Palveluyhdistys Kaseva ry:n

Tietosuoja- ja tietoturvapolitiikka

Laatija: Anne Simola, toiminnanjohtaja

Hyväksynyt: Palveluyhdistys Kaseva ry hallitus 5.4.2018

SISÄLTÖ

Johdanto

Tieto on keskeisessä roolissa Palveluyhdistys Kasevan toiminnassa ja palveluiden tuotannossa. Jotta tieto on tehokkaasti hyödynnettävissä, tiedon hallinta- ja käsittelykäytäntöjen tulee toimia asianmukaisesti kaikissa tilanteissa. Yhdistyksen hallitus määrittelee tässä politiikassa tietosuojaa ja tietoturvallisuutta koskevat periaatteet ja linjaukset.

Politiikka toimii perustana yhdistyksen tietosuojaa ja tietoturvallisuutta koskeville ohjeille, joiden tehtävänä on tarkentaa politiikkaa ja auttaa sen käytäntöön soveltamisessa. Politiikka on osa yhdistyksen riskienhallintajärjestelmää

Tämä politiikka koskee jokaista yhdistyksen työntekijää, luottamushenkilöä ja sidosryhmän edustajaa, joka työnsä tai toimeksiantonsa puitteissa käsittelee yhdistyksen omistamaa tai hallinnoimaa tietoa. Tätä politiikkaa sovelletaan kaikkeen tietoon mukaan lukien henkilötietoihin ja muuhun tietoon riippumatta sen esitystavasta, muodosta, suojaustasosta, elinkaaren vaiheesta, esiintymisympäristöstä tai siirtotiestä.

Tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita keinoja, joilla suojataan yhdistyksen omistamaa tai hallinnoimaa tietoa niin normaalitilanteissa, normaaliolojen häiriötilanteissa kuin poikkeusoloissakin.

Tietosuojalla tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen lainmukaista käsittelyä ja niiden suojaamista luvattomalta käytöltä ja muulta käsittelyltä. Tietosuoja- ja tietoturvallisuus tulee aina ottaa huomioon mahdollisimman varhaisessa vaiheessa toiminnan suunnittelua.

Tietoturva

Toteutuakseen tietoturvallisuus vaatii seuraavien, painoarvoltaan tapauskohtaisesti vaihtelevien asioiden, toteutumista:

- Luottamuksellisuus: Tieto on vain tietoon oikeutettujen käytettävissä.
- Eheys: Tietoa ei ole muutettu tahallisesti tai tahattomasti, eikä tieto ole muuttunut teknisen häiriön seurauksena.
- Saatavuus: Tieto, tietojärjestelmä tai palvelu on siihen oikeutettujen henkilöiden ja järjestelmien saatavilla ja käytettävissä silloin kun sitä tarvitaan.
- Kiistämättömyys: Tiedonkäsittelytoimenpiteet suoritetaan niin, että käsittelyn osapuolet voidaan yksiselitteisesti tunnistaa sekä toimenpiteitä toteutettaessa, että jälkikäteen.

Tietoturvallisuus yhdistyksessä sisältää tiedon suojaamisen lisäksi toimintaympäristön turvallisuuteen, tietosuojaan ja muihin turvallisuuden osa-alueisiin liittyviä toteutuksia, joista yhdistyksen kannalta keskeisimpiä ovat:

- toimenpiteet, joilla turvataan toimintaympäristön sekä tiedon luottamuksellisuus, eheys, saatavuus ja jatkuvuus
- velvoittavien tietosuojasäädösten mukaiset toimenpiteet, joilla varmistetaan henkilön yksityisyydensuojan ja muiden sitä turvaavien oikeuksien toteutuminen henkilötietoja käsiteltäessä.
- toimenpiteet, järjestelmät ja rakenteet, joiden avulla yhdistyksen tiloja, siellä olevia ihmisiä, tietoa ja muuta omaisuutta suojataan fyysisiltä ja kiinteistövahingoilta, vahingoittamisyrityksiltä ja oikeudettomilta henkilöiltä.
- tietoturvallisuuteen vaikuttavat toimenpiteet, joita suoritetaan henkilöstöprosessissa ennen palvelussuhdetta, sen aikana ja sen päättymisen yhteydessä.
- sopimustekniset toimenpiteet, joilla varmistetaan tässä politiikassa kuvattujen periaatteiden toteutuminen myös sidosryhmien kanssa tehtävässä yhteistyössä.

Tietosuoja

Henkilötietojen käsittely

Yhdistys on sitoutunut käsittelemään henkilötietojen ainoastaan siinä laajuudessa kuin se on kulloisenkin käsittelyn kannalta tarpeen sekä yhdistyksen lakisääteisten velvoitteiden täyttämiseksi. Henkilötietojen käsittelemisen tulee perustua aina kulloinkin sovellettavassa lainsäädännössä määriteltyyn käsittelyperusteeseen. Yhdistys pyrkii siihen, että se ei käsittele virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja. Käsiteltävien henkilötietojen oikeellisuus pyritään varmistamaan ja tietoja voidaan päivittää rekisteröidyltä tai ulkopuolisista luotettavista lähteistä.

Henkilötietojen säilytys

Yhdistys säilyttää henkilötietoja voimassa olevan lainsäädännön mukaisesti ja vain niin kauan, kuin on tarpeen etukäteen määriteltyjen tarkoitusten toteuttamiseksi. Soveltuvan lainsäädännön velvoitteista johtuen tietoja voidaan joutua säilyttämään edellä mainittua ajanjaksoa pidempään. Henkilötietojen säilytysajat on kuvattu jokaisesta henkilörekisteristä laaditussa erillisessä selosteessa.

Yhdistys pyrkii kohtuullisin keinoin pitämään hallussaan olevat henkilötiedot oikeellisina poistamalla tarpeettomia tietoja sekä päivittämällä vanhentuneita tietoja. Tiedot merkitään rekisteriin sellaisina kuin ne saadaan rekisteröidyltä ja niitä päivitetään sen mukaan, mitä rekisteröity ilmoittaa yhdistykselle.

Henkilötietojen luovutukset ja siirrot

Yhdistys voi käyttää alihankkijoita ja palveluntarjoajia henkilötietojen käsittelyssä. Henkilötietoja voidaan luovuttaa yhdistyksen alihankkijoille ja palveluntarjoajille vain siinä määrin, kun ne osallistuvat yhdistyksen henkilötietojen käsittelyyn ja palveluiden toteuttamiseen. Tällaiset kolmannet osapuolet eivät saa käyttää tietoja mihinkään muuhun, kuin yhdistyksen määrittämiin tarkoituksiin. Yhdistys velvoittaa heidät pitämään tiedot salassa ja huolehtimaan asianmukaisesti riittävästä tietoturvan tasosta henkilötietojen suojaamiseksi.

Mikäli yhdistys käyttää tietojen käsittelyssä palveluntarjoajia, joilla voi olla pääsy tietoihin EU-/ETA-alueen ulkopuolelta, yhdistys huolehtii siirtojen asianmukaisesta ja lainmukaisesta toteuttamisesta henkilötietojen käsittelyä koskevan lainsäädännön mukaisesti.

Henkilötietoja voidaan luovuttaa toimivaltaisen viranomaisen esittämien vaatimusten ja lakiin perustuvien edellytysten mukaisesti.

Rekisteröityjen informointi

Yhdistys informoi rekisteröityjä aina asianmukaisesti henkilötietoja käsittelystä siinä vaiheessa, kun henkilötietoja alun perin kerätään. Jokaisesta yhdistyksen ylläpitämästä henkilörekisteristä laaditaan lainmukainen seloste, jota pidetään asianmukaisesti saatavilla yhdistyksen toimipaikassa tai muualla, kuten yhdistyksen verkkosivulla.

Rekisteröityjen oikeuksien toteuttaminen

Lainsäädännössä rekisteröidyille annetaan heidän henkilötietoja koskevia oikeuksia. Mikäli rekisteröidyn henkilötietoja on tallennettu yhdistyksen rekisteriin, rekisteröidyllä on oikeus saada tiedot oikaistuksi, täydennetyksi, siirretyksi tai poistetuksi sekä oikeus rajoittaa tai kieltää henkilötietojensa käsittely henkilötietojen käsittelyä koskevan lainsäädännön mukaisesti.

Mikäli rekisteröity haluaa käyttää tietojaan koskevia oikeuksia, rekisteröidyn tulee tehdä kirjallinen pyyntö yhdistykselle tai henkilökohtaisesti yhdistyksen toimitiloissa. Tietosuojasta vastaava henkilö käsittelee kaikki rekisteröityjen oikeuksia koskevat pyynnöt ennalta määriteltyjen ohjeiden mukaisesti. Yhdistys sitoutuu vastaamaan pyyntöihin yhden (1) kuukauden sisällä pyynnön esittämisestä, ellei ole erityisiä syitä pidentää vastaamisaikaa. Yhdistys voi pyytää rekisteröityä tarkentamaan pyyntöään ja varmentamaan henkilöllisyyden ennen pyynnön käsittelemistä. Yhdistys voi kieltäytyä pyynnön toteuttamisesta sovellettavassa laissa säädetyllä perusteella.

Tietoturvaloukkausten käsitteleminen

Tietosuojasta vastaava henkilö yhdessä muiden työntekijöiden kanssa on vastuussa tietoturvaloukkausten asianmukaisesta hoitamisesta ennalta määriteltyjen ohjeiden mukaisesti. Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen käsittely vahingossa tai lainvastaisesti tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Esimiehet, työntekijät, sidosryhmien edustajat ja alihankkijat ovat velvollisia ilmoittamaan kaikista havaitsemistaan tietoturvaloukkauksista heti tietosuojasta vastaavalle henkilölle. Tietosuojasta vastaava henkilö arvioi tietoturvaloukkauksen todennäköisiä seurauksia rekisteröityjen oikeuksien kannalta ja toimii ennalta määriteltyjen ohjeiden mukaisesti. Tietosuojasta vastaava henkilö huolehtii asianmukaisten ilmoitusten tekemisestä valvontaviranomaisille ja rekisteröidyille noudattaen lainsäädännön asettamia aikarajoja.

Tietosuojasta vastaava henkilö pitää kirjaa kaikista tietoturvaloukkauksista sekä raportoi kaikki tietoturvaloukkaukset tietoturvaryhmälle ja johdolle.

Tietosuojaa koskevat vaikutustenarvioinnit

Uusien palveluiden, tietojärjestelmien ja prosessien tietosuoja-asiat pyritään ottamaan asianmukaisesti huomioon jo suunnitteluvaiheessa. Suunniteltuun henkilötietojen käsittelyyn liittyvät riskit pyritään tunnistamaan jo etukäteen, jotta voidaan varmistaa tietosuojan korkea taso. Tietosuojasta vastaava henkilö otetaan mukaan suunniteltaessa uusia henkilötietojen käsittelytoimia kuten perustettaessa uutta henkilörekisteriä, tilattaessa uutta järjestelmää tai vaihtaessa palveluntarjoajaa, jotta henkilö voi arvioida tarvetta suorittaa tietosuojalainsäädännön mukainen tietosuojaa koskeva vaikutustenarviointi.

Riskienhallinta

Riskienhallintaa toteutetaan yhdistyksen riskienhallintapolitiikan mukaisesti. Politiikassa kuvattu prosessi (mukaan lukien raportointi, seuranta, vastuut) toimii myös toiminnan ja palvelujen tietosuojan- ja tietoturvallisuuden perustana. Periaatteena on, että riskienhallintaprosessia käytetään säännöllisesti toteutettavaan sisäisten ja ulkoisten tietoon kohdistuvien ja tiedosta aiheutuvien riskien hallintaan.

Varautuminen yhdistyksessä turvaa ensisijaisesti kriittisten toimintojensa ja palveluidensa jatkuvuuden normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa. Varautumista toteutetaan ylläpitämällä, harjoittelemalla ja testaamalla tarvittavia valmius- ja muita suunnitelmia. Varautumiseen liittyvät roolit ja vastuut kuvataan em. suunnitelmissa.

Tavoitteena on varautua toiminnan häiriöihin ja keskeytyksiin niin, että toimintaa voidaan jatkaa mahdollisimman normaalisti, häiriöiden haittavaikutuksia rajoittaa sekä toipua häiriöistä mahdollisimman nopeasti. Lain tuomat velvoitteet sekä yhdistyksen sisäinen ohjeistus asettavat vaatimuksia yhdistyksen tietoturvakäytännöille.

Tavoitteiden saavuttamiseksi toteutetut ja suunnitellut toimenpiteet, seurantakäytäntöineen, kuvataan yhdistyksen tietoturvasuunnitelmassa. Tietoturvatavoitteet saavutetaan vain, jos kaikki yhdistyksen toimintaan osallistuvat noudattavat yhteisesti sovittuja periaatteita.

Organisointi, roolit ja vastuut

Tietoturvallisuuteen liittyvät roolit vastuineen on organisoitu yhdistyksen sääntöjen mukaisesti. Yhdistyksen hallitus seuraa tietosuojan- ja tietoturvallisuuden toteutumista. Hallitus hyväksyy tietosuoja- ja tietoturvapolitiikan ja siihen ehdotetut muutokset. Hallituksella on vastuu yhdistyksen sisäisen valvonnan ja riskienhallinnan järjestämisestä. Toiminnanjohtajalla on kokonaisvastuu tietosuojan- ja tietoturvallisuuden toteuttamisesta ja niiden toteutumisen raportoinnista hallitukselle.

Toiminnanjohtaja kantaa vastuun käytännön tietosuoja- ja tietoturvapolitiikan toteutumisesta ja esittelee tarvittavat muutokset hallitukselle. Toiminnanjohtaja hyväksyy palveluun ja toimintaan liittyvät ohjeet ja linjaukset. Toiminnanjohtajan tukena tietosuoja- ja tietoturvaasioissa ovat yksiköiden vastaavat esimiehet.

Esimiehet

Esimiehillä on yleisvastuu tietosuoja- ja tietoturvan toteutumisesta omalla vastuualueellaan. Esimiehet vastaavat erityisesti:

- oman organisaationsa perehdyttämisestä yhdistyksen tietoturva- ja henkilötietojen käsittelyä koskeviin ohjeisiin sekä jokaisen työntekijän työtehtäviin liittyviin vastuisiin, ja
- työntekijän käyttöoikeuksien ja - valtuuksien lisäämisestä ja poistamisesta työntekijän palvelussuhteen päättyessä tai henkilön siirtyessä toisiin tehtäviin sekä
- yhdistykselle kuuluvan tiedon ja muun omaisuuden palauttamisesta.

Henkilöstö

Henkilöstö vastaa:

- ohjeiden noudattamisesta, ja lisäksi
- jokaisen vastuulla on tietosuojaan- ja tietoturvaan liittyvien poikkeamien, uhkien ja riskien ilmoittaminen välittömästi, tietosuojasta vastaavalle henkilölle / toiminnanjohtaja tai omalle esimiehelleen.
- Palvelusuhteen päättyessä yhdistykselle kuuluvan tiedon ja muun omaisuuden palauttamisesta

Tietojärjestelmän (asiakashallintajärjestelmä, Fastroi / Nappula) omistaja vastaa tietojärjestelmänsä ja sen sisältämän tiedon riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta.

Käyttöoikeudet tietojärjestelmään hyväksyy henkilön esimiehen hakemuksen perusteella tietojärjestelmän omistaja tai hänen valtuuttamansa taho. (Järjestelmän Pääkäyttäjä). Prosessin omistaja vastaa prosessinsa riskienhallinnasta ja varautumisesta sekä tietoturvallisuuden toteutumisesta. Lisäksi hän vastaa prosessin riippuvaisuuksien tunnistamisesta ja kriittisyyden arvioinnista.

Tietosuojasta ja tietoturvasta vastaava henkilö

Toiminnanjohtaja toimii tietosuojasta ja tietoturvasta vastaavana henkilönä.

Tietosuojasta ja tietoturvasta vastaava henkilö:

- vastaa henkilötietojen käsittelyn lainmukaisuudesta yhdistyksessä
- antaa tietosuojaa koskevia neuvoja ja ohjeita työntekijöille
- laatii ja ylläpitää ajantasaista dokumentaatiota
- laatii tarvittaessa tietosuojaa koskevia vaikutustenarviointeja
- toimii yhteyspisteenä tietosuojaviranomaisille ja rekisteröidyille
- vastaa rekisteröityjen oikeuksia koskevien pyyntöjen käsittelystä
- huolehtii tietoturvaloukkauksia koskevien ilmoitusten tekemisestä viranomaisille ja rekisteröidyille
- huolehtii tietoturvaloukkausten dokumentoinnista
- edistää tietoturvallisuuden toteutumista yhdistyksessä
- vastaa työryhmän toiminnasta, riskien hallintajärjestelmän toimivuudesta
- tietosuoja- ja tietoturvapolitiikan ja dokumentaation valmistelusta ja kehittämisestä
- raportoi tietosuoja- ja tietoturvan toteutumisesta hallitukselle sekä
- vastaa tietoturvallisuuteen liittyvästä viestinnästä.

Tietosuoja- ja tietoturvaryhmä

Toiminnanjohtaja ja asumisyksikköjen esimiehet muodostavat tietosuoja- ja tietoturvaryhmän, joka

- seuraa tietosuojan- ja tietoturvan yleistä kehittymistä, uhkia ja riskejä sekä tietoturvallisuuden ja tietosuojan toteutumista yhdistyksessä.
- analysoi ja arvioi em. kokonaisuutta ja tekee siihen perustuen kehitysehdotuksia yhdistyksen tietosuojan ja tietoturvallisuuden parantamiseksi.
- toimii tukena tietosuoja- ja tietoturva - asioissa.

Yhdistyksessä ei ole tarvetta erikseen nimetä tietoturvavastaavaa.

Tietohallinto vastaa teknisestä tietoturvallisuudesta, sitä tukevien tietoturvalinjausten tekemisestä ja asetettujen tietoturvavaatimusten toteuttamisesta. Tietohallinto seuraa ja informoi tietoturvaryhmässä vastuualueensa tietoturvallisuuden toteutumisesta.

Asiakirjahallinto vastaa asiakirjatiedon hallinnasta ja siihen liittyvästä ohjeistuksesta. Sisäinen tarkastus vastaa tietoturvallisuuden toteutumisen asianmukaisuudesta ja riittävyyden arvioinnista sekä tarkastamisesta.

Henkilöstöhallinto vastaa tietoturvallisuuden ja tietosuojan toteutumisesta henkilöstöprosessissa. Tähän vastuuseen sisältyvät:

- henkilöstön ohjeistaminen ja tukeminen
- tietoturvakoulutusten ja -perehdytysten organisointi yhdessä tietohallinnon kanssa.

Käyttöoikeudet yhdistyksen omistamaan ja hallinnoimaan tietoon sekä tietojärjestelmiin myönnetään työtehtävien hoitoon tarvittavassa laajuudessa.

Mahdollisiin laiminlyönteihin ja väärinkäytöksiin sovelletaan lakien lisäksi yhdistyksen ohjeita.

Tietoturvatietous ja -osaaminen

Esimies huolehtii uudessa tehtävässä aloittavan työtekijän perehdyttämisestä tietoturva- ja tietosuojaohjeisiin, sekä työntekijän omissa työtehtävissä tarvittavaan erityisosaamiseen.

Yhdistyksen tietoturvadokumentaatio kokonaisuudessaan on henkilöstön saatavilla yhdistyksen sisäisissä informaatiokanavissa työtehtävien edellyttämässä laajuudessa.

Tietoturvallisuuden toteuttaminen

Yhdistyksen tietoturvallisuutta toteutetaan tietoturvasuunnitelman pohjalta, tietoturvallisuuden hallintajärjestelmässä kuvattavilla, tietoturvallisuuden parantamiseen tähtäävillä johtamis- ja muilla käytännöillä. Keskeistä toteuttamisessa on, että yhdistyksellä on riittävät kyvykkyydet aktiivisesti:

- johtaa tietoturvallisuutta
- seurata toimintaympäristön tilaa
- havaita ja tunnistaa uhkat varautua poikkeamiin ja häiriöihin ennakolta sekä reagoida tilanteen edellyttämällä tavalla
- periaatteena on, että tieto on ensisijaisesti julkista ja avointa, jolloin tiedon eheys- ja saatavuusvaatimukset korostuvat.