Tietoturva- ja tietosuojakäsikirja

Laatija: Tietosuojavastaavat
Hyväksyjä: Tietosuojatyöryhmä 5/2020

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

SISÄLTÖ

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

Päivitykset:

pvm	päivitetty tieto	päivittäjä

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

1. Johdanto

EU:n yleisen tietosuoja-asetuksen (GDPR) tarkoituksena on suojella luonnollisen henkilön oikeuksia ja vapauksia henkilötietojen käsittelyssä. Asetusta alettiin soveltaa 25.5.2018 kaikessa henkilötietojen käsittelyssä. Uutena yleislakina tuli voimaan 1.1.2019 kansallinen Tietosuojalaki, jossa on täydennetty ja täsmennetty EU:n tietosuoja-asetuksen määräyksiä. Näiden lisäksi henkilötietojen käsittelyä ohjaavat monet muut lait, kuten esim. Julkisuuslaki ja sosiaali- ja terveydenhuollon erityislainsäädäntö.

Organisaatio vastaa siitä, että sen työntekijöillä on käytössään riittävä ohjeistus lainsäädännön huomioimiseksi. Työntekijä puolestaan vastaa omalta osaltaan henkilötietojen käsittelystä ja tietoturvan ja tietosuojan huomioimisesta arjen työtehtävissä.

Tämä on Siun soten sisäinen ohje, joka on tarkoitettu kaikille Siun soten työntekijöille ja opiskelijoille. Ohjetta päivitetään tarpeen mukaan, viimeisin versio on intran tietosuojaohjeissa.

2. Keskeisiä käsitteitä

Tietosuoja
Tietosuoja tarkoittaa henkilön yksityisyyden suojaamista. Se on perusoikeus, jolla turvataan lainsäädännön vaatimusten mukainen ja turvallinen henkilötietojen käsittely siten, että henkilön yksiytyisyyden suoja tai oikeusturva ei vaarannu.

Tietoturva
Tietoturva on yksi tietosuojan toteuttamisen keino. Tietoturva tarkoittaa muun muassa teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan tiedon *luottamuksellisuus* ja *eheys*, *saatavuus* ja *käytettävyys* sekä *rekisteröidyn oikeuksien* toteutuminen.

Tietosuojavaltuutettu
Tietosuojavaltuutettu on koko Suomen kansallinen valvontaviranomainen tietosuoja-asioissa. Tietosuojavaltuutettu valvoo henkilötietojen käsittelyn lainmukaisuutta ja rekisteröidyn oikeuksien toteutumista. Tietosuojavaltuutetun toimiston sivut.

Tietosuojavastaava
Tietosuojavastaava on organisaation johdon nimittämä asiantuntija, jonka tehtävät ja asema on määritelty EU:n yleisessä tietosuoja-asetuksessa. Tietosuojavastaava neuvoo ja ohjeistaa tietosuojalainsäädännön mukaisista velvollisuuksista, valvoo henkilötietojen käsittelyä ja osallistuu henkilötietojen käsittelyn suunnitteluun eri toiminnoissa. Siun sotessa tietosuojavastaavan tehtäviin on nimetty kaksi tietosuoja-asiantuntijaa: Maarit Riikonen (sosiaalipalvelut) ja Mirja Vilpponen (terveyspalvelut) .

Henkilötieto
Henkilötietoa on kaikki sellainen tieto, josta luonnollinen henkilö voidaan suoraan tai epäsuorasti tunnistaa. Tunnistetietoja ovat esim. nimi, henkilötunnus, sijaintitieto, verkkotunnistetieto tai jokin fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä tai näiden yhdistelmä. Epäsuora tunnistaminen tarkoittaa sitä, että henkilö voidaan tunnistaa tietoja yhdistämällä.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

Henkilötietojen käsittely
Henkilötietojen käsittely tarkoittaa henkilötietoihin kohdistettua toimintaa. Käsittely voi olla joko automaattista tietojärjestelmällä tapahtuvaa tai manuaalista käsittelyä, esim. asiakirjojen mapittamista. Tiedon käsittelyä on tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen tai asettaminen saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poisto tai tuhoaminen. Myös tiedon katseleminen tai haku sähköisestä järjestelmästä on henkilötietojen käsittelyä.

Rekisteri
Rekisteri tarkoittaa henkilötiedoista koostuvaa tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein. Rekisterissä olevat tiedot on kerätty samaa käyttötarkoitusta varten. Rekisterin sisältämät tiedot voivat olla sähköisessä järjestelmässä tai/ja paperilla.

Rekisterinpitäjä
Rekisterinpitäjällä tarkoitetaan sitä tahoa, jonka käyttötarkoituksia varten henkilötietoja kerätään. Rekisterinpitäjällä on vastuu siitä, että EU-asetuksen periaatteita noudatetaan henkilötietojen käsittelyssä.

Rekisteröity
Rekisteröity tarkoittaa henkilöä, jonka tietoja käsitellään. EU-asetus takaa erilaisia oikeuksia rekisteröidylle suhteessa omiin tietoihinsa.

3. Tietosuojatyön vastuunjako

Siun sotessa noudatettavat tietosuojan ja tietoturvan tavoitteet, periaatteet sekä tietosuojan organisointi ja vastuut on koottu Siun soten yhtymähallituksen hyväksymään *Tietoturva- ja tietosuojapolitiikkaan*. Siihen pohjautuvat tietosuojaan liittyvät suunnitelmat sekä henkilötietojen käsittelyä koskevat ohjeet ja määräykset.

Siun soten johto vastaa tietoturva- ja tietosuojatyön organisoinnista, toteutuksesta hallinnollisella tasolla ja varmistaa tietosuojatyöhön tarvittavat resurssit. Palvelualueiden johtajat on nimetty tietojärjestelmien vastuuhenkilöiksi, ja he määrittelevät vastuualueellaan toiminnassa käytettävien tietojärjestelmien tietoturvatarpeet ja käyttöoikeuksien myöntämisperiaatteet.

Toimitusjohtajan nimittämä Tietosuojatyöryhmä kokoontuu 3-4 kertaa vuodessa. Työryhmään kuuluu rekisterinpitäjän edustajina toimialuejohtajat sekä digijohtaja, tiedonhallintapäällikkö, turvallisuuspäällikkö ja tietosuoja-asiantuntijat. Ryhmä voi kutsua tarvittaessa muita asiantuntijoita kokouksiin.

Vastuu tietosuojan toteuttamisesta kuuluu omalta osaltaan myös kaikille Siun soten työntekijöille ja viranhaltijoille. Jokainen Siun soten työntekijä on salassapito- ja vaitiolovelvollinen ja vastuussa henkilötietojen käsittelystä omassa tehtävässään. Salassapito- ja vaitiolovelvollisuus on voimassa myös palvelussuhteen päättymisen jälkeen.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

4. Henkilötietojen käsittelyä koskevat periaatteet

EU-asetuksessa säädetään henkilötietojen käsittelyä koskevista periaatteista, jotka ohjaavat rekisterinpitäjää toimimaan rekisteröidyn vapauksia ja oikeuksia kunnioittavalla tavalla.

Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa, että rekisterinpitäjän on otettava edellä kuvatut tietosuojaperiaatteet huomioon ja sisällytettävä ne kaikkiin henkilötietojen käsittelyn vaiheisiin mahdollisimman varhaisessa vaiheessa. Periaatteet pitää huomioida jo siinä vaiheessa, kun suunnitellaan henkilötietojen käsittelyä sisältäviä toimintoja ja prosesseja tai kehitetään tietojärjestelmiä.

Tietosuojaperiaatteiden toteuttamiseksi rekisterinpitäjän on toteutettava tarpeelliset organisatoriset ja tekniset toimenpiteet. Organisatorisia toimenpiteitä ovat mm. henkilöstön koulutus, henkilöstölle annetut ohjeet ja määräykset ja salassapitoa koskevat sitoumukset (salassapito- ja käyttäjäsitoumus). Tekniset toimenpiteet liittyvät muun muassa käyttäjien yksilöintiin ja tunnistamiseen, käyttöoikeuksien määrittelyyn tehtävien mukaan ja käytön jälkeen tapahtuvaan lokitarkastukseen.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

5. Rekisterinpitäjän velvollisuudet

Rekisteröidyn informointi

- Rekisterinpitäjän on toimitettava rekisteröidylle henkilötietojen käsittelyä koskevat tiedot. Informaatio pitää olla tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä muodossa selkeällä kielellä ja helposti saatavilla.
- Informaatio on luettavissa Siun soten internetsivulla kohdassa Henkilötietojen käsittely. Informaatio löytyy myös Siun soten intrasta, josta sen voi tulostaa toimintayksikön ilmoitustaululle (tulostettava versio).
- Siun soten internetsivuilla annetaan yleisinformaatiota henkilötietojen käsittelystä sekä kerrotaan rekisteröidyn oikeuksista ja niiden toteuttamisesta. Siellä on myös tietosuojaselosteet palveluittain sekä tietosuojavastaavien yhteystiedot.

Rekisterinpitäjän osoitusvelvollisuus

- Organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä. Tämä edellyttää sitä, että henkilötietojen käsittelyyn liittyvät prosessit ja tietosuojaperiaatteiden käytännön toteutus dokumentoidaan.

Siun sotessa rekisterinpitäjän osoitusvelvollisuutta toteutetaan tuottamalla mm. seuraavia dokumentteja:

- *Tietoturva- ja tietosuojapolitiikka* muodostaa johdon hyväksymän perustan tietosuojan puitteille ja linjauksille sekä vastuille.
- *Periaatteet ja suunnitelmat* ovat kuvauksia käytännön toteutuksesta ja periaatteista.
  - Käyttövaltuus- ja pääsynhallintaperiaatteet
  - Tiedonohjauksen periaatteet
  - Tiedonohjaussuunnitelma
  - Omavalvontasuunnitelma
  - Tietosuojan valvontasuunnitelma
- *Tietosuojaa koskevat vaikutusten arvioinnit (DPIA)*
- *Tietosuojaohjeistus ja koulutusmateriaali*
  - Tietosuojan *verkkokoulutus ja suoritustodistus*
- *Intranetin tietosuojasivustot työntekijöille*
  - *Tietoturva- ja tietosuojakäsikirja*
  - *muu tietosuojakoulutusmateriaali*
- *Seloste henkilötietojen käsittelytoimista*
- *Rekisteröidyn informaatio Siun soten internetsivulla sekä tietosuojaselosteet*
- *Henkilötietojen käsittelyn ehdot -liite* sopimuksiin tuottajille, jotka toimivat Siun soten lukuun ja käsittelevät Siun soten rekisterinpidon alaisia henkilötietoja
- *Tietoturvaloukkausten dokumentointi*
- *Lokitietojen valvonta ja dokumentointi*
- *Tietotilinpäätös, jolla* raportoidaan vuosittain tietosuojan tilasta Siun soten johdolle.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

6. Rekisteröidyn oikeudet

EU-asetuksen mukaan rekisterinpitäjän yhtenä velvollisuutena on toteuttaa rekisteröidyn oikeuksia. Henkilötietojen käsittelyn peruste vaikuttaa siihen, mitä oikeuksia rekisteröidyllä on. Esimerkiksi oikeutta tietojen poistamiseen ei sovelleta lakisääteisiin rekistereihin eli rekisteröity ei voi vaatia tietojaan poistettavaksi esimerkiksi potilasrekisteristä, mikäli tiedot ovat oikein.

Oikeus saada tietoa henkilötietojen käsittelystä

- Rekisteröidyllä on oikeus saada tieto
  - hänen henkilötietojensa keräämisestä sekä käsittelystä
  - häneen kohdistuvasta tietoturvaloukkauksesta.
  - henkilötietojen oikaisuista tai poistoista, jos niistä on tehty ilmoitus tahoille, joille henkilötietoja on luovutettu.
- Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin.

Oikeus saada pääsy tietoihinsa (Tietojen tarkastusoikeus)

- Henkilöllä on oikeus tietää, käsitelläänkö hänen henkilötietojaan vai ei, ja mitä henkilötietoja hänestä on tallennettu.
- Terveydenhuollon tiedot arkistoituvat Kanta-palveluun, ja rekisteröidyt voivat katsoa omat potilastietonsa Omakanta -verkkopalvelusta.
- Tiedot on mahdollista saada myös paperisessa muodossa, jolloin tarkastuspyyntö tehdään kirjallisesti Siun soten internetsivulla olevalla lomakkeella.

Oikeus tietojen oikaisemiseen

- Henkilöllä on oikeus vaatia, että häntä koskevat virheelliset, epätarkat tai puutteelliset henkilötiedot oikaistaan tai täydennetään ilman aiheetonta viivytystä.
- Lisäksi henkilöllä on oikeus vaatia, että tarpeettomat henkilötiedot poistetaan. Tarpeettomuutta ja virheellisyyttä arvioidaan tietojen tallennushetken mukaan.
- Pyyntö tehdään kirjallisesti Siun soten internetsivulla olevalla korjauspyyntölomakkeella

Oikeus tietojen poistamiseen

- Henkilöllä on tietyissä poikkeustapauksissa oikeus saada henkilötietonsa kokonaan poistettua organisaation rekistereistä.
- Poistamisoikeutta ei ole silloin, kun henkilötietojen käsittely perustuu lakisääteisen velvoitteeseen.

Oikeus käsittelyn rajoittamiseen

- Henkilöllä voi tietyissä tilanteissa olla oikeus pyytää henkilötietojensa käsittelyn rajoittamista siksi aikaa, kunnes hänen tietonsa on asianmukaisesti tarkistettu ja korjattu tai täydennetty.

Oikeus siirtää tiedot järjestelmästä toiseen

- Kyseinen oikeus on ainoastaan silloin, jos henkilötietojen käsittely perustuu suostumukseen tai sopimukseen.

- Tämä oikeus ei koske sellaista henkilötietojen käsittelyä, joka on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Näin ollen oikeutta ei sovelleta Siun soten henkilörekistereihin.

Vastustamisoikeus

- Henkilöllä on oikeus henkilökohtaiseen, erityiseen tilanteeseensa perustuen vastustaa henkilötietojensa käsittelyä.
- Vastustamisoikeutta ei ole silloin, kun henkilötietojen käsittely perustuu lakisääteiseen velvoitteeseen.

Oikeus tehdä valitus viranomaiselle

- Henkilöllä on oikeus tehdä valitus valvontaviranomaiselle, jos hän katsoo, että henkilötietojen käsittelyssä rikotaan EU:n yleistä tietosuoja-asetusta.
- Suomessa tämä valvontaviranomainen on tietosuojavaltuutettu.

Rekisteröidyn oikeuksia koskevat ohjeet ja lomakkeet löytyvät Siun soten internetsivulta kohdasta Asiointi → Asiakas- ja potilastiedot.

7. Käyttöoikeudet tietojärjestelmiin

Järjestelmien käyttöoikeudet määritellään Siun soten käyttövaltuusperiaatteiden mukaisesti (Käyttövaltuus- ja pääsynhallintaperiaatteet). Työyksikön esimies määrittelee, mitä järjestelmiä työntekijä tarvitsee työtehtävissään. Esimies vastaa alaistensa käyttöoikeuksien muuttamisesta ja poistamisesta.

Käyttäjä tunnistetaan **käyttäjätunnuksella tai toimikortilla**. Käyttäjätunnus ja salasana sekä toimikortti ovat henkilökohtaisia, eikä niitä saa luovuttaa kenellekään toiselle. Saadessaan käyttäjätunnuksen tai toimikortin käyttäjä sitoutuu niiden huolelliseen säilyttämiseen.

Toimikortti on Digi- ja väestörekisteriviraston (DVV) myöntämä henkilökohtainen varmennekortti, jolla tunnistaudutaan luotettavasti potilas- ja asiakastietojärjestelmiin.

- Toimikortti vastaa digitaalista henkilöllisyystodistusta, jolla voidaan tunnistautua useisiin eri palveluihin (esim. Omakanta, Medinet, Miunpalvelut, vero.fi, poliisi,fi jne.).
- Lisätietoja toimikortista ja sen tilaamisesta saa Siun soten intrasta kohdasta Avain- ja kuvauspalvelut.

Jokainen käyttäjä vastaa omalla käyttäjätunnuksellaan järjestelmien käytöstä sekä asiakirjoihin tehdyistä merkinnöistä ja tietojen katselusta.

Työsuhteen päättyessä oikeus käyttää laitteistoja ja ohjelmistoja päättyy. Työntekijä on velvollinen poistamaan henkilökohtaisia tietoja sisältävät tiedostot ja sähköpostiviestit. Työsuhteen päätyttyä työnantajalla on oikeus käsitellä kaikkia työntekijän työsuhteen aikana tekemiä työhön liittyviä tiedostoja.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

8. Potilas- ja asiakastietojen käsittely, salassapito ja vaitiolovelvollisuus

Potilas- ja asiakastietojen ensisijainen käyttötarkoitus on potilas- ja asiakassuhteen hoitaminen sekä siihen liittyvien palvelujen toteuttaminen. Rekisterinpitäjän luvalla tietoja voidaan käyttää myös toissijaisessa käyttötarkoituksessa, kuten tutkimus, opetus ja tietojohtaminen (Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019)).

Potilastiedot ja sosiaalihuollon asiakastiedot ovat salassa pidettäviä, eikä niitä saa ilmaista sivullisille. Salassapitovelvollisuus sisältää asiakirjasalaisuuden, vaitiolovelvollisuuden ja hyväksikäyttökiellon.

- Salassa pidettävää asiakirjaa ei saa näyttää eikä luovuttaa sivullisille ilman laissa säädettyä oikeutta tai asiakkaan suostumusta.
- Vaitiolovelvollisuus on asiakirjasalaisuutta laajempi, sillä se ulottuu myös suullisesti saatuihin tai tallentamattomiin tietoihin. Vaitiolovelvollisuus jatkuu myös työsuhteen päättymisen jälkeen.
- Hyväksikäyttökielto tarkoittaa sitä, että vaitiolovelvollinen henkilö ei saa käyttää salassa pidettäviä tietoja omaksi tai toisen hyödyksi tai vahingoksi.

Työntekijällä on oikeus käsitellä potilas- ja asiakastietoja silloin, kun hän osallistuu potilaan hoitoon, sosiaalihuollon palvelun antamiseen tai niihin liittyviin tehtäviin. Tietoja saa käsitellä vain siinä laajuudessa, kuin senhetkiset työtehtävät edellyttävät. Potilas- ja asiakastietojen käsittelystä on erilliset ohjeet Siun soten intran tietosuojasivulla (*Potilasrekisterin tietosuojaohje* ja *Ohje sosiaalihuollon asiakastietojen käsittelystä*).

Potilas- ja asiakastietojärjestelmien käyttäjälokiin tallentuu merkintä kaikista potilas- tai asiakastietojen käsittelytapahtumista. Lokitiedoista näkyy, kuka on käsitellyt kyseisen potilaan/asiakkaan tietoja. Lokitietoja seurataan kuukausittain valvontasuunnitelman mukaisesti sekä potilaiden/asiakkaiden tai esimiehen pyynnöstä. Mikäli tarkastuksessa ilmenee väärinkäytöksiä, niistä ilmoitetaan esimiehelle. Asiattoman tietojen käsittelyn sanktiot määräytyvät väärinkäytöksen vakavuuden mukaan. Siun soten YT-toimikunnassa hyväksytty *Tietosuojan seuranta ja valvontasuunnitelma* se löytyy intran Tietosuojasivulta.

9. Turvakiellon alaisen osoitteen käsittely

Henkilö, jolla on perusteltu syy epäillä oman tai perheensä turvallisuuden olevan uhattuna, voi hakea Maistraatista turvakieltoa. Turvakiellon alaisia tietoja ovat henkilön ja hänen kanssaan samassa taloudessa asuvan puolison tai lapsen osoite-, asuinpaikka-, seurakunta-, vaali- ja yhteystiedot. Turvakiellon alaisia tietoja ei saa tallentaa järjestelmiin. Potilas- ja asiakastietojärjestelmissä turvakielto ilmenee asiakkaan henkilötietojen osoitekentässä tekstinä ”Lisätietoja Maistraatista”. Turvakiellon alaisen postin käsittelystä Siun sotessa on erillinen ohje intran tietosuojasivulla (*Turvakieltopostin käsittely*).

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

10. Internetin käyttö

Internetin käytössä tulee olla huolellinen, sen tietoturvariskien vuoksi. Useimmat käyttäjään kohdistuvat hyökkäykset (mm. haittaohjelmien levitys) ja kalastelut tehdään juuri Internetin kautta. Kaikki tarkoitukseltaan haitallinen ja hyvän tavan vastainen Internetin käyttö on kielletty.

Huomioi internetin käytössä seuraavat asiat:

- Suhtaudu kriittisesti Internetissä olevan tiedon luotettavuuteen ja oikeellisuuteen.
- Huomioi tekijänoikeudet ja asianmukaiset lähdeviittaukset, jos kopioit tietoa Internetistä.
- Käytä vain tunnettuja, luotettuja ja asiallisia palveluja. Jos epäilet palvelua haitalliseksi, ota yhteys Meitan ServiceDeskiin.
- Jos kirjaudut palveluun, jossa kysytään salasanaa, selain ehdottaa usein salasanan tallentamista. Tätä ei pidä koskaan tehdä, sillä se mahdollistaa tunnuksesi luvattoman käytön.
- Työnantajan sähköpostiosoitteen saa luovuttaa vain sellaiseen internetpalveluun rekisteröidyttäessä, jolla on selkeä yhteys työtehtäviin.
- Poistu aina palvelusta sen omalla uloskirjautumistoiminnolla
- Internetin välityksellä ei saa välittää salassa pidettävää tai luottamuksellista tietoa ilman asianmukaista salausta/suojausta.
- Ohjelmien lataaminen ja asentaminen Internetin kautta on kielletty.
- Jos käytät julkisia päätelaitteita tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet-selaimen välimuisti (sivuhistoria) ja evästeet (cookies)
- Työnantajan internetyhteyden ja työvälineiden käyttö muiden työnantajien töihin tai omiin sivuansioihin on kielletty, ellei erikseen ole toisin sovittu.
- Organisaation sisäisten tietojärjestelmien ja -verkkojen käyttöön tarkoitettua henkilökohtaista käyttäjätunnusta ja salasanaa ei saa käyttää internetissä oleviin palveluihin rekisteröitymiseen.
- Internetselaimen tietoturva-asetuksia ei saa heikentää.

11. Sähköpostin käyttö

Siun sotella on käytössään Microsoft Outlook sekä Outlook Web Access –sähköpostiohjelmat. Web Access on Outlookin Internet -selainpohjainen käyttöliittymä.

Sähköposti on työväline, joka on tarkoitettu ensisijaisesti työasioiden hoitamista varten. Sähköpostia saa käyttää kohtuullisessa määrin myös yksityiseen viestintään, mutta yksityisviestit on pidettävä erillään työviesteistä tekemällä niille oma, selkeästi nimetty kansio.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

Työnantajan sähköpostia ei saa käyttää henkilökohtaisten tarjouspyyntöjen tai tarjousten tekemiseen eikä kaupankäyntiin tai muiden sellaisten oikeustoimien tekemiseen, joiden yhteydessä vastaanottajan on vaikeaa tulkita, onko kyseessä henkilökohtainen vai työasia. Työntekijöille suositellaan yksityisasioiden hoitamiseen erillisen henkilökohtaisen sähköpostiosoitteen hankkimista ja käyttöä.

Työntekijä vastaa sähköpostin käytöstä, sähköpostilaatikon sisällöstä ja sisällön ylläpidosta.

Huomioi sähköpostin käytössä seuraavat asiat:

- Salassa pidettäviä tietoja ei saa lähettää suojaamattomassa sähköpostissa. Käytä salassa pidettävien ja arkaluontoisten tietojen välitykseen suojattua sähköpostia.
- Sähköpostiviestien automaattinen edelleen lähetys ulkoiseen sähköpostiosoitteeseen (esim. oma henkilökohtainen sähköposti) on kielletty.
- Sähköpostin liitetiedostot ovat yleisimpiä virusten ja muiden haittaohjelmistojen leviämistapoja. Älä koskaan avaa tuntemattomalta lähettäjältä tullutta, epätavallisesti otsikoidun tai muuten oudon sähköpostiviestin liitetiedostoa tai viestissä olevaa internetlinkkiä. Ota tarvittaessa yhteyttä Meitan ServiceDeskiin ennen epäilyttävän liitetiedoston avaamista.
- Varmista viestin lähettäjän aitous, jos vähänkin epäilet sitä. Sähköpostin lähettäjätieto on helppo väärentää. Vastaavasti kuka tahansa voi lähettää viestin sinun nimissäsi.
- Roskapostiviesteihin ”spammiin” ei pidä vastata vaan ne tulee poistaa avaamatta.
- Ketjukirjeiden lähettäminen työnantajan laitteista sähköpostitse on kielletty. Ketjukirjeet ovat haittaohjelmien levittäjiä ja kuormittavat turhaan tietotekniikkaresursseja.
- Sähköpostitse kiertävät vitsit, adressit tms. sisältävät vaaran sähköpostiosoitteen joutumisesta roskapostilistalle, koska ihmiseltä toiselle siirtyvien viestien mukana kulkee suuri määrä sähköpostiosoitteita.
- Jos sähköpostiviesti päätyy väärään sähköpostiosoitteeseen, on viestin saajalla aina vaitiolovelvollisuus ja hyväksikäyttökielto viestin sisältöön ja tunnistetietoihin. Jos saat virheellisen viestin, lähetä siitä tieto viestin lähettäjälle. Viestiä ei saa lähettää eteenpäin ulkopuolisille henkilöille.
- Sähköpostin käyttöoikeus päättyy työsuhteen päättyessä. Työntekijän tulee poistaa henkilökohtaiset viestit ja ilmoittaa viestintäkumppaneilleen, ettei sähköpostiosoite ole enää voimassa.

11.1 Loma-ajat ja pidemmät poissaolot

Työtehtävien keskeytymättömän hoitamisen vuoksi työntekijällä on velvollisuus käyttää sähköpostijärjestelmän automaattista vastaustoimintoa ilmoittaakseen poissaolostaan, sen kestosta ja siitä kuka hoitaa hänen tehtäviään poissaolon aikana.

Työntekijä voi esimiehen luvalla asettaa sähköpostitiliinsä sähköpostiviestien automaattisen edelleen lähetyksen esimiehen hyväksymään toisen työntekijän sähköpostiosoitteeseen.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

Henkilöllä, joka vastaanottaa edelleen lähetetyt viestit, on oikeus avata vain työhön liittyviä viestejä, ei toisen työntekijän henkilökohtaisia viestejä. Henkilöä sitoo vaitiolovelvollisuus saapuneista viesteistä työsuhteen aikana ja sen jälkeen. Suositeltavaa on, että työntekijä ja esimies sopivat edelleen lähetyksestä kirjallisesti (esim. sähköpostitse) ja että sopimukseen sisällytetään myös työntekijän suostumus. (Laki yksityisyyden suojasta työelämässä 759/2004, 20 §, 3 momentti).

11.2. Työnantajan oikeus lukea työntekijän sähköpostia

Työnantajalla on oikeus hakea esille työntekijän henkilökohtaiseen työsähköpostiin tulleita tai siitä lähteneitä viestejä ainoastaan laissa säädettyjen edellytysten täyttyessä. Ensin työntekijälle on järjestettävä mahdollisuus varautua poissaoloon jollakin näistä toimista:

- työntekijä käyttää poissa ollessaan automaattivastausta, josta ilmenee poissaolon kesto ja sijaisen yhteystiedot
- työntekijä kääntää sähköpostit toiselle työntekijälle, joka ottaa työviestit vastaan ja arvioi, onko työnantajan välttämätöntä saada tieto viestistä.

Työntekijän esimiehen tulee olla yhteydessä Siun soten tietosuojavastaaviin varmistaakseen lainmukaisten edellytysten täyttymisestä. Tämän jälkeen hän tekee Meitalle toimituspyynnön ja hankkii mahdollisuuksien mukaan työntekijän suostumuksen työntekijän sähköpostiin tehtäviin toimenpiteisiin. Ennen viestien avaamista arvioidaan otsikoiden ja lähettäjätietojen perusteella, mitkä viestit kuuluvat työnantajalle. Viesteihin kohdistuneet toimenpiteet kirjataan avauspöytäkirjaan. Avaukseen osallistuneita henkilöitä sitoo vaitiolovelvollisuus.
(Lisätietoja Meitan ohjeesta: *Työntekijöiden sähköpostin ja työtiedostojen hakeminen ja avaaminen.*)

11.3 Roskaposti

Roskaposti tarkoittaa ei-toivottua, suurina massoina lähetettyä, ei kenellekään erityisesti kohdistettua sähköpostiviestintää. Roskaposti on yleisin keino haitallisten web-osoitteiden, huijausten, virusten ja haittaohjelmien levittämiseen. Lisäksi roskaposti ruuhkauttaa sähköpostijärjestelmiä ja tukkii käyttäjien sähköpostilaatikoita. Siun soten sähköpostin ylläpitäjällä Meitalla on käytössä roskapostisuodatin, joka poistaa automaattisesti suurimman osan roskaposteiksi tunnistettavista viesteistä.

Jos saat roskapostia, toimi näin:

- Poista roskapostiviestit välittömästi
- Älä vastaa roskapostiviestiin, vaikka siinä olisi linkki, johon ilmoittamalla pääset pois jakelulistalta.
- Älä avaa mitään roskapostissa tullutta liitetiedostoa tai linkkiä.
- Ilmoita tietojenkalasteluviesteistä Meitan ServiceDeskiin.
- Outlook ja Outlook Web Access –sähköpostiohjelmissa on roskapostin käsittelyyn joitakin toimintoja, joilla voit määritellä mitä roskapostiksi tulkituille viesteille tehdään.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

12. Suojatun sähköpostin käyttö asiakastyössä

Lähetettäessä arkaluonteista ja salassa pidettävää tietoa sähköpostitse, on käytettävä aina suojattua sähköpostia. Suojatun sähköpostin käyttöoikeus on maksullinen tuote, jonka voi tilata Meitalta.

Suojatun sähköpostin käytössä on kolme tasoa:

1. ”Kirje” -taso
   - vastaanottajan osoitteen perään lisätään **.s**
     (esim. etunimi.sukunimi@siunsote.fi.s)
   - käytetään esim. viranomaisyhteistyössä, jos vastaanottajaa ei tarvitse tunnistaa vahvasti.

2. ”Kirjattu kirje” -taso (SMS-tunnistautuminen)
   - vastaanottajan osoitteen perään lisätään **.GSM-nro** ja **.s**
     (esim. etunimi.sukunimi@siunsote.fi.0501234567.s)
   - käytetään, jos asiakkaalla/potilaalla ei ole käytössä pankkitunnuksia
   - vastaanottaja saa viestin avaamiseen tarvittavan PIN-koodi tekstiviestinä.

3. Vetuma-taso (pankkikortti tai henkilökorttitunnistautuminen)
   - vastaanottajan osoitteen perään lisätään **.vastaanottajan henkilötunnus** ja **.s**
     (esim. etunimi.sukunimi@siunsote.fi.010101-0101.s)
   - käytetään asiakkaalle/potilaalle lähetettävissä viesteissä, kun tarvitaan vastaanottajan vahva tunnistaminen.
   - vastaanottaja voi avata viestin pankkitunnuksilla tai henkilökortilla.

Tilaus- ja käyttöohjeet löytyvät Meitan palvelupistesivulta kohdasta Ohjedokumentit → Sähköpostin ja kalenterin käyttöön liittyvät ohjeet → Suojattu sähköposti

13. Tekstiviesti asiakastyössä

Tekstiviestit lähetetään Mediatrin kautta, jos työntekijällä on käytössään Mediatri. Mediatrissa on tarkistettu puhelinnumero ja asiakkaalta on saatu tekstiviestilupa.

Jos tekstiviestiä ei voida lähettää Mediatrin kautta, viesti ei voi sisältää salassa pidettävää tietoa, vaan ainoastaan yleistä informaatiota. Tällainen viesti ei voi sisältää esim. asiakkaan tunnistetietoja tai tietoja mistä asiakkuuden voi tunnistaa, koska viesti voi mennä väärään numeroon tai väärälle henkilölle.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

14. Pilvipalvelut

Kun tiedot tai ohjelmistot ovat pilvessä, ne eivät ole omalla työasemalla tai Meitan hallinnoimalla palvelimella vaan pilvipalvelua tarjoavan yrityksen palvelimella missä päin maailmaa tahansa. Pilvessä voi olla palveluita, ohjelmistoja ja tietoja, kuten esimerkiksi Facebook, Instagram, Skype, Office 365, OneDrive.

Pilvipalveluiden käyttöön kohdistuu riskejä, koska palvelut ovat toisen organisaation ylläpitämiä ja palvelimet sijaitsevat usein EU:n ulkopuolella. Tämän vuoksi kaikkea tietoa ei voi niihin tallentaa.

Uusien järjestelmien ja pilvipalvelujen käyttöönoton suunnittelu on tehtävä huolellisesti ennen järjestelmän käyttöönottoa yhdessä Meitan sekä Siun soten turvallisuusyksikön, tiedonhallintayksikön ja ICT-yksikön kanssa. Järjestelmästä/palvelusta on tehtävä EU-tietosuoja-asetuksen 35 artiklan mukainen vaikutustenarviointi (DPIA) ennen käyttöönottoa/pilottia. Ohjeet Siun soten intran Tietosuojasivulla (*Tietosuojan vaikutustenarviointi (DPIA)*).

Ohjeita pilvipalveluiden käyttöön:

- Käsittele tietoja pilvipalveluissa Siun soten tietojen tallennus ja käsittelyohjeiden mukaan (Ohje Siun soten intrassa: *Tietoaineiston luokittelu- ja käsittelyohje*)
- Jos epäilet, ettei pilvipalvelua ole arvioitu tietoturvan ja tietosuojan näkökulmasta tai tietosuojan vaikutustenarviointia ei ole tehty, ota yhteys Siun soten tietosuojavastaaviin.
- Koska pilvipalvelut ovat käytössä laajasti, niihin yritetään tehdä paljon hyökkäyksiä. Ole siis erityisen tarkkana tietojen kalasteluyritysten takia.
- Pilvipalveluihin voidaan kirjautua mistä vain, joten käytä kaksivaiheista tunnistautumista kirjautuessasi pilvipalveluihin. Siun sotella käytetään Meitan hallinnoimaa O365-pilvipalvelua, jossa on käytössä kaksivaiheinen tunnistautuminen sisäverkon ulkopuolelta.

15. Teams-neuvottelupuhelut

Teams-neuvottelupuhelua on mahdollista käyttää työpaikan neuvotteluissa ja tiimipalavereissa, joissa käsitellään asiakastietoja. Salassa pidettäviä tietoja sisältävien tiedostojen jakaminen on Teamsin kautta kielletty, koska ne tallentuvat tällöin yhteiseen O365 -pilvipalveluun. Tarkemmat ohjeet Teamsin käytöstä löytyy intran tietosuojasivulta (Whatsapp- ja Teams-palvelujen käyttö).

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

16. Sosiaalinen media

Sosiaalisen median keskusteluryhmiä (Facebook-, WhatsApp jne.) ei saa käyttää asiakas- tai potilastyössä. Viesteissä ja sivustoilla ei saa olla tietoja, joista paljastuu henkilö tai asiakkuus. Sosiaalisessa mediassa ei saa myöskään julkisesti arvostella työyhteisöä, esimiestä tai eikä käsitellä työpaikan sisäsäisiä tai luottamuksellisia asioita.

Sosiaalisen median palveluja voi käyttää vain yleisten asioiden tiedottamiskanavana. Tiedotuskäyttöön tarkoitetuista sosiaalisen median kanavista vastaa viestintäyksikkö: viestinta@siunsote.fi

Huomioi sosiaalisen median käytössä seuraavat asiat:

- Käyttäessäsi sosiaalisen median palveluja olet itse vastuussa siellä käymistäsi keskusteluista ja esittämistäsi mielipiteistä.
- Mitä enemmän jaat tietoa itsestäsi Siun soten työntekijänä, sitä helpommaksi teet tietojen keräämisen ja hyödyntämisen valeidentiteettiä tai Siun soten työntekijänä esiintymistä varten. Tietojasi voidaan käyttää hyväksi myös tietojenkalastelussa (phishing) sekä haittaohjelmien levityksessä (baiting), esim. tekemällä haittaohjelman sisältävän sähköpostin sisällön tutummaksi vastaanottajalle.
- Sosiaalisen median palveluiden ylläpitäjät voivat päästä käsiksi kaikkeen palvelussa käsiteltävään tietoon, myös kahdenvälisiin keskusteluihin. Internettiin päätynyttä tietoa voi olla mahdotonta poistaa jälkikäteen.

17. Työkansiot verkossa ja pilvessä

Kaikilla Siun soten työntekijöillä, joilla on verkon käyttäjätunnus (MAD-tunnus) on oma verkkokansio (X: -asema). Tämän lisäksi on käytettävissä O365-pilvipalvelussa OneDrive -työkansiot. Molemmat kansiot on tarkoitettu työssä tarvittavien tietojen tallentamiseen ja ne varmuuskopioidaan tietyin väliajoin.

Huomioi nämä asiat tietojen tallennuksessa:

- OneDrive -työkansioita koskevat erilaiset tietojen käsittelysäännöt, kuin omaa verkkokansiota (X:). **Noudata Siun soten tietojen tallennus ja käsittelyohjeita** (Ohje Siun soten intrassa: *Tietoaineiston luokittelu- ja käsittelyohje*).
- OneDrivessä tallennustila on lähes rajoittamaton, kun taas verkkokansiossa (X:) tallennustila on rajoitettu.
- Älä tallenna tietoja työasemallesi, sillä niitä ei varmisteta. Jos joku työasema hajoaa tai se varastetaan, tiedot menetetään.
- Työsuhteen päättyessä työkansiot poistetaan. Siirrä tarvittavat työhön liittyvät tiedostot esimiehen kanssa sovitulle henkilölle.

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

18. Etätyö ja etäkäyttö

Siun soten *etätyön tietoturva- ja tietosuojaohje* löytyy intran tietosuojasivulta. Ohje koskee kaikkea toimiston ulkopuolella tehtävää työskentelyä (esim. kotona, matkoilla, hotellissa, toisen organisaation tiloissa ym.), kaikkia työvälineitä (tietokone, puhelin, mobiililaitteet, ulkoiset tallennusvälineet) ja kaikkea tietoaineistoa.

19. Mobiililaitteet

Mobiililaitteisiin (älypuhelimet ja tabletit) voidaan tallentaa merkittävät määrät tietoa. Lisäksi mobiililaitteita käytettäessä on suurempi riski, että laite katoaa laite tai joutuu varkauden kohteeksi.

Käyttäjä vastaa käytössään olevista mobiililaitteista.

Noudata huolellisuutta ja huomioi seuraavat asiat:

- Suojaa mobiililaite suojakoodilla ja käytä automaattista lukitusta
- Salaa mobiililaite, kun mahdollista. Älä tallenna laitteeseen luottamuksellista tai salassa pidettävää tietoa. Salattuun mobiililaitteeseen voit tallentaa organisaation sisäistä tietoa (*Tietoaineiston luokittelu- ja käsittelyohje*). Jos tarvitset apua salauksessa, ota yhteys Meitan ServiceDeskiin.
- Päivitä mobiililaite aina uusimpaan versioon.
- Asenna sovelluksia vain luotetuista paikoista (mm. Google Play, AppStore, Intune-yritysportaalin Google Play).
- Jos mobiililaitteesi katoaa tai varastetaan, ota välittömästi yhteyttä Meitan ServiceDeskiin.

20. Ulkoiset tallennusvälineet

Ulkoisia tallennusvälineitä ovat USB-muistitikut ja ulkoiset kovalevyt sekä CD- tai DVD-levykkeet. Käyttäjä vastaa käytössään olevista ulkoisista tallennusvälineistä.

Noudata huolellisuutta ja huomioi seuraavat asiat:

- Jos tallennat ulkoiselle tallennusvälineelle organisaation sisäistä, luottamuksellista tai salassa pidettävää tietoa, on tallennusväline salattava. (Tietoaineiston luokittelu- ja käsittelyohje).
- Potilas- ja asiakastietojen tallettaminen ulkoiselle tallennusvälineelle on kielletty.
- Älä käytä tuntemattomia ulkoisia tallennusvälineitä Siun soten työasemissa (haittaohjelmien riski).
- Toimita käytöstä poistettavat USB-muistitikut ja ulkoiset kovalevyt Meitalle tuhottavaksi.
- Tarkempia tietoja tietosuojajätteen käsittelystä: ympäristöinsinööri Susanna Hellberg 013 330 4361

Laatija: tietosuojavastaavat
Hyväksytty tietosuojatyöryhmässä 5/2020

21. Tietoturvaloukkauksesta ilmoittaminen

Tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niitä luovutetaan luvattomasti sivulliselle tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole käsittelyoikeutta. Tietoturvaloukkaus voi tapahtua vahingossa tai tahallisesti.

Tietoturvaloukkauksia ovat esimerkiksi asiakas- tai potilastietojen postittaminen väärälle henkilölle, asiakas- tai potilastietojen katselu ilman asiallista syytä, tietojen kirjaaminen väärälle henkilölle, toisen henkilön käyttäjätunnuksen käyttäminen, kadonnut muistitikku, varastettu tietokone tai murtautuminen henkilötietoja sisältävään järjestelmään.

EU-asetuksen mukaan rekisterinpitäjän on dokumentoitava kaikki tietoturvaloukkaukset ja tehtävä niistä ilmoitus viranomaiselle (Tietosuojavaltuutettu) sekä henkilölle, jonka tietoja on loukattu. Ilmoitus on tehtävä 72 tunnin kuluessa loukkauksen ilmitulosta, joten tietoturvaloukkauksiin on reagoitava nopeasti.

Jokainen Siun soten työntekijä on velvollinen ilmoittamaan omalle esimiehelleen tai Siun soten tietosuojavastaavalle havaitessaan tietoturvaloukkauksen tai epäillessään sellaisen tapahtuneen (Lisätietoja intrassa: *Tietoturvaloukkauksesta ilmoittaminen*).

22. Väärinkäytökset ja niiden seuraamukset

Jokaisella työntekijällä on velvollisuus noudattaa Siun soten tietosuojaohjeita ja yleistä lainsäädäntöä. Jokaisella on myös ilmoitusvelvollisuus havaitsemistaan tietoturvaan ja tietosuojaan liittyvistä väärinkäyttöepäilyistä. Siun sotessa tietosuojaa valvovat tietosuojavastaavat. Tietoturvan ja tietosuojan valvonnan periaatteet ja tarkoitukset sekä väärinkäytösten seuraamukset on kuvattu Tietosuojan valvontasuunnitelmassa. (Intrassa: *Siun sote Tietosuojan seuranta ja valvonta*). Lievien rikkomusten seuraamukset ovat usein esimiehen toimeenpanemia hallinnollisia toimia ja vakavat rikkomukset johtavat tutkintapyynnön tekemiseen poliisille.

Lisätietoja tietosuojavastaavilta:

Maarit Riikonen
Tietosuoja-asiantuntija, sosiaalipalvelut
Puh. 013 330 8260
maarit.riikonen@siunsote.fi

Mirja Vilpponen
Tietosuoja-asiantuntija, terveyspalvelut
Puh. 013 330 8269
mirja.vilpponen@siunsote.fi