Asiaa tietosuojasta

Maarit Päivike

Lahti 20.9.2018

Yleinen tietosuoja-asetus (GDBR)

- Soveltaminen alkanut 25.5.2018
- Tietosuoja-asetuksen tehtävänä on suojata luonnollisten henkilöiden oikeutta henkilötietojen suojaan ja taata henkilötietojen vapaa liikkuvuus EU-alueella.

- Asetus sisältää sääntelyn mm. siitä milloin saa kerätä ja käsitellä henkilötietoja ja mitä velvollisuuksia henkilötietojen käsittelyyn liittyy.

SOSTE

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

SOSTE

Tietosuojalaki

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

SOSTE

Tietosuojalaki

Esityksen mukaan tietosuojalaissa on tarkoitus säätää mm. :

- henkilötietojen käsittelyn oikeusperusteesta ja erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelystä eräissä tilanteissa,
- tietoyhteiskunnan palvelujen tarjoamiseen lapselle sovellettavasta ikärajasta,
- valvontaviranomaisesta sekä muutoksenhausta valvontaviranomaisen päätöksiin.
- henkilötunnuksen käsittelystä
- tietyistä rajoituksista rekisteröidyn oikeuteen tutustua itseään koskeviin henkilötietoihin ja rekisterinpitäjän velvollisuuteen antaa henkilötietojen käsittelystä tietoja rekisteröidylle.
- henkilötietojen käsittelystä journalistisia tarkoituksia, tieteellisiä tutkimustarkoituksia ja tilastollisia tarkoituksia varten.

SOSTE

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 yhdistyksen tietojärjestelmissä
- Myös paperisessa muodossa olevat henkilötiedot

SOSTE

Soveltamisala

- Manuaalinen käsittely: asiakaskortisto tai sen osa
- Koskee siten käytännössä kaikkia organisaatioita, myös yhdistyksiä; esim. yksikin asiakas tai työntekijä tai muutamia jäseniä
- Ulkopuolella henkilötietojen käsittely, jota henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa

Henkilötieto

- Käsite henkilötietolakia vastaava mutta asetuksen määritelmä yksityiskohtaisempi
- Henkilötieto: Henkilötietoja ovat kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, kuten esimerkiksi työntekijään, jäseneen tai asiakkaaseen, liittyvät tiedot. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa esimerkiksi nimen, henkilötunnuksen, puhelinnumeron, sijaintitiedon tai hänelle tunnusomaisen esimerkiksi fyysisen, geneettisen tai taloudellisen tekijän perusteella.

SOSTE

Henkilötieto

- Henkilötieto: kaikenlaiset 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 perusteella voidaan tietää tai saada selville, kenestä on kyse, tieto on henkilötieto.
- Tunnistettu tai tunnistettavissa oleva luonnollinen henkilö, johon tiedot liittyvät, on rekisteröity.

SOSTE

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 kuulu, esim toimeksianto-, alihankinta- tai yhteistyösuhteessa henkilötietojen käsittelyyn osallistuva taho. Henkilötietojen käsittelijöitä ovat esimerkiksi yritykset, jotka tarjoavat palkkahallinnon palveluja tai IT-järjestelmää koskevia palveluja, joissa käsitellään henkilötietoja

SOSTE

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

SOSTE

Käsitteitä

- 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.
- Sen pohjalta voi tarkistaa, onko henkilötietojen käsittelyssä huomioitu asetuksen vaatimukset ja Mitä toimenpiteitä tietosuoja-asetuksen sääntely edellyttää

SOSTE

Kokonaiskuva sisältää vähintään:

- mitä henkilötietoja yrityksessä käsitellään esimerkiksi it-järjestelmissä ja eri rekistereissä ja kenen tietoja käsitellään
- mitä tarkoituksia varten eli miksi henkilötietoja käsitellään, mistä tiedot on saatu
- luovutetaanko tai siirretäänkö henkilötietoja organisaation ulkopuolelle
- mikä laillinen käsittelyperuste oikeuttaa henkilötietojen käsittelyn (millä perusteella käsitellään)
- miten henkilötietoja käsitellään, millainen sisäinen dokumentointi ja ohjeistus henkilötietojen käsittelystä on
- miten ja missä vaiheessa rekisteröityjä informoidaan henkilötietojen käsittelystä
- onko henkilötietojen käsittelyä ulkoistettu ja jos on, mitä henkilötietoja ja käsittelytoimia ulkoistus koskee ja millaiset sopimukset ulkoistuksista on laadittu
- siirretäänkö henkilötietoja käsiteltäväksi EU:n ulkopuolelle
- kuinka henkilötietojen käsittelyn turvallisuudesta huolehditaan (tietoturva ja riskienhallinta)
- Kuinka kauan henkilötietoja säilytetään

SOSTE

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.
- Huom samaan rekisteriin kuuluvia tietoja voi olla useassa paikassa-olisiko mahdollisuus keskittää

SOSTE

Tietosuojaperiaatteet

- Vastaavat monilta osin henkilötietolain periaatteita, täsmentyvät
- Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys: Henkilötietojen käsittelyn laillinen peruste, esim. oikeutettu etu, sopimus, suostumus, lakiin perustuva
- Läpinäkyvyys: rekisteröidylle, miten ja missä määrin heitä koskevia tietoja kerätään ja käsitellään. Nämä tiedot helposti saatavilla. Rekisterinpitäjä ja käsittelyn tarkoitus -)tietosuojakäytännöt saataville

Tietosuojaperiaatteet

- Käyttötarkoitussidonnaisuus: Kerättävä tiettyä laillista käyttötarkoitusta varten
- Yhdistyksen on henkilötietojen käsittelyn osalta siten aina määritettävä, mitä tarkoitusta tai tarkoituksia varten niitä kerätään ja käsitellään. Määrittäminen kuvaa sen, minkä tehtävien hoitamiseksi rekisterinpitäjä kerää ja käsittelee henkilötietoja. Esimerkiksi asiakastietoja on mahdollista käsitellä useita hyväksyttäviä tarkoituksia varten, kuten esimerkiksi asiakassuhteen hoitamiseksi ja kehittämiseksi, rekisterinpitäjän tuotteiden markkinoimiseksi. Yhdistyksen jäsentietoja on mahdollista käsitellä esim. jäsenviestintään

SOSTE

Tietosuojaperiaatteet

- Tietojen minimointi: Asianmukaisia ja olennaisia sekä rajoitettu siihen, mikä on tarpeen käyttötarkoituksen kannalta
- Tietojen täsmällisyys: päivitys, virheelliset tiedot oikaistaan tai poistetaan
- Tietojen säilytyksen rajoittaminen (elinkaari): henkilötietoja tulee säilyttää vain niin kauan kun on käyttötarkoitus edellyttää, mahd. lyhyt

Tietosuojaperiaatteet

- Tietojen eheys ja luottamuksellisuus: henkilötietojen asianmukainen turvallisuus, suojattava luvattomalta käytöltä ja vahingossa tapahtuvalta häviämiseltä
- Rekisterinpitäjän osoitusvelvollisuus (todistustaakka siirtyy selkeämmin rekisterinpitäjälle) Rekisterinpitäjän on pystyttävä osoittamaan, että periaatteita on noudatettu - Dokumentointi
- Mitä periaatteet tarkoittavat käytännössä
- Miten ne toteutuvat toiminnassa

Tietosuojaperiaatteet

- Sisäänrakennettu ja oletusarvoinen tietosuoja
- Tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain tarkoituksen kannalta tarpeellisia tietoja
- Esim. henkilöstön koulutus ja ohjeet, tilojen ja ohjelmistojen valvonta, tietoturva
- Suunnittelu: tiedon määrä, käsittelyn laajuus, säilytysaika

SOSTE

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
- Dokumentoi

SOSTE

Perusteet käsittelylle

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

Käsittelyperusteet yhdistyksessä

- **Suostumus (esim. suoramarkkinointi kuluttajalle, terveystietojen käsittely)**
- **Sopimus (työntekijöiden henkilötietojen käsittely, tilaus, palvelun toteuttaminen, yhdistyksen jäsenyys?)**
- **Lakisääteiset velvoitteet (jäsenluettelo, nimi ja kotipaikka)**
- Elintärkeä etu
- Yleinen etu
- **Oikeutettu etu (henkilötietojen käsittely yhdistyksen tiedottamista, viestintää ym yhdistystoimintaa varten)**

- Vähintään yksi tulee täyttyä

SOSTE

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

SOSTE

Suostumus

- Suostumusta osoittava toimi voi esimerkiksi olla se, että rekisteröity rastittaa ruudun vieraillessaan internetsivustolla, valitsee tietoyhteiskunnan palveluiden teknisiä asetuksia tai esittää muun lausuman tai toimii tavalla, jolla hän selkeästi osoittaa hyväksyvänsä henkilötietojensa käsittelyn esitettyihin käyttötarkoituksiin. Suostumusta ei sen sijaan voi antaa esimerkiksi valmiiksi rastitetuilla ruuduilla.
- Lapsille tietoyhteiskunnan palveluita tarjoavien rekisterinpitäjien on tärkeätä huomioida, että henkilötietolaista poiketen tietosuoja-asetus antaa ko. palveluita tarjottaessa erityistä suojaa lasten henkilötiedoille. Tietoyhteiskunnan palveluilla tarkoitetaan asetuksessa sähköisesti etäpalveluina palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettavia palveluita, joista tavallisesti maksetaan korvaus.

SOSTE

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

SOSTE

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
- Rekisteröidyn yksiselitteinen suostumus tai jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää

Sopimus

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

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, tietosuojavaltuutetun sivuilla vertailuohje
- Voiko rekisteröity kohtuudella olettaa henkilötietojen keräämisen yhteydessä, että voidaan käsitellä ko. tarkoitukseen

SOSTE

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

SOSTE

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
- Rekisteröityjen saatavilla tulee olla ohjeet miten oikeuksia voi käyttää

SOSTE

Rekisteröidyn oikeudet

- saada tietoa henkilötietojensa käsittelystä
- saada pääsy tietoihin
- oikaista tietoja
- poistaa tiedot ja tulla unohdetuksi
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- vastustaa tietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi.

SOSTE

Rekisteröidyn oikeus saada pääsy tietoihin

- Rekisteröidyillä oikeus saada vahvistus käsitteleekö häntä koskevia henkilötietoja
- Pääsy omiin tietoihin: Jäljennös tiedoista ja tietosuojaseloste tai muu dokumentaatio
- Selosteesta tms ilmenee asetuksessa määritellyt tiedot
- Yhdistyksellä pitää siten olla tieto mihin tietoja on tallennettu – prosessi dokumentoitava

SOSTE

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

Poisto-oikeus

- Henkilötietoja ei enää tarvita siihen tarkoitukseen joita varten ne kerättiin tai muutoin käsiteltiin
- Suostumuksen peruutus
- Lainvastainen käsittely
- Vastustamisoikeus
- Kerätty tarjottaessa tietoyhteiskunnan palveluja lapselle
- Huom: jos oikeutettu etu voimassa – ei oikeutta tulla unohdetuksi
- Ei määritellä miten tulee teknisesti poistaa

SOSTE

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

SOSTE

Rekisteröityjen informointi

- Rekisteröityjen tulee saada tieto, miten henkilötietoja kerätään ja käytetään sekä missä määrin käsitellään (tiiviisti, läpinäkyvästi, helposti ymmärrettävästi ja saatavasti ja selkeällä ja yksinkertaisella kielellä)
- Toimitettavat tiedot kun kerätään henkilöltä itseltään:
- Yritys, yhteyshenkilön/tietosuojavastaavan yhteystiedot
- Käsittelyn tarkoitukset
- Oikeusperuste

Rekisteröityjen informointi

- Oikeutetut edut
- Vastaanottajat
- Siirrot
- Säilytysaika tai sen määrittämiskriteerit
- Rekisteröidyn oikeudet

Kun tiedot kerätään muualta:

- Käsiteltävät henkilötietoryhmät
- Mistä tiedot saatu

Informointitavat

- Kirjallisesti tai muulla tapaa, tapauksen mukaan sähköisesti
- Asetus ei tarkemmin määrittele formaattia tai tapaa
- Tietosuojaseloste hyvä tapa

Yhdistyksen jäsentiedot

- Hallituksella on velvollisuus pitää yhdistyksen jäsenistä jäsenluotteloa
- Yhdistyksen jäsenillä on oikeus saada tieto jäsenluetteloon sisältyvistä nimi- ja kotipaikkatiedoista (YhdL 11 §). Muiden jäsentietojen keräämiseen,

tallentamiseen, käyttöön ja luovuttamiseen sovelletaan tietosuoja-asetusta ja lainsäädäntöä (esim. jäsenten

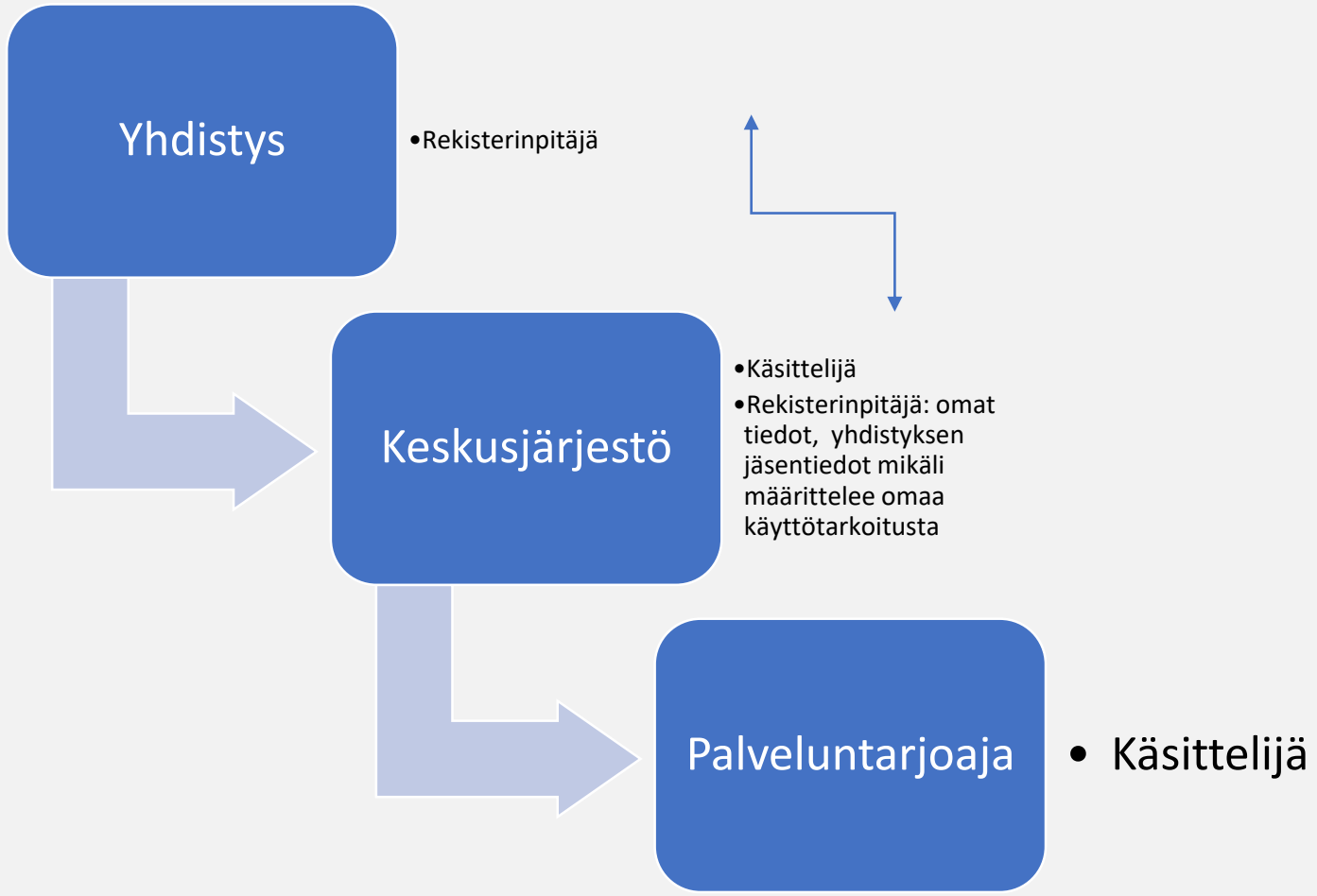
sähköpostiosoitteet).

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

SOSTE

Keskitetty jäsenrekisteri



SOSTE

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

SOSTE

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

SOSTE

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

SOSTE

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

SOSTE

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

SOSTE

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

SOSTE

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

Henkilötietojen luovuttaminen tai siirtäminen

- Sekä luovuttajalla ja luovutuksen saajalla tulee olla peruste henkilötietojen käsittelyyn
- Arvioitava ennen luovutusta
- Siirtäminen kun ei käsitellä siirron saajan omiin tarkoituksiin
- Siirto EU:n ulkopuolelle – asetuksessa erillistä sääntelyä, esim. asianmukaiset suojatoimet, vakiolausekkeita, vastaanottajan kyky huolehtia velvotteista

SOSTE

Luovutussopimukset

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

SOSTE

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, henkilötietojen laatu vaikuttaa
- Rekisterinpitäjän tulee suojata koko henkilötiedon elinkaari

Tietoturva

- Luottamuksellisuus: henkilötiedot oltava vain niihin oikeutettujen käytössä, esim. salasanat, turvallinen hävitys
- Eheys: Säilyttäminen muuttumattomana keräämisen, käsittelyn ja siirtämisen aikana
- Käytettävyys ja vikasietoisuus

Tietoturvaloukkaus

- Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

- Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen.

Tietoturvaloukkaus

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi:

- hävinnyt tiedonsiirtoväline, kuten USB-tikku
- varastettu tietokone
- hakkerointi
- haittaohjelmatartunta
- kyberhyökkäys
- tulipalo datakeskuksessa
- tiliotteen postitus väärälle henkilölle.

Tietoturvaloukkaus

- Tietoturvaloukkauksiin on pystyttävä reagoimaan mahdollisimman nopeasti.

- Rekisterinpitäjän täytyy arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu sen kohteena olleille henkilöille (ei aiheudu riskiä, riski, korkea riski)
- Riskin taso määrittää ne toimenpiteet, joihin rekisterinpitäjän on ryhdyttävä. Toimenpiteitä ovat esimerkiksi:
- tietoturvaloukkauksen dokumentointi
- ilmoitus valvontaviranomaiselle
- ilmoitus rekisteröidylle.

SOSTE

Velvollisuus ilmoittaa tietoturvaloukkauksista

- Ilmoitus valvontaviranomaiselle 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

SOSTE

Velvollisuus ilmoittaa tietoturvaloukkauksista

- Dokumentointi
- Valmistella prosessi mahdollisten tietoturvaloukkasten varalle
- Miten loukkaus tunnistetaan, ilmoitetaan, selvitetään, dokumentoidaan
- Toimintaohjelmat
- Henkilöstön osaaminen
- Ilmoituksen sisältö: Kuvaus tietoturvaloukkauksesta, kohde, arvio lukumääristä, yhteystiedot, josta lisätietoja, toimenpiteet

SOSTE

Tietoturvaloukkaus (tietosuojavaltuutettu)

- Huomioi arviossa seuraavat asiat:

1. Tietoturvarikkomuksen tyyppi
2. Henkilötietojen luonne, arkaluntoisuus ja määrä
3. Tunnistamisen helppous
4. Rekisteröityjen ominaisuudet
5. Rekisterinpitäjän ominaisuudet
6. Tietovuodon seurauksien vakavuus

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

SOSTE

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.

SOSTE

Valvonta ja sanktiot

- Tietosuojavaltuutettu valvontaviranomainen
- Jokaisella rekisteröidyllä oikeus tehdä valitus, jos katsoo että häntä koskevien henkilötietojen käsittelyssä rikotaan asetusta
- Sakot
- Vahingonkorvausvastuu

Valmistautuminen ja nykytila

- Rekisteröityjen informointi (tietosuojakäytännöt)
- Tekniset ja organisatoriset toimenpiteet esimerkiksi ohjeet henkilöstölle tietosuojan toteuttamiseksi, omavalvonnan kautta tapahtuva käytönvalvonta, tietojärjestelmien tietoturva, tietojen salaus ja muut suojatoimenpiteitä.
- Säilytysajat
- Kerättävät tiedot (tarpeellisuus, minimointi)
- Käsittelyperusteiden tarkistaminen ja määritys
- Mahdollinen tietosuojavastaavan nimeäminen

SOSTE

Toimenpiteet ja dokumentit osoitusvelvollisuuden toteuttamiseksi

- Toimenpiteet ja dokumentit osoitusvelvollisuuden toteuttamiseksi

- Jotkut tietosuoja-asetuksen velvoitteet kohdistuvat vain osaan organisaatioista tai henkilötietojen käsittelytoimista. Esimerkkejä tällaisista velvollisuuksista ovat tietosuojavastaavan nimittäminen, tietosuojaa koskevan vaikutustenarvioinnin laatiminen, ennakkokuuleminen ja velvollisuus laatia seloste käsittelytoimista.
- On suositeltavaa dokumentoida, millä tavalla on päädytty näiden velvoitteiden noudattamista tai noudattamatta jättämistä koskevaan ratkaisuun.

SOSTE

Toimenpiteet ja dokumentit osoitusvelvollisuuden toteuttamiseksi

- Seloste käsittelytoimista eli henkilötietojen käsittelyn yleinen kuvaus (tietosuoja-asetuksen artikla 30). Koskee myös henkilötietojen käsittelijää
- Tietosuojaperiaatteiden sisäänrakennettu toteutuminen omassa toiminnassa (5 art. + 25 art.)
- Mahdolliset tietosuojaa koskevat laajemmat toimintaperiaatteet (24.2 art.)
- Informointikäytännöt (12-14 art.)

SOSTE

Toimenpiteet ja dokumentit osoitusvelvollisuuden toteuttamiseksi

- Käsittelyn oikeusperustetta koskevat arviot (6–10 art.)
- Jos käsitellään suostumuksen perusteella, suostumukseen liittyvä dokumentaatio (7 art. + 8 art.)
- Jos käsitellään rekisterinpitäjän tai sivullisen oikeutetun edunperusteella, tätä koskeva tasapainotesti (6.1.f art.)
- Muut sisäiset ja ulkoiset ohjeistukset (12, 13, 14, 24, 25, 28, 29, 32 art.)
- Riskiarvioita koskeva dokumentaatio sekä toteutetut tekniset ja organisatoriset suojatoimenpiteet
- Sisäiset ja ulkoiset ohjeet rekisteröidyn oikeuksien toteuttamiseksi
- Ohjeet henkilötietoja käsitteleville työntekijöille ja henkilötietojen käsittelijöille
- Sisäiset tarkastukset ja auditoinnit

SOSTE

Toimenpiteet ja dokumentit osoitusvelvollisuuden toteuttamiseksi

- Vaikutustenarviointeja (35 art.)ja ennakkokuulemista (36 art.) koskeva dokumentaatio
- Henkilötietojen tietoturvaloukkausten dokumentointi (33 + 34 art.) ja tätä koskeva prosessi
- Tietosuojavastaavan asemaan ja tehtäviin liittyvä dokumentaatio (37-39 art.) •On suositeltavaa aina dokumentoida perusteet sille, jos organisaatio päätyy henkilötietojen käsittelyä koskevassa asiassa eri ratkaisuun, kuin tietosuojavastaava on suositellut
- Henkilötietojen käsittelyyn liittyvät sopimukset (28 artikla)
- Yhteisrekisterinpitäjien vastuualueet (29 art.)
- Mahdollinen johtavan valvontaviranomaisen määrittämistä koskeva dokumentaatio (56 art.)
- Henkilötietojen siirtoa kolmansiin maihin koskeva dokumentaatio (5 luku)

SOSTE

Osaksi toimintaa

- Dokumentaation ja toimenpiteiden riittävyyttä on arvioitava säännöllisesti – dynaamiset asiakirjat, päivitykset
- Dokumentaation hallinta
- Järjestelmähankinnat
- Henkilötietojen kerääminen uusiin käyttötarkoituksiin

Usein kysyttyä

- Säilytysajat (jotka eivät määräydy lakien perusteella)
- Pitääkö järjestön nimetä tietosuojavastaava
- Alaikäisen henkilötietojen käsittely
- Riittävä/paras tapa rekisteröityjen informoinnille
- Milloin tulee tehdä ilmoitus tietosuojaloukkauksesta
- Työsähköpostin käyttö ja henkilötietojen käsittely

SOSTE

Linkkejä

https://tietosuoja.fi/organisaatiot

https://tietosuoja.fi/lainsaadanto

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

SOSTE

Linkkejä

- WP 29 laatii ohjeistusta

- https://www.finlex.fi/fi/esitykset/he/2018/20180009
- PeVL 14/2018, 9.5.2018

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

SOSTE

Kiitos!

Maarit Päivike
lakimies
040 571 1314, maarit.paivike (a) soste.fi
Yliopistonkatu 5, 00100 Helsinki
SOSTE Suomen sosiaali ja terveys ry.