Ajankohtaista tietosuojasta

5.4.2018

Maarit Päivike

SOSTE Suomen sosiaali ja terveys ry
SOSTE Finlands social och hälsa rf
SOSTE Finnish Federation for Social Affairs and Health

Yleinen tietosuoja-asetus (GDBR)

- Tullut voimaan 25.4.2016
- Soveltaminen alkaa 25.5.2018
- Nykyisen henkilötietolain pääpiirteet säilyvät
- Myös uusia velvoitteita rekisterinpitäjille ja oikeuksia rekisteröidylle

Muutoksia muuhun lainsäädäntöön

Esimerkiksi

- Laki yksityisyyden suojasta työelämässä, työterveyshuoltolaki, sairasvakuutuslaki, tietoyhteiskuntakaari, työehtosopimukset
- Laki potilaan asemasta ja oikeuksista, laki sosiaalihuollon asiakasasiakirjoista, laki sosiaalihuollon asiakkaan asemasta ja oikeuksista, sosiaalihuoltolaki, laki toimeentulosta, lastensuojelulaki, päihdehuoltolaki, laki sosiaali- ja terveydenhuollon asiakasmaksuista

Tietosuojalaki

- Tietosuojalaki, Hallituksen esitys HE 9/2018 vp (Täytäntöönpanotyöryhmän mietintö julkaistu 21.6.2017)
- Täydentää ja täsmentää tietosuoja-asetusta, yleislaki, ei itsenäinen ja kattava kokonaisuus
- Yhtenäinen kokonaisuus asetuksen kanssa
- Voimaan 25.5.2018
- Viranomaistehtävät tietosuojavaltuutetulle

Asetuksen tarkoitus ja soveltamisala

- Lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä
- Sovelletaan automaattiseen henkilötietojen käsittelyyn sekä henkilötietojen käsittelyyn, kun ne muodostavat rekisterin osan tai niiden on tarkoitus muodostaa rekisterin osa
- Aina, kun henkilötietoja käsitellään järjestön tai yrityksen tietojärjestelmissä

Soveltamisala

- Aina, kun henkilötietoja käsitellään järjestön tai yrityksen tietojärjestelmissä
- Manuaalinen käsittely: asiakaskortisto tai sen osa
- Koskee siten käytännössä kaikkia järjestöjä ja yrityksiä; esim. yksikin asiakas tai työntekijä
- Ulkopuolella henkilötietojen käsittely, jota henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa

Henkilötieto

- Käsite henkilötietolakia vastaava mutta asetuksen määritelmä yksityiskohtaisempi
- **Henkilötieto:** Kaikenlaiset tunnistettua tai tunnistettavissa olevaa henkilöä koskevat tiedot, jotka voidaan liittää häneen. Tiedot, joita käytetään tai todennäköisesti käytetään tarkoituksena arvioida tai kohdella tietyllä tavalla kyseistä henkilöä tai vaikuttaa hänen asemaansa tai käyttäytymiseensä. Tiedot, joiden käyttö todennäköisesti vaikuttaa henkilön oikeuksiin tai etuihin, kun otetaan huomioon kaikki kyseiseen asiaan liittyvät seikat. Riittää, että kyseistä henkilöä saatetaan kohdella eri tavoin kuin muita siksi, että näitä tietoja on käsitelty.

Henkilötieto

- **Henkilötieto: k**aikenlaiset tunnistettua tai tunnistettavissa olevaa henkilöä koskevat tiedot, jotka voidaan liittää häneen
  - Esim. henkilön nimi, postiosoite, sähköpostiosoite, henkilötunnus, syntymäaika, henkilönumero, sukupuoli, ammatti, kuva videohaastattelusta, puhelutallenteet, valvontakameratallenteet, tietokoneen IP-osoite, laite ID, sormenjälki, auton rekisteritunnus ovat henkilötietoja, jos tieto voidaan tunnistaa tiettyä henkilöä koskevaksi
  - Määritelmä on laaja. Lyhyesti: jos tiedon perusteellavoidaan tietää tai saada selville, kenestä on kyse, tieto on henkilötieto.

Rekisterinpitäjä ja käsittelijä

- **Rekisterinpitäjä** määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot
  - Ensisijaisessa vastuussa
  - Esim. työnantaja – työntekijöiden tiedot, yhdistys – yhdistyksen jäsenten tiedot
- **Käsittelijä** Rekisterinpitäjän lukuun työskentelevä taho, jonka tehtäviin henkilötietojen käsittely kuuluu
  - Toimeksianto-, alihankinta- tai yhteistyösuhteessa henkilötietojen käsittelyyn osallistuva taho
  - Asetuksesta vastuun kasvu

Muita käsitteitä

- **Käsittely**: toimintoja, joita kohdistetaan henkilötietoihin. Esim. tietojen kerääminen, tallentaminen, säilyttäminen muokkaaminen, haku, kysely, luovuttaminen, yhdistäminen, poistaminen … aina kun henkilötietoja käytetään
- **Profilointi**: automaattinen käsittely, jolla henkilötietoja käyttämällä arvioidaan henkilön tiettyjä ominaisuuksia
- **Anonymisointi**: henkilötiedon tunnistettavuuden poistaminen

Käsitteet jatkuu

- **Pseudonymisoiminen:** Henkilötietojen käyttäminen käsittelemistä siten, että ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Lisätiedot säilytetään erillään
- **Suostumus**: Mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu henkilötietojen käsittelyyn
- **Tietoturvaloukkaus**: seurauksena käsiteltyjen henkilötietojen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy

Henkilötietojen käsittelyn arviointi

- Organisaation on hahmotettava kokonaiskuva henkilötietojen käsittelyn nykytilasta
- Kenen tietoja käsitellään, mihin tarkoituksiin ja millä perusteella, luovutetaanko tai siirretäänkö henkilötietoja organisaation ulkopuolelle ja kauanko niitä säilytetään.
- Miten ja missä yhteydessä henkilötietoja kerätään
- Tietoturva, Riskienhallinta
- Miten informaatiovelvollisuus täytetään (selosteet)
- Mitä toimenpiteitä tietosuoja-asetuksen sääntely edellyttää

Henkilötietojen käsittelyn arviointi

- Olennaista on tunnistaa hankitaanko tiedot rekisteröidyltä itseltään vai muualta
- Tietosuoja-asetuksen säännösten kannalta yhtä tärkeää kuin henkilötietojen käsittelyä koskevien tietojen toimittaminen rekisteröidylle on toimittamisen tapa sekä informoinnissa käytetty kieli.
- Tarkoituksen määrittämiseen tulee kiinnittää erityistä huomiota. Rekisteröidyllä tulee olla selkeä käsitys siitä, mihin kaikkiin tarkoituksiin hänen henkilötietojaan käsitellään. Huomaa, että organisaatio voi käsitellä henkilötietoja useissa eri tarkoituksissa.

Periaatteet

- Vastaavat monilta osin henkilötietolain periaatteita, täsmentyvät
- Tietosuojaperiaatteet:
  - Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys: Henkilötietojen käsittelyn laillinen peruste, esim. oikeutettu etu, sopimus, suostumus, lakiin perustuva
  - Käyttötarkoitussidonnaisuus: Kerättävä tiettyä laillista käyttötarkoitusta varten, ei saa käsitellä määriteltyjen tarkoitusten kanssa yhteensopimattomalla tavalla

Periaatteet

- Tietojen minimointi: Asianmukaisia ja olennaisia sekä rajoitettu siihen, mikä on tarpeen käyttötarkoituksen kannalta
- Tietojen täsmällisyys
- Tietojen säilytyksen rajoittaminen (elinkaari): henkilötietoja tulee säilyttää vain niin kauan kun on käyttötarkoitus edellyttää, mahd. lyhyt
- Tietojen eheys ja luottamuksellisuus
- Rekisterinpitäjän osoitusvelvollisuus (todistustaakka siirtyy selkeämmin rekisterinpitäjälle)

Periaatteet

Osoitusvelvollisuus

- Pystyttävä osoittamaan, että periaatteita on noudatettu

Sisäänrakennettu ja oletusarvoinen tietosuoja

- Tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain tarkoituksen kannalta tarpeellisia tietoja
- Tiedon määrä, käsittelyn laajuus, säilytysaika

Henkilötiedon elinkaari

Suunnittelu

- Peruste ja käyttötarkoitus, säilytysajat, hävittäminen, ohjeistus ja käytännöt

Ylläpito

- Virheettömyys, tietoturva, ohjeistuksen noudattaminen ja valvonta, rekisteröidyn oikeudet

Päättyminen

- Säilytysaikojen noudattaminen, velvollisuus tietojen säilyttämiseen, hävittäminen ja arkistointi

Riskienhallinta

- Riskiperusteinen lähestymistapa: asetuksen velvoitteet ja asianmukaiset suojatoimet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin
- Rekisterinpitäjän on tehtävä perusteellinen arvio henkilötietojen riskeistä
- Toimenpiteet riskin minimoimiseksi

Perusteet käsittelylle

- Oikeusperuste
- Rekisterinpitäjän on arvioitava vaikuttaako asetus sen käyttämiin käsittelyn oikeusperusteisiin
- Tunnistettava millä laissa säädetyllä perusteella henkilötietoja käsitellään

Käsittelyperusteet

- **Suostumus**
- **Sopimus**
- **Lakisääteiset velvoitteet**
- Elintärkeä etu
- Yleinen etu
- **Oikeutettu etu**

- Vähintään yksi tulee täyttyä

Suostumus

- Rekisteröity antanut suostumuksen henkilötietojen käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten
- Vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn
- Todennäköisesti ei tarvitse pyytää uudestaan, jos on annettu em. tavalla

Arkaluonteiset tiedot

- Rotu tai etninen alkuperä
- Poliittiset mielipiteet
- Uskonnollinen tai filosofinen vakaumus
- Ammattiliiton jäsenyys
- Geneettiset tai biometriset tiedot
- Terveyttä koskevat tiedot
- Seksuaalinen käyttäytyminen ja suuntautuminen

Suostumus arkaluonteisten tietojen käsittelyyn

- Nimenomainen suostumus ko. tietojen käsittelyyn yhtä tai useampaa käyttötarkoitusta varten
- Pysyvä asiakasrekisteri / itse antaa yksittäiseen tarkoitukseen
- Huom laki yksityisyyden suojasta työelämässä: tarpeellisuusvaatimuksesta ei voida poiketa edes työntekijän suostumuksella

Henkilötunnus

- Henkilötieto, jonka käsittelyllä on asetettu erityisiä edellytyksiä
- Tullaan säätämään tietosuojalaissa
- Rekisteröidyn yksiselitteinen suostumus tai jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää

Henkilötunnus

- Lisäksi:

Luotonannossa, saatavan perimisessä, vakuutustoiminnassa luottolaitostoiminnassa, maksupalvelutoiminnassa, vuokraus- ja lainaustoiminnassa, luottotietotoiminnassa, terveydenhuollossa, sosiaalihuollossa ja sosiaaliturvan toteuttamisessa, virka-, työ- ja muita palvelusuhteita koskevissa asioissa

- Tietosuojavaltuutettu: asiakasrekistereissä, joissa tuotteita laskutusta vastaan

Lapsen henkilötietojen käsittely

- Tietoyhteiskunnan palvelujen tarjoaminen lapselle, jos niihin liittyy henkilötietojen käsittelyä, on lainmukaista, jos lapsi on vähintään 13-vuotias
- Alle 13 v, vanhemman suostumuksella

Sopimus

- Rekisteröity osapuolena sopimuksessa, esim. verkkokauppa
- Työsopimus esim. palkkojen maksaminen

Lakisääteiset velvoitteet

- Käsittely lakisääteisen velvoitteen noudattamiseksi
- OYL – osakasluettelo
- YhdL – jäsenluettelo
- Työntekijän palkkatiedot verottajalle

Oikeutettu etu

- Rekisteröidyn ja rekisterinpitäjän välillä merkityksellinen ja asianmukainen suhde
- Ei ole sallittua, jos rekisteröidyn edut tai oikeudet syrjäyttävät oikeutetut edut, esim. alaikäinen tai käsittely laajempaa kuin käyttötarkoituksen perusteella voidaan katsoa tarpeelliseksi
- Vertailuvastuu rekisterinpitäjällä
- Voiko rekisteröity kohtuudella olettaa henkilötietojen keräämisen yhteydessä, että voidaan käsitellä ko. tarkoitukseen

Suoramarkkinointi

- Voidaan katsoa oikeutetun edun piiriin kuuluvaksi. Voidaan siten jatkossakin lähettää potentiaalisille asiakkaille sillä edellytyksellä, että vastaanottajille kerrotaan mahdollisuudesta kieltää suoramarkkinointi.
- Anna ihmisille oikeus kieltäytyä suoramarkkinoinnista, johon käytetään heidän antamiaan tietoja.
- Kielto-oikeudesta on ilmoitettava selkeästi ja erillään muusta tiedotuksesta
- Ei varsinaisia muutoksia aikaisempaan asetuksen myötä
- Sähköisen viestinnän tietosuoja-asetus valmisteilla

Huoneentaulu rekisteröidyn oikeuksista (tietosuojavaltuutettu)

- Oikeus saada läpinäkyvää informaatiota
- Oikeus saada pääsy tietoihin (tarkastusoikeus)
- Oikeus tietojen oikaisemiseen (virheen oikaisu)
- Oikeus tietojen poistamiseen (oikeus tulla unohdetuksi)
- Oikeus käsittelyn rajoittamiseen
- Oikeus siirtää tiedot järjestelmästä toiseen
- Vastustamisikeus
- Oikeus tulla informoiduksi tietoturvaloukkauksista
- Oikeus saada valvontaviranomaiselta apua
- Oikeus luottaa tietoturvaan

Rekisteröidyn oikeudet

- Rekisterinpitäjän velvollisuus toteuttaa rekisteröidyn oikeuksia
- Huomioitava prosessien ja tietojärjestelmien suunnittelussa
- Varmistettava, että nykyiset prosessit ja tietojärjestelmät taipuvat muutoksiin
- Jonkin verran uusia oikeuksia
- Informointivelvollisuus

Oikeus saada läpinäkyvää informaatiota

- Rekisterinpitäjän on toimitettava henkilötietojen käsittelyä koskevat tiedot rekisteröidylle tiiviisti, läpinäkyvästi, helposti ymmärrettävässä ja saatavassa muodossa
- Tieto ilman aiheetonta viivytystä tai viim. kk
- Informointihetki: tietojen keräämishetki, jos kerätään henkilöltä itseltään
- Muusta lähteestä: kohtuullinen aika
- Tietosuoja-/rekisteriseloste / seloste käsittelytoimista

Selosteet ja informointi

- Rekisteröityjen tulee saada tieto, miten henkilötietoja kerätään ja käytetään sekä missä määrin käsitellään
- Toimitettavat tiedot kun kerätään henkilöltä itseltään:
- Yritys, yhteyshenkilön/tietosuojavastaavan yhteystiedot
- Käsittelyn tarkoitukset
- Oikeusperuste
- Oikeutetut edut
- Vastaanottajat
- Siirrot

Selosteet ja informointi jatkuu

- Säilytysaika tai sen määrittämiskriteerit
- Rekisteröidyn oikeudet

Kun tiedot kerätään muualta:

- Käsiteltävät henkilötietoryhmät
- Mistä tiedot saatu

Rekisteröidyn oikeus saada pääsy tietoihin

- Oikeus saada jäljennös häntä koskevista henkilötiedoista
- Ei määrämuotoa pyynnölle
- Rekisterinpitäjä voi pyytää lisätietoja, jotka ovat tarpeen rekisteröidyn henkilöllisyyden vahvistamiseksi
- Lähtökohtana maksuttomuus
- Kuukauden määräaika, voidaan jatkaa

Yhdistyksen jäsentiedot

- Yhdistyksen jäsenillä on oikeus saada tieto jäsenluetteloon sisältyvistä nimi- ja kotipaikkatiedoista (YhdL 11 §). Muiden jäsentietojen keräämiseen, tallentamiseen, käyttöön ja luovuttamiseen sovelletaan yitosuoja-asetusta ja lainsäädäntöä (esim. jäsenten sähköpostiosoitteet).

Vaikutustenarviointi

- Tietosuojaa koskeva vaikutustenarviointi on menettely, jolla parannetaan vaatimusten noudattamista ja osoitetaan niiden noudattaminen.
- Tietosuojatyöryhmän Ohje: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/ibVehxmcp/Ohjeet_tietosuojaa_koskevasta_vaikutustenarvioinnista.pdf

Vaikutustenarviointi

- Tietosuojaa koskevan vaikutustenarvioinnin avulla on tarkoitus kuvata henkilötietojen käsittelyä, arvioida sen tarpeellisuutta ja oikeasuhteisuutta
- Tukea luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien henkilötietojen käsittelystä aiheutuvien riskien hallintaa arvioimalla riskit ja määrittelemällä toimenpiteet, joilla niihin puututaan.
- Pakollista, jos todennäköisesti aiheuttaa korkean riskin

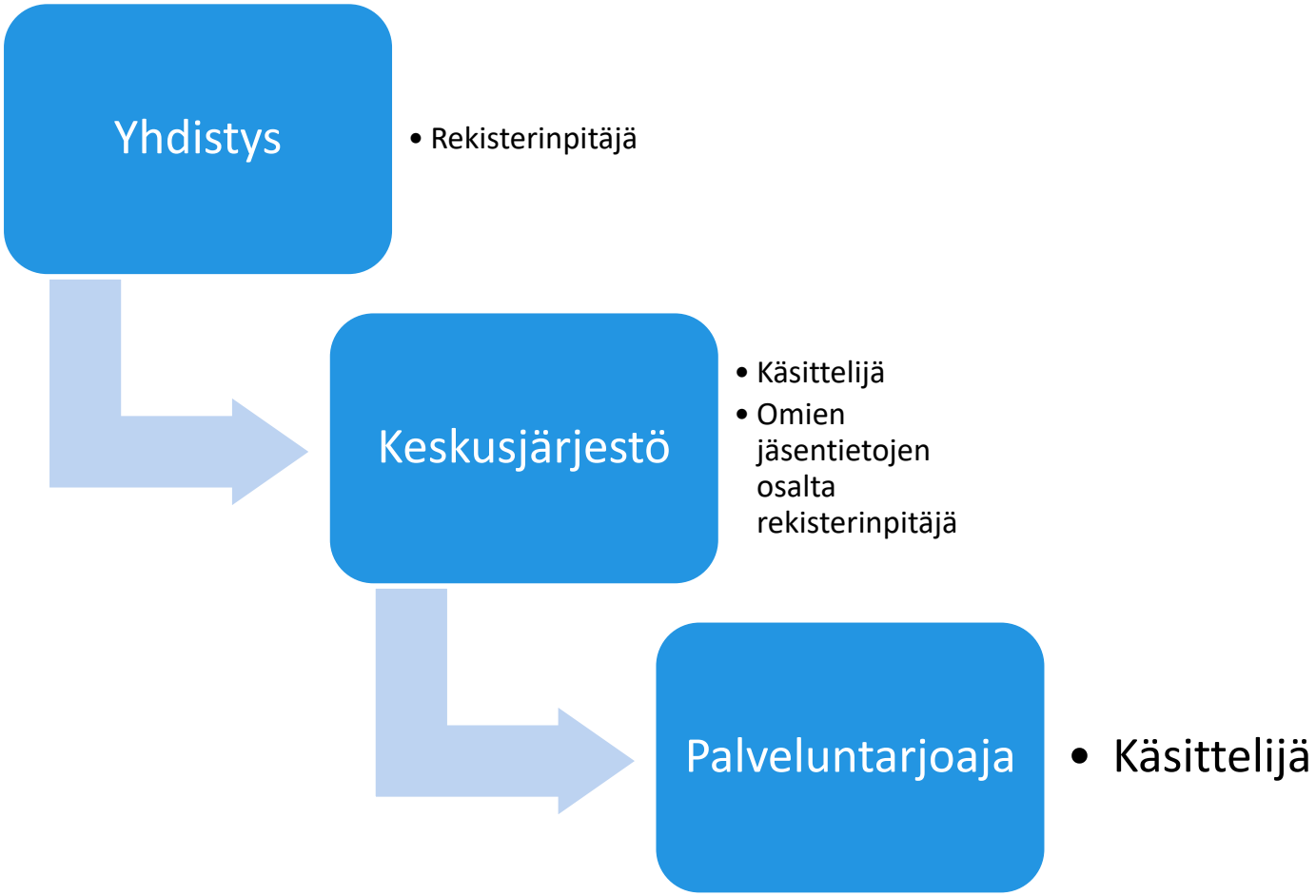
Vaikutustenarviointi

- Vaikka tietosuojaa koskevan vaikutustenarvioinnin tekemisen ehdot eivät täyttyisikään, rekisterinpitäjillä on edelleen yleinen velvollisuus toteuttaa toimenpiteitä, joilla hallitaan rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä. Käytännössä tämä tarkoittaa, että rekisterinpitäjien on jatkuvasti arvioitava riskejä, joita niiden käsittelytoimet aiheuttavat.

Riskinhallinta

- ”Riskillä” tarkoitetaan skenaariota, jolla kuvataan tapahtumaa ja sen seurauksia ja arvioidaan niiden vakavuutta ja todennäköisyyttä. ”Riskinhallinta” voidaan puolestaan määritellä koordinoiduksi toiminnaksi, jolla ohjataan ja valvotaan organisaatiota riskien osalta.

Keskitetty jäsenrekisteri



Keskitetty jäsenrekisteri

- Henkilötietojen luovuttaminen, mikäli keskusjärjestö päättää kerättävistä henkilötiedoista ja käsittelytoimista sekä käyttää tietoja myös omiin tarkoituksiinsa - rekisterinpitäjä
- Yhteisrekisteri
- Henkilötietoja voi luovuttaa vain, jos sekä luovuttajalla että saajalla on laillinen peruste henkilötietojen käsittelyyn

Sopimukset

- Henkilötietojen käsittely usein yhteistyötä
- Edellytyksenä kirjallinen sopimus mikäli käsittelee toisen lukuun
- Vähimmäissisältö:

- Henkilötietojen käsittelyn kohde ja kesto
- Käsittelyn luonne ja tarkoitus
- Mitä henkilötietoja käsitellään
- Rekisteröityjen ryhmät – esim. yhdistyksen jäsenet
- Rekisterinpitäjän oikeudet ja velvollisuudet
- Varautuminen muokkauksiin

Asetuksen edellyttämät sopimusehdot

1. Henkilötietojen käsittely rekisterinpitäjän ohjeiden mukaisesti

- Kirjalliset ohjeet

2. Salassapitovelvollisuudet

- Henkilötietojen käsittelijöiden työntekijöiden työsopimuksissa

3. Käsittelyn turvallisuudesta huolehtiminen

- Käsittelijän arvioitava riskit ja toteutettava niiden lieventämiseksi tarpeelliset toimenpiteet

Asetuksen edellyttämät sopimusehdot

- Turvallisuustaso voidaan varmistaa esim:
- Pseudonymisointi
- Kyky taata järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus
- Kyky palauttaa tietojen saatavuus nopeasti ja pääsy tietoihin vian sattuessa
- Menettely, jolla testataan, tutkitaan ja arvioidaan toimenpiteiden tehokkuutta turvallisuuden varmistamiseksi

Asetuksen edellyttämät sopimusehdot

4. Alihankkijat

- Käyttäminen edellyttää rekisterinpitäjän lupaa
- Sopimuksessa voi olla yleinen oikeus käyttää sopivia alihankkijoita tai hyväksymismenettely
- Käsittelijä vastuussa alihankkijan velvoitteiden suorittamisesta rekisterinpitäjälle
- Vastuut huomioitava käsittelijän ja alihankkijan sopimuksessa

Asetuksen edellyttämät sopimusehdot

5. Rekisteröityjen pyyntöihin vastaaminen
- Sovittava mikäli käsittelijä vastaa pyyntöihin , joita rekisteröidyt mahdollisesti esittävät tietosuoja-asetuksen johdosta
- Tekninen toteuttaminen tai varsinainen pyyntöihin vastaaminen

6. Käsittelijän avustusvelvollisuus
- Kuuluu: käsittelyn turvallisuus, tietoturvaloukkauksesta ilmoittaminen, vaikutustenarvioinnin teettäminen, ennakkokuuleminen

Asetuksen edellyttämät sopimusehdot

7. Tietojen poistaminen tao palauttaminen käsittelyn päättyessä

- Huom. Erityislainsäädäntö voi edellyttää tietojen säilyttämistä käsittelytoimien päättymisen jälkeen

8. Auditointioikeus ja tarkastukset

- Sallittava
- Käsittelijän on saatettava rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen asetuksen ja tietojenkäsittelysopimuksen mukaisten velvoitteiden noudattamisen osoittamista varten

Vastuut ja kustannukset

- Asetuksessa on vastuita, joita ei voi sopimuksella siirtää, esim. hallinnollisen sanktion tai vahingonkorvausvelvollisuuden kohdentamisesta
- Voidaan sopia em. Osapuolten välillä, mutta ei suhteessa kolmansiin eli rekisteröityihin tai viranomaisiin
- Välittömät ja välilliset vahingot
- Kustannustenjaosta kannattaa sopia

Sopimusehtoja (malleja)

- Käsittelijällä ei ole oikeutta käyttää Henkilötietoja muuhun kuin määritettyyn käyttötarkoitukseen
- Käsittelijän on ylläpidettävä selostetta vastuullaan olevista toimista asetuksen edellyttämien velvoitteidensa täyttämisen osoittamiseksi

Mallilauseita

- Käsittelijän on ilmoitettava tietoturvaloukkauksesta ilman aiheetonta viivytystä siitä, kun käsittelijä on tullut tietoiseksi siitä tietoiseksi
- Käsittelijän on tehtävä ilmoitus riittävässä ajassa rekisterinpitäjän ilmoitusvelvollisuuksien täyttämiseksi,
- Käsittelijän on dokumentoitava tietoturvaloukkaukset ja ryhdyttävä kaikkiin tarpeellisiin toimenpiteisiin henkilötietojen suojaamiseksi

Luovutussopimukset

- Hyvä kirjata, että kyseessä nimenomaan henkilötietojen luovuttaminen
- Millä perusteella luovutetaan
- Osapuolet päivittävät tietosuojaselosteet tai muuten informoivat rekisteröityjä
- Luovutukset tulee käydä ilmi tietosuojaselosteesta
- Mitä tietoja luovutetaan, milloin, tietoturva, voimassaolo

Tietoturva

- Rekisterinpitäjän ja henkilötietojen käsittelijän on siirtymäaikana selvitettävä, vastaavatko tietojen suojaamista kokevat käytännöt ja toimenpiteet asetuksen sääntelyä
- Rekisterinpitäjän on arvioitava riskit ja toimittava näiden riskien lieventämiseksi
- Rekisterinpitäjän tulee suojata koko henkilötiedon elinkaari

Velvollisuus ilmoittaa tietoturvaloukkauksista

- Ilmoitus mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta
- Ilmoituksen voi jättää tekemättä ainoastaan mikäli loukkauksesta ei todennäköisesti aiheudu henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä
- Henkilötietojen käsittelijän velvollisuus ilmoittaa rekisterinpitäjälle
- Ilmoitusvelvollisuus rekisteröidylle mikäli aiheuttaa korkean riskin henkilöiden oikeuksille ja vapauksille

Velvollisuus ilmoittaa tietoturvaloukkauksista

- Dokumentointi
- Valmistella prosessi mahdollisten tietoturvaloukkasten varalle
- Miten loukkaus tunnistetaan, ilmoitetaan, selvitetään, dokumentoidaan
- Toimintaohjelmat
- Henkilöstön osaaminen

Tietosuojavastaava

- Velvollisuus:
- julkisen sektorin toimija
- rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa, tai
- Ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomioita tai rikkomuksia koskeviin tietoihin9

Tietosuojavastaava

- Järjestön on varmistuttava tuleeko nimittää tietosuojavastaava
- Myös silloin, kun yleisessä tietosuoja-asetuksessa ei nimenomaisesti vaadita tietosuojavastaavan nimittämistä, organisaatioiden voi olla hyödyllistä nimittää tietosuojavastaava vapaaehtoisesti.
- Tietosuojatyöryhmä kannustaa tällaista vapaaehtoista nimittämistä.
- Järjestöissä kannattaa ainakin nimetä henkilö, jonka tehtävään kuuluu tietosuojaan liittyvät asiat

Tietosuojavastaava

- Jos organisaatio nimittää tietosuojavastaavan vapaaehtoisesti, tietosuojavastaavan nimittämiseen, asemaan ja tehtäviin sovelletaan 37–39 artiklan vaatimuksia samalla tavoin kuin tilanteessa, jossa nimittäminen on pakollista.
- Tietosuojavastaavan toimialaan kuuluvat kaikki rekisterinpitäjän tai henkilötietojen käsittelijän suorittamat käsittelytoimet riippumatta siitä, onko nimitys ollut pakollinen vai vapaaehtoinen.

Valmistaudu

1. Kartoita ja dokumentoi nykytilanne; sitouta henkilöstö
   - Minkälaisia henkilötietoja käsitellään? Mistä tiedot on kerätty ja mihin niitä luovutetaan? Käyttötarkoitus/käsittelyn peruste→ dokumentoi!
   - Selosteet, informointi ja rekisteröidyn oikeuksien toteutuminen
   - Henkilötietojen käsittelyn ulkoistussopimukset

Valmistaudu

2. Varmista organisaatiosi osaaminen ja resurssit
    - Vastuu tietosuojasta, tiedon omistajuus, (tietosuojavastaava)
    - Raportointi johdolle/hallitukselle, henkilötietojen käsittelyn suunnittelu
    - Ohjeistukset, perehdytys ja koulutus, valvonta
    - Valvonta ja prosessi tietoturvaloukkausten ilmoittamiseen
3. Varmista järjestelmähankintojen osalta, että henkilötietojen käsitte otetaan huomioon jo suunnitteluvaiheessa
4. Seuraa viranomaisten ohjeistusta ja kansallisia muutoksia

Mitä pitää dokumentoida?

- Nykytilan arviointi
- Riski- ja vaikutustenarviointi (sis. Tietosuojavastaavan nimeäminen)
- Ohjeistus käsittelystä, Millä perusteella käsitellään, kuvaus teknisistä ja organisatorisista turvatoimista, miten periaatteet huomioitu
- Tietosuojaselosteet: rekistereissä saa olla vain tietoa, joka on etukäteen laaditun suunnitelman mukaista
- Sopimukset päivitettävä vastaamaan asetuksen vaatimuksia

Dokumentoi (osoitusvelv)

- Organisaatioiden tulee laatia kirjallinen kuvaus niiden toteuttamasta henkilötietojen käsittelystä (seloste käsittelytoimista)
- Seloste on organisaation sisäinen asiakirja. Se toimii apuvälineenä henkilötietojen käsittelyn hahmottamisessa, ja sen tarkoituksena on osaltaan osoittaa, että henkilötietoja käsitellään tietosuojalainsäädännön mukaisesti.

Dokumentoi (selosteet)

- Käsittelytoimet:
- Rekisterinpitäjän, tämän edustajan sekä tietosuojavastaavan nimi ja yhteystiedot
- Hlötietojen käsittelyn tarkoitukset ja oikeusperuste
- Kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
- Vastaanottajat ja luovutukset
- Siirtäminen
- Poistamisen suunnitellut määräajat
- Yleinen kuvaus teknisistä ja organisatorisista toimista
- Rekisteröidyn oikeudet

Dokumentoi

- Käsittelijän pidettävä kirjallista selostetta kaikista rekisterinpitäjän lukuun
- Kirjallinen ja sähköinen muoto
- Vapautus selosteen laatimisesta

Linkkejä

- WP 29 laatii ohjeistusta
- https://www.finlex.fi/fi/esitykset/he/2018/20180009
- Ohje Miten valmistautua EU:n tietosuoja-asetukseen?

http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Tietosuoja-asetus: http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL

Linkkejä

- Työryhmämietintö:

http://julkaisut.valtioneuvosto.fi/handle/10024/80098

http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/on/03/nainlaadittietosuoja-asetuksenedellyttamanselosteenkasittelytoimista.html

www.tietosuoja.fi

http://www.it-ehdot.fi/tutustu-ehtoihin

Lähteet

- Tietosuoja-asetus
- HE 9/2018
- Tietosuojavaltuutetun www-sivut
- Selvityksiä ja ohjeita 4/2017 OM: Miten valmistautua EU: tietosuoja-asetukseen?
- Hanninen, Minna – Laine, Elli – Rantala, Kati – Rusi, Mari – Varhela, Markku: Henkilötietojen Käsittely. 2017.
- Koskela, Sari: Luento 3.11.2017 (SOSTE)

Kiitos!

maarit.paivike@soste.fi, p.040 571 1314

www.soste.fi

SOSTE

SOSTE Suomen sosiaali ja terveys ry
SOSTE Finlands social och hälsa rf
SOSTE Finnish Federation for Social Affairs and Health

RAY TUKEE
ray
HYVIÄ TEKOJA