Kokkola
Karleby

Tietotilinpäätös

Julkinen
2020

Huhtikuu 2021

Sisällysluettelo

1 Tietotilinpäätöksen tarkoitus

Tässä tietotilinpäätöksessä kuvataan Kokkolan kaupungin tietoturvan ja tietosuojan nykytilaa: miten kaupunki varmistaa tietoturvan ja tietosuojan toteutumisen ja miten se on vuoden 2020 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.

Vuonna 2020 jatkettiin tietoturvan ja tietosuojan kehittämistyötä koko kaupungin osalta. Käytänteitä ja prosessien toimivuutta päästiin testaamaan myös todellisissa tilanteissa, tosin vakavammilta tilanteilta vielä säästyttiin. Tietosuojavastaava siirtyi kesäkuussa 2020 sivistyskeskuksen hallintopäälliköksi ja hoiti tietosuojavastaavan velvollisuuksia oman työnsä ohella.

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 mahdolliset puutteet. Tietosuojasäännösten noudattaminen on rekisterinpitäjän vastuulla, eikä tietosuojavastaava ole henkilökohtaisessa vastuussa asetuksen tai lain rikkomisesta.

Kaupungilla on noin kahden kuukauden välein kokoontuva tietoturva-/tietosuojaryhmä (jatkossa 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, keskushallinnosta, tietohallinnosta (2 edustajaa), pelastustoimesta, kaupunkiympäristöstä, maaseututoimesta, Kokkolan vedeltä ja viestinnän edustaja. Lisäksi ryhmässä käy tarvittaessa kutsuttuna muita asiantuntijoita.

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

TT/TS-ryhmä osallistui vuonna 2020 Taisto–harjoitukseen. Taisto on Digi- ja väestötietoviraston hallinnoima tietoturvan ja tietosuojan yhteinen harjoitus, joka koostui tällä kertaa koko päivän etätapahtumasta. Tietohallinnon edustaja toimi harjoituksen sihteerinä. Harjoituksessa harjoitellaan mahdollisia tietoturva- ja tietosuojapoikkeamia. Tällä kertaa harjoiteltiin, mitä tulisi tehdä, jos tietoja vuotaisi palkkaohjelmistosta. Tietosuojan osalta arvioitiin tilannetta, käytiin läpi ilmoitusprosessi ja päädyttiin tekemään tarvittavat ilmoitukset. Kaupungin johtoryhmä osallistui harjoitukseen tarvittaessa (kutsuttiin paikalle). Harjoituksessa käytettiin yhdessä sovittuja viestinnän kanavia (johtoryhmän WhatsApp, sähköposti) ja pohdittiin myös, missä kohdin todellisessa tilanteessa käytettäisiin esimerkiksi sosiaalisen median kanavia.

Taisto-harjoituksen tuloksena ymmärrettiin, että erinäisten ilmoitusten (tietosuojavaltuutettu, krp, kyberturvallisuuskeskus) tekemiseen kuluu huomattavan paljon aikaa. Ilmoituslomakkeet ovat pitkiä ja vaativat erikseen oman henkilön niitä täyttämään. Edellisiin vuosiin verrattuna harjoituksessa ehdittiin kuitenkin paljon pidemmälle ja sen lopputuloksena ymmärretään paremmin sekä harjoituksien vaatimaa työpanosta että tositilanteessa käytettävää prosessia.

Henkilötietojen käsittelyn yleisohje julkaistiin 2020 alkupuolella. Se täydentää jo aiemmin käytössä olleita tietosuojan muistilistoja. Yleisohjeessa mennään muistilistoja syvemmälle tietosuojan periaatteisiin ja käytänteisiin.

Kaupungilla on yhä ohjeena, että kaikkien työntekijöiden, sekä uusien että vanhojen, tulee tehdä Vahti-tietosuojatesti. Testi on nettitesti, jossa käydään läpi tietosuojan perusasioita. Testin tehneiden määrästä ei ole nykyiseltään tietoa.

Seloste käsittelytoimista –dokumentin täyttäminen on aloitettu syksyn 2019 aikana ja se jatkuu yhä. Se on kirjallinen kuvaus kaupungin organisaation tekemästä henkilötietojen käsittelystä. Tätä työtä on tarkoitus jatkaa osana henkilötietoinventaaria vuonna 2021. Selosteen täyttäminen ja ylläpitäminen ovat toimialojen vastuulla. Tietosuojavastaava ohjeistaa selosteen täyttämisessä.

Vuonna 2019 aloitettiin tietosuojankin kannalta oleellinen tiedonohjaussuunnitelmaprojekti (tos-projekti). Tos-työ edistää myös tiedon elinkaaren hallintaa rajaamalla henkilötietojen käsittelyä sähköisissä järjestelmissä. Tiedonohjaussuunnitelmatyö jatkui vuoden 2020 alkupuolella aktiivisesti, joskin työhön tuli viivettä tiedonhallinnan asiantuntijan siirtyessä uusiin tehtäviin elokuussa. Syksyllä tehtävään palkattu määräaikainen osa-aikainen työntekijä on saanut edistettyä tos-työtä, mutta se viivästyi alun perin suunnitellusta aikataulusta ja valmistunee Dynasty-asianhallintajärjestelmän osalta vuoden 2021 aikana. Tos-työn sivutuotteena syntyy myös tieto siitä, missä Dynasty-asiakirjoissa on henkilötietoja.

Tiedon elinkaaren hallintaa toteutetaan myös arkistonmuodostussuunnitelmien kautta. Arkistonmuodostussuunnitelmat vaativat kuitenkin päivitystä. Päivitysprosessi on tarkoitus aloittaa tos-projektin valmistuttua.

Tilaisuudet, koulutukset ja tapahtumat vuonna 2020 (pois lukien tos-työ)	
Päivämäärä	**Tilaisuus**
Kevät 2020	KPMG:n tietoturvan/suojan auditointi ja kehityssuunnitelmat
30.1.2020	TT/TS-ryhmän kokous
11.3.2020	TT/TS-ryhmän kokous
13.5.2020	TT/TS-ryhmän kokous
17.6.2020	TT/TS-ryhmän kokous
26.8.2020	TT/TS-ryhmän kokous
21.10.2020	TT/TS-ryhmän kokous
29.1.2020	Valtakunnallinen Taisto-harjoitus
26.11.2020	TT/TS-kokous
Syksy 2020	Digiturvamallin hankinta Teamsiin, aloitus kevät 2021

3 Lainsäädäntö ja muu ohjeistus

Toukokuussa 2018 voimaan tullut EU:n yleinen tietosuoja-asetus (GDPR) vahvistaa rekisteröityjen oikeuksia omiin henkilötietoihinsa. 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. Asetus velvoittaa myös Kokkolan kaupunkia varmistamaan, että asetuksen oikeudet toteutuvat.

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 ja politiikat:

- tietosuojan muistilista työntekijälle
- tietosuojan muistilista asiakaspalveluun
- tietosuojan muistilista esimiehille
- henkilötietojen käsittelyn yleisohje
- tietoturvapolitiikka (päivitetty vuonna 2020, jolloin laajennettiin tietosuojaosiota)

4 Rekisteröityjen oikeuksien toteutuminen

Kokkolan kaupunki on laatinut prosessit tietopyyntöihin sekä omien tietojen poistamiseen ja korjaamiseen. Tietosuojavastaava on päivittänyt näihin prosesseihin vaaditut lomakkeet vuoden 2019 aikana. Lomakkeet löytyvät kaupungin verkkosivuilta ja asiakaspalvelusta. Lomakkeiden täyttöön saa tarvittaessa apua joko tietosuojavastaavalta tai asiakaspalvelusta. Vuoden 2020 aikana ei tullut tietopyyntöjä.

Kokkolan kaupunki on vuoden 2019 aikana aloittanut rekisteriselosteiden päivittämisen tietosuojaselosteiksi. Tietosuojaselosteet vastaavat paremmin GDPR:n vaatimuksiin. Tavoitteena on vuoden 2021 aikana päivittää loputkin selosteet ja tehdä tietosuojaselosteet prosessikohtaisesti. Aiemmin rekisteriselosteet on tehty järjestelmäkohtaisesti. Tietosuojaselosteet, rekisteröidyn oikeudet ja yleinen tietosuojainfo löytyvät kaupungin verkkosivuilta tietosuoja-otsikon alta.

Kaupungin henkilöstöllä on velvollisuus ilmoittaa mahdollisesta tietosuojaloukkauksesta tietosuojavastaavalle. Tietosuojavastaava arvioi tilanteen ja tekee tarvittaessa ilmoituksen kansalliselle tietosuojavaltuutetulle sekä rekisteröidylle. Tietosuojavastaavalla on 72 tuntia aikaa ilmoituksen tekemiseen, joten tiedon on kulkeuduttava nopeasti. Kaupungille on tehty tietosuojaloukkauksen prosessikaavio vuonna 2018. Prosessia harjoiteltiin Taisto 2.2 – harjoituksen yhteydessä ja TT/TS-ryhmä on suunnitellut pienimuotoisempaa harjoitusta, jossa keskityttäisiin vain tietosuojaloukkauksiin. Vuonna 2020 Kokkolan kaupungin työntekijät ilmoittivat yhden tietosuojaloukkauksen tietosuojavastaavalle. Tietosuojavastaava teki tästä ilmoituksen tietosuojavaltuutetulle.

Lisäksi selviteltiin yhtä vanhempaa tapausta, josta tehtiin jälkikäteen ilmoitus tietosuojavaltuutetulle. Oleellista tällaisissa tapauksissa olisi tietosuojavastaavan perusteellinen

informointi heti tietosuojaloukkauksen tapahduttua, jotta tällaisia myöhässä tehtyjä ilmoituksia ei tarvitsisi tehdä.

Ilmoitusten tekemiseen on tarkoitus tulevaisuudessa käyttää myös palautejärjestelmää. Ilmoituksen voisi silloin kirjata palautejärjestelmään omaan lomakkeeseen, jonka kautta tieto mahdollisesta tietosuojaloukkauksesta tulisi halutussa formaatissa. Tavoitteena on, että palautejärjestelmä laskisi myös ilmoituksen tekemisen kynnystä.

Rekisteröidyn oikeuksiin kuuluu, että vain rekisteröidyn asiaa käsittelevät saavat katsoa hänen tietojaan. Kaupunki suorittikin henkilötietojen käsittelijöiden tarkastukset ohjelmien osalta. Lopettaneiden työntekijöiden käyttöoikeudet poistettiin järjestelmien sen salliessa. Väestötietoja voi organisaatiossamme selata joko Väestötietojärjestelmän (VTJ) tai Trimble-järjestelmän kautta. Väestötietoja käyttävien henkilöiden esimiesten piti vuoden 2019 aikana hakea oikeuksia uudestaan. Näin poistettiin tarpeettomat käyttäjät. Trimble-järjestelmän väestötietoselausoikeuksia rajoitettiin niin, että suurin osa työntekijöistä käyttää nyt väestötietohakua VTJ:n kautta, sillä VTJ:n tuottama loki on helpommin saatavilla (lokitus tapahtuu rekisterinpitäjä DVV:n toimesta). Tämä työ jatkui vielä vuonna 2020, jolloin viimeisetkin hakemukset saapuivat.

5 Arviointi, kehittäminen ja tiedon hyödyntäminen

KMPG-tietosuoja-auditointi oli suurin yksittäinen tietosuojan arviointi, joka kaupungilla tehtiin vuonna 2020. Siitä kumpuavat seuraavien vuosien kehittämistoimet. Auditoinnissa yhdeksi suurimmista haasteista koettiin resursointi. Resursoinnin parantamiseksi ehdotetaan jokaiselle toimialalle omaa tietosuoja-asioista vastaavaa henkilöä. Näin tietoinventaarin tekeminen, sopimusten läpikäyminen ja seloste käsittelytoimista –dokumentin täyttö onnistuisi nopeammin. Nämä olivat kriittisimmät tietosuoja-auditoinnissa esiin nousseet kehittämiskohteet.

Toinen haaste on ollut koulutuksen ulottaminen koko henkilöstöön. Oman työn ohessa tietosuojatyötä tekevä tietosuojavastaava ei ehdi kouluttaa koko henkilöstöä. Koulutusten osalta tavoitteena on, että tulevina vuosina työntekijät voisivat kouluttautua erillisessä koulutusjärjestelmässä erilaisten videoiden, testien ja muun materiaalin avulla. Järjestelmästä saisi lokin siitä, kuka on suorittanut koulutukset. Samalla olisi mahdollista tehdä täsmäkoulutusta henkilöstöryhmille, joiden työssä on erityistä henkilötietojen käsittelyä, kuten esimerkiksi varhaiskasvattajat tai laskutuksesta vastaavat.

Tietoinventaarityön jatkaminen on ajankohtainen seuraavan vuoden aikana. Järjestelmissä olevien henkilötietojen kartoittaminen on pääsääntöisesti helpompaa kuin esimerkiksi verkkolevyllä tai paperilla säilytettyjen henkilötietojen, eli niin sanotun rakenteettoman datan, kartoittaminen. Ongelmaksi voikin muodostua juuri nämä jäsentämättömät henkilötiedot. On oleellista, että tietoinventaaria tekevät ihmiset ymmärtävät, mitkä kaikki tiedot lasketaan henkilötiedoiksi.

Tietosuoja-asetuksen 25. artikla velvoittaa henkilötietojen käsittelijää huomioimaan mahdolliset riskit. Sellaisille prosesseille, joissa henkilötietojen käsittelyyn liittyy riskejä, tulisi tehdä vaikutuksenarvioinnit (PIA/DPIA) ja ennakkokuulemiset. Näitä ei ole vielä toteutettu kaupungissamme, mutta mahdollisia toimintamalleja on tietosuojavastaavan toimesta tarkasteltu.

Tietoturvan ja tietosuojan kehittäminen on jatkuva prosessi. Vuonna 2020 toteutettu tietoturva- ja tietosuojaryhmän kokoonpanon laajentaminen johtaa toivottavasti myös laajempaan tietoturvan ja –suojan haasteiden ja mahdollisuuksien tiedostamiseen. Vuoden 2021 tavoitteena on KPMG auditoinnin myötä esiin nousseiden kehittämistöiden jatkaminen.

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/