13.12.2023

Sisällys

1. Tietotilinpäätös

1.1. Yleistä

Tämän kalenterivuosittain laadittavan tietosuojaraportin tarkoituksena on kuvata tietojen käsittelyn nykytilaa ja henkilötietojen käsittelyyn liittyviä tietosuojaan ja tietoturvallisuuteen liittyviä toimenpiteitä Koulutuskeskus Salpaus -kuntayhtymässä. Raportin tehtävänä on toimia suunnittelun työkaluna, auttaa seuraamaan asetettujen tavoitteiden toteutumista sekä palvella seuraavan vuoden tavoitteiden kuvaamisen välineenä. Raportti palvelee myös tietosuojalainsäädännön rekisterinpitäjälle asettamien velvoitteiden seurannassa. Järjestyksessä kuudennesta tietotilinpäätöksen laatimisesta on vastannut tietosuojavastaava tietohallinnon toimijoiden kanssa.

1.2. Tietosuojan hallintamalli

Tietosuojaa hallinnoidaan Koulutuskeskus Salpaus -kuntayhtymän tietosuojan hallintamallin mukaisesti. Hallintamalli sisältää tietoturva- ja suojapolitiikka- asiakirjat. Organisaation johto vastaa tietosuojasta mm. hyväksymällä vuosittain tehdyt toimenpiteet ja seuraavan vuoden tavoitteet. Tietosuojan ja tietoturvallisuuden keskeisten tehtäviin sisältyvien vastuiden ja tavoitteiden määrittely on sisällytetty kuntayhtymän hallintosääntöön ja vastuut on jalkautettu toimintaan ko. työtehtäviä hoitaville henkilöille.

Kuntayhtymän hallinnollinen ja tekninen tietoturvaryhmä toimivat linkkeinä organisaation ja henkilöstön välisissä tietosuojaa- ja tietoturvallisuutta käsittelevissä asioissa. Työryhmien tehtäviä on käsitelty aikaisemmissa tietotilinpäätöksissä. Tässä raportissa kuvataan kertauksena hallinnollisen tietoturvaryhmän tehtävät lyhyesti, sillä tietosuojatyötä ohjataan pääsääntöisesti tämän työryhmän kautta. Tekninen tietoturvaryhmä keskittyy erityisesti tietoturvallisuuden varmistamiseen ja kehittämiseen kuntayhtymän tasolla.

Tietosuojan ja tietoturvan keskeiset toimijat ovat esittäneet johtoryhmälle tilannekatsauksen kolme kertaa vuoden 2023 aikana. Aiheena ovat olleet ajankohtaisten asioiden ohella henkilöstön tietosuoja- ja tietoturvaosaamisen tilanne (koulutukset henkilöstölle) sekä käytäntöjä ja linjauksia koskevat asiat.

1.3. Tietosuoja ja laki viranomaisen tiedonhallinnasta

Tietosuojaa ja tietoturvallisuutta koskeva lainsäädäntö on uudistunut voimakkaasti viime vuosien aikana. Tämä johtuu Euroopan Unionin yleisestä tietosuoja-asetuksesta, joka astui täysimääräisesti voimaan keväällä 2018. Tietosuoja-asetus toi mukanaan paineita uudistaa kansallista lainsäädäntöä ja sovittaa sääntelyä yhteensopivaksi tietosuoja-asetuksen kanssa.

Tiedonhallintaa koskeva laki viranomaisen tiedonhallinnasta eli yleisesti tiedonhallintalaki ulottuu lisäksi tietosuojaa ja -turvallisuutta koskeviin velvoitteisiin. Kuntayhtymän hallintosääntöä päivitettiin keväällä 2021, jolloin käytiin läpi tiedonhallinnan vastuut tuolloin voimaan astuneen tiedonhallintalain näkökulmasta. Yhtymäkokous hyväksyi hallintosäännön 17.5.2021 (52§).

Koulutuskeskus Salpaus -kuntayhtymä on tiedonhallintalaissa säädetty tiedonhallintayksikkö, jonka tulee toiminnassaan ottaa huomioon mm.:

- tietoaineistojen ja tietojärjestelmien turvallisuutta koskevat vaatimukset

- tietosuojaa ja tietoturvallisuuteen liittyvien riskien tunnistaminen
- erilaisten ko. lain vaatimusten mukaisten kuvausten laatiminen
- vaikutusten arviointi muutostilanteissa.

Tietosuojatyö Koulutuskeskus Salpauksessa painottuu lainsäädännön vaatimuksista johdettuihin käytännön toimenpiteisiin. Tarkastelun kohteena ovat esimerkiksi tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys sekä tietojärjestelmien hankintaa koskevat vaatimukset. Tietoaineistojen turvallisuuden varmistaminen ja tietojen turvallinen siirtäminen tietoverkoissa ovat keskeisiä sääntelykohteita, joihin vastataan käytännön toimin.

Tietosuojatyön tärkeimpiä tehtäviä organisaatiossa ovat henkilötietojen käsittelyn lainmukaisuuden varmistaminen ja rekisterinpitäjälle asetettujen velvoitteiden noudattaminen. Organisaation tietosuojavastaava toimii sekä rekisterinpitäjän että rekisteröityjen tukena varmistamassa henkilötietojen suojaa koskevan lainsäädännön noudattamista. Tietosuojavastaavan tukena kuntayhtymässä toimii hallinnollinen tietoturvaryhmä. Työryhmä on kokoontunut vuoden 2023 aikana joka toinen kuukausi yhteensä kuusi kertaa.

Hallinnollinen tietoturvaryhmä on perustettu ohjaamaan, koordinoimaan ja valvomaan tietoturvaa organisaatiotasoisesti. Työryhmän tehtävänä on raportoida Salpauksen tietoturva- ja tietosuojan tilanteesta johtoryhmälle, ohjata ja ohjeistaa teknisen tietoturvaryhmän toimintaa sekä ottaa huomioon tietosuojalainsäädännön vaatimukset arvioidessaan nykytilaa suhteessa kuntayhtymän tiedonhallintaan.

2. Hallinnollisen tietoturvaryhmän toiminta vuonna 2023

2.1. Tietosuojatyön keskeiset tavoitteet vuonna 2023 ja niiden toteutuminen

Vuosittain tietosuojatyöhön asetetaan joitakin keskeisiä tavoitteita päivittäisten tehtävien hoidon oheen. Tavoitteet määritellään sekä esiin nousseiden tarpeiden sekä mm. tietosuojaan liittyvän vuosittaisen tilintarkastajien suorittaman tarkastuksen pohjalta.

Tavoitteita ovat olleet:

- tietosuojaselostekäytännön uudistaminen
- henkilöstön tietosuoja- ja tietoturvallisuusosaamisen vahvistaminen (tietoturvakurssin suorittaminen)
- opiskelijoiden tietosuojaosaamisen edistäminen asiakaspalveluun suuntautuvissa oppimistehtävissä ja -tilanteissa
- tiedonhallintalain vaatimusten tarkastelu eri tiedonhallinnan osa-alueissa
- teknisten tietoturvaratkaisujen kehittäminen

Edellä mainittuja tavoitteiden toteutumista on kuluneen vuoden aikana tarkastelu hallinnollisen tietoturvaryhmän tapaamisissa, joissa on käsitelty mm. seuraavia asioita:

- ✓ tilannekohtaiset teknisen tietoturvaryhmän asiat ja tietoturvaan kohdistuneet tapahtumat (seurantataulukko)
- ✓ tiedonhallintalakiin liittyviä asioita (kuvaukset ja suositukset)
- ✓ johtoryhmän tilannekatsaukset

- ✓ henkilötietojen käsittelyyn liittyviä asioita: tietojärjestelmien jatkuvuus- ja toipumissuunnitelmat
- ✓ tietosuojaan liittyvien toimintojen kuvaukset: tietosuojaselostekäytännön uudistaminen ja selosteiden päivittäminen (BDO: n tietosuojatarkastus huomioiden)
- ✓ tietosuojan vaikutustenarviointi, käytänteet, lomakkeet ja tilanne
- ✓ henkilöstökoulutus: tietoturvakurssin suoritustilanne
- ✓ valtakunnallinen TAISTO23-harjoitus
- ✓ tietotekniset tietoturvaratkaisut ja kehittämisen tilanne.

Tietosuojatarkastus

BDO: n tilintarkastajien tietosuojaan liittyvä tarkastus sekä vuosien 2021 ja 2022 aikaisten tilintarkastajien suositusten nykytilaan. Seurantatarkastus toteutettiin syksyllä 2023.

Tarkastusraportissa todettiin, että tilintarkastajien antamat toimenpidesuositukset ovat pääosin arvioitu toteutuneiksi. Rekisteri-/tietosuojaselosteiden päivitystyö on edelleen kesken, sillä työ on vienyt arvioitua enemmän aikaa mm. tietosuojavastaavalle asetettujen kysymysten vuoksi ja selosteiden saavutettavuudesta huolehtimiseen, joka on ollut tietosuojavastaavan tehtävänä.

Tilintarkastuksessa huomiota kiinnitettiin tietosuojaselosteiden rekisteröidyn oikeuksien kuvaamiseen. Tarkastuksesta on laadittu erillinen tarkastusraportti, jossa mm. todetaan, että suosituksiin on tehty toimenpiteitä tai sovellettu vaihtoehtoisia toteutustapoja. Raportti toimii osaltaan osoitusvelvollisuuden toteuttajana, joka kuvaa mitä toimenpiteitä on tehty tai parannettu raportin huomioiden pohjalta.

TAISTO23 -harjoitus

Digi- ja väestötietovirasto järjesti kansallisen TAISTO23 -harjoituksen, johon Salpauksen henkilöstöä osallistui viimevuotiseen tapaan samalla kokoonpanolla. Harjoitus on tietosuoja- ja tietoturvaloukkauksia simuloiva harjoitus, joka laittaa organisaatioiden omat toimintamallit ja -prosessit käytännön testiin kuvitteellisten harjoitustilanteiden avulla. Harjoitus on suunniteltu yhteistyössä Keskusrikospoliisin, Kuntaliiton, Kyberturvallisuuskeskuksen ja tietosuojavaltuutetun toimiston kanssa. Parin viime vuoden aikana tekoäly on ottanut huimia harppauksia ja sen integroiminen moniin ICT-palveluihin on yleistynyt.

Harjoitus on aikaisemman kokemuksen perusteella todettu hyödylliseksi, sillä se auttaa Salpausta ylläpitämään ja kehittämään digitaalisen turvallisuuden johtamista, hallintaa ja viestintää. Salpauksessa harjoitukseen osallistui johdon lisäksi tietohallinnon, viestinnän edustaja sekä tietosuojavastaavat.

Henkilöstön digiturvaosaaminen

Henkilöstölle on järjestetty kaksi tietoturvallisuuden ja tietosuojan perusvalmiuksiin kohdennettua kurssia, joilla on varmistettu henkilöstön perusosaaminen. Vuoden 2023 aikana Henkilöstön tietoturvakurssin on suorittanut 78 % henkilöstöstä. Arjen tietosuojaa Salpauksessa kurssi toteutettiin aikaisemmin ja sen on suorittanut 98 % henkilöstöstä. Vuoden aikana tutustuttiin myös tarjolla oleviin koulutuspaketteihin, mikäli jatkossa hyödynnettäisiin myös kaupallista koulutustarjontaa henkilöstön tietoturvallisuuden parantamiseksi. Digiturvaosaamisen ylläpitäminen ja jatkuva parantaminen on osa arjen toimintaa ja tästä syystä siihen panostetaan erilaisin ohjeistamalla ja kouluttamalla henkilöstöä.

3. Tietoturvallisuuden edistäminen vuonna 2023

3.1. Tekniset tietoturvaratkaisut ja keskeiset kehittämiskohteet

Salpauksen verkkoyhteyksien ja IT-konehuoneiden kehittäminen mm. varoajan kasvattaminen mahdollisten odottamattomien sähkökatkojen varalta, sekä toimenpiteet verkkoyhteyksien ja organisaation IT-palveluiden vikasietoisuuden lisäämiseksi.

Salpaus hankki tietoturvavakuutuksen, joka sisältää myös tietoturvatapahtumien selvitys- ja toipumisasiantuntijapalvelun. Tällä varaudutaan mahdollisiin tietoturva- ja tietosuojapoikkeamiin sekä nopeampaan reagointiin ja normaalitilanteeseen palautumiseen.

Salpauksen IT-palveluiden ja tietojärjestelmien lokienhallintaa kehitettiin ottamalla käyttöön lokienhallintaratkaisu. Ratkaisulla tarjoaa asiantuntijoille työkalun poikkeuksien havainnointiin jatkuvasta lisääntyvästä lokimäärästä, sekä toimenpiteiden automatisointiin.

Kaksivaiheinen (vahva) tunnistautuminen on käytössä koko henkilöstöllä keskeisissä palveluissa, vuoden 2023 aikana käyttö laajennettiin koskemaan myös opiskelijoita.

Henkilöstölle otettiin käyttöön Microsoft -palveluihin tietoturvaominaisuuksia, joilla parannetaan uhkilta suojautumista sekä havainnoidaan ja ohjataan loppukäyttäjiä mahdollisten henkilötietietovuotojen varalta.

3.2. Tietoturvatapahtumat

Tekninen tietoturvaryhmä raportoi säännöllisesti hallinnolliselle työryhmälle vuosineljänneksittäin tapahtuneista tietosuojaa ja -turvaa koskevista toimista. Vuoden 2023 tapahtumista on laadittu oheinen määrällinen taulukko eri osa-alueittain.

Osa-alueet	**Q1**	**Q2**	**Q3**	**Q4**
Hallinnollinen tietoturva				
Fyysinen tietoturva				
Laitteistoturvallisuus	3	7	6	3
Ohjelmistoturvallisuus	3		1	5
Tietoaineiston turvallisuus				1
Tietoliikenneturvallisuus	2		1	3
Henkilöstöturvallisuus	18	14	16	17
Käyttöturvallisuus	22	6	7	8

Tietoturvallisuuteen liittyvät tapahtumat vuonna 2023 edellisvuosien tapaan ovat olleet luonteeltaan vähäriskisiä, eivätkä ne ole aiheuttaneet erityisiä riskejä tietoturvallisuuden vaarantumiseen tai henkilötietoloukkauksiin. Toiminnan häiriötön jatkuminen on kyetty varmistamaan kaikilta osin.

Henkilöstöturvallisuus-osio pitää sisällään yksittäisiä neuvonta- ja tiedotustapahtumia. Ne Liittyvät esimerkiksi erilaisiin roskasähköpostiviesteihin, ajankohtaisiin tietoturvaa koskeviin haavoittuvuusilmoituksiin ja erilaisiin tietojenkalastelukampanjoihin, joista henkilöstön on hyvä olla tietoinen.

Tietosuojaan kohdistuvat loukkaukset

Organisaatiossa on laadittu prosessikuvaus, jonka mukaisesti tietosuojaloukkaukset käsitellään. Vakavimmilta tietosuojaloukkauksilta on onnistuttu välttymään, joten prosessikuvauksen toimivuutta ei ole juurikaan päästy testaamaan todellisessa tilanteessa.

Rekisterinpitäjä vastaa siitä, että henkilöstö tuntee tietosuojaan liittyvät henkilötietojen käsittelyperusteet. Yleisesti ottaen on havaittu, että henkilötietojen käsittely vaatii edelleen lisäohjeistusta ja perehdytystä.

4. Tietosuojatyön tavoitteet vuonna 2024

4.1. Havaittuja kehittämistarpeita

Hallinnollinen tietoturvaryhmä tarkastelee yleisiä tietosuojaan ja tietoturvallisuuteen liittyviä toimenpiteitä ja asettaa kehittämiskohteita.

Aiemmin mainitut tietosuojaselosteet päivitetään ja niiden julkaisuprosessi uudistetaan. Selosteet julkaistaan yleisessä tietoverkossa alkuvuoden 2024 aikana. Yksi keskeinen tavoite on toteuttaa käytännönläheinen tietosuoja/tietoturvaharjoitus henkilöstölle.

Tietosuojasääntelyn ohella tiedonhallintalaki on tuonut mukanaan uusia velvoitteita, jotka kohdentuvat sekä tietosuojaan ja tietoturvallisuuteen. Näitä ovat esimerkiksi organisaation muutostilanteissa laadittava muutosvaikutusten arviointi ja tietosuojan vaikutustenarviointi. Arviointeja on toistaiseksi laadittu vain muutama, joten niiden laatiminen tulee nostaa tavoitteiksi vuonna 2024. Arvioinnit perustuvat velvoittavaan lainsäädäntöön. Arjen toiminnassa ne ovat riskien arvioimista ja ennakoimista, ja siten perustoimintoja digiturvallisuuden edistämisessä.

Henkilötietojen käsittelyn osaamista ei voi korostaa liikaa. Vuonna 2024 laaditaan lisäohjeita mm. henkilötietojen luovutuskäytänteisiin ja tarkennusta yleisiin tietosuoja-asetuksen henkilötietojen käsittelyperusteisiin. Näiden osaamisessa on todettu olevan edelleen puutteita.

Muita vuodelle 2024 asetettuja tavoitteita ovat:

- lokienhallintamallin kehitys ja käyttöönotto
- henkilötietojen käsittelyohjeen päivittäminen ja jalkauttaminen (arjen toiminnassa ja TAISTO23 harjoituksessa ilmenneiden havaintojen ja puutteiden huomioiminen ohjeistuksessa)
- tiedonhallintalautakunnan julkaisemien uusien suositusten huomioiminen tietosuojan ja -turvan osalta
- edistää keinoja, joilla parannetaan henkilöstön tietämystä digiturvallisuudesta muuttuvissa tilanteissa (esim. jalkauttaa uusia toimintatapoja ja yleinen tietoturvaosaaminen ja käytännöt)

- tekniset tietoturvaratkaisut ja kehittämiskohteet mm. suojaus- ja valvontaratkaisujen kehitys, datan varmistusratkaisut yms.

Muun lainsäädännön vaikutus tietosuojaan ja tietoturvaan

Hyvinvointialueiden muutokset ovat lisänneet tarvetta lisätä henkilötietojen käsittelyyn liittyvää tietoisuutta kuten tiedonantovelvoitteiden ja tiedon luovutuskäytänteiden hallintaa sekä oikeutta käsitellä henkilötietoja opiskeluhuoltoon liittyvissä tilanteissa ja tietopyynnöissä.

Laissa ammatillisesta koulutuksesta tarkoitettu opiskelijahuolto sisältää opetussuunnitelman mukaisen opiskeluhuollon ja opiskeluhuollon palvelut, joita ovat psykologi- ja kuraattoripalvelut sekä opiskeluterveydenhuollon palvelut. Näiden tietojen rekistereiden tallennus tapahtuu sekä potilasrekisteriin, kuraattorin asiakasrekisteriin ja koulutuksen järjestäjän ylläpitämään opiskeluhuoltorekisteriin. Rekistereiden väliset tietojen salassapito- ja luovutuskäytännöt ovat nousseet vahvempaan rooliin hyvinvointialueiden aloittaessa toimintansa.

Tietojen saannista säädetään myös oppivelvollisuuslaissa, jonka mukaan oppivelvollisen ohjaus- ja valvontavastuussa olevalla koulutuksen järjestäjällä on salassapitosäännösten estämättä oikeus saada laissa säädettyjen tehtävien hoitamiseksi välttämättömät tiedot oppivelvolliseen liittyen tietyissä tilanteissa.

Parhaillaan käynnissä oleva julkisuuslakiuudistus tulee koskemaan tietopyyntöjä koskevan sääntelyn tarkastelua ja prosessien selkiyttämistä sekä yksityisyyden suojan ja julkisuusperiaatteen edellytyksiä. Myös tämä lakiuudistus tulee vaikuttamaan tietoturvallisuutta ja tietosuojaa koskeviin rekisterinpitäjän velvoitteisiin.

Loppuvuodesta 2023 on Tiedonhallintalautakunta valmistellut kaksi uutta suositusta (TihL 5 §); suositus tiedonhallintamallin ylläpidosta ja tiedonhallinnan muutosvaikutusten arvioinnista, jotka koskevat myös tietosuoja- ja tietoturvavaatimuksia. Suositukset ovat olleet Lausuntopalvelussa tiedonhallintayksiköiden kommentoitavina ja niiden soveltaminen käynnistyy vuoden 2024 aikana.

4.2. Henkilörekistereiden tietosuoja ja tietoturvallisuus

Kyberturvallisuuskeskus julkaisi elokuussa tiedotteen, joka koski kuntien keskeisiä henkilörekistereitä ja niiden tietoturvaa. Tiedotteessa nostettiin esiin mm. opetuksen hallintajärjestelmät ja kolmansien osapuolten pääsy niihin. Riskitasoa nostaa käsiteltävien tietojen luonne, sillä rekisterit sisältävät usein salassa pidettäviä ja erityisiä henkilötietoryhmiä käsitteleviä tietoja. Näitä ovat terveystiedot, sosiaalihuoltolain alaiset tiedot, opiskelijoiden arviointia ja turvakiellon alaisia tiedot. Alaikäisten henkilöiden tietoja tulee lisäksi suojata tietosuojalainsäädännön mukaisesti erityisellä huolella.

Keskeiset prosessit ja käsiteltävä tietoaineisto tulee suunnitella mm. seuraavat lähtökohdat huomioiden:

- Mitä tietoa käsitellään?
- Mihin tarpeeseen tietoja käsitellään?
- Mihin tietoja tallennetaan?
- Mikä on tiedon elinkaari?
- Ketkä tietoa käsittelevät?

- Miten tiedonkäsittelyn vastuut jakautuvat?

Uusia tietojärjestelmiä hankittaessa kyseisiä velvoitteita voidaan kuvata ja tarkastella esimerkiksi tietosuojan vaikutustenarvioinnissa ja laajemmin muutosvaikutusten arviointia laadittaessa.

Vuoden 2023 keskeiset kysymykset opintohallinnossa liittyivät lisäksi käyttöoikeuksien antamiseen opiskeluhuollon psykologi- ja kuraattoripalveluille. Asia käynnistyi apulaistietosuojavaltuutetun aloitteesta Opetus- ja kulttuuriministeriölle, Sosiaali- ja terveysministeriölle, Opetushallitukselle sekä Terveyden ja hyvinvoinnin laitokselle.

Kysymyksiä Tietosuojavaltuutetun toimistoon tuli sekä koulutuksen järjestäjiltä että hyvinvointialueilta ja asian todettiin vaativan tarkempaa selvittelyä. Rekisterinpitäjän vastuusta säädetään yleisellä tasolla tietosuoja-asetuksen 24 artiklassa. Apulaistietosuojavaltuutettu on todennut mm., että asiassa on kyse opiskelijoiden henkilötietojen luovuttamisesta toiselle rekisterinpitäjälle. Kysymyksessä epäselvyyttä on aiheuttanut mm. mitä ”käyttöoikeudella” tarkoitetaan, kuten esimerkiksi opiskelijoiden ”tietojen sähköistä luovuttamista” opiskelijarekisteristä opiskeluhuollon toimijoille sekä pääsyä rekistereihin. Asiaan liittyvää informaatiota ja ohjeistusta on laatinut Opetushallitus, joka on laatinut verkkosivuilleen laajan tietopaketin aiheesta https://www.oph.fi/koulutus-ja-tutkinnot/tietojen-luovutus-koulutuksesta-opiskeluhuoltopalveluille .