Kokkola
Karleby

Tietotilinpäätös

2022

Huhtikuu 2023

Hyväksytty: kaupunginhallitus
8.5.2023 § 192

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 2022 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 2022	
Päivämäärä	**Tilaisuus**
23.2.2022	TT/TS-ryhmän kokous
18.5.2022	TT/TS-ryhmän kokous
24.8.2022	TT/TS-ryhmän kokous
26.10.2022	TT/TS-ryhmän kokous
10.11.2022	Valtakunnallinen Taisto-harjoitus
7.12.2022	TT/TS-kokous

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 2022 Taisto-harjoitukseen. Harjoitukseen osallistui myös johtoryhmän jäseniä, markkinointi- ja viestintäpäällikkö sekä työsuojelupäällikkö. Taisto on Digi- ja väestötietoviraston hallinnoima tietoturvan ja tietosuojan yhteinen harjoitus, joka koostui tällä kertaa puolen päivän etätapahtumasta. Tietohallinnon edustaja toimi harjoituksen sihteerinä. Harjoituksessa harjoitellaan mahdollisia tietoturva- ja tietosuojapoikkeamia. Vuonna 2022 Taisto-harjoituksen teemoissa korostui sähkökatkoihin varautuminen liittyen vallitsevaan energiakriisiin. Taisto-harjoituksen yhteydessä todettiin, että on tärkeää varautua ennakkoon energiakriisin vaikutuksiin varsinkin kriittisten tietojärjestelmien osalta. Taisto-harjoitus herätti keskustelua ja toimenpide-esityksiä toiminnan jatkuvuuteen ja toipumiseen kohtuullisessa ajassa. Harjoituksessa nostettiin myös esille katkojen ja muiden poikkeuksellisten tilanteiden kohdistuvat kyberuhat. Kyberhyökkäykset saattavat lisääntyä, kun kaupungin perus- tai tukitoiminnot ovat haavoittuvaisimmillaan. Taisto-harjoituksen jälkeen on päivitetty useita sisäisiä tietoturvaohjeita ja lisätty henkilöstön tietoisuutta haitallisen informaation tunnistamisessa. Harjoituksen myötä on tehty useita konkreettisia toimia tietoturvan parantamiseen ja näitä toimenpiteitä jatketaan vuonna 2023.

Vuonna 2022 päivitettiin myös uusien työntekijöiden käyttöoikeussitoumus. Käyttöoikeussitoumuksen avulla sitoutetaan järjestelmien käyttäjät organisaation tietosuoja- ja tietoturvaperiaatteiden noudattamiseen. Sitoumus käydään läpi työntekijän kanssa ja se koskee kaikkia organisaatiossa käytössä olevia tietojärjestelmiä. Sitoumuksen osia ovat salassapito- ja

vaitiolovelvollisuus, käyttäjätunnukset ja salasana, työaseman käyttö, sähköpostin ja internetyhteyksien käyttö, tietosuoja- ja tietoturvaohjeet ja rikkomusten seuraamukset.

2.2 Dokumentointi

Osana rekisterinpitäjän osoitusvelvollisuutta seloste käsittelytoimista –dokumentin täyttäminen jatkuu yhä. Seloste käsittelytoimista dokumentointia valmistuu myös organisaation Digiturvamalli-sovellukseen. 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 digiturvamallin 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 Digiturvamalli- sovelluksen 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 2022 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 Digiturvamalli- sovelluksessa.

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. Kaupungilla oli vuonna 2022 tekeillä rekisteröidyn informointilomake tietoturvaloukkaustilanteessa. Vuonna 2022 tietosuojaloukkausilmoituksia ei ole tehty.

Kaupungin henkilöstöllä on velvollisuus myös ilmoittaa tietoturvaloukkauksista. Tietoturvaloukkausilmoitukset tehdään kyberturvakeskukselle. Vuonna 2022 tietoturvaloukkausilmoituksia ei ole tehty.

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. Ilmoituskanavan vaikutuksenarviointi valmistui ja sitä päivitetään tarpeen mukaan.

Muutosvaikutusten arvioinnin prosesseja ja niiden työstämisiä on arvioitu sisäisesti. Kaupungin sisäinen TT/TS ryhmä on linjannut, että tietojärjestelmien nimien näkyvyyttä on alettu rajoittamaan julkisessa dokumentoinneissa kuten tietosuojaselosteissa ja asiakirjajulkisuuskuvauksessa. Tietojärjestelmien nimet eivät ole olennaisia kuntalaisen tai asiakkaan osoitusvelvollisuutta tai kaupungin tiedottamisintressiä ajatellen. Myös henkilötietojen näkyvyyttä julkisissa dokumenteissa on neuvottu vähentämään.

Tietoturvan ja tietosuojan kehittäminen on jatkuva prosessi. 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. Lisäksi rekisterinpitäjän dokumentointivelvollisuutta on pyritty korostamaan. Tiedonhallintalain myötä sähköisen säilyttämisen vaatimus (alkaen 1.1.2022) luo lisävastuita ja haasteita myös tietosuojan- ja tietoturvan toteuttamiseksi. Myös tietojärjestelmien lokitietojen kerääminen ja säilyttäminen tuo lisätyötä tiedonhallinnan alueelle. Lisäksi digipalvelulain vaatimukset tuovat varmasti lisähaasteen tietoturvan ja tietosuojan alueelle.

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