ppshp | POHJOIS-POHJANMAAN SAIRAANHOITOPIIRI

Omavalvontasuunnitelma ja EU-tietosuojadirektiivi

Sosiaalihuollon tiedonhallinnan Kanta työpaja 4.5.2017

Jenni Siermala
Tietoturvasuunnittelija

EUROPEAN PARLIAMENT BACKS STRONGER EU DATA PROTECTION

Euranet Plus Network · March 12, 2014

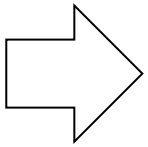
ppshp

Voimassa oleva henkilötietolaki

Henkilötietojen käsittely

Rekisterinpitäjä

Henkilörekisteri



YLEISET PERIAATTEET

Hyvä tietojenkäsit-telytapa

Suunnittelu- ja huolellisuusvelvollisuus

Käyttötarkoitussidon-naisuus ja tarpeellisuusvaatimus

Asiakkaan informointi

Käsittelyn yleiset edellytykset

Tietojen laatu ja hävittäminen

ERITYISET VAATIMUKSET

- Arkaluontoiset henkilötiedot ja henkilötunnus
- Tarkastus- ja korjausoikeus
- Tietoturva ja vaitiolovelvollisuus
- Luovutukset ja siirrot
- Ilmoitukset tietosuojavaltuutetulle

ppshp

EU:n tietosuoja-asetus

SELKEYTTÄÄ NYKYISTÄ
Peruskäsitteet
Yleiset periaatteet
Käsittelyn oikeutus
Suostumus
Tarkastus- ja korjausoikeus
Oikeus tulla unohdetuksi
Riskiarviot korostuvat

TÄYDENTÄÄ NYKYISTÄ
Tietosuojavastaavan asema
Informointivelvollisuus
Käsittelijän rooli määritetty
Lapsen asema
Henkilötietojen siirrot kolmansiin maihin
Profilointi
Tietoturvallisuus

KOKONAAN UUTTA
Sisäänrakennettu ja oletusarvoinen tietosuoja
Tilintekovelvollisuus
Käsittelytoimintojen kuvaaminen
Tietojen siirrettävyys
Vaikutusten arviointi, riskien arviointi
Ilmoitus tietoturvaloukkauksesta
Ennakkohyväksyntä ja ennakko kuuleminen
Sanktiot, hallinnolliset seuraamukset
Viranomaisorganisaatio
(Tietosuojavaltuutetun asema)
Ryhmäkanne -oikeus
Vahingonkorvaus

ppshp

Siirtymäajalla

Voimassa nyt, lakkaa 2018

Henkilötietojen käsittely

Rekisterinpitäjä

Henkilörekisteri

YLEISET PERIAATTEET

Hyvä tietojenkäsit -telytapa

Suunnittelu- ja huolellisuusvelvollisuus

Käyttötarkoitussidon-naisuus ja tarpeellisuusvaatimus

Asiakkaan informointi

Käsittelyn yleiset edellytykset

Tietojen laatu ja hävittäminen

ERITYISET VAATIMUKSET

- Arkaluontoiset henkilötiedot ja henkilötunnus
- Tarkastus- ja korjausoikeus
- Tietoturva ja vaitiolovelvollisuus
- Luovutukset ja siirrot
- Ilmoitukset tietosuojavaltuutetulle

Soveltaminen 25.5.2018 alkaa alkaen

SELKEYTTÄÄ NYKYISTÄ
Peruskäsitteet
Yleiset periaatteet
Käsittelyn oikeutus
Suostumus
Tarkastus- ja korjausoikeus
Oikeus tulla unohdetuksi
Riskiarviot korostuvat

TÄYDENTÄÄ NYKYISTÄ
Tietosuojavastaavan asema
Informointivelvollisuus
Käsittelijän rooli määritetty
Lapsen asema
Henkilötietojen siirrot kolmansiin maihin
Profilointi

KOKONAAN UUTTA
Sisäänrakennettu ja oletusarvoinen tietosuoja
Tilintekovelvollisuus
Käsittelytoimintojen kuvaaminen
Tietojen siirrettävyys
Vaikutusten arviointi, riskien arviointi
Ilmoitus tietoturvaloukkauksesta
Ennakkohyväksyntä ja ennakko kuuleminen
Sanktiot, hallinnolliset seuraamukset
Viranomaisorganisaatio
(Tietosuojavaltuutetun asema)
Ryhmäkanne -oikeus
vahingonkorvaus

ppshp

Omavalvontasuunnitelma

Asiakasorganisaatio / palvelun antaja
vastaa omavalvontasuunnitelmasta ja asiakas- ja potilastietojen käsittelystä toiminnassaan

Välittäjäorganisaatio
vastaa omasta omavalvontasuunnitelmastaan ja välittäjäpalvelun sertifiointivaatimusten täyttämisestä, sen tietoturva-auditoinnista sekä välittäjäpalveluilta vaadittavista ilmoituksista

Järjestelmän valmistaja
vastaa järjestelmään kohdistuvien vaatimusten toteuttamisesta järjestelmässä

Tietojärjestelmäpalvelun tuottaja
vastaa järjestelmään kohdistuvien vaatimusten todentamisesta sekä sertifioinnista (mukaan lukien yhteistestaus ja tietoturvallisuuden auditointi), tietojärjestelmäpalvelun tuottamisesta palvelun antajille sekä tietojärjestelmiin liittyvistä ilmoituksista

ppshp

Tekninen toteuttaminen

EU: tietosuoja-asetus

- Velvoittaa rekisterinpitäjää toteuttamaan asianmukaiset **tekniset ja organisatoriset toimenpiteet**, jotta henkilötietojen käsittely on turvattua.
- Henkilötiedot tulee suojata
  - siirron
  - tallennuksen
  - käsittelyn aikana
- oikeudetta vahingossa tapahtuvalta
  - tuhoamiselta
  - muuttamiselta
  - luovuttamiselta
  - pääsyltä.

Omavalvonta

- Sote-palveluntuottajien on lain ja määräysten mukaisesti huolehdittava tietoturvallisuuden toteutumisesta toiminnassaan.
- Omavalvonta on keino tämän tavoitteen toteuttamiseen.
- Omavalvontaa toteutetaan omavalvontasuunnitelman laatimisen ja sen toteuttamisen kautta.
- Suunnitelmassa on otettava kantaa siihen,
  - miten asiakas- ja potilastietojen käsittelyssä ja tietojärjestelmien käytössä huolehditaan keskeisistä tietoturvallisuuteen vaikuttavista asioista.

ppshp

Tietoturvallisuuden toteuttaminen

- Riskianalyysi
  - Asetus velvoittaa rekisterinpitäjää ottamaan huomioon uusimman tekniikan
  - Toteuttamiskustannukset
  - Arvioimaan tietoturvakeinojen kohtuullisuutta verrattuna arvioituun riskiin

ppshp

Tietoturvallisuuden toteuttaminen

- Turvallinen verkko- ja järjestelmäarkkitehtuuri sisältäen esimerkiksi
  - asianmukaiset palomuurit
  - verkkojen eriyttämisen,
  - palvelinten kovennukset
  - henkilötietojen ja tietojen siirtoväylien salaamisen

Tietoturvallisuuden toteuttaminen

- Tietojärjestelmien hankinta, kehitys ja ylläpito
  - Tietoturvavaatimusten määrittäminen hankintaa ja kehitystä varten
  - Henkilötietojen käytön rajoittaminen tietojärjestelmien testauksessa
  - Tietoturvatestauksen suorittaminen järjestelmien hyväksyntätestauksen yhteydessä
  - Henkilötietoja käsittelevien järjestelmien ylläpitohenkilöstön sijainnin huomioiminen

ppshp

Tietoturvallisuuden toteuttaminen

- Pääsynhallinta
  - Pääsyn rajaaminen ja pääsyoikeuksien hallinta
  - Pääsynhallinnassa tulee ottaa huomioon myös etäyhteydet EU:n tai Euroopan talousalueen ulkopuolelta
    - etäyhteyden ottaminen rinnastetaan henkilötietojen siirtoon, jos toimenpiteessä käsitellään henkilötietoja

ppshp

Tietoturvallisuuden toteuttaminen

- Omaisuuden ja tiedon hallinta
  - Tietovälineiden käsittely sekä tiedon luokittelu ja luokitellun tiedon käsittelyohjeistukset
  - Henkilöstölle tulee olla selvää, miten henkilötietoja on sallittua käsitellä esimerkiksi pilvipalveluun
  - Tallentamisessa
  - sähköpostilla siirtämisessä
  - siirrettäville tietovälineille tallentamisessa.
  - Valtionhallinnossa suojaustasot (IV – III – II – I) määräävät tiedon luokittelua ja käsittelyä.

ppshp

Tietoturvallisuuden toteuttaminen

- Päivitysten ja muutosten hallinta
  - Ohjelmistokomponenttien haavoittuvuuksien saatavilla olevien päivitysten seuranta ja hallinta (CERT-ryhmät)
  - Järjestelmien tietoturvallisuudesta huolehtiminen päivitysten ja muutosten yhteydessä
  - Muutosten hallinnasta ja jäljitettävyydestä huolehtiminen

ppshp

Tietoturvallisuuden toteuttaminen

- Fyysinen turvallisuus
  - Tilaturvallisuudesta huolehtiminen tarvittavin pääsykontrollein ja -rajauksin
  - Tietovälineiden joilla henkilötietoja käsitellään
    - turvallinen huolto
    - hävittäminen

Tietoturvallisuuden toteuttaminen

- Henkilöstöturvallisuus
  - Henkilöstön tietoturvatietoisuuden ja osaamisen varmistaminen koulutuksilla ja ohjeilla
  - Vaitiolo- ja salassapitosopimukset henkilöstön sekä alihankkijoiden kanssa
  - Tarvittaessa ja lain mahdollistaessa tehtävät henkilöiden turvallisuusselvitykset

Tietoturvallisuuden toteuttaminen

- Toimittajien ja sopimusten hallinta
  - Tietoturva- ja tietosuojavaatimusten määrittely sopimuksen/hankinnan kohteelle ja alihankkijoille
  - Sovittava tietoturvan ja tietosuojan hallinnan menettelyt
  - Henkilötietojen käsittelyn seuranta
  - Valvonta
  - Tietoturvaraportointi
  - Tietoturvapoikkeamien hallinta

ppshp

Tietoturvallisuuden toteuttaminen

- Toiminnan jatkuvuuden hallinta
  - Henkilötietojen
    - varmuuskopioinnista huolehtiminen
    - niitä käsittelevien järjestelmien kapasiteetin hallinta
  - Tarvittavat suunnitelmat epäsuotuisiin tilanteisiin ja niistä toipumiseen, jotta voidaan taata henkilötietojen saatavuus esimerkiksi teknisen vian sattuessa
    - ICT toipumissuunnitelma

ppshp

Tietoturvallisuuden toteuttaminen

- Käsittelyn valvonta ja seuranta
  - Rekisterinpitäjän tulee voida jälkikäteen todentaa lokitiedostoista
    - kuka on suorittanut henkilötietojen haun järjestelmästä
    - mitä henkilötietoja on katsottu
    - muutettu
    - lisätty
    - poistettu
    - milloin toimenpide on suoritettu (aikaleima).
  - Menettelyt, joilla lokitiedostoja
    - seurataan
    - miten epäillyt väärinkäytökset käsitellään
  - tietojen käsittelyn seuranta- ja valvontatehtävät ovat selkeästi vastuutettu ja riittävästi resursoidut
  - Myös mahdolliset seuraamukset henkilötietojen väärinkäytöksistä olisi hyvä kartoittaa ja määritellä etukäteen
  - Rekisteröityjen viestinnän osana olisi syytä viestiä myös tietojen käsittelyn seurannasta ja mahdollisten väärinkäytösten seuraamuksista
  - Seurantaa on mahdollisuuksien mukaan hyvä suorittaa automatisoidusti, sillä lokia muodostuu tyypillisesti hyvin paljon

Tietoturvallisuuden toteuttaminen

- Tietoturva-organisaation määrittäminen, roolit ja vastuut sisältäen henkilöstölle määriteltävät tietoturvavastuut.
- Tietoturvan hallintatehtävien määrittäminen vuosikelloon.
- Tietoturvan säännöllinen
  - Mittaaminen
  - Todentaminen
  - Kehittäminen
- Tietoturvaa voidaan todentaa esimerkiksi
  - Teknisellä testauksella
  - hallinnollisten prosessien auditoimisella

ppshp

Kiitos!

ppshp.fi