Tietotilinpäätös

2025

Julkinen

2025

Sisällysluettelo

1 Tietotilinpäätöksen tarkoitus ja säädösperusta

Tietotilinpäätöksen tarkoituksena on antaa Kokkolan kaupungin kokonaiskuva henkilötietojen käsittelyyn liittyvästä tietosuojan, tietoturvan ja tiedonhallinnan tilasta vuonna 2025. Tietotilinpäätös toimii samalla tärkeänä osana EU:n yleisen tietosuoja-asetuksen (EU 2016/679, jäljempänä tietosuoja-asetus) 5. artiklan osoitusvelvollisuuden toteutumista. Osoitusvelvollisuus tarkoittaa sitä, että organisaation pitää pystyä osoittamaan noudattavansa tietosuoja-asetusta henkilötietojen käsittelyssä sekä toteuttavansa tietosuojaperiaatteita myös käytännössä. Tietotilinpäätöksen avulla kaupunki voi näyttää, että se noudattaa myös muita tietoturvaa ja tietosuojaa määrittäviä periaatteita.

Yksi tapa osoitusvelvollisuuden toteutumista on dokumentointi: tietotilinpäätöksessä pyritään osoittamaan, että tietosuoja- ja tietoturvaperiaatteet ja henkilötietoihin liittyvät prosessit ovat kunnossa.

Henkilötietojen suojaamistoimenpiteitä toteutetaan tietoturva-toimenpiteillä. Vuonna 2019 voimaan tullut tiedonhallintalaki eli laki julkisen hallinnon tiedonhallinnasta 906/2019 on ainoa laki, joka säätää tietoturvan toteuttamisen toimenpiteistä. Tiedonhallintalain 2. pykälän 8. kohdan mukaan *tietoturvallisuustoimenpiteillä* tarkoitetaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Lisäksi kohdan 9. mukaan *tiedonhallinnalla* tarkoitetaan viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvia toimia ja tietoturvallisuustoimenpiteitä viranomaisen tietoaineistojen, niiden käsittelyvaiheiden ja tietoaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaineistojen tallentamistavasta ja muista käsittelytavoista. Tiedonhallintalain mukaiset vaatimukset on huomioitu 2024 päivitetyssä Kokkolan kaupungin hallintosäännössä.

Tietosuojalaki (105/2018) on kansallinen laki, joka täsmentää ja täydentää EU:n yleistä tietosuoja-asetusta. Tietosuojalaki määrittää kansallisen tietosuojavaltuutetun nimittämisestä ja sen toimivaltuuksista. Laissa säädetään myös muun muassa erityisten henkilötietoryhmien käsittelystä, henkilötunnusten käsittelystä ja lapsiin sovellettavasta ikärajasta tietoyhteiskunnan palveluita tarjottaessa.

2 Tietoturvan ja tietosuojan järjestäminen

2.1 Kaupunginhallitus

Hallintosäännön 59 a pykälän mukaiset tiedonhallinnan tehtävät.

Kokkolan kaupunki on tiedonhallintalain mukainen tiedonhallintayksikkö. Kaupunginhallitus toimii tiedonhallintayksikön johtona.

Kaupunginhallitus vastaa siitä, että tiedonhallintalain 4.2 §:n vastuut, käytännöt ja valvonta on määritelty kaupungissa.

Tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut ovat:

1.vastuu tiedonhallintalain mukaisten kuvausten koostamisesta ja ylläpidosta (tiedonhallintamalli (5 §), muutosvaikutusten arviointi (5 §) ja asiakirjajulkisuutta koskeva kuvaus (28 §).

2.vastuu 19 §:ssä säädetystä tietoaineistojen sähköiseen muotoon muuttamisesta ja saatavuudesta.

3.vastuu tietoturvallisuusjärjestelyistä, tietojärjestelmien toiminnasta ja yhteentoimivuudesta sekä tietovarantojen yhteentoimivuudesta (2 §:n 13 kohta, 5 §, 12–17 §, 22–24 §)

4.vastuu asianhallinnan ja palvelujen tiedonhallinnan järjestämisestä sekä tietoaineistojen säilyttämisen järjestämisestä (21 §, 25–27 §).

2.2 Kaupungin johtoryhmä mukaan lukien kaupunginjohtaja

Tietoturva ja tietosuojatyön toteuttamisen kokonaisvastuu on kaupungin johdolla, ja kaupunginjohtaja vastaa ja valvoo tietoturvan ja tietosuojan järjestämisestä. Johto myös varmistaa työlle riittävät resurssit. Johdon linjaukset sekä tietosuojan että tietoturvan osalta näkyvät kaupungin tietoturvapolitiikassa, joka hyväksyttiin kaupunginhallituksessa toukokuussa 2020.

Tietoturvavastaava ja tietosuojavastaava raportoivat kaupungin johtoryhmälle tietoturvan ja tietosuoja toteutumisesta sekä mahdollisista riskeistä ja poikkeamista.

2.3 TT/TS eli tietoturva- ja tietosuojaryhmä

Kaupungilla on noin kahden kuukauden välein kokoontuva tietoturva-/tietosuojaryhmä eli TT/TS-ryhmä, joka käsittelee ajankohtaisia tietoturvaan ja tietosuojaan liittyviä aiheita ja linjaa kaupungin tietoturva- ja tietosuojatyötä johdon politiikan mukaisesti. Ryhmä voi antaa suosituksia, tehdä tiedotteita, viedä tärkeitä asioita johtoryhmälle ja valvoa tietosuojan ja –turvan toteutumista kaupunkiorganisaatiossa. Ryhmään kuuluu edustus keskeisiltä toimialoilta ja tukipalveluista sekä tarvittaessa kutsuttuja asiantuntijoita. Tietosuoja-/tietoturvaryhmän kokoonpanoa päivitetään jatkuvasti.

2.4 Tietoturvavastaava

Kokkolan kaupungille on nimetty tietoturvavastaava, joka on määritelty tietohallintopäällikön tehtäviin.

Vuoden 2020 tietoturvapolitiikassa on lueteltu tietoturvavastaavan tehtävät, joka on hyväksytty kaupunginhallituksessa 8.6.2020 pykälällä 289. Sen mukaan tietoturvavastaavan tehtäviin kuuluu seuraavat osiot

-Tietoturvavastaava vastaa organisaation tietoturvallisuustason määrittelystä ja arvioinnista

- raportoida esimiehelle (talousjohtaja) ja tarvittaessa kaupungin johdolle tietoturvaan liittyvistä muutoksista ja poikkeamista

-toimii tietoturva-/tietosuoja ryhmän eli TT/TS puheenjohtajana

-vastaa tietoturvasuunnitelmien tekemisestä, tietoturvatyön toteutuksesta sekä valvonnasta

- edistää tietoturvatietouden levittämistä ja tietoturvallisesta toimintatavasta toimintayksikössä ja sen ostamissa palveluissa, sekä raportoinnista johdolle

Operatiivisella tasolla toiminnasta vastaa vastuualueen päällikkö. Kaupungin tietoturvavastaava ja talousjohtaja seuraavat lainsäädännön muutoksia ja ohjeistavat tarvittavat muutokset johdolle ja henkilöstölle.

Tietoturvavastaava eli tietohallintopäällikkö kuuluu talous- ja tietohallintopalveluiden alaisuuteen. Talous- ja tietohallintopalveluille kuuluu huolehtia Konsernihallinnon ja-palvelujen toimintasäännön (hyväksytty kaupunginhallituksessa 16.12.2024/§525) mukaisesti kaupungin tietohallinto- ja tietoliikennepalvelujen kehittämisestä ja tuottamisesta. Toimintasäännön mukaan tietohallintopäällikkö huolehtii kaupungin tietohallinto- ja tietoliikennepalvelujen tuottamisesta ja kehittämisestä sekä huolehtia ja kehittää kaupungin tietoturva ja tietosuoja-asioita.

On huomioitava, että tietosuojasäännösten ja tietoturvaohjeiden noudattaminen on jokaisen rekisterinpitäjän vastuulla, eikä tietoturvavastaava ole henkilökohtaisessa vastuussa asetuksen tai lain rikkomisesta.

2.5 Tietosuojavastaava

Kokkolan kaupungille on nimetty tietosuoja-asetuksen mukainen tietosuojavastaava (data protection officer) joka on määritelty tiedonhallinnan asiantuntijan tehtäviin. Tietosuojavastaava on organisaation sisäinen, riippumaton asiantuntija. Tietosuojavastaavan tehtävänä on toimia yhteyshenkilönä sekä rekisteröidyille että tietosuojavaltuutetulle.

Tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa. Tietosuojavastaava on otettava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn ja kehittämiseen, esimerkiksi, kun suunnitellaan tai kehitetään tietojärjestelmiä.

Vuoden 2020 tietoturvapolitiikassa on lueteltu tietosuojavastaavan tehtävät, joka on hyväksytty kaupunginhallituksessa 8.6.2020 pykälällä 289.

Tietosuojavastaavan tehtäviin kuuluu yllä mainitun lisäksi:

- seurata tietosuojasääntöjen noudattamista organisaatiossa ja tuoda esiin mahdollisia puutteita.

-antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille

-antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarvioinnin toteutusta

-on rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa

-on tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa.

Tietosuojavastaava eli tiedonhallinnan asiantuntija kuuluu kaupunginkanslian alaisuuteen. Konsernihallinnon ja -palveluiden toimintasäännön (hyväksytty kaupunginhallituksessa 16.12.2024/§525) mukaisesti tiedonhallinnan ohjaus kuuluu kaupunginkanslialle.

Tietosuojavastaava raportoi kaupungin johtoryhmälle tietosuojan toteuttamisesta ja mahdollisista riskeistä. Kaupungin tietosuojavastaavat ja hallintojohtaja seuraavat tietosuojalainsäädännön muutoksia ja ohjeistavat tarvittavat muutokset johdolle ja henkilöstölle. Tietosuoja-asetuksen 24 artiklan 1 kohdan mukaan johdon tulee rekisterinpitäjän vastuulla toteuttaa rekisterinpitäjälle kuuluvat tarvittavat tekniset ja organisatoriset toimenpiteet, joilla se voi varmistaa sekä osoittaa, että se

rekisterinpitäjänä noudattaa henkilötietojen käsittelyssä tietosuoja- asetusta. Operatiivisella tasolla toiminnasta vastaa vastuualueen päällikkö.

Tietosuojasäännösten ja tietoturvaohjeiden noudattaminen on jokaisen rekisterinpitäjän vastuulla, eikä tietosuojavastaava ole henkilökohtaisessa vastuussa asetuksen tai lain rikkomisesta.

2.6 Tietohallinto

Tietohallinto on vastuussa kaupungin IT-ympäristön teknisestä tietoturvasta. Kaupungin IT-laitteissa hyödynnetään yhtenäisiä ja keskitetysti hallittuja tietoturvaratkaisuja, jotka takaavat järjestelmien suojauksen ja toimintavarmuuden. Tietohallinnon rooli on jatkuvasti kehittyvä, ja sen merkitys korostuu erityisesti digitalisaation ja teknologian nopean kehityksen myötä. On tärkeää, että tietohallinto toimii tiiviissä yhteistyössä toimialueiden kanssa ja tukee organisaation strategisia tavoitteita.

2.7 Toimialajohtajat, esihenkilöt

Toimialajohtajien ja esihenkilöiden vastuut ja tehtävät ovat kuvattu kaupungin sisäisessä tietosuoja- ja tietoturvaohjeistuksessa *henkilötietojen käsittelyn yleisohje* sekä *tietosuojan muistilista esihenkilöt*. Ohjeet löytyvät kaupungin sisäisestä Intranetistä.

Tukea ja ohjausta henkilötietojen oikeaoppiseen käsittelyyn Kokkolan kaupungilla saa omalta esihenkilöltä sekä tietosuojavastaavalta. Esihenkilöt ovat vastuussa siitä, että alaiset saavat riittävän koulutuksen ja perehdytyksen henkilötietojen käsittelyyn. Osa verkkokursseista on sellaisia, joiden suorittamista valvotaan, jolloin voidaan osoittaa organisaation huolehtineen kouluttamisvelvollisuudesta. Toimi- /palvelualueet huolehtivat oman alansa substanssi- ja lainsäädäntöosaamisesta ja kouluttavat ja ohjeistavat henkilöstön paitsi organisaation yhteisiin, myös aluetta koskeviin tarkempiin henkilötietojen käsittelyohjeisiin. Esihenkilön tehtävänä on myös varmistaa, että alaisilla on käytössään riittävä ohjeistus työtehtäviensä suorittamiseen tietosuojalainsäädännön mukaisesti.

Toimialajohtajat tai esihenkilöt valvovat ja kartoittavat mihin tietoihin ja tietojärjestelmiin työntekijällä on pääsyoikeus. Työntekijällä tulee olla oikeus tietojen käsittelyyn vain silloin, kun siihen on olemassa peruste. Tietoja saa käsitellä vain siinä käyttötarkoituksessa ja laajuudessa kuin on välttämätöntä. Tämän lisäksi myönnettävät pääsyoikeudet riippuvat henkilön roolista.

Kun työntekijä siirtyy organisaation sisällä toiseen rooliin tai kokonaan organisaation ulkopuolelle, on esihenkilön huolehdittava käyttöoikeuksien muokkaamisesta tai poistamisesta.

Uuden työntekijän aloittaessa esihenkilö ohjeistaa työntekijää tutustumaan käyttäjäsitoumukseen, jonka työntekijä allekirjoittaa. Käyttäjäsitoumus sisältää

1. salassapito- ja vaitiolovelvollisuus

2. käyttäjätunnukset ja salasanat

3. työaseman käyttö

4. sähköpostin ja internetyhteyksien käyttö

5. tietosuoja- ja tietoturvaohjeet

6. rikkomusten seuraamukset.

Tietosuoja-asetuksen 24 artiklan 1 kohdan mukaan johdon tulee rekisterinpitäjän vastuulla toteuttaa rekisterinpitäjälle kuuluvat tarvittavat tekniset ja organisatoriset toimenpiteet, joilla se voi varmistaa sekä osoittaa, että se rekisterinpitäjänä noudattaa henkilötietojen käsittelyssä tietosuoja- asetusta. Operatiivisella tasolla toiminnasta vastaa vastuualueen päällikkö.

2.8 Pääkäyttäjät

Jokaisella tietojärjestelmällä on omistajayksikkö ja järjestelmän/sovelluksen vastuuhenkilö (pääkäyttäjä). Tietojärjestelmän vastuuhenkilön velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten (esim. kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn) määrittely.

Tietojärjestelmien omistaja nimeää pääkäyttäjät kaikille järjestelmille. Pääkäyttäjät vastaavat järjestelmien sisäisten käyttöoikeuksien hallinnasta. Käyttövaltuudet myönnetään henkilökohtaisesti ja ainoastaan niihin tietoihin, jotka ovat välttämättömiä työn suorittamiseksi. Tietojärjestelmän pääkäyttäjän velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asettavien vaatimusten (esim. kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn) määrittely.

2.9 Henkilöstö

Tietosuoja ja tietoturva on jokaisen viranhaltijan ja työntekijän vastuulla. Työntekijöiden vastuut on kuvattu kaupungin sisäisessä tietosuoja- ja tietoturvaohjeistuksessa *henkilötietojen käsittelyn yleisohje sekä tietosuojan muistilista työntekijät* ja *tietosuojan muistilista asiakaspalvelu.* Ohjeet löytyvät kaupungin Intranetistä. Kukin työntekijä (mukaan lukien harjoittelija, opiskelija, työllistetty jne.) vastaa roolissaan siitä noudattaa salassapitoa ja vaitiolovelvollisuutta koskevia säädöksiä. Sisäinen ohjeistus tarjoaa tietoa tiedon turvallisesta käsittelystä ja säilyttämisestä.

Jokainen työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteuttamisesta sekä tietoturvaohjeiden noudattamisesta. Jokainen henkilö on velvollinen tietoturvaan/tietosuojaan liittyvien uhkien ja poikkeamien raportoimisesta. Ilmoituksen voi tehdä omalle esihenkilölle, tietoturvavastaavalle tai tietosuojavastaavalle.

3 Lainsäädäntö, lailliset perusteet ja muu ohjeistus

Kokkolan kaupunki noudattaa viranomaistyössään tietosuoja- asetusta, tietosuojalakia sekä tiedonhallintalakia osana viranomaisvelvoitteita.

Tietosuoja-asetuksen myötä kansalaisilla on oikeus tarkistaa hänestä tallennetut tiedot, tarvittaessa korjata ne tai vaatia tietojen poistamista rekisteristä. Kansalainen voi myös vastustaa henkilötietojensa käsittelyä ja estää automaattinen päätöksenteko tietyin edellytyksin. Näihin liittyvät lomakkeet löytyvät Kokkolan kaupungin tietosuojasivulta.

Tietosuoja-asetuksen mukaan henkilötietojen käsittelylle pitää löytyä laillinen peruste. Laillinen peruste voi olla

-rekisteröidyn suostumus

-sopimus

-rekisterinpitäjän lakisääteinen velvoite

-elintärkeiden etujen suojaaminen

-yleistä etua koskeva tehtävä tai julkinen valta

-rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.

Kokkolan kaupungin tietosuojaohjeet on laadittu voimassa olevan lainsäädännön mukaisesti. Henkilöstön käytössä ovat seuraavat ohjeet:

-tietosuojan muistilista työntekijälle

-tietosuojan muistilista asiakaspalveluun

-tietosuojan muistilista esimiehille

-henkilöstön tietoturvaohje

-henkilötietojen käsittelyn yleisohje

-tietoturvapolitiikka (päivitetty vuonna 2020, jolloin laajennettiin tietosuojaosiota)

-tietoturvaohje pähkinänkuoressa henkilöstö

-tiedonhallinnan toimintaohje- asiakirjahallinto ja arkistointi

4 Ajankohtaisia asioita

4.1 Taisto- harjoitus

Vuonna 2025 tietosuoja- ja tietoturvaryhmän (TT(TS) jäsenet sekä viestintä ja osa johtoryhmän jäsenistä osallistuttiin valtakunnalliseen Taisto-harjoitukseen, jossa käsiteltiin mm. tunnusten kalastelua, haittaohjelmatilannetta, haavoittuvuuden kiireellistä paikkausta sekä käyttöoikeuspoikkeamaa pilvipalvelussa. Harjoitus vahvisti valmiuksia havaita, raportoida ja hallita häiriötilanteita.

Taisto-harjoitus eteni totutun intensiiviseen tahtiin, ja ryhmälle saapui uusia tehtäviä tiiviissä tahdissa. Viestintäkanavien kautta välitetyt vaatimukset ja toimenpidepyynnöt vaihtelivat sisällöltään ja kiireellisyydeltään. Sosiaalisessa mediassa havaittiin maalittamisilmiöitä, ja erilaisissa huijausyrityksissä oli tyypillisesti kiireellisyyttä ja painetta nopeisiin ratkaisuihin. Kokonaisuutena harjoitus asetti työntekijöiden harkintakyvyn ja työprosessien huolellisuuden erityisen tarkastelun kohteeksi.

Jokaisen harjoituskokonaisuuden keskeinen piirre oli tilanteen asteittainen laajeneminen: Alkuperäinen tilanne kehittyi nopeasti moniulotteiseksi ja haastavaksi kokonaisuudeksi. Tilanteen hallinta edellytti osallistujilta kärsivällisyyttä, paineensietokykyä sekä kykyä erottaa olennaiset tiedot harhaanjohtavasta informaatiosta. Kapeakatseinen tai yksipuolinen lähestymistapa ei palvele tarkoitustaan monimutkaisissa ja nopeasti muuttuvissa tilanteissa.

Taisto-harjoituksissa on useasti korostunut tietohallinnon merkitys häiriötilan akuutissa vaiheessa. Häiriöiden tehokas hallinta edellyttää keskittymistä olennaisten toimintojen turvaamiseen ja vähemmän kriittisistä asioista voidaan tarvittaessa tinkiä tilanteen vakauttamiseksi mahdollisimman nopeasti.

Harjoitusten aikana havainnoitiin muun muassa seuraavia seikkoja:

1. Tietohallinto on häiriötilanteen alkuvaiheessa keskeisessä roolissa: olemassa oleva häiriö pyritään minimoimaan mahdollisimman nopeasti ensisijaisilla torjunta- ja rajaamistoimilla.
2. Kaupungin viestinnän tulee olla yhtenäistä, keskitettyä ja ennalta harjoiteltua. Esimerkiksi lehdistötiedotteet laaditaan vakiomallin mukaan ja ylimääräisiä spekulatiivisia kommentteja tulee välttää.
3. Deepfake-teknologiaa hyödynnetään yhä enemmän huijauksissa. Tämä tulee ottaa huomioon ja käyttää ennalta sovittuja vahvistusmenettelyjä.
4. Kiireeseen ei tule reagoida kiirehtimällä: jos jokin herättää epäilyksiä ja siihen liitetään painetta nopeisiin toimiin, kyseessä on suurella todennäköisyydellä huijaus.

4.2 Tietosuojadokumentaatio

Tietosuojan ja tietoturvan hallintajärjestelmä mahdollistaa tiedonhallintalain ja tietosuoja- asetuksen monipuolisen dokumentaatiotyön. Kaupungin johtoryhmässä käsiteltiin dokumentaatiossa havaittavia etenemishaasteita. Haasteiden selättämiseksi tietohallinnossa laitettiin alkuun Kick Off- tyylinen projekti. Projektin alkuvaiheessa tehdään käyttöjärjestelmän toiminnallisuus mahdollisimman tutuksi. Projektin etenemisestä raportoidaan sen edetessä.

Dokumentaatio työn lisäksi on viety useita tiedonohjauksen projekteja eteenpäin. Vuonna 2025 valmistui päivitetty tiedonhallinnan toimintaohje alaotsikolla asiakirjahallinto ja arkistointi. Kyseisen toimintaohjeen ensisijaisena painopisteenä on tiedon elinkaaren hallinta, eikä se varsinaisesti käsittele laajemmin tietoturvaan tai tietosuojaan liittyviä toimenpiteitä. Tiedonhallintaohje ohjeistaa toimialoja huolehtimaan tiedon elinkaaren kuvausvelvoitteista, johon kuuluvat tiedonohjaussuunnitelma ja arkistonmuodostussuunnitelmat. Kyseiset elinkaarikuvaukset ovat osana tietoturvallista viranomaistoimintaa.

Vaikutuksenarviointi dokumentaatiovelvoitteiden täyttämiseksi organisaatioon on otettu käyttöön uusi ohjelmisto. Tämän avulla valmistui vuoden 2025 aikana yksi vaikutustenarviointi, ja aloitettiin kaksi. Kaupungin tietosuojavastaava ja tietohallintopäällikkö osallistuvat ohjelmistotoimittajan järjestämään työpajatoimintaan M365 Copilotin osalta.

Myös tiedonhallintalain velvoitteiden piiriin kuuluva kaupungin asiakirjajulkisuuskuvaus päivitettiin vastaamaan nykytilaa. Kuvauksesta puuttui työllisyyspalvelu ja kotoutumisen palvelu- /tietovarantokuvaus.

4.3 Henkilöstön kouluttaminen

Vuonna 2025 kaupungin koulutuspalvelut siirrettiin uudelle alustalle, joka korvasi aiemman eOppiva-palvelun. Kaikki työntekijöiden koulutukset ja oppimissisällöt hallinnoidaan uuden palvelun kautta.

Kaikkien kaupungin työntekijöiden tuli suorittaa Tietoturva julkishallinnossa 2025 -koulutus. Koulutuksen tavoitteena on varmistaa ajantasainen osaaminen tietoturvan periaatteista ja käytännöistä.

Koulutuksen suorittamisen jälkeen työntekijät raportoivat suorituksen omalle esihenkilölleen. Esihenkilöt vastasivat suoritusten kirjaamisesta henkilöstöhallinnon järjestelmään. Esihenkilöiden vastuulla oli varmistaa, että kaikki tiimin jäsenet suorittivat koulutuksen määräajassa.

Kaupungin Intranet sisältää useita kategorioita, joissa kaupungin henkilöstö voi tutustua tiedonhallinnan ja tietosuojan ohjeistukseen.

Toimialueita kannustetaan osallistumaan oman substanssinsa tietoturva- ja tietosuojakoulutuksiin.

4.4 Muita ajankohtaisia asioita

Työllisyyspalvelujen tietosuojaverkosto ja ohjeistus henkilöstölle

Tietosuojavastaava ja työllisyyspalveluiden asiantuntija osallistuivat vuonna 2025 lanseerattuun työllisyysalueiden tietosuojavastaavaverkostoon. Tietosuojavastaavien verkosto kokoaa ympäri Suomea vastuukuntien tietosuojavastaavat ja työllisyyspalvelun tai työllisyysalueen tietosuojayhteyshenkilöt sekä KEHA-keskuksen tietosuojavastaavan. Verkoston tarkoituksena on edistää yhtenäisiä toimintatapoja henkilötietojen käsittelyssä ja rekisteröityjen oikeuksien toteuttamisessa työllisyysalueilla. Kerran kuukaudessa kokoontuva asiantuntijajoukko käy asialistan perusteella läpi ajankohtaisia aiheita. Verkostotoiminnan puitteissa kehitetään tietosuojakäytäntöjä sekä osallistutaan yhteisen tietosuojaohjeistuksen laatimiseen.

Verkostotoiminnan yhteydessä vuonna 2025 syksyllä päätettiin aloittaa Kokkolan kaupungin vastuukuntaroolin myötä Keski-Pohjanmaan työllisyysalueen tietosuoja- ja tietoturvaohjeistus. Ohjeistus laaditaan yhteistyössä kaupungin tietosuojavastaavan ja työllisyyspalveluiden asiantuntijoiden kanssa. Ohjeistuksen kohderyhmänä ovat Keski-Pohjanmaalla työllisyyspalveluissa työskentelevä henkilöstö. Kyseinen ohjeistus tuo esille rekisterinpitäjän velvollisuutta viranomaistoiminnassa ja kaupungin sisäisen ohjeistuksen mukaisesti tuo esille jokaisen viranhaltijan ja työntekijän velvollisuutta aktiivisena toimijana tietosuojan parissa.

Tiedonhallintalautakunnan selvityspyyntö työvoimapalveluille

Vuonna 2025 tiedonhallintalautakunta lähetti selvityspyynnön Kokkolan kaupungin työvoimapalveluille, jonka aiheena oli tiedonhallintalain 5 §:ssä säädettyjen muutoksenvaikutuksen arvioinnin ja tiedonhallintamallin ylläpidon toteuttamisesta työvoimapalveluiden uudistuksessa. Työllisyysjohtaja, tietohallintopäällikkö ja tiedonhallinnan asiantuntija koostivat omista substanssista käsin vastaukset tiedonhallintalautakunnalle. Selostuksessa kuvattiin ajantasainen kuvaus ajantasaisesta tiedonhallintadokumentoinnista. Selvityksessä kuvattiin palvelun tiedonhallinnan ja tietoturvan järjestämisen periaatteet sekä keskeiset hallinnolliset ja tekniset kontrollit vaaditulla tasolla. Selvityksessä kuvattiin myös työllisyyspalveluiden henkilöstöä koskeva tietoturvan ja tietosuojan koulutusvelvollisuutta.

Varhaiskasvatuksen sähköinen arkistointi

Kokkolan kaupungin varhaiskasvatuksen toimialalla on vuoden 2025 aikana aloitettu valmistelut varhaiskasvatuksen tietojärjestelmän asiakirjojen ja hakemusten siirtämiseksi sähköiseen arkistointiin. Tavoitteena on parantaa tietojen hallintaa sekä varmistaa asiakirjojen lainmukainen käsittely, säilytys, arkistointi ja hävittäminen. Käyttöönotto on suunniteltu vuodelle 2026.

Digiturvan kokonaiskuvapalvelu

Kokkolan kaupunki päivitti keväällä 2025 tietonsa Digiturvan kokonaiskuvapalveluun, joka tukee julkisia organisaatioita digiturvallisuuden arvioinnissa, seurannassa ja raportoinnissa. Palvelun avulla voi luoda tilannekuvia johdolle ja suunnitella jatkotoimenpiteitä digitaalisen turvallisuuden parantamiseksi. Palvelu tuottaa myös vertailutietoa toimialan ja kokoluokan muiden organisaatioiden sekä koko julkisen hallinnon tilanteesta.

Digitaalisten palveluiden ensisijaisuus askeleet

Hallitusohjelman mukaisesti Suomi siirtyy asteittain digitaalisten palveluiden ensisijaisuuteen viranomaisviestinnässä. Vuoden 2026 alusta alkaen viranomaisposti toimitetaan ensisijaisesti digitaalisesti kaikille, jotka asioivat sähköisesti. Ne, jotka eivät voi käyttää digipalveluita, saavat jatkossakin viranomaispostin paperilla, elleivät itse valitse toisin.

Kokkolan kaupungilla on jo osassa järjestelmistä mahdollisuus digitaaliseen viestintään.

Oppilashallinnon kokonaishallintojärjestelmä

Vuonna 2025 Oppilashallinnon -järjestelmään otettiin käyttöön kaksivaiheinen kirjautuminen. Järjestelmän käyttöoikeudet on tarkistettu ja uusien käyttäjien osalta varmistettu, että oikeudet myönnetään vähimmäisperiaatteen mukaisesti, eikä työtehtäviin nähden ylimääräisiä oikeuksia anneta.

Kriittinen infra

Kaupunkiympäristön toimialalla on toteutettu Kuntaliitolta saatujen ohjeistusten mukaisesti paikkatietojen suojaamiseen liittyviä toimenpiteitä kohdentuen kriittisen infraan. Kaupunkiympäristön toimiala on edistänyt myös muita yhteisiä sekä sisäisiä käytäntöjä aiheeseen liittyen.

5 Tietoturvapoikkeamien prosessi

Kaupungin henkilöstöllä on velvollisuus ilmoittaa mahdollisesta tietosuojaloukkauksesta tietosuojavastaavalle. Tietosuojavastaava arvioi tilanteen ja tekee tarvittaessa yhteistyössä rekisterinpitäjän kanssa ilmoituksen kansalliselle tietosuojavaltuutetulle sekä rekisteröidylle. Ilmoitukset tehdään lainsäädännön edellyttämissä määräajoissa. Organisaatiolla on toimintaprosessikuvaukset tietosuoja- ja tietoturvapoikkeamien käsittelyyn sekä lakisääteisiin ilmoituksiin.

6 Riskienhallinta sekä toiminta häiriötilanteissa

Riskienhallinta on olennainen osa organisaation tietoturvan ja tietosuojan varmistamista. Sen tavoitteena on tunnistaa, arvioida ja hallita tietoon liittyviä riskejä, jotka voivat vaikuttaa toimintaan, sidosryhmiin ja lainsäädännön vaatimuksiin.

Riskienhallinta on jatkuva ja systemaattinen prosessi, joka sisältyy kaikkiin organisaation toimintoihin. Se tukee päätöksentekoa, parantaa tietojen käsittelyn turvallisuutta ja varmistaa, että tietoja suojataan asianmukaisesti.

Vuoden aikana on toteutettu tietoturva- ja tietosuojariskien arviointeja sekä haavoittuvuustarkastuksia. Lisäksi tietoturva- ja tietosuojakoulutuksia on järjestetty osana organisaation jatkuvaa kehittämistä. Koulutuksilla on pyritty vahvistamaan henkilöstön osaamista ja valmiuksia tunnistaa sekä torjua tietoturvariskejä.

Häiriötilanteet ovat olennainen osa organisaation toimintaympäristöä, ja niiden ennakoiminen on keskeinen osa riskienhallintaa. Häiriötilanteilla viitataan tilanteisiin, joissa organisaation normaalit toiminnot keskeytyvät tai niihin kohdistuu merkittäviä häiriöitä. Tällaisia tilanteita voivat olla esimerkiksi tietoturvaloukkaukset, järjestelmäviat, palvelukatkokset tai lainsäädännön muutoksista johtuvat haasteet. Vuonna 2025 on parannettu dokumentaatio liittyen kyberhäiriö ja varautumisohjeisiin.

Riskienhallintajärjestelmänä käytetään organisaation kokonaisvaltaiseen riskienhallintaan tarkoitettua ohjelmistoa, joka auttaa tunnistamaan liiketoiminnan riskejä, arvioimaan niiden vaikutuksia sekä seuraamaan riskien käsittelyä. Työkalu pohjautuu riskienhallinnan viitekehysstandardiin, ja riskit jaetaan siinä strategisiin, taloudellisiin, operatiivisiin ja vahinkoriskeihin. Ohjelmisto mahdollistaa organisaatiolle systemaattisen tavan hallita ja raportoida erilaisia riskejä sekä niihin liittyviä riskin vaikutuksia pienentäviä toimenpiteitä.

7 Arviointi ja kehittäminen

Tietoturvan ja tietosuojan kehittämistä on vuoden aikana arvioitu ja tuettu useilla eri tarkastuksilla ja analyyseillä. Näiden tarkoituksena on ollut tunnistaa nykytilan vahvuudet ja kehityskohteet sekä varmistaa lainsäädännön ja viranomaisvaatimusten noudattaminen.

7.1 KPMG

KPMG toteutti kaupungille lakisääteisen tilintarkastuksen yhteydessä IT-tarkastuksen. Tarkastus toteutettiin UIT-haastattelulla (Understanding of IT), jonka tarkoituksena oli selvittää organisaation IT-ympäristön ja tietoturvan toteuttamisen nykytilaa. Haastattelussa käytiin läpi IT-toiminnan hallintamalli, riskienhallinta, järjestelmien käytettävyys sekä tietoturvaan liittyvät menettelyt.

Tarkistuksen löydösten perusteella tunnistettiin sekä nykyisiä vahvuuksia että kehityskohteita, joihin liittyvät toimenpiteet on otettu osaksi jatkuvaa parantamista.

7.2 Sisäinen tarkastus

Vuonna 2025 Kokkolan kaupungin sisäinen tarkastaja toteutti sisäisen tarkastuksen tietoturvan ja tietosuojan osalta. Tarkastuksen tavoitteena oli arvioida tietoturvan osa-alueiden toteutumista sekä niihin liittyvien prosessien, ohjeiden ja käytäntöjen toimivuutta. Lisäksi tarkastuksen viitekehykseen kuului uhkaaviin tilanteisiin varautumisen arviointi.

Kyselyt kohdennettiin keskeisille tietohallinnon ja tiedonhallinnan vastuurooleille. Saatujen vastausten perusteella laadittiin tarkastusraportti 5.2.2025. Raportissa käsiteltiin seuraavia osa-alueita: 1) toimintaa ohjaavat säännöt ja määräykset, 2) havainnot, 3) riskit, 4) suositukset ja 5) suositusten kriittisyys. Suosituksissa korostettiin henkilöstön tietoturva- ja tietosuojakoulutuksen järjestämistä laajemmin kuin nykyinen kahden vuoden välein suoritettava eOppiva-tietoturvatesti. Lisäksi esitettiin, että henkilöstöä tulee muistuttaa säännöllisesti ajankohtaisilla tiedotteilla ja kattavalla materiaalilla intranetissä tietoturvaan ja tietosuojaan liittyen. Raportin lopuksi painotettiin riittävien resurssien turvaamista tulevaisuudessa. Raportin kriittisyys oli kehityssuositustasolla, jonka mukaan jo olemassa olevia kontrolleja voidaan tehostaa.

Kyseisen tarkastuksen jälkeen tehtiin useita toimenpiteitä, joista yksi mainittiin aiemmin kohdassa 4.3 Henkilöstön kouluttaminen.

7.3 NIS2- direktiivin mukainen GAP- analyysi

NIS2-direktiivin GAP-analyysi on prosessi, jolla organisaatio vertaa nykyisiä tietoturvakäytäntöjään ja -toimenpiteitään NIS2-direktiivin vaatimuksiin löytääkseen puutteet (gaps) ja luodakseen suunnitelman vaatimusten täyttämiseksi, mikä on kriittistä sanktioiden välttämiseksi ja kyberturvallisuuden parantamiseksi. Analyysi kattaa nykytilan kartoituksen, soveltamisalan määrittelyn ja konkreettisten kehityskohteiden tunnistamisen.

GAP-analyysin jälkeen organisaatiossa on toimeenpantu keskeisiä kehitystoimenpiteitä jatkuvan parantamisen periaatteen mukaisesti. Työtä jatketaan osana vuoden 2025 tietoturvan kehittämisohjelmaa, jota päivitetään säännöllisesti voimassa olevan lainsäädännön, auditointien tulosten sekä havaittujen kehitystarpeiden perusteella.

7.4 Tekoäly toimenpiteet

Syksyllä toteutettiin yhteistyössä ulkopuolisen asiantuntijakumppanin kanssa kolme työpajaa, joiden tavoitteena oli rakentaa organisaatiolle turvallinen ja hallittu polku tekoälyn hyödyntämiseen. Työpajoissa määriteltiin tiekartta tekoälyn käyttöönotolle, sisältäen keskeiset vaiheet ja tietoturvavaatimukset. Lisäksi laadittiin riskienhallinnan ja tietosuojan periaatteet, jotka ohjaavat tekoälyratkaisujen turvallista käyttöä. Kick-

off-tilaisuudessa korostettiin tekoälyn strategista merkitystä ja sen roolia organisaation digitalisaation vauhdittajana.

Ulkopuolisen asiantuntijakumppanin tuella toteutettiin kolmen osan koulutuskokonaisuus, jonka tavoitteena oli vahvistaa henkilöstön osaamista ja lisätä käytännön valmiuksia tekoälyn hyödyntämiseen. Koulutussarjassa käsiteltiin tekoälyn perusteita ja keskeisiä käyttötapoja, Copilot Chat -ratkaisun käytännön soveltamista sekä promptien muotoilua ja roolien määrittelyä tekoälysovelluksille vuonna 2026 järjestettävässä osuudessa. Koulutusten rinnalla tarjottiin nonstop-koulutuksia, jotka mahdollistivat jatkuvan oppimisen ja matalan kynnyksen tuen henkilöstölle.

Kokkolan kaupungin tietoturvan ja tietosuojan kehittäminen on jatkuva prosessi ja kaupungissa toteutetaan riskilähtöistä ajattelutapaa. Kaupungin johto on sitoutunut kyberturvatyön tukemiseen. Tiedonhallintalaki suuntaa organisaatioita kohti kokonaisvaltaista tiedonhallinnan ylläpito- ja kehittämistyötä.

8 Hyödyllisiä linkkejä

Tietosuojavaltuutetun sivut: www.tietosuoja.fi

EU:n yleinen tietosuoja-asetus: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Tiedonhallintalaki: https://www.finlex.fi/fi/laki/alkup/2019/20190906

Tietosuojalaki: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Kokkolan kaupungin tietosuojasivut:
https://www.kokkola.fi/asiointi_ja_yhteystiedot/tietosuoja/fi_FI/tietosuoja/