SASKY koulutuskuntayhtymä

Tiedonhallinnan, tietoturvan ja tietosuojan raportti (tietotilinpäätös)

Sisältö

1 Tietotilinpäätöksen tarkoitus

Tässä tietotilinpäätöksessä kuvataan keskeisiä toimenpiteitä, kuinka SASKY koulutuskuntayhtymä huolehtii tiedonhallinnasta, tietoturvasta ja tietosuojasta. Tietotilinpäätöksellä vastataan myös EU Yleinen tietosuoja-asetuksen osoitusvelvollisuuteen (artikla 24, rekisterinpitäjän vastuu).

Tiedonhallinnan vastuut sekä tietoturva- ja tietosuojapolitiikka-asiakirja määrittää vastuut, valtuudet ja valvontavastuut. Siinä määritetään myös seuranta- ja raportointikäytänteet.

Yhtymähallituksen tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuista määrätään hallintosäännössä. Jokaisella työntekijällä on vastuu sitoutua ja kouluttautua tietoturva- ja tietosuoja-asioihin sekä noudattaa annettuja ohjeistuksia.

Tietotilinpäätöksen laatimisesta on vastannut hallinto- ja talousjohtaja, tietosuojavastaava ja tietohallintopäällikkö. Tietotilinpäätös laaditaan kerran vuodessa keväällä.

2 Tiedonhallinnan, tietoturvallisuuden ja tietosuojan toteuttaminen

SASKY koulutuskuntayhtymän tiedonhallinta on tiedon keräämistä, organisointia ja tallentamista niin, että tieto saadaan käyttöön tarkoituksenmukaisesti ja hallitusti. Edellä mainitun kokonaisuuden johtaminen edellyttää vastuiden, käytäntöjen ja valvonnan määrittelyä. Lisäksi tiedonhallinnan sekä tietoturvan ja tietosuojan onnistunut toteuttaminen edellyttää poikkihallinnollista yhteistyötä kuntayhtymän eri tulosalueiden sekä muiden toimijoiden ja yhteistyötahojen kesken. Myös kuntayhtymälle palveluita tuottavien yritysten ja muiden kuntayhtymäorganisaation lukuun toimivien on sitouduttava noudattamaan kuntayhtymän tiedonhallintaan liittyviä ohjeita sekä tietoturva- ja tietosuojavaatimuksia. Jokaisen on tunnettava vastuunsa tiedonhallinta-, tietoturva- ja tietosuojatyössä. Toiminnan läpinäkyvyys ja viestintä ovat myös tiedonhallinnassa välttämättömiä toimintatapoja.

Yhtymähallituksella on

1. vastuu tiedonhallintalain mukaisten kuvausten koostamisesta ja ylläpidosta (tiedonhallintamalli, muutosvaikutusten arviointi ja asiakirjajulkisuutta koskeva kuvaus),
2. vastuu tietoaineistojen sähköiseen muotoon muuttamisesta ja saatavuudesta,
3. vastuu tietoturvallisuusjärjestelyistä, tietojärjestelmien toiminnasta ja yhteentoimivuudesta sekä tietovarantojen yhteentoimivuudesta

4. vastuu asianhallinnan ja palvelujen tiedonhallinnan järjestämisestä sekä tietoaineistojen säilyttämisen järjestämisestä.

Hallinto- ja talousjohtaja toimii asiakirjahallinnon johtavana viranhaltijana. Hallinto- ja talousjohtaja johtaa yhtymähallituksen alaisena asiakirjahallintoa ja vastaa kuntayhtymän pysyvästi säilytettävistä asiakirjatiedoista sekä

1. vastaa yhtymähallituksen asiakirjahallinnon viranomaistehtävien valmistelusta ja täytäntöönpanosta
2. ohjaa ja kehittää asiakirjahallintoa osana kuntayhtymän tiedonhallintaa
3. hyväksyy tiedonkäsittelyn, säilytyksen ja arkistoinnin ohjeistuksen
4. vastaa keskusarkistosta ja pysyvästi säilytettävistä asiakirjatiedoista
5. laatii kuntayhtymän asiakirjahallinnon ohjeen ja valvoo, että tehtävät hoidetaan annettujen ohjeiden mukaisesti sekä
6. huolehtii asiakirjahallintoon liittyvästä koulutuksesta ja neuvonnasta.

2.1 Tietosuojavastaava

SASKY koulutuskuntayhtymään on nimetty tietosuojavastaava. Tietosuojavastaava on riippumaton asiantuntija, joka tukee henkilöstöä henkilötietojen asianmukaisessa käsittelyssä. Tietosuojavastaava seuraa ja valvoo tietosuojalainsäädännön ja tietosuojaa koskevien tiedonhallintalain periaatteiden noudattamista ja raportoi päätöksentekijöille ja operatiiviselle johdolle sekä tarvittaessa tietosuojaviranomaiselle tietoonsa tulleista poikkeamista. Tietosuojavastaava toimii yhteyshenkilönä kansalliseen tietosuojan valvontaviranomaiseen ja kansalaisiin päin. Tietosuojavastaava osallistuu pyydettäessä tietosuojan vaikutusten arviointiin ja valvoo arviointien toteutusta. Tietosuojavastaava osallistuu tietoturva- ja tietosuojatyöryhmän sekä tiedonhallintatyöryhmän työhön.

2.2 Tietoturvan vastuuhenkilö

Tietohallintopäällikkö toimii hallinto- ja talousjohtajan alaisuudessa tietoturvan vastuuhenkilönä ja vastaa tietoturvaan liittyvien asioiden kehittämisestä, ohjeistamisesta, tiedottamisesta sekä toteutuksen seurannasta yhteistyössä tietosuojavastaavan sekä tietoturva- ja tietosuojatyöryhmän kanssa. Tietoturvan vastuuhenkilö vastaa tietoturvaohjeistuksen laatimisesta ja päivittämisestä yhteistyössä tietoturva- ja tietosuojatyöryhmän kanssa. Tietoturvan vastuuhenkilö tukee tietoturvariskien ja -vaatimusten huomioimisessa tietojärjestelmiä kehitettäessä ja hankittaessa. Lisäksi tietoturvan vastuuhenkilö tukee tietohallintoa tavoitteiden toteuttamisessa, ICT-riskienhallinnassa ja tietoturvan tilannekuvan raportoimisessa. Tietoturvan vastuuhenkilö vastaa tietoturvaan liittyvien poikkeustilanteiden tutkinnasta ja hallinnasta ICT-

jatkuvuussuunnitelman mukaisesti. Tietoturvan vastuuhenkilö osallistuu tietoturva- ja tietosuojatyöryhmän sekä tiedonhallintatyöryhmän työhön.

2.3 Tietoturva- ja tietosuoja-asioiden perehdytys ja ohjeistus

Henkilöstö osallistuu säännöllisesti tietosuojakoulutukseen, joka toteutetaan sähköisellä alustalla suoritettavana koulutuksena ja testinä. Uudet palkattavat henkilöt suorittavat testin osana perehdyttämistä. Testin hyväksytysti suorittaminen on pakollista. Tietoturva- ja tietosuojaohjeistus on tallennettu intranetiin. Opetushenkilöstö ohjaa ja neuvoo tarvittaessa opiskelijoita uusien sähköisten välineiden ja palveluiden käyttöönotossa.

2.4 Tietosuojasta tiedottaminen

Henkilötietojen käsittelytoimet kuvataan tietosuojaselosteissa, joihin on kirjattu tietojen käyttötarkoitus, oikeusperusteet, tietosisältö, tietojen luovutus ja rekisteröityjen oikeudet. Tietosuojaselosteet julkaistaan verkkosivuilla, jossa ne toimivat asiakkaiden informaatioasiakirjoina. Jos rekisterissä käsitellään ainoastaan henkilöstön henkilötietoja, käsittelystä tiedotetaan intranetissa.

3 Tiedonhallinta, asiakirjajulkisuus ja rekisteröidyn oikeudet

3.1 Tiedonhallintalaki ja tiedonhallintamalli

Vuoden 2020 alussa tuli voimaan tiedonhallintalaki (laki julkisen hallinnon tiedonhallinnasta 906/2019). Laki määrittelee merkittäviä kuvaus- ja dokumentointivelvoitteita kunnille. Siirtymäsäännökset ovat voimassa vuoden 2023 loppuun. SASKY koulutuskuntayhtymän tiedonhallintamalli on sisäinen määräys siitä, miten tiedonhallinta ja tietojenkäsittely on toteutettava tiedonhallintamallin mukaisesti käsiteltäessä tietoaineistoja.

Tiedonhallintamalli auttaa:

1. hallitsemaan jatkuvasti lisääntyvän tietomäärän
2. hahmottamaan ja hallitsemaan tiedon elinkaarta
3. tunnistamaan ja hallitsemaan myös uusien digitaalisten palvelujen käyttämiseen liittyviä riskejä

Tiedonhallintamallissa on lain mukaiset toimenpiteet aikataulutettu ja vastuut määritetty.

3.2 Asiakirjajulkisuuskuvaus

SASKY koulutuskuntayhtymän asiakirjajulkisuuskuvaus on julkaistu nettisivustolla. Asiakirjajulkisuuskuvauksen tarkoituksena on antaa yleiskuvaus siitä, miten koulutuskuntayhtymän asiarekisteri sekä palvelujen tiedonhallinta ovat jäsentyneet. Tietoaineistojen kuvausten yhteydessä on esimerkinomaisesti lueteltu hakutekijöitä, joilla tietoja voidaan hakea tietovarannon sisältämistä tietojärjestelmistä tai arkistoista. Asiakirjajulkisuuskuvaus sisältää myös kuntayhtymätasoisen ohjeistuksen siitä, miten tietoja voidaan pyytää.

3.3 Rekisteröidyn oikeudet ja niiden toteutuminen

Rekisteröidyn oikeuksista kerrotaan SASKY koulutuskuntayhtymän nettisivuilla (https://sasky.fi/sasky/tietosuojaseloste/). Samasta osoitteesta löytyvät myös eri henkilötietorekistereiden tietosuojaselosteet, joissa on ilmoitettu kunkin rekisterin vastuuhenkilöt. Rekisteröidyt voivat ottaa oikeuksiinsa liittyvissä asioissa yhteyttä tietosuojavastaavaan ja tarvittaessa myös tietosuojavaltuutetun toimistoon.

Henkilötietojen tietoturvaloukkauksesta tulee ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta on ilmoitettava myös rekisteröidylle ilman aiheetonta viivytystä silloin, kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietoturvaloukkauksista ilmoittaminen (artikla 33) tapahtuu tietosuojavastaavan, tietohallintopäällikön ja hallinto- ja talousjohtajan harkinnan mukaan.

4 Seuranta ja mittaaminen

4.1 Henkilörekistereihin kohdistuvat tietopyynnöt

Saapuneet tietopyynnöt kirjataan asianhallintajärjestelmään. Vuonna 2022 ei ole tullut henkilörekistereihin kohdistuvaa tietopyyntöä.

4.2 Tietosuoja- ja tietoturvapoikkeamat

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole oikeutta käsitellä tietoja. Tietoturvaloukkaus voi tapahtua vahingossa tai tahallisesti. Henkilötietojen tietoturvaloukkauksia ovat esimerkiksi tietojen lähettäminen väärälle henkilölle, kadonnut henkilötietoja sisältävä paperi, omaan työhön kuulumattomien henkilötietojen

katselu, kadonnut tai varastettu tietokone tai muu älylaite tai murtautuminen henkilötietoja sisältävään järjestelmään.

Vuonna 2022 tietosuoja- tai tietoturvapoikkeamia ei havaittu.

4.3 Ilmoituskanava

SASKY koulutuskuntayhtymässä on käytössä väärinkäytösilmoituskanava (whistleblowing). Ilmoittajasta ei tallenneta IP-osoitetta tai mitään muitakaan yksilöintitietoja järjestelmään. Järjestelmässä on kattavat tietoturva- ja tietosuojakontrollit luottamuksellisuuden takaamiseksi. Jokaisesta ilmoituksesta tehdään ratkaisu kolmen kuukauden kuluessa, jos se on mahdollista. Käsittelijät antavat ratkaisun tiedoksi ilmoittajalle, kun käsittely on saatu päätökseen.

Vuonna 2022 tehtiin yksi ilmoitus ammatilliseen opetukseen liittyvistä toimintatavoista.

5 Arviointi ja kehittäminen

Henkilötietojen käsittelyssä noudatetaan hyvää tiedonhallintatapaa ja toimintatapoja arvioidaan ja kehitetään arviointien perusteella edelleen.

5.1 Tiedonohjaussuunnitelma ja tiedonhallintamalli

Tiedonhallintaan ja tiedonhallintaympäristöön merkittävästi vaikuttava projekti on vuosina 2021–22 asianhallintajärjestelmän version päivitys ja muuttuneiden käytänteiden perehdytys henkilöstölle. Tätä ennen on päivitetty tiedonohjaussuunnitelma (TOS). Sähköisen tiedonhallintamallin rakentaminen aloitettiin kuluneena vuonna. Malliin kuvataan toimintaprosessit, tietovarannot, tietoaineistot ja tietojärjestelmät. Kuvausten valmistuttua järjestelmästä voidaan muodostaa ajantasaisia, vaatimusten mukaisia dokumentaatioita ja raportteja.

5.2 Riskienhallinta ja arviointi

Tietoturvan ja tietosuojan riskienarviointi tehdään tarvittaessa ja koko toiminta arvioidaan vähintään kerran vuodessa. Arvioinnissa määritetään riskin taso ja hallintatoimenpiteet. Riskienarviointiin liittyy myös sisäisen valvonnan ja riskienhallinnan kysely henkilöstölle ja yhtymähallitukselle.

Seuraukseltaan ja todennäköisyydeltään korkeimpia tietohallinnon tunnistettuja riskejä (riskitaso = 9-12 (todennäköisyys * seuraus)) on arvioitu olevan kolme kappaletta:

1. Palvelinympäristön vika
2. Pitkä sähkökatko datacenterissä

3. Henkilöstöön liittyvät riskit, henkilöstövaje ja osaamisvaje

Seuraukseltaan ja todennäköisyydeltään korkeimpia tietosuojariskejä (riskitaso =12-8) on arvioitu olevan kolme kappaletta:

1. Henkilötietojen käsittely pilvipalveluympäristöissä eri laitteilla
2. Henkilötietojen säilytys, suojaamattomat tallennusmediat, arkistointiohjeistuksen ja säilytysohjeiden puuttuminen
3. Tietovuoto, henkilötietojen huolimaton käsittely, tahallinen henkilötietojen luovutus tai identiteettivarkaus

Riskeille on määritetty hallintatoiminepiteet riskin pienentämiseksi.

5.3 Tietoturvan ja tietosuojan arviointi

Itsearvioinnissa arvioidaan tietosuojan hallinnan nykytilaa. Aihealueina ovat ne vaatimukset, jotka tietosuoja-asetuksen ja hyvien käytäntöjen mukaisen tietosuojan hallinnan ja henkilötietojen käsittelyn tulee täyttää. Vaatimukset jakautuvat tietosuojan hallintaa sekä tiedon elinkaarta ja prosesseja koskeviin vaatimuksiin. Tietoturvan osalta arvioidaan tiedon suojaamisen menettelyihin ja tekniikkaan liittyviä aihealueita, jotka ovat keskeisiä henkilötietojen suojaamisen kannalta. Toiminta on kehittynyt parempaan suuntaan kehitettäväksi päätettyjen kokonaisuuksien osalta. Asetuksen mukaisessa toimintatavassa on edelleen puutteita joidenkin toimintojen kuvauksissa. Lisäksi kehittämistarvetta on opiskeluun liittyvien henkilötietojen luovutus- ja käsittelysopimuksissa, joista edelleen puuttuu opetushallituksen ohjeistuksia.

Vuoden 2021 lopulla käyttöön otettiin palvelu, joka auttaa arvioimaan sitä, toteutuuko tietosuoja-asetuksen vaatimukset kyseisten sovellusten, ohjelmistojen ja sähköisten palveluiden osalta. Palvelussa arvioidaan kaikki jo käytössä olevat sekä uudet ohjelmistot ja palvelut ja se on osa Saskyssa tehtävää kokonaisarviota. Kokonaisarvioon kuuluu tietoturvan ja tietosuojan lisäksi pedagoginen soveltuvuus ja/tai hallinnollisen käytettävyyden arviointi.

5.4 Kehittäminen

Toimintoja kehitetään arviointien ja tietoturva- ja tietosuojatyöryhmän esittämän vuosittaisen kehittämissuunnitelman avulla. Keskeiset kehittämistoimet ovat

1. Henkilöstön koulutuksen ja perehdytyksen kehittäminen
2. Prosesseissa syntyvien henkilötietorekisterien ja henkilötietojen siirtoihin liittyvien asioiden tarkistus ja tarvittaessa toimien ja ohjeistusten päivitys
3. Käyttöoikeushallinnan kehittämisen jatkaminen
4. Tiedonhallintalain voimaantuloon liittyvien vaatimusten huomioiminen

5. Tekoäly-direktiivin voimaantulon seuranta sekä tietojen luovutuksiin liittyvän Schrems2-sopimuksen seuranta.