Tietotilinpäätös

2023

Sisällysluettelo

1 Tietotilinpäätöksen tarkoitus

Tässä tietotilinpäätöksessä kuvataan Kokkolan kaupungin tietoturvan ja tietosuojan nykytilaa. Tietotilinpäätöksen tarkoituksena on kuvata kuinka kaupunki varmistaa tietoturvan ja tietosuojan toteutumista, ja miten se on vuoden 2023 aikana kehittänyt tietoturvaan ja tietosuojaan liittyviä prosesseja. Tietotilinpäätös toimii samalla tärkeänä osana osoitusvelvollisuuden toteutumista, sillä sen avulla kaupunki osoittaa noudattavansa tietosuoja-asetusta, ja muita tietoturvaa ja tietosuojaa määrittäviä periaatteita. Tietotilinpäätös laaditaan kerran vuodessa.

2 Tietoturvan ja tietosuojan toteuttaminen

Kokkolan kaupungille on nimetty tietoturvavastaava, joka on määritelty tietohallintopäällikön tehtäviin. Tietoturvavastaava vastaa organisaation tietoturvallisuustason määrittelystä ja arvioinnista ja raportoinnista sekä muusta hallinnollisesta tietoturvasta ja toimii tietoturvaryhmän puheenjohtajana. Hän vastaa tietoturvasuunnitelmien tekemisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta toimintayksikössä ja sen ostamissa palveluissa, sekä raportoinnista johdolle.

Kokkolan kaupungille on nimetty tietosuojavastaava, joka on määritelty tiedonhallinnan asiantuntijan tehtäviin. Tietosuojavastaava on organisaation sisäinen, riippumaton asiantuntija. Tietosuojavastaavan tehtävänä on toimia yhteyshenkilönä sekä rekisteröidyille että tietosuojavaltuutetulle. Hän seuraa tietosuojasääntöjen noudattamista organisaatiossa ja tuo esiin mahdollisia puutteita. Tietosuojasäännösten noudattaminen on rekisterinpitäjän vastuulla, eikä tietosuojavastaava ole henkilökohtaisessa vastuussa asetuksen tai lain rikkomisesta.

Kaupungilla on noin kahden kuukauden välein kokoontuva tietoturva-/tietosuojaryhmä eli TT/TS-ryhmä, joka käsittelee ajankohtaisia tietoturvaan ja tietosuojaan liittyviä kysymyksiä 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. 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.

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

Tilaisuudet, koulutukset ja tapahtumat vuonna 2023	
Päivämäärä	**Tilaisuus**
22.2.2023	TT/TS-ryhmän kokous
17.5.2023	TT/TS-ryhmän kokous
25.10.2023	TT/TS-ryhmän kokous
18.12.2023	Valtakunnallinen Taisto-harjoitus

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.

2.1 Ajankohtaisia asioita

TT/TS-ryhmä osallistui vuonna 2023 Taisto-harjoitukseen. Harjoitukseen osallistui myös johtoryhmän jäseniä. Taisto on Digi- ja väestötietoviraston hallinnoima tietoturvan ja tietosuojan yhteinen harjoitus, joka koostui tällä kertaa puolen päivän etätapahtumasta. Harjoituksessa harjoitellaan mahdollisia tietoturva- ja tietosuojapoikkeamia. Vuonna 2023 Taisto-harjoituksen teemat keskittyivät tietojenkalasteluun ja hybridivaikuttamiseen sekä tekoälyn tuomiin haasteisiin. Tehtävinä oli muun muassa pohtia tekoälyn uhkavaikutuksia sekä sitä, miten tekoälyn tulemiseen voi varautua uhkien ennakkotorjunnassa. Taisto-harjoituksen ennakkotehtäväjohdannossa kuvattiin muun muassa sitä, että vaikka organisaatiot eivät itse käyttäisi tekoälyä, ulkopuoliset toimijat saattavat käyttää sitä organisaatiota vastaan kohdistettujen kampanjoiden muodossa. Tämän ohella organisaation alihankkijat tai muut palvelun tuotantoketjun toimijat saattavat hyödyntää sitä omassa toiminnassaan. Puolen päivän harjoituksen aiheena oli tekoälyavusteinen laaja tietojenkalastelukampanja Suomessa tai Euroopassa. Puolen päivän harjoituksen myötä Kokkolan kaupunki aloitti valmistelemaan tekoälyohjeistusta henkilöstön työn tueksi.

Kokkolan Vesi osallistui 21.3.2023 Instan järjestämään kolme tuntia kestävään vesihuoltolaitosten kyberharjoitukseen. Harjoituksen sisällön olivat suunnitelleet Kyberturvallisuuskeskuksen, Huoltovarmuuskeskuksen, ELY-keskuksen, Kuntaliiton, HSY:n, Vesilaitosyhdistyksen ja Instan asiantuntijoista koostuva työryhmä. Harjoitusten teemoina oli laitosten IT- ja OT-järjestelmiin ulkopuolelta kohdistuvat häiriötilanteet, fyysinen turvallisuus ja mainehaitat.

2.2 Dokumentointi

Osana rekisterinpitäjän osoitusvelvollisuutta seloste käsittelytoimista –dokumentin täyttäminen jatkuu yhä. Seloste käsittelytoimista dokumentointia valmistuu myös tietosuojan ja tietoturvan hallintajärjestelmäsovellukseen. Seloste käsittelytoimista on kirjallinen kuvaus kaupungin organisaation tekemästä henkilötietojen käsittelystä. Myös netissä julkaistavat tietosuojaselosteet toteuttavat tätä yhdessä kaupungin tiedonohjaussuunnitelman (TOS) kanssa. Tiedonohjaussuunnitelmaan on mahdollista vastata siihen missä tehtävissä tai asiakirjoissa oletusarvoisesti käsitellään henkilötietoja ja mikä on henkilötietojen käsittelyn peruste. Selosteiden ja hallintajärjestelmän täyttäminen ja ylläpitäminen ovat toimialojen vastuulla. Tietosuojavastaava ohjeistaa ja opastaa dokumentoinnin toteuttamisessa.

Tiedonhallintalain (laki julkisen hallinnon tiedonhallinnasta, 906/2019) myötä tulevia vaatimuksia on edistetty äsken mainitun hallintajärjestelmäsovelluksen avulla. Tiedonhallintamallia varten on laadittu kuvaukset tietovarannoista, tietoaineistoista, toimintaprosesseista sekä tietojärjestelmistä.

3 Lainsäädäntö ja muu ohjeistus

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

Erityisiä henkilötietoryhmiä, kuten etnistä alkuperää, terveyttä tai ammattiliiton jäsenyyttä koskevia tietoja ei lähtökohtaisesti saa käsitellä. Käsittely on kuitenkin mahdollista silloin, kun tietosuoja-asetukseen tai kansalliseen lainsäädäntöön on säädetty poikkeus.

Tietosuojalaki 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.

Kokkolan kaupungin tietosuojaohjeet on laadittu sekä tietosuoja-asetuksen että tietosuojalain 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

4 Rekisteröityjen oikeuksien toteutuminen

Tietosuojaselosteiden päivittämistä ja niiden julkaisua on tehty vuoden 2023 aikana aktiivisesti. Myös tietämystä rekisterinpitäjän velvollisuuksista on pyritty tiedottamaan läpi kuntaorganisaation. Myös tiedonhallintalain (906/2019) vaatimuksia on viety eteenpäin organisaatiossa. Tätä toteuttavia toimenpiteitä ovat muun muassa verkkosivuilta löytyvä asiakirjajulkisuuskuvaus sekä kaupungissa sisäisesti laatima tiedonhallintamalli, joka sijaitsee tietosuojan ja tietoturvan hallintajärjestelmässä.

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 tietoturvaloukkaustilanteessa. Vuonna 2023 tietosuojaloukkausilmoituksia ei ole tarvinnut tehdä tietosuojavaltuutetulle.

Kaupungin henkilöstöllä on velvollisuus myös ilmoittaa tietoturvaloukkauksista. Tietoturvaloukkausilmoitukset tehdään kyberturvakeskukselle. Vuonna 2023 Kokkolan kaupunkiin kohdistui muutamia sähköpostihuijausyrityksiä. Huijausyrityksistä ilmoitettiin tiedoksi kyberturvallisuuskeskukselle.

5 Arviointi ja kehittäminen

Tietosuoja-asetuksen 35. artikla velvoittaa tekemään vaikutuksenarvioinnit (PIA/DPIA) ja ennakkokuulemiset sellaisille prosesseille, joissa henkilötietojen käsittelyyn liittyy riskejä. Kansallinen tietosuojavaltuutetun toimisto on julkaissut vuonna 2021 viralliset ohjeistukset ja työkalut vaikutuksenarvioinnin tekemiseen. Muutamia vaikutuksenarviointeja on jo tehty.

Muutosvaikutusten arvioinnin prosesseja ja niiden työstämisiä arvioidaan sisäisesti. Tietohallinnon ja tietosuojavastaavan sekä muutaman yksikön asiantuntijan välisenä yhteistyönä valmistui yhä päivittyvä tietojärjestelmähankintojen esiselvityslomake. Esiselvityksen avulla Kokkolan kaupunki pyrkii pääsemään lähemmäksi tiedonhallintalain ja tietosuoja-asetuksen vaatimuksia.

Tietoturvan ja tietosuojan kehittäminen on jatkuva prosessi. Kaupungin johto on sitoutunut kyberturvatyön tukemiseen. Tiedonhallintalaki suuntaa organisaatioita kohti kokonaisvaltaista tiedonhallinnan ylläpito- ja kehittämistyötä. Tiedonhallintalain uusien käsitteiden myötä koko kaupunkiorganisaation henkilöstöltä odotetaan itsenäisempää vastuuta ja arviointikykyä tietosuojan ja tietoturvan toteuttamisessa.

6 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

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

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

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