



Tietotilinpäätös

2024

Julkinen

Huhtikuu 2025

Hyväksytty KH

28.4.2025/§193

Sisällysluettelo

1 Tietotilinpäätöksen tarkoitus ja säädöserusta	3
2 Tietoturvan ja tietosuojan järjestäminen	3
2.1 Kaupunginhallitus	3
2.2 Kaupungin johtoryhmä mukaan lukien kaupunginjohtaja	4
2.3 TT/TS eli tietoturva- ja tietosuojaryhmä	4
2.4 Tietoturvavastaava	4
2.5 Tietosuojavastaava	5
2.6 Tietohallinto	6
2.7 Toimialajohtajat, esihenkilöt	6
2.8 Pääkäyttäjät	7
2.9 Henkilöstö	7
3 Lainsäädäntö, lailliset perusteet ja muu ohjeistus	7
4 Ajankohtaisia asioita	8
4.1 Taisto- harjoitus	8
4.2 Tietosuojadokumentaatio	9
4.3 Henkilöstön kouluttaminen	10
4.4 Muita ajankohtaisia asioita	10
5 Tietoturvapoikkeamien käsittely ja poikkeamista ilmoittaminen	11
6 Riskienhallinta sekä toiminta häiriötilanteissa	11
7 Arviointi ja kehittäminen	12
7.1 KPMG:n tarkastus	12
7.2 Muutosvaikutuksen arviointi	12
7.3 Tekoäly toimenpiteet	12
8 Hyödyllisiä linkkejä	13

1 Tietotilinpäätöksen tarkoitus ja säädöspöerusta

Tietotilinpäätöksen tarkoituksena on antaa Kokkolan kaupungin kokonaiskuva henkilötietojen käsittelyyn liittyvästä tietosuojaan, tietoturvan ja tiedonhallinnan tilasta vuonna 2024. 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 tietoaaineistojen 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 tietoaaineistojen, niiden käsittelyvaiheiden ja tietoaaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaaineistojen tallentamistavasta ja muista käsittelytavoista. Tiedonhallintalain mukaiset vaatimukset on huomioitu 2024 päivitetystä Kokkolan kaupungin hallintosäännössä.

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

2 Tietoturvan ja tietosuojaan 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 tietoaaineistojen 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 tietosuojaan järjestämisestä. Johto myös varmistaa työlle riittävät resurssit. Johdon linjaukset sekä tietosuojaan että tietoturvan osalta näkyvät kaupungin tietoturvapoliitikassa, 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 tietosuojaan ja -turvan toteutumista kaupunkiorganisaatiossa. Ryhmässä on mukana tietoturva- ja tietosuojavastaavan lisäksi edustajat sivistystoimesta, varhaiskasvatuksesta, opetuspalveluista, konsernihallinnosta, tietohallinnosta (2 edustajaa), kaupunkiympäristöstä, Kokkolan vedeltä ja viestinnästä. Mukana ryhmässä on myös sisäinen tarkastaja. Tämän lisäksi ryhmässä käy tarvittaessa kutsuttuna muita asiantuntijoita. Tietosuoja-/tietoturvaryhmän kokoonpanoa päivitetään jatkuvasti.

2.4 Tietoturvavastaava

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

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

- Tietoturvavastaava vastaa organisaation tietoturvaluustason 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 vastualueen 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 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 tietoturvapoliitikassa 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 pyydettyä 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 seuraavat kohdat:

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 raportoisesta. 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 tietosujoaohjeet 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
- tietoturvapoliittikka (päivitetty vuonna 2020, jolloin laajennettiin tietosuojaosiota)
- tietoturvaohje pähkinänkuoressa henkilöstö

4 Ajankohtaisia asioita

4.1 Taisto- harjoitus

Kokkolan kaupungin johtoryhmä, tietosuojavastaava, tietohallinto, sisäinen tarkastaja sekä viestintä osallistui jälleen vuonna 2024 marraskuussa vuosittaiseen Taisto-harjoitukseen. Vuoden 2024 harjoituksessa harjoiteltiin organisaatioiden toimintakykyä haastavissa tietoturvatilanteissa.

Taisto- harjoituksen aiheita olivat

1. laaja tietomurto, joka kohdistui laajaan määrään henkilötietoja ja erityisiä henkilötietoja
2. kohdennettu tietojenkalastelu ja maalittamiskampanja

3. fyysisen turvallisuuden ja digitaalisen turvallisuuden uhka, johon liittyi vakoileva ja haitallinen laite eli niin sanottu O.MG- kaapeli

4. internetin saatavuuteen kohdistuva uhka: laaja maanlaajuinen tietoliikenneongelma.

Jokaisen harjoituksen ytimessä oli tilanteen asteittainen laajeneminen: harjoituksen viestikanavat tulvivat ja kunkin tilanteen mukaan oli olennaista erottaa harhaanjohtava ja totuudenmukainen tieto.

Taisto- harjoituksessa on usein todettu, että tietohallinto on häiriön akuutissa vaiheessa tärkeässä merkityksessä. Vallitseva häiriötila pitää päästä minimoimaan mahdollisimman nopeasti. Testitilanteen alussa havaittiin kipukohta, joka liittyi tilannekuvan arvioimisen hankaluuteen. Tilannekuvan realistinen arvioiminen on haastavaa ja tulevia mahdollisia haittoja on vaikea arvioida. Vasta tilanteen edetessä ongelman laajuus tulee muodostumaan ja häiriön aste tarkentumaan. Jatkuvalle vuorovaikutteisella tilanteen arvioinnilla on merkitystä viestinnän ja monen muun kaupungin toiminnon vuoksi.

Taisto- harjoituksessa kohdattiin myös sosiaalisen median kanavista tulevat uhat. Harjoituksen erilaiset kuvitteelliset somekanavat täyttyivät aiheeseen liittyvistä mielipiteistä ja keskusteluista. Harjoituksen yhteydessä todettiin myös, että kaupungin sisäisen ohjeistuksen tulee olla kunnossa. On myös tärkeää muodostaa selkeä tilannekuva ja tehdä lyhyt tiedote henkilöstölle, julkisuuteen sekä erikseen tarvittaessa sidosryhmille. Disinformaatioon on vastattava oikealla tiedolla.

Harjoituksien edetessä havainnointiin muun muassa myös seuraavia asioita:

1. Tietohallinto on häiriön ensimmäisessä vaiheessa olennaisessa merkityksessä: olemassa oleva häiriö pitää päästä minimoimaan mahdollisimman nopeasti. Ensisijaisia toimenpiteitä ovat tietoliikenteen sulkeminen, palvelimien eristys ja haavoittuvaisuuksien paikkaaminen.

2. Kaupungin viestintä tulee olla yhtenäistä ja keskitettyä: tällä menettelyllä varmistetaan myös asiantuntijoiden työrauha.

3. On tarkennettava mitkä toiminnot ovat sellaisia, joita ei voi hoitaa, kun tietoliikenne on poikki. Kaupungilla on sisäisiä suunnitelmia, miten toiminta turvataan myös häiriötilanteissa.

4. Tarkasteltiin poikkeustilanteen vaikutuksia kunnan perustoimintoihin ja palveluihin: koulut ja päiväkodit voida jatkaa toimintaa myös poikkeustilanteessa tietyin edellytyksin mutta varsinainen päätöksenteko voi olla tauolla.

Harjoituksen edetessä havaittiin kehityskohteita, jotka liittyivät poikkeustilanteen hallintaan: miten viestitään sisäisesti ja ulkoisesti, jos tietoliikenne ei toimi? Totesimme myös, että olisi tärkeää, että tarvittava ohjeistus olisi sähköisen lisäksi myös paperimuotoisena.

4.2 Tietosuojadokumentaatio

Tietosuojadokumentaatiota ja tiedonhallinnan velvoitteita on viety eteenpäin tietosuojan ja tietoturvan hallintajärjestelmässä, jossa voi toteuttaa monipuolista

tietosuoja- asetuksen mukaista osoitusvelvollisuutta. Tämän lisäksi useita tiedonohjauksen projekteja eli tiedonohjaussuunnitelma ja arkistonmuodostussuunnitelma- projekteja on aloitettu toimialueilla ja viety eteenpäin. Vuonna 2024 huomio kohdistui myös uuden sähköisen arkiston käyttöönottoon, joka on osa tiedon elinkaaren aktiivista hallintaa. Elinkaaren hallintaan kuuluu myös se, että tieto ei säily liian kauan. Sähköinen arkisto vaatii toimiakseen TOS- ohjauksen ja se on osa tietosuojavelvoitteen toteuttamista.

Tietosuojadokumentaatiota eli osoitusvelvollisuutta toteutetaan Kokkolan kaupungilla seuraavasti:

- tiedonhallintamalli
- Tiedonohjaussuunnitelma (TOS) ja arkistonmuodostussuunnitelma (AMS)
- tietosuojaselosteet
- vaikutuksenarvioinnit DPIA

4.3 Henkilöstön kouluttaminen

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

Kaupungilla on yhä ohjeena, että kaikkien työntekijöiden, sekä uusien että vanhojen, tulee käydä läpi eOppiva- koulutusympäristön kurssimateriaali. Kurssin lopussa testataan opitun materiaalin ymmärtäminen testillä. Kurssin suoritusprosenttia seurataan ja tekemättä jättämisestä huomautetaan. Vuonna 2024 tietoturvan ja tietosuojan koulutusta aloitettiin uudistamaan. Kaupungille hankittu Eduhouse toimisi tulevaisuudessa keskitettynä koulutusalueena kaupungin henkilöstölle.

Vuonna 2024 tietoturavastaava ja tietosuojavastaava pitivät tietoturvan ja tietosuojan koulutuksen henkilöstölle. Kyseiseen koulutukseen osallistui 36 henkilöä. Tallenne on katsottavissa myöhemmin kaupungin Intranetissä.

Toimialueita kannustetaan osallistumaan oman substanssin tietoturva- ja tietosuojakoulutuksiin. Henkilöstöpalveluiden henkilöstö (mukaan lukien palkanlaskenta ja työsuojelu) on käynyt Eduhousen oman hr:lle suunnatun koulutuksen: Palkanlaskennan ja hr:n tietoturvan keskeiset trendit

4.4 Muita ajankohtaisia asioita

Kaupungilla on otettu laajemmin käyttöön tietoturallinen Suomi.fi tunnistautumisen kautta tapahtuva salatun viestin lähettäminen. Suojattu viestiyhteys mahdollistaa erityisten henkilötietojen tai salassa pidettävien asioiden lähettämisen kaupungille.

Ylen uutisotsikoihin 30.10.2024 noussut Wilma- järjestelmä ja sen tietoturvariskit olivat kaupungin tietoturva- asiantuntijoiden keskustelussa. Järjestelmän haavoittuvuudet liittyvät heikkojen salasanojen ja käyttäjänimien yhdistelmiin. Kaupungin opetuspalvelut päättivät perustaa työryhmän vuodelle 2025 Wilma-tietoturva-aiheiden ympärille.

Helsingin kaupungin tietomurto oli vuoden 2024 näkyvin kotimaassa tapahtunut tietoturvaluutinen. Tapauksen myötä tiedonhallinnan asiantuntija yhdessä kaupungin johdon kanssa muistutti ja ohjeisti työkoneen hallintaan liittyvistä toimenpiteistä kaupungin sisäisessä viestintäkanavassa. Tiedotteessa varoiteltiin kasautuneen ja turhaan säilyvän tiedon haitallisista vaikutuksista ja siihen kohdistuvasta hallinnasta. Tiedotteessa muistutettiin jokaista työntekijää aktiivisesti poistamaan turhaan säilyviä tiedostoja tai siirtämään ne asialliseen niihin kuuluviin järjestelmiin. Tiedotteessa muistutettiin myös ylläpitämään arkistonmuodostussuunnitelmia, tiedonohjaussuunnitelmaa ja tiedonhallintamallia.

Kaupunkiympäristön toimiala on osallistunut Kuntaliiton koordinoimaan koulutukseen: paikkatietojen julkaisu julkishallinnon organisaatioissa. Lisäksi paikkatiedot osallistuivat Puolustusministeriön järjestämään Paikkatietoseminaariin.

5 Tietoturvapoikkeamien käsittely ja poikkeamista ilmoittaminen

Kaupungin henkilöstöllä on velvollisuus ilmoittaa mahdollisesta tietosuojaloukkauksesta tietosuojavastaavalle. Tietosuojavastaava arvioi tilanteen ja tekee tarvittaessa yhteistyössä rekisterinpitäjän kanssa ilmoituksen kansalliselle tietosuojavaltuutetulle sekä rekisteröidylle. Tietosuojavastaavalla on 72 tuntia aikaa ilmoituksen tekemiseen, joten tiedon on kulkeuduttava nopeasti. Kaupungille on tehty tietosuojaloukkauksen prosessikaavio vuonna 2018 jota voi hyödyntää tarvittaessa. Tietohallinto on tehnyt myös toimintaohjeen kyberhyökkäystapahtumalle. Kaupungilla on myös tarvittaessa käytössä vuonna 2022 tehty rekisteröidyn informointilomake tietoturvaloukkaustilanteesta.

Kaupungin henkilöstöllä on velvollisuus myös ilmoittaa tietoturvaloukkauksista. Tietoturvaloukkausilmoitukset tehdään kyberturvakeskukselle. Vuonna 2024 Kokkolan kaupunkiin kohdistui muutamia sähköpostihuijausyrityksiä. Huijausyrityksistä ilmoitettiin tiedoksi kyberturvallisuuskeskukselle.

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 ennakointi 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 2024 on parannettu dokumentaatio liittyen kyberhäiriö ja varautumisohjeisiin.

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:n tarkastus

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 käytettävyyks sekä tietoturvaan liittyvät menettelyt.

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

7.2 Muutosvaikutuksen arviointi

Tiedonhallintalain 2. luvun 5. pykälän muutosvaikutusarviointityötä on jatkettu kaupungin asiantuntijajoukolla tietojärjestelmän esiselvityslomakkeen muodossa. Kyseistä lomaketta voi hyödyntää hankinnan suunnittelu- ja/tai tarjouspyyntövaiheessa. Lomaketta voidaan käyttää hankinnan suunnitteluvaiheessa, kun käydään markkinavuoropuhelua potentiaalisten toimittajien kanssa, eikä ole vielä varmuutta, millaisia vähimmäisvaatimuksia hankinnan kohteena olevalle tietojärjestelmälle voidaan asettaa. Jos tietojärjestelmältä vaadittavat vähimmäisvaatimukset ovat jo selvillä, voidaan lomaketta käyttää tarjouspyyntövaiheessa, kun mietitään, mitä kaikkia vaatimuksia tietojärjestelmälle asetetaan. Lomaketta voi soveltuvin osin käyttää jokaisessa tietojärjestelmähankinnan suunnitteluvaiheessa (mukaan lukien sovellukset ja ohjelmistot).

Kyseisen esiselvityksen avulla Kokkolan kaupunki pyrkii pääsemään lähemmäksi tiedonhallintalain ja tietosuoja-asetuksen vaatimuksia sekä sen avulla ennakoimaan taloudellisia ja toiminnallisia riskejä. Lisäksi lomakkeella pyritään edistämään yhteen toimivuuden ja tietoturvallisuuden toteutumista sekä investointien kannattavuutta. Lisäksi lomaketta voidaan hyödyntää jo hankituissa tietojärjestelmissä esimerkiksi versiopäivityksen yhteydessä. Vuonna 2024 lomaketta parannettiin tietosuojan ja tiedonhallinnan näkökulmasta. Lisäksi tiedonhallintalain 17. pykälän mukaista lokitointia on lomakkeessa parannettu.

7.3 Tekoäly toimenpiteet

Kokkolan kaupungin asiantuntijajoukko työsti vuonna 2024 kaupungin henkilöstölle tekoälyohjeistuksen ”tekoälyn hallittu ja turvallinen käyttö”. Kokkolan kaupunki on linjannut, että Kokkolan kaupungilla kaikki tekoälyä koskevat hankinnat käsitellään sisäisessä IT-kehittämisyryhmässä. Kokkolan kaupunki on myös linjannut, että

tekoälysovelluksia ei saa asentaa työkoneelle, vaan tekoälyä käytetään selainpohjaisissa versioissa. Tekoälysovelluksissa tulee käyttää henkilökohtaisia sähköpostitunnuksia, lukuun ottamatta Microsoft Edgen sisäänrakennettua Copilottia, joka käyttää automaattisesti oletuksena työsähköpostitiliä. Muita sovelluksia käyttäessäsi käyttäjiltä edellytetään omia henkilökohtaisia tunnuksia (esim. oma henkilökohtainen s-posti kuten Gmail).

Tämän lisäksi Kokkolan kaupungin TT/TS ryhmä on keskustellut tekoälyasetuksesta.

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

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>

Tietosuoja laki: <https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>

Kokkolan kaupungin tietosuojasivut:

https://www.kokkola.fi/asiointi_ja_yhteystiedot/tietosuoja/fi_FI/tietosuoja/