - 9. Tietoturva (4.9.2018)
  - 9. Valvonta (17.11., 8.12., tammi-helmikuun työpajat 2018)
  - 11. Koulutus ja tietoisuus (8.12.2017)

Ryhmätehtävä 29.9.2017

Ryhmätehtävä – työpaja #4

#tuki2018 #stöd2018

1. Miten käytännössä rekisterinpitäjän velvollisuudet (rekisteröityjä kohtaan/muut velvoitteet) toteutetaan omassa organisaatiossa?
2. Mitkä velvollisuudet ovat vaikeimpia/hankalimpia toteuttaa?

Kotitehtävä 29.9.2017

Kotitehtävä – työpaja #4

#tuki2018 #stöd2018

1. Kartoita oman organisaatiosi tietosuojaan liittyvät politiikat ja muu olemassa oleva dokumentaatio – milloin viimeksi päivitetty ja mitä tulee päivittää seuraavaksi?
2. Selvitä kuinka rekisterinpitäjän vastuut ja raportointi on määritetty organisaatiossasi.
3. Onko käsittelyn oikeusperusteet määritetty?

Tietosuojan itsearviointityökalu

Tietosuojan arviointityökalu – tarvittavat tiedot

Osa-alue	Tietosuojan osa-alue	Aihe-alue	Keneen vaatimus kohdistuu?	Ylemmän tason vaatimus	Tarkemmat vaatimukset	Dokumentaatio / vaadittu näyttö	Havainnot	Katselmoidut dokumentit	Riskit	Kypsyystaso	Viittaus GDPR
1	**Tietosuojan hallinnointi**										
	Organisaation hallinnolliset rakenteet, roolit ja vastuut henkilötietojen keräämisen, käytön, luovuttamisen, poistamisen sekä suojaamisen, käsittelytoimien suunnittelun, valvonnan ja rekisteröityjen oikeuksien toteuttamisen osalta.	Tietosuojan hallintamalli		Organisaation hallinnolliset rakenteet, roolit ja vastuut henkilötietojen keräämisen, käytön, luovuttamisen, poistamisen sekä suojaamisen, käsittelytoimien suunnittelun, valvonnan ja rekisteröityjen oikeuksien toteuttamisen osalta.	Kattava tietosuojan hallintamalli on muodostettu (dokumentoitu, kommunikoitu ja implementoitu). Tietosuojaan liittyvät roolit ja vastuut ovat selvästi määritelty koko 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 raportoimista ylimmälle johdolle. Tietosuojavastaavaan liittyvä ilmoitus on tehty valvontaviranomaiselle.	Kuvaukset hallintarakenteista, raportointiketjuista ja määritetyistä vastuista Kuvaukset vastuista työnkuvauksissa Evidenssi tietosuojavastaavan nimittämisestä Tietosuojavastaavan työnkuvaus ja evidenssi riittävästä resursoinnista Osoitus valvontaviranomaiselle tehdystä tietosuojavastaavaa koskevasta ilmoituksesta (nimitys ja identiteetti)					Art 24, 27, 37, 38, 39
		Tietosuojaorganisaatio		Tehtävät liittyen tietosuojan jatkuvan kehittämisen ja ylläpidon ohjelman (Privacy Program) hallinnointiin, kuten tietosuojatyön budjetointi. resursointi (ml. tietosuojavastaava tai tietosuojan vastuuhenkilö), strateginen tavoiteasetanta sekä toiminnan jatkuva kehittäminen, arviointi ja mittaaminen.	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 suorituskykymittarien (KPI) asettaminen ja seuranta Tietosuojaorganisaation tehtävienjako on määritetty, dokumentoitu ja osoitettu tarkoituksenmukaisille henkilöille. On olemassa prosessi sen varmistamiseksi, että tietosuojaorganisaation resurssitarpeet tunnistetaan vähintään vuodeksi eteenpäin.	Dokumentoidut budjettiluvut Dokumentoidut suorituskykymittarit (KPI) Osoitus suorituskykymittarien (KPI) seurannasta Dokumentoidut tietosuojaorganisaation tehtävät					Art 24, 27, 37, 38, 39
2	**Henkilötieto-inventaario**										
	Organisaation kuvauskanta henkilötietojen käsittelytoimista, sisältäen kuvauksen mm. siitä mitä henkilötietoja organisaation eri prosesseissa käsitellään, mihin käyttötarkoituksiin, missä tietoa säilytetään ja	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.	On olemassa keskitetty, ajantasainen ja kattava 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 käsittelytoimiin liittyvien asioiden tunnistamisesta: - Henkilötietojen ja niiden luokituksen tunnistaminen - Henkilötietoja käsittelvien prosessien kartoitus - Henkilötietojen käsittelyyn liittyvien tietojärjestelmien kartoitus - Prosesseihin liittyvien henkilötietojen käsittelyperusteiden kartoitus					Art 30

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

#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 viestintätekniikkakeskus

OIKEUSMINISTERIÖ
JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto