ESPOON ELÄKEKOTISÄÄTIÖ TIETOTURVAN JA TIETOSUOJAN OMAVALVONTASUUNNITELMA

01.06.2018 Irene Valo

Sisältö

1) Johdanto

Espoon Eläkekotisäätiö on yleishyödyllinen säätiö, joka toimii voittoa tavoittelemattomana, kolmannen sektorin palvelujen tuottajana, joka on perustettu 1973. Toiminnan tarkoituksena on rakennuttaa tai hankkia ja ylläpitää espoolaisille eläkeläisille kiinteistöjä, joissa pienasunnon lisäksi tarjotaan terveydenhuoltoon ja sosiaaliseen vuorovaikutukseen liittyviä, fyysistä ja psyykkistä kuntoa tukevia palveluja. Säätiö voi harjoittaa myös muuta kiinteistö- ja palvelutoimintaa, kuten ravitsemistoimintaa ja tuottaa fysioterapia palveluja. Toiminnan tavoitteena on elinvoimaisen, monipuolisen palvelutoiminnan ylläpitäminen ja kehittäminen siten, että se niveltyy hyvin toimivaksi osaksi Espoon muuta välimuotoisen palvelun verkostoa.

Palvelutalo Hopeakotka ja Hopeakuu ovat Espoon Eläkekotisäätiön ylläpitämiä palvelutaloja, jotka toimivat osana Espoon sosiaali- ja terveydenhuollon palvelujärjestelmää. Lisäksi Espoon Eläkekotisäätiöllä on Senioritalo Hopeakallio, joka toimii ikäihmisten vuokratalona, jossa on mahdollisuus asua myös tilapäisesti esim. putkiremontti. Toimintamme kuuluu välimuotoisiin palveluihin ja on tarkoitettu ensisijaisesti espoolaisille henkilöille, joiden asuminen omassa kodissa ei onnistu kotipalvelujen tukemana, mutta terveydentila tai toimintakyky ei edellytä laitoshoitoa.

Sosiaali- ja terveydenhuollon palvelun antajien, apteekkien ja itsenäisten ammatinharjoittajien, Kansaneläkelaitoksen sekä Kanta-välityspalveluiden tuottajien tulee tehdä omavalvontasuunnitelma. (Määräys 2/2015,THL/1305/4.09.00/2014). Suunnitelman avulla ylläpidetään ja kehitetään organisaation tietoturvaa ja tietosuojaa.

Espoon Eläkekotisäätiö on varmistanut kaikilta ohjelmien tuottajilta, joiden servereille tallentuu henkilörekisterit, että heidän konesalinsa ovat suomessa ja he noudattavat uutta tietosuojalakia.

2) Suunnitelman kohde

Tämä omavalvontasuunnitelma koskee säätiön eri tietosuoja, tietoturva ja tietojärjestelmiä. Tietosuojan omavalvontasuunnitelma liitetään erillisenä säätiön omavalvontasuunnitelmaan, jotka löytyvät kotisivuiltamme osoitteesta www.eeks.fi. Omavalvontasuunnitelmat päivitetään vuosittain tai tarvittaessa. Tämän omavalvontasuunnitelman piiriin kuuluvat: Espoon Eläkekotisäätiön asiakastietojärjestelmät, jotka ovat:

- *asiakastietojärjestelmä DomaCare*
- *Hilmo – hoitoilmoitusjärjestelmä*
- *Solarforce-henkilöstöhallinto-ohjelma*
- *Emce-laskutus- ja palkkahallinto-ohjelma*
- *Titania tuntienseuranta järjestelmä*

3) Määritelmät

1. **"henkilötiedoilla**’ kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella,
2. ’**käsittelyllä**’ toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista,
3. ’**rekisterillä**’ mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu,
4. ’**rekisterinpitäjällä**’ luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti,
5. ’**henkilötietojen käsittelijällä**’ luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun,
6. ’**vastaanottajalla**’ luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja, oli kyseessä kolmas osapuoli tai ei. Viranomaisia, jotka mahdollisesti saavat henkilötietoja tietyn tutkimuksen puitteissa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti ei kuitenkaan pidetä vastaanottajina; näiden viranomaisten on käsiteltävä kyseisiä tietoja sovellettavia tietosuojasääntöjä noudattaen käsittelyn tarkoitusten mukaisesti,

4) Tietosuoja organisaatio

Tietosuoja organisaation roolit jakaantuvat seuraavasti:

Espoon Eläkekotisäätiön hallitus:
- Hyväksyy omavalvontasuunnitelman (ml. tietosuojaperusteet)
- Strategiset päätökset tietosuojatyöhön
- Vastaa tietosuojatyön budjetoinnista

Toiminnanjohtaja (tietosuojavastaava):
- Vastuu aktiivisesta tietosuojan kehittämisestä ja hallinnasta
- Varmistaa, että tietosuoja vastuukysymysten dokumentointi on asianmukaisesti ylläpidetty
- Määrittää yksityisyyden suojaa koskevat tavoitteet ja toimenpiteet
- Tarjoaa asiantuntemusta yksityisyyden suojasta ja tietosuojasta
- Seuraa tietosuoja perusteiden noudattamista

Esimiehet:
- Valvoo, avustaa ja tukee tietosuoja-asioissa niiden syntyessä
- Toimivat yhteyspisteinä yksityisyyden suojaan liittyvissä kysymyksissä ja asioissa
- Vastuu yksityisyyden suojaamiseen liittyvien riskien tunnistamisesta ja raportoinnista

Kaikki työntekijät:
- Noudattaa tietosuojaperiaatetta
- Ilmoittaa rikkomuksista

5) Tietosuojaperusteet

Henkilötiedot Espoon Eläkekotisäätiössä
- voidaan kerätä vain oikeudenmukaisiin, asianmukaisiin, laillisiin ja ennalta määritettyihin tarkoituksiin, kun ennakoitavissa oleva tieto tarvitsee, ja tiedot ovat välttämättömiä toimintasitoumusten täyttämiseksi, toiminnan harjoittamiseksi, toiminnan kehittämiseksi ja palvelujen tarjoamiseksi asiakkaille. Kun tietoja kerätään tiettyihin erityistarkoituksiin, niitä ei saa käyttää mihinkään muuhun tarkoitukseen, joka on ristiriidassa näiden tarkoitusten kanssa.
- Henkilötietoja ei saa säilyttää pidempään kuin on tarpeen niiden tietojen tarkoituksiin, joihin tiedot on kerätty.
- on pidettävä yllä, ja on tärkeää varmistaa tiedon ajantasaisuus
- henkilöstölle sallitaan pääsy järjestelmiin siinä määrin kuin se on tarpeen heidän tehtäviensä suorittamiseksi
- Henkilöstöön voi kuulua myös palveluntarjoajien tai palveluntarjoajien palveluntarjoajia tai toimittajia.

Henkilötietojen siirto

- Espoon Eläkekotisäätiö ei siirrä henkilötietoja EU: n tai ETA: n ulkopuolelle, ellei sitä ole riittävästi suojattu. Jos henkilötietoja luovutetaan EU: n tai ETA: n ulkopuolelle, tarvittaessa käytetään erityisiä suojatoimia (kuten Euroopan komission myöntämät mallikyselyt).

6) Rekisteröijän oikeudet

Yleistä tietosuojasta annetussa asetuksessa määritellään useita oikeuksia, jotka otetaan huomioon prosesseissa ja toiminnoissa. Espoon Eläkekotisäätiö on sitoutunut huolehtimaan rekisteröityjen oikeuksista. EU: n GDPR: n ja Suomen lainsäädännön vaatimusten mukaan.

Espoon Eläkekotisäätiö:

- varmistaa, että rekisteröidylle tiedotetaan tiedonkeruun laajuudesta ja perustasta
- tiedotetaan henkilöille, joilla on pääsy tietoihin
- korjata virheet kerätyissä henkilötiedoissa, joko pyynnöstä tai tarvittaessa
- toimittaa kaikki asiaankuuluvat henkilötiedot määritellyssä muodossa rekisteröidylle hänen pyynnöstään
- poistaa kaikki henkilökohtaiset tiedot, kun lain mukainen tiedon tallennusaika on päättynyt

7) Yleiset tietoturvakäytännöt

Työntekijät jotka käyttävä edellä mainittuja ohjelmia perehdytetään normaaliin perehdytysohjelman kautta näiden käyttöön ja tietoturva- ja salassapitovelvollisuuksiin. Jokainen työntekijä ja hallinto allekirjoittavat vaitiololupauksen. Henkilö, joka arkistoi asiakastietojärjestelmästä syntyvät dokumentit, saa Espoon kaupungin ohjeistuksen mukaisen perehdytyksen tehtävään.

Asiakastietojärjestelmän Doma Care:n pääkäyttäjät luovat työntekijöille tehtävän mukaiset käyttäjätunnukset ja poistavat ne henkilön työsuhteen päätyttyä. Säätiöllä on päätetty eri käyttäjäryhmät ja heidän käyttäjäoikeudet. Emce-laskutusohjelmaan tulee tunnukset ohjelman pääkäyttäjältä, jota hallinnoin tilitoimistomme. Sähköpostikäytännöt ovat sellaiset, ettei mitään postia lähetetä niin, että siitä kävisi henkilön tunnistaminen (sotu) ilmi. Tarvittaessa käytetään turvapostia, jolla pystytään suojamaan ao. tietojen leviäminen. Lähetämme Yliopiston Apteekkiin asukkaiden apteekkisopimukset, lääketilaukset ja/tai Uniikkidosetti tilaukset sekä lääkemuutokset. Ne lähetetään salatulla viestillä www.turvaposti.fi kautta Yliopiston Apteekin Annosjakeluyksikköön.

Solarforce-ohjelma on vain esimiesten käytössä ja siihen antavat tarvittavat tunnukset HR-tunnukset omaavat työntekijät.

a) Toimintamallien koulutus ja perehdytys

Säätiölle on laadittu kattava perehdytys ohjelma, jossa käydään uuden työntekijän kanssa läpi tietoturvaan ja ohjelmiin liittyvät asiat. Henkilön tullessa säätiölle töihin hänen osaamisensa kartoitetaan ja koulutukset liitteineen tallennetaan HR (Solaforce)-ohjelmaan. Tähän ohjelmaan tallennetaan kaikki tulevat koulutukset, jolloin esimiesten on helppo seurata henkilön osaamisen kehittymistä.

b) Tietojärjestelmien käyttökoulutus

Perehdytysohjelman mukaisesti käydään läpi eri tietojärjestelmät sen mukaan, mitä ao. henkilö tehtävässään tarvitsee. Perehdytysohjelma on kolmivaiheinen, ensin esimies perehdyttää säätiön laajemman perehdytysohjelman mukaisesti, johon sisältyy tietoturva-asiat ja ohjelmat sekä vaitiolovelvollisuus. Lisäksi käydään läpi sähköpostin ja internetin käyttöoikeuden, jonka jälkeen työntekijä allekirjoittaa ao. paperit. Toinen vaihe tapahtuu yksikössä, jossa tiimivastaavat käyvät läpi kyseisin yksikön toimintatavat, johon kuuluu esim. turvapostin lähettäminen apteekki tai muille samankaltaisille yksilöille sekä DomaCaren käyttöopastuksen.

c) Riittävä kokemus

Seurataan perehdytyksen yhteydessä ja varmistetaan osaaminen lisäkouluttamisella ja opastuksella omassa yksikössä tehtävän mukaisesti.

d) Ohjeet ja koulutus potilastietojen käsittelystä

Kirjalliset ohjeet löytyvä IMS-laadunhallintaohjelmasta

8) Käyttöympäristön ja useiden järjestelmien yhteiset tietoturvakäytännöt

Rekisteriselosteet löytyvät jokaisesta yksiköstä ja ilmoitustauluilta.

a) Menettelyt virhe- ja ongelmatilanteissa

Kaikki järjestelmä rekisterit ovat ulkoistettu, joten ongelmatilanteissa otamme yhteyttä IT-tukeen, joka on Nebula Oy:n Helpdesk.

b) Järjestelmien käyttöohjeiden hallinnointi ja saatavuus

Asiakastietojärjestelmän hallinnointi tapahtuu pääkäyttäjien kautta. Käyttäjäkohtaiset luvat myöntää esimies aina työntekijälle suunnitelman mukaisesti. Työntekijä perehdytetään näin ohjelmiin perehdytysohjelman mukaisesti. Ohjelma päivitykset tulevat keskitetysti ohjelman toimittajilta tai it-tuesta.

Riittävät käyttöohjeet ovat käytettävissä ohjelman toimittajilta, joilla on myös omat Helpdeskit.

c) Järjestelmien asennus ja ylläpito yleisesti

Järjestelmien toimittajilla on vastuu ohjelmien ylläpidosta ja päivityksistä sekä asennuksista tietosuojanlainmukaisesti.

d) Tilojen, työasemien, tallennusvälineiden ja tulosteiden turvallisuus

Espoon Eläkekotisäätiöllä on toimistotila, jotka sijaitsevat lukituissa tiloissa, joihin ulkopuolisilta pääsy estetty. Näissä tiloissa käytetään edellä mainittuja ohjelmia. Työntekijät on ohjeistettu sulkemaan aina ohjelmat poistuessaan tilasta.

Kaikkiin työasemiin on päivitetty virusohjelmat. Kaikki salasanat ja koodit ovat esimiesten hallinnoimia, ei yleisessä käytössä. It-palvelutoimittaja varmistaa, että virusohjelmat ovat ajan tasalla.

Espoon kaupungin käyttämät ohjelmat meidän koneilla on asennettu kaupungin it-palvelutoimittajan kautta ja varmistettu niiden turvallisuus.

Kaikki tulostimet sijaitsevat suljetuissa toimistoissa, joten niitä ei pääse ulkopuoliset katsomaan.

e) Muut käyttöympäristön käytännöt.

Jokaisella ohjelman toimittajalla on omat tukipalvelut. Operaattoreiden kanssa on tehty sopimukset, joissa he sitoutuvat noudattamaan uutta tietoturvalakia. Heidän serverinsä sijaitsevat suomessa, joten heillä on vastuu näistä tallenteista.

Etäyhteyksiä on kaksi kappaletta, joista toinen on toiminnanjohtajalla ja toinen it-päälliköllä. Heidän koneisiin on asennettu asianmukaiset tietoturvaohjelmat ja palomuurit.

Langattomat verkot hallinnoin Ainacom.

9) Käyttövaltuuksien, pääsynhallinnan ja käytön seurannan yleiset käytännöt

a) Käyttäjäryhmät

Käyttäjäryhmät löytyvät ao. ohjelmistojen käyttäjäryhmien kohdalta. Sieltä löytyvät kaikki käyttäjät, joilla on voimassa olevat oikeudet ao. ohjelmistoon. Samoin sieltä löytyy pääkäyttäjät, joilla on oikeus antaa käyttäjäoikeuksia.

b) Käyttövaltuushallinnan ja käytön seurannan käytännöt

Pääkäyttäjien tulee säännöllisin väliajoin tarkistaa käyttäjien tilanteet. Poistaa sellaisilta henkilöiltä käyttäjäoikeuden, jotka eivät enää työskentele meillä tai muuttaa tarpeen mukaan käyttäjäoikeuksia.

Kaikista käyttäjistä jää jälki ohjelmistoon, josta voidaan tunnistaa ja todentaa ohjelman käyttäjät. Lokien hallinta saadaan ao. operaattorilta.

Lainvastaisten asiakastietojen käsittelystä, jos sellainen havaitaan, tulee heti tehdä kirjallinen selvitys asiasta ja tapahtuneesta. Selvityksen pohjalta tehdään jatkotoimenpiteet ja päätökset seuraamuksista.

Kelan tietokantaan tai Kanta-palveluun emme pääse.