

5.1.2026

Sisällys

1. Tietotilinpäätös ja sen tehtävä	2
1.1. Yleistä – tietosuojaa ei ole ilman tietoturvaa	2
1.2. Tietotilinpäätös	2
2. Tietosuojan vastuunjako Koulutuskeskus Salpaus -kuntayhtymässä	3
2.1. Rekisterinpitäjä	3
2.2. Tietosuojavastaava	4
2.3. Tietosuojan hallintamalli	4
3. Tietosuojan keskeiset tavoitteet vuonna 2025 ja niiden toteutuminen	5
3.1. Keskeisiä toimia tietosuojan edistämiseksi	5
3.2. Saatuja oppeja vuodelle 2026	7
4. Tietoturvallisuuden edistäminen vuonna 2026	8
4.1. Tekniset tietoturvaratkaisut ja keskeiset kehittämiskohteet	8
4.2. Tietoturvatapahtumat vuonna 2025	9
5. Tietosuojatyön tavoitteet vuodelle 2026	9
5.1. Havaittuja kehittämistarpeita	9
5.2. Tietosuoja on tiedonhallintaa	10

5.1.2026

1. Tietotilinpäätös ja sen tehtävä

1.1. Yleistä – tietosuojaa ei ole ilman tietoturvaa

Tietosuojalla on perinteisesti tarkoitettu henkilötietojen käsittelyä koskevien oikeuksien ja velvollisuuksien huomioon ottamista rekisterinpitäjän toiminnassa sekä luonnollisten henkilöiden yksityisyyden suojan ja oikeusturvan varmistamisessa. Tietosuojalla pyritään ohjaamaan hyviin henkilötietojen käsittely- ja tietosuojakäytäntöihin. Samalla turvataan yksityiselämää, etuja, oikeuksia ja vapauksia.

Tietoturvalla tarkoitetaan tietosuojan näkökulmasta niitä teknisiä ja hallinnollisia toimenpiteitä, joilla yllä mainittuja rekisteröidyn oikeuksia turvataan. Toimenpiteitä ovat ennen kaikkea tiedon laadun, eheyden ja luottamuksellisuuden säilyttäminen sekä tiedon suojaaminen teknisin ja hallinnollisin keinoin.

Tietosuojatyön organisointi ja varsinainen tietosuojatyön tekeminen kehittävät koko henkilöstön tietosuojaosaamista ja muuttavat toiminta- ja asiakasprosessit lainmukaisiksi ja joustaviksi.



1.2. Tietotilinpäätös

Tietotilinpäätös on keskeinen osa tietosuojan toteutumisen seuranta ja EU:n yleisen tietosuoja-asetuksen (EU 2016/679, jäljempänä tietosuoja-asetus) määrittelemää osoitusvelvollisuutta (5 artikla). Osoitusvelvollisuus tarkoittaa, että organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä. Osoitusvelvollisuuden toteuttaminen edellyttää henkilötietojen käsittelyyn liittyvien prosessien ja tietosuojaperiaatteiden käytännön toteuttamisen dokumentointia.

5.1.2026

Tietotilinpäätöksen tehtävänä on toimia myös suunnittelun työkaluna ja auttaa seuraamaan asetettujen tavoitteiden toteutumista. Raportti on osa rekisterinpitäjälle lainsäädännössä asetettujen velvoitteiden seuranta. Vuoden 2025 tietotilinpäätös sisältää joitain keskeisiä vuoden aikana esiin tulleita asioita ja toimenpiteitä. Tietosuojatyö kuntayhtymässä on jatkuvaa ja suunnitelmallista toimintaa.

2. Tietosuojan vastuunjako Koulutuskeskus Salpaus -kuntayhtymässä

2.1. Rekisterinpitäjä

Koulutuskeskus Salpaus -kuntayhtymä on rekisterinpitäjä, joka vastaa henkilötietojen käsittelystä. EU:n yleisessä tietosuojasetuksessa määritellään rekisterinpitäjä ”luonnolliseksi henkilöksi tai oikeushenkilöksi, viranomaiseksi tai virastoksi tai muuksi elimeksi, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot”.¹



Rekisterinpitäjä päättää, miksi henkilötietoja kerätään ja miten niitä käsitellään. Tähän sisältyy mm. tietojen keruun, säilytyksen ja poistamisen periaatteet. Rekisterinpitäjä vastaa siitä, että kaikki käsittelytoimet ovat tietosuojalainsäädännön mukaisia, ja että tämä voidaan osoittaa. Rekisteröityjen on voitava luottaa siihen, että he voivat käyttää oikeuksiaan, kuten esimerkiksi tarkastaa tietonsa ja vaatia niiden oikaisua, mikäli tiedoissa on virheitä. Rekisterinpitäjän velvollisuuksiin kuuluu arvioida käsittelyyn liittyvät riskit ja toteuttaa tekniset ja organisatoriset toimet, kuten tietojen salaaminen tai henkilöstön koulutus. Tietosuojaperiaatteet kuten tietojen minimointi, käyttötarkoitussidonnaisuus ja läpinäkyvyys on sisällytettävä kaikkiin prosesseihin.

¹ GDPR, 4 artikla, kohta 7

5.1.2026

2.2. Tietosuojavastaava

Tietosuojavastaavan tehtävät, työnkuva ja asema määritellään tietosuoja-asetuksen 39 artiklassa. Työnkuvassa korostuvat sekä seuranta- että valvontatehtävät. Tietosuojavastaava toimii yhteistyössä valvontaviranomaisen (Tietosuojavaltuutettu) kanssa, tukee rekisteröityjä oikeuksien toteuttamisessa, neuvoo ja ohjaa kaikissa tietosuojakysymyksissä. Tietosuojavastaava on tukena ja valvoo tietosuojan vaikutustenarviointien laatimista sekä muiden tietosuojavaatimusten noudattamista. Organisaation tietosuojavastaava toimii sekä rekisterinpitäjän että rekisteröityjen tukena varmistamassa henkilötietojen suojaa koskevan lainsäädännön noudattamista.

2.3. Tietosuojan hallintamalli

Tietosuoja hallinnoidaan Koulutuskeskus Salpaus -kuntayhtymän tietosuojan hallintamallin mukaisesti. Kuntayhtymän johto vastaa tietosuojasta mm. hyväksymällä vuosittain tehdyt toimenpiteet ja asetetut 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 tietosuoja- ja tietoturvallisuutta käsittelevissä asioissa. Tietosuojan ja tietoturvan tilasta raportoidaan johdolle säännöllisesti vuosineljänneksittäin.

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. Näitä ovat mm:

- tietoaineistojen ja tietojärjestelmien turvallisuutta koskevat vaatimukset
- tietosuoja ja tietoturvallisuuteen liittyvien riskien tunnistaminen
- erilaisten tietosuoja- ja tietoturvasäästöjen vaatimusten mukaisten kuvausten laatiminen
- vaikutusten arviointi muutostilanteissa.

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 tietosujalainsäädännön vaatimukset arvioidessaan nykytilaa suhteessa kuntayhtymän tiedonhallintaan. Hallinnollinen tietoturvaryhmä on kokoontunut vuoden aikana kuusi kertaa.

5.1.2026

3. Tietosuojan keskeiset tavoitteet vuonna 2025 ja niiden toteutuminen

3.1. Keskeisiä toimia tietosuojan edistämiseksi

Hallinnollinen tietoturvaryhmä tarkastelee yleisiä tietosuojaan ja tietoturvallisuuteen liittyviä toimenpiteitä ja asettaa vuosittaiset kehittämiskohteet tietosuojatyölle.

Tietosuojasääntelyn ohella tiedonhallintalaki asettaa velvoitteita, jotka kohdentuvat sekä tietosuojaan ja tietoturvallisuuteen. Näitä ovat esimerkiksi organisaation muutostilanteissa laadittava muutosvaikutusten arviointi ja tietosuojan vaikutustenarviointi. Vuoden 2025 aikana on aloitettu tietosuojan vaikutustenarviointityö sekä Salpausvetoisena, että ulkoisen palveluntarjoajan Ilona IT:n Sovelluskirjasto -palvelua hyödyntämällä. Mukana arviointeja laatimassa on ollut myös muiden ammatillisten koulutuksenjärjestäjien oppilaitoksia. Tavoitteena on jatkaa yhteistyötä, kun lisää halukkaita oppilaitoksia ilmaantuu mukaan kyseisen palveluntarjoajan kautta.

Tietosuojan vaikutustenarviointeja on toistaiseksi laadittu uusien käyttöönotettavien palveluiden osalta. Tulevana vuonna 2026 vaikutuksen arvioinnit tullaan laatimaan myös jo käytössä olevista keskeisistä ja kriittisistä palveluista. Arvioinnit edistävät riskien arvioimista ja ennakoinnista ja hallintaa, ja ovat siten perusteltuja digiturvallisuuden edistämisessä.

Keväällä helmikuussa 2025 Salpauksen verkkoon kohdentui palvelunestohyökkäyksiä, jotka aiheuttivat palveluiden käytön hidastumista ja tilapäisiä häiriöitä. Tapahtuman johdosta Salpauksen verkkoon hankittiin DDoS-hyökkäysten estopalvelu tietoliikenneoperaattorilta. Tämän jälkeen verkossa ei ole esiintynyt vastaavia palvelunestohyökkäyksiä.

Yhtenä tavoitteena oli arvioida ja päivittää GDPR-tietopyyntöjen vastaamisen käytäntöjä. Prosessista laadittiin kuvaus nykytilasta. Lisäksi Salpauksen verkkosivuille laadittiin sähköiset asiakirjapohjat, joiden avulla rekisteröity on tunnistettavissa ja voi käyttää oikeuksiaan. Sähköisten lomakkeiden ohella paikan päällä asiointi, puhelin ja sähköpostiviestin välityksellä tapahtuva yhteydenotto on edelleen mahdollinen, kun rekisteröity haluaa ottaa yhteyttä ja kysyä omien henkilötietojensa käsittelystä.

Henkilöstön osaamista varmisteltiin syyskuussa tietohallinnon kalasteluharjoituksella. Harjoitus osoitti, että henkilöstö oli entistä valveutuneempaa, eikä suurempia haksahduksia tapahtunut. Osaamista vahvistetaan koulutusten avulla, esimerkiksi toukokuussa opetus- ja ohjaushenkilöstölle järjestettiin aiheesta tietoturva- ja tietosuojaworkshop. Tietosuojasta ja tietoturvallisuudesta on järjestetty koulutusalojen digimentoreille omat tietoiskut.

Wilma-järjestelmän tietoturvaa tarkasteltiin alkuvuodesta asian noustua esiin julkisissa tiedotusvälineissä vuoden 2024 lopulla. Asian yhteydessä korostettiin lasten (alle 18 v.) asemaa erityisen haavoittuvana ryhmänä. Wilma-järjestelmässä mainitut mahdolliset tietoturva-aukot tarkasteltiin myös Salpauksen osalta. Kuntaliitto julkaisi aiheeseen liittyen tiedotteen, jonka pohjalta varmistettiin koulutuksessa käytettyjen tietojärjestelmien tiedonhallintalain vaatimustenmukaisuutta mm. vastuita, ohjeita ja käyttöoikeuksien hallinnan käytäntöjä.

5.1.2026

Dynasty-asianhallintajärjestelmän käyttöoikeudet tarkasteltiin ja poistettiin oikeudet osalta käyttäjiä, jotka eivät valmisteile tai osallistu päätöksenteon valmisteluun tai tarvitse työtehtävissään pääsyä järjestelmään.

Henkilöstöä varten laadittiin henkilöstön perehdytysmateriaaliin ohjeistusta salassapidosta ja salassa pidettävien tietojen käsittelystä Salpauksessa.

Sähköisen arkistojärjestelmän käytönoton myötä tiedon käsittelyssä huomioidaan myös henkilötietoluonne sekä mm. asiakirjojen julkisuus- ja salassapito, kun asiakirjoja siirretään pysyvässäilytykseen arkistointijärjestelmään. Tietoja käsitellään lainsäädännön vaatimusten mukaisesti ja viranomaisten määräykset huomioiden.

Kuntayhtymässä on vuoden aikana laadittu tekoälypolitiikka-asiakirja tietosuojapolitiikan ja tietoturvapoliitiikan rinnalle. Tekoälyn käyttö perustuu vastuullisuuteen, läpinäkyvyyteen ja eettisiin periaatteisiin. Sen hyödyntämisessä korostetaan tietosuoja ja tietoturva, jotka varmistetaan kaikissa tilanteissa. Tekoälyä käytetään tukemaan erilaisia toimintoja, kuten opetusta, ohjausta, viestintää ja hallintoa, ja sen käyttö noudattaa kansallisia ja EU:n säädöksiä, mukaan lukien GDPR ja EU AI Act. Näin varmistetaan, että tekoälyn käyttö on lainsäädännön ja eettisten suositusten mukaista koulutuksessa.

Vuoden 2025 muita tavoitteita, joita on vuoden aikana edistetty:

- tietosuojan vaikutustenarviointien laatiminen Ilona IT Sovelluskirjastossa yhteistyössä muiden toimijoiden ja koulutuksenjärjestäjien kanssa
- esim. tietosuojan alkukartoitukset osana hankintaprosessia
- Osallistuminen valtakunnalliseen Digi- ja väestötietoviraston järjestämään TAISTO25-harjoitukseen. Harjoituksessa ilmenevien havaintojen ja mahdollisten puutteiden huomioiminen ohjeistuksessa ja toimintamalleissa

Tietoturvallisuuteen liittyvien tavoitteiden toteutumista on kuluneen vuoden aikana tarkastelu hallinnollisen tietoturvaryhmän tapaamisissa, joissa on käsitelty mm.:

- ✓ 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
- ✓ tietosuojan vaikutustenarviointi, käytänteet, lomakkeet ja tilanne
- ✓ henkilöstökoulutus: tietoturvakurssin suoritus tilanne sekä uudet tietoturvallisuuteen liittyvät koulutukset Elsa verkko-oppimisympäristössä
- ✓ valtakunnallinen TAISTO25-harjoitus
- ✓ tietotekniset tietoturvaratkaisut ja kehittämisen tilanne.

5.1.2026

3.2. Saatuja oppeja vuodelle 2026

Keväällä Helsingin kaupungin kasvatus- ja koulutusala joutui toukokuussa tietoturvaloukkauksen kohteeksi. Maamme toistaiseksi laajin hyökkäys tuotiin laajasti julkisuuteen koko koulutuskentällä. Tavoitteena oli kertoa johdonmukaisesti ja yksityiskohtaisestikin, millainen tapahtuma oli kokonaisuutena ja millaisia johtopäätöksiä voitiin hyökkäyksestä tehdä. Valtioneuvoston asettama riippumaton tutkintaryhmä laati aiheesta raportin ja järjesti yleisen tiedotustilaisuuden, jossa tutkinnan johtopäätökset julkistettiin.

Tietomurron kohteena oli laaja joukko, jopa 300 000 henkilöä. Hyökkääjän onnistui päästä Kasvatus- ja koulutussalan verkkoon pimeästä verkosta löytämänsä käyttäjätunnuksen ja salasanan avulla. Tietomurrossa vaarantui henkilötiedot, jotka olivat vuotaneissa sadoissa tuhansissa asiakirjoissa, joita hyökkääjä sai haltuunsa. Näiden joukossa oli myös erittäin arkaluonteista henkilötietoa varhaiskasvatuksesta, lastensuojelusta ja koulutuksesta. Selvityksessä ei ilmennyt tarkasti, mitä tietoja hyökkääjälle päätyi.

Tietomurto mahdollistui puutteellisesta ylläpidetyistä palvelemista, heikosta tietoturvalvonnasta ja sekavista ohjeistuksista. Tietomurtoa on käsitelty Salpauksessa ja asiaa esiteltiin myös johtoryhmälle tietoturvakatsauksen yhteydessä. Tapaus nosti esiin ennakkoinnin ja varautumisen merkityksen sekä ennakoivat toimenpiteet vastaavan tapahtuman torjumiseksi kuntayhtymässä.

Tietomurron onnistuminen johtuu harvoin yhdestä virheestä. Tietoverkkorikollisuus on kasvava rikollisuuden ala ja sen aiheuttamat haitat ovat organisaatioille merkittäviä. Julkinen hallinto kiinnostaa kohteena myös rikollisia, johtuen esim. henkilötietojen määrästä ja laadusta.

Marraskuissa TAISTO25-harjoituksessa oli jälleen kattavasti erilaisia uhkatilanteita ja harjoitteita. Harjoitteiden perusteella kiinnitämme tulevana vuonna Salpauksessa huomiota ohjeistuksen ja toimintamallien osalta mm.

- Matalan kynnyksen nopeiden suojaustoimenpiteiden kehittäminen ja ohjeistus, ylläpidolliset rajoitustoimenpiteet, joilla voidaan välttää mahdollisten poikkeamien eskaloituminen laajemmiksi ongelmiksi.
- Poikkeustilanteissa kohdennetun viestinnän nopeus ja tavoitavuus, viestintäjärjestelmät ja varajärjestelmät (mm. Secapp) sekä niihin liittyvät toimintamallit ja osaaminen.
- Jatkuvan tietoturva- ja tietosuojakoulutusten tärkeys ja niiden kattavuus henkilöstön osalta. Huomioiden erilaiset kehittyvät huijaukset ja tietojenurkinnat, sekä myös nykyaikaisten pilvipalveluiden käytön osaaminen, ettei luottamuksellista tietoa jaeta vahingossa tarpeettomasti liian laajalle.
- Toimintamallit ja ohjeet, joilla varaudutaan kehittyviin nykyaikaisiin laskutushuijauksiin.

5.1.2026

4. Tietoturvallisuuden edistäminen vuonna 2026

4.1. Tekniset tietoturvaratkaisut ja keskeiset kehittämiskohteet

Teknisten tietoturvaratkaisujen kehitys kohdentuu varautumiseen, sekä hallinnan ja havainnoinnin kehittämiseen:

- Valvonnan ja lokienhallinnan kehittäminen tekoälypohjaisilla suojausratkaisuilla
- Tietoturva-avunomistuksen (SOC) selvitystä jatketaan
- Dokumenttienhallintaratkaisun uudistaminen
- IT-ympäristön palveluiden hajauttaminen ja pilvipalvelukäyttöönnotot
- Varautumissuunnitelmien katselmointi ja päivitys

Osaamisen varmistamisen tueksi toteutetaan jatkossakin eettisen hakkeroinnin menetelmien käyttäjille ns. tietoturvaosaamistestausta, jossa herätellään ja testataan esim. kalasteluviestien tunnistamista. Menetelmää käytetään henkilöstön osaamispuutteiden havainnollistamiseen ja koulutuksen kohdentamiseen.

Salpauksen verkkoyhteyksien ja IT-palveluiden tuottaminen vaatii jatkuvaa kehittämistä, jatketaan palveluiden hajauttamista ja pilvipalveluiden käytön laajentamista, joilla parannetaan palveluiden vikasietoisuutta.

Salpauksen IT-palveluiden ja tietojärjestelmien lokienhallintaa kehitetään edelleen, hyödyntäen teknisiä ratkaisuja, jotka tarjoavat asiantuntijoille työkaluja poikkeuksien havainnointiin jatkuvasta lisääntyvästä lokimäärästä, sekä toimenpiteiden automatisointiin.

Uudistetaan organisaation dokumenttienhallintaratkaisu ja toimintamalleja. Nykyaikaisella ratkaisulla saadaan tietoturvaominaisuuksia, joilla parannetaan uhkilta suojautumista sekä havainnointia sekä tiedonhallintaa koko elinkaaren osalta.

IT-varautumissuunnitelmien kartoitus ja päivitys. Kerätään IT-ympäristöön liittyvät varautumissuunnitelmat ja dokumentaatiot, päivitetään materiaali tarvittavilta osin ja varmistetaan suunnitelmien käytettävyyttä myös poikkeustilanteissa (paperiversio).

TAISTO 2025-harjoituksessa tunnistetut kehityskohteet toimintamalleihin ja ohjeistuksiin

- Organisaation palveluihin kirjautumisen estäminen ulkomailta (EU-maiden ulkopuolelta). Laaditaan tarvittava ohjeistus ja väliaikaisia tunnuskohtaisia poikkeuksia ulkomaille suuntautuvia matkustamista varten.
- Secappin viestintäratkaisun käytön varmistaminen
 - Ohjelman käytön ja toimivuuden säännöllinen testaus koko henkilöstöllä
 - Ohjeistuksen päivittäminen, sekä palvelun käytettävyyden varmistaminen poikkeustilanteissakin
- Henkilöstön tietoturvakoulutus ja osaamisen varmistaminen
 - Henkilöstön pakollinen joka vuotinen tietoturvakoulutus /-perehdytys
- Toimintamallit laskutushuijauksiin
 - mm. soittovarmistus matkapuhelimella aina epäilyttävän maksumääräyksen tekijälle, maksuhyväksynnät aina useamman henkilön toimesta

5.1.2026

- Pilvipalveluiden tiedonhallinta, erityisesti ylijakamisen ehkäiseminen
 - Käyttäjien ohjeistus ja koulutukset palveluiden käytössä. Mahdolliset ylläpidolliset rajoitukset ja oletusjakoasetuksien tiukentaminen.

4.2. Tietoturvatapahtumat vuonna 2025

Tekninen tietoturvaryhmä raportoi säännöllisesti hallinnolliselle työryhmälle vuosineljänneksittäin tapahtuneista tietosuojaa ja -turvaa koskevista toimista.

Osa-alueet	Q1	Q2	Q3	Q4	Yhteensä
Hallinnollinen tietoturva					
Fyysinen tietoturva					
Laitteistoturvallisuus					
Ohjelmistoturvallisuus	2			2	4
Tietoaineiston turvallisuus	1				1
Tietoliikenneturvallisuus	1			1	2
Henkilöstöturvallisuus	14	14	17	8	53
Käyttöturvallisuus	5	4	6	6	21

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

Henkilöstöturvallisuuden sisältämä luku pitää sisällään yksittäisiä neuvonta- ja tiedotustapahtumia. Tapahtumat liittyvät esimerkiksi erilaisiin roskasähköpostiviesteihin, ajankohtaisiin tietoturvaa koskeviin haavoittuvuusilmoituksiin ja erilaisiin tietojenkalastelukampanjoihin, joista henkilöstöä tiedotetaan tarpeen mukaan.

Määrällisesti eniten tapahtumia on kohdistunut henkilöstöturvallisuuteen. Lukeman kasvu selittyy myös tietoturvatietoisuuden ja valppauden lisääntymisestä. Kokonaismäärässä ei kuitenkaan ole tapahtunut merkittävää muutosta.

5. Tietosuojatyön tavoitteet vuodelle 2026

5.1. Havaittuja kehittämistarpeita

Hallinnollinen tietoturvaryhmä tarkastelee yleisiä tietosuojaan ja tietoturvallisuuteen liittyviä toimenpiteitä ja nostaa esiin kehittämiskohteita. Säännöllinen eri kanavien seuranta (mm. Kuntaliitto, Digi- ja väestötietovirasto, Kyberturvallisuuskeskus, Tiedonhallintalautakunta) kuuluu osana tietosuoja- ja tietoturvatyöhön.

5.1.2026

Vuonna 2026 osallistutaan aiempaan tapaan valtakunnalliseen Digi- ja väestötietoviraston järjestämään TAISTO26-harjoitukseen. Harjoitus tuottaa mm. kehittämistarpeita toimintamallien jatkuvaan parantamiseen ja havainnoimaan puutteita myös tietosuojatyössä.

Tietosuoja on jatkuvaa toimintaa, joka vaatii seurantaan henkilötietojen käsittelyn parantamiseksi ja erilaisten uhkien huomioimiseksi ja torjumiseksi. Tietosuojan vaikutustenarviointien laatiminen parantaa myös tätä tavoitetta, kun mahdolliset riskit voidaan ajoissa kartoittaa.

Henkilöstön osaaminen on yksi keskeisimmistä tavoitteista tietosuojan edistämisessä, jota vahvistetaan myös vuonna 2026 parantamalla henkilöstölle aikaisemmin laadittua koulutusmateriaalia Elsa-verkkoympäristössä.

5.2. Tietosuoja on tiedonhallintaa

Tietosuoja on osa tiedonhallintaa, jonka ympärillä on vahva eri lakien muodostama säädösverkosto. Viime vuosien aikaisen lainsäädännön ja erityisesti tietosuojalainsäädännön ja julkisuuslakiuudistuksen vaikutukset heijastuvat henkilötietojen käsittelyyn.

Tietojen käsittelyssä tulisi keskeisten prosessien osalta tarkastella mm.:

- Mitä tietoa käsitellään: julkista vai salassa pidettävää
- miten henkilötiedot on huomioitu,
- mihin tarpeeseen tietoja käsitellään,
- mihin tietoja tallennetaan,
- mikä on tiedon elinkaari,
- ketkä tietoa käsittelevät,
- miten tiedonkäsittelyn vastuut jakautuvat.

Ei siis ole riittävää rajata tietojen käsittelyä pelkästään tietosuojasääntelyn varaan.

Julkisuudessa esiintyy yhä useammin erilaisia otsikoita tietosuojaan ja tietosuojarikkomuksiin liittyen. Myös Tietosuojavaikuttetun ohjeiden lisääntyminen on merkki tietosuojaloukkausten ja -rikkomusten kasvusta. Varsinaisista ammatilliseen koulutukseen liittyviltä oikeustapauksilta on toistaiseksi välttytty.