Tietotilinpäätös 2020

Sipoon kunta

31.5.2021

SIPOO
SIBBO

Sisällysluettelo

1 Tietotilinpäätöksen tarkoitus kunnassa

Tämä on Sipoon kunnan tietotilinpäätös. Tietotilinpäätös on koontiraportti, joka syntyy sisäisen tarkastelun tuloksena ja auttaa hahmottamaan kuvaa tietojen käsittelyn nykytilasta sekä arvioi tietosuojan ja tietoturvan toteutumista. Lisäksi se sisältää tietosuojaan ja tietoturvaan liittyviä kehittämistarpeita ja -toimenpiteitä. Tietotilinpäätöksen tarkoituksena on antaa kokonaiskuva kunnan tiedon, tietoturvallisuuden ja tietosuojan hallinnan tilasta. Sitä voi pitää niin johdon työvälineenä kuin myös osana EU:n yleisen tietosuoja-asetuksen osoitusvelvollisuuden täyttämistä. Osoitusvelvollisuus tarkoittaa lakien, hyvän tietojenkäsittelytavan ja hyvän tiedonhallintatavan noudattamista. Tietotilinpäätöksen tavoitteena on lisätä avoimuutta ja luottamusta siihen, että organisaatiossa noudatetaan organisaation luomia tietoturva- ja tietosuojaperiaatteita ja käsitellään henkilötietoja niiden mukaisesti. Hyvin hoidetulla tietosuojatyöllä vaikutetaan organisaation tehokkuuteen ja kilpailukykyyn. Tietotilinpäätös on tarkoitettu kunnan sisäiseen käyttöön johtamisen raportiksi sekä sidosryhmille tietojen käsittelyn kuvaukseksi. Se toimii myös suunnittelun ja toiminnan ohjauksen sekä raportoinnin ja johtamisen tukena.

2 Tietoturvallisuuden ja tietosuojan toteuttaminen Sipoon kunnassa

Rekisterinpitäjä on tietosuoja-asetuksen (artikla 24) mukaan vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja käytännössä myös osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutusta, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tilivalvontaa ja käytönvalvontaa, tietojen salausta, tietojen anonymisointia tai pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, käyttövalvontaa, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, tietotilinpäätösprosessia, käytännesääntöjen sekä sertifikaattien käyttöä.

Tietosuojan ja tietoturvan kehittämiseen on alettu panostamaan merkittävästi vuoden 2018 jälkeen. Kolmen edellisen vuoden aikana on toteutettu mm. henkilötietoaineistojen kartoitukset, tietosuoja- ja tietoturvaohjeiden laatiminen ja päivittäminen sekä useita tietosuojakoulutuksia henkilöstölle. Digitalisoinnilla ja datan turvallisella hyödyntämisellä pyritään rakentamaan kuntalaisille asiakaslähtöiset, luotettavat ja kustannustehokkaat palvelut. Tämä kaikki edellyttää, että tietosuojasta ja tietoturvasta huolehditaan riittävällä tasolla. Tietosuoja- ja tietoturvaperiaatteet tulee siis konkretisoida käytännön tasolle ja istuttaa osaksi organisaation toimintaa.

2.1 Henkilötietojen käsittely Sipoon kunnassa

Sipoon kunta kunnioittaa tietosuoja-asetuksessa määriteltyjä tietosuojaperiaatteita. Henkilötietojen käsittelyssä noudatetaan seuraavia vaatimuksia:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus
- rekisterinpitäjän osoitusvelvollisuus

Tässä tietotilinpäätöksessä kuvataan, miten em. periaatteet toteutuvat kunnan toiminnassa. Sipoon kunnan tietotilinpäätös on kokonaisuudessaan julkinen raportti.

2.2 Tietosuojan ja tietoturvan organisointi, ohjeistus ja koulutus

Sipoon kunnalla on tietosuoja- ja tietoturvapolitiikka, viimeisin päivitetty versio on hyväksytty Kunnanhallituksessa 12.3.2019. Yleiset tietoturvavastuut ja tiettyihin tehtäviin liittyvät tietoturvavastuut on kuvattu tietosuoja- ja tietoturvapolitiikassa.

2.2.1 Henkilötietojen tekniset ja organisatoriset suojauskeinot

Henkilötietojen käsittelyssä käytettävien tietojärjestelmien hallinnassa noudatetaan kunnan tietoturvasäännöstöä ja tietosuojaohjeita. Teknisesti tietojärjestelmät ja niiden käyttöliittymät ovat suojattu mm. palomuurilla ja järjestelmien tiedot varmuuskopioidaan säännöllisesti.

Tietojärjestelmien käyttöoikeudet on käyttöoikeusryhmien avulla rajattu siten, että kullakin käyttäjällä on pääsy vain työtehtävissään tarvitsemiinsa tietoihin. Käytönvalvontaa toteutetaan eri tietojärjestelmissä olevilla lokeilla. Tällä hetkellä kunnassa ei ole keskitetty käyttöoikeuksien hallintaa. Tarkoitus on, että IT-palvelut vastaavat keskitetystä käyttöoikeuksien hallinnasta. Käyttöoikeuksien hallinnan tekninen alusta on hankittu vuonna 2020 ja sen käyttö aloitetaan kevään 2021 aikana. Tämän projektin myötä järjestelmiin määritellään tehtävien mukaiset oikeudet sekä käyttöoikeudet pidetään ajantasaisina (TiHL 16§).

IT-palvelut-yksikkö vastaa työasemien, mobiililaitteiden, palvelimien, verkkolaitteiden ja muiden järjestelmien hankinnasta, käyttöönotosta ja ylläpidosta. Työasemien asennuspalvelu on ulkoistettu. Sovellushankinnat hoidetaan yhteistyössä sovellusta käyttävän yksikön, hankintapalveluiden ja IT-palveluiden kesken. Järjestelmien etäkäyttö tapahtuu salattujen yhteyksien kautta.

2.2.2 Kunnan tietoturvallisuus- ja tietosuojariskit

Tietoturvapoikkeamiin varautumisesta on Tietoturvapoikkeamiin hallinta -ohje. Vuoden 2019 aikana käyttöön otettu työntekijöiden tietoturvailmoituslomake on käytössä edelleen. Havaitut ja tietoon tulleet tietoturvapoikkeamat kirjataan ja luokitellaan yhtenäisesti, jonka jälkeen Tietoturvatiimi käsittelee ne määritellyn prosessin mukaisesti. Tämä mahdollistaa yhtenäisen ja asiantuntevan toimenpiteiden suunnittelun, koordinoinnin ja dokumentoinnin.

Covid-19-pandemian vuoksi osa kunnan työntekijöistä siirtyi keväällä tekemään etätöitä. Tietoturva, tietosuoja ja nettiturvallisuus ovat etätyössä kotona yhtä tärkeitä elleivät jopa tärkeämpiä kuin työpaikalla.

Etätyöhön liittyy tietoturvariskejä. Työntekijän tulee noudattaa etätyössä kunnan tietoturvasta ja tietosuojasta antamia ohjeita sekä raportoida mahdollisista tietoturvaa vaarantavista seikoista esimiehelleen ja Tietoturvatiimille. Tietoturvatiimi on antanut tarkentavia ohjeita etätyön tekemisestä ja yhteisistä menettelytavoista. Kunnan on turvattava palvelut kuntalaisille myös pandemian aikana. Tämä on asettanut haasteita tietoturvatyölle. Etätyöskentelyssä IT-ympäristön suojaaminen on tärkeää ja tähän työhön on panostettu. Vuoden aikana on korostunut myös tietoturvaan liittyvien kontrollien tarve, kuten järjestelmiin pääsyn tarkkailu ja tietoliikenteen valvonta.

Tietosuoja-asetus edellyttää tietoturvallista tietojenkäsittelyä ja sen jatkuvaa monitorointia. Kunnan on tullut määritellä ja toimeenpanna sekä henkilöstön että asiakastiedon turvaamiseksi tekniset ja organisatoriset toimenpiteet. Tämä vaatimus korostuu nyt, kun tieto liikkuu vapaammin fyysisten rajojen yli. Kunnan tulee lisäksi testata, tutkia ja arvioida säännöllisesti toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Kyberrikollisuus on herännyt koronan tuomiin mahdollisuuksiin. Kyberrikolliset ovat tehneet jo tietojen kalastelua ja haittaohjelmien levittämistä organisaatioiden toimintamallimuutoksia hyödyntäen. Tietoturvapoikkeamat voivat muodostua tietosuoja- tai muulle viranomaiselle raportoitaviksi asioiksi sekä aiheuttaa suurta tuhoa toiminnalle. Siksi on tärkeää, että kunta on varautunut toimintaohjein mahdollisia kyberturvallisuuden uhkatilanteita varten. Tämä työ kehitetään jatkuvasti kunnalla.

Merkittävin kybermaailman uhkatekijä oli edelleen vuonna 2020 organisaatioihin kohdistettu sähköpostitilien tietojenkalastelu, jonka tarkoituksena oli saada haltuun työntekijöiden sähköpostitunnuksia. Sipoon kunta on ottanut asteittain käyttöönsä muun muassa pilviteknologiaan perustuvan sähköpostipalvelun vuodesta 2018 alkaen, ja näiden käyttäjätunnuksia on yritetty kalastella vuoden 2020 aikana selvästi aikaisempaa vuotta enemmän. Tämä ilmiö on näkynyt myös valtakunnallisella tasolla, muun muassa Kyberturvallisuuskeskuksen varoituksissa. Sähköposteihin liittyvä eritasoinen tietojenkalastelu voidaan arvioida suurimmaksi yksittäiseksi kuntaan vuonna 2020 kohdistuneeksi uhaksi.

Vuonna 2020 lisääntyivät myös ns. huijauspuhelut. Puheluidenkin tavoitteena on saada haltuun työntekijöiden käyttäjätunnuksia. Varastetuilla käyttäjätunnuksilla tavoitellaan yleensä taloudellista hyötyä seuraamalla organisaation maksuliikennettä. Lisäksi onnistuneeseen tietojenkalasteluun liittyy erilaisia maine- ja sääntelyriskejä. Lähes aina tietojenkalastelun seurauksena vaarantuu henkilötietoja, jolloin tapahtumasta on tehtävä ilmoitus tietosuojavaltuutetulle. Mikäli riski arvioidaan korkeaksi, on oltava yhteydessä myös loukkauksen kohteena oleviin henkilöihin.

Uudet kalastelukampanjat muuttuvat yhä älykkäämmiksi, jolloin niiden torjuminen on vaikeampaa. Vuonna 2020 henkilöstön tietoisuutta tietojenkalastelun vaaroista lisättiin koulutuksilla ja ohjeilla ja asiasta tiedotettiin toistuvasti kunnan Intrassa. Kunnassa on 15.4.2020 otettu käyttöön monivaiheinen tunnistautuminen (MFA), jolla kyetään pienentämään tuntuvasti tietojenkalasteluun lankeamisen todennäköisyyttä.

Riskien osalta kunta on arvioinut, että suurin riski on loppukäyttäjässä. Inhimillinen virhe on yleisemmin syynä tietoturvaloukkaukseen kuin koneen tekemä virhe. Tämä tarkoittaa sitä, että rikollinen osapuoli, on hyödyntänyt pääsääntöisesti ihmisiin kohdistuvaa haavoittuvuutta tai poikkeama on johtunut inhimillisestä virheestä joko prosessissa tai yksittäisen henkilön työtehtävissä. Tietoturvallisuuden kehittämisessä tulee teknisen kyvykkyyden lisäksi huomioida prosessien turvallisuus sekä haavoittuvuuksien inhimillinen ulottuvuus. Siksi kunta on erityisesti panostanut henkilöstön informointiin, ohjeistuksiin ja koulutuksiin. Lisäksi Tietoturvatiimi vierailee työyksiköissä pyydettäessä.

2.2.3 Riskienhallinta ja tietoturvapoikkeamien käsittely

Vuosittain käydään läpi IT-riskienarviointi. Arviointiin kuuluvat myös tietosuoja- ja tietoturvariskit. Vaikutustenarviointi tehdään aina otettaessa käyttöön uutta teknologiaa, käsiteltäessä laajamittaisesti erityisiä henkilötietoryhmiä (EU:n yleinen tietosuoja-asetus, artiklat 9 ja 10) koskevia henkilötietoja sekä muissa valvontaviranomaisen ohjeistamissa tilanteissa.

Tietoturvapoikkeamiin varautumisesta on Tietoturvapoikkeamien hallinta -ohje. Kaikki tietoturvapoikkeamat kirjataan järjestelmään.

2.3 Kunnan ohjeistukset

Tietosuoja- ja tietoturvapolitiikkaa täydentävät tietoturvasäännöt, henkilöstön tietoturvaohjeet, tietosuoja- ja tietoturvaohjeet sekä koulutusaineistot. Henkilökunta sitoutuu salassapitoon työsopimuksessaan. Erillinen tietoturvasitoumus vaaditaan kaikilta työntekijöiltä. Sitoumus tulee olla allekirjoitettu sähköisesti. Mikäli tietoturvasitoumusta ei ole allekirjoitettu, käyttäjätunnukset lukitaan. Vuoden 2020 aikana otettiin käyttöön Sipoon ”Salassapito- ja tietoturvasitoumus”. Kaikkien ulkopuolisten ostopalveluiden, kuten konsulttien ja projektinvetäjien sekä muiden henkilöiden, joilla on pääsy Sipoon kunnan tietoihin ja järjestelmiin, tulee jatkossa allekirjoittaa erillinen ”Salassapito- ja tietoturvasitoumus”.

Vuoden 2020 aikana Tietoturvatiimi on laatinut tai uudistanut seuraavia kunnalla käytössä olevia dokumentteja:

Ohjeet:

- Tietoturva etätyössä / Datasäkerhet i distansjobb
- Turvallisuusopas uusi normaali COVID19 jälkeen / Säkerhetsopus Livet efter COVID19
- Tunnista kalasteluansa
- Selaustietojen poisto
- Conditional Access ja MFA
- Tiedossa olevat ongelmat ja ratkaisut (MFA)
- Miten otan O365 salasanapalvelun käyttööni / Hur jag tar O365 lösenordtjänsten ibruk
- Miten vaihdan salasanan itse / Hur byter jag själv mitt lösenord
- Sopimukset henkilötiedot ja EUn tietosuoja-asetus
- Discord
- Outlook Appin sähköpostin allekirjoituksen määrittäminen (Android)
- Tietoturva Perusteet Wistec

Lomake:

- Salassapito- ja tietoturvasitoumus kolmas sopijapuoli

Johtuen Covid-19 -pandemiasta, Tietoturvatiimi on tiedottanut Intrassa entistäkin enemmän sekä tietosuojaan että tietoturvaan liittyvistä asioista. Myös valtuutetuille on viestitetty enemmän Tietoturvatiimin puolesta. Tietoturvatiimi on vuoden 2020 aikana ohjeistanut muun muassa seuraavista asioista:

- Turvaposti ja Avauslinkki (päivitys Avauslinkin käyttöönoton jälkeen)
- Useita varoituksia sähköpostitse saapuvista tietojenkalasteluviesteistä
- Koronavilkku työpuhelimeesi
- Käytännön muutoksia kameravalvonnan käsittelyssä
- Microsoft 10 -Ohjelmiston tietoturvapäivitys
- Näin teet Teams-kokouskutsun
- Osallistuminen Zoom-sovelluksen kautta koulutukseen/tapahtumaan
- Pieni muistutus koskien tietoturvaa ja -suojaa
- Signal- pikaviestintäpalvelu
- WhatsApp-sovelluksen asentaminen Sipoon kunnan hallitsemiin mobiililaitteisiin
- Sipoo-aiheinen taustakuva Teamsissä
- Teamsin käyttö asiakastyössä ja sisäisessä käytössä
- Tietoturvatiimin terveiset poikkeusoloaikana
- Turvatulostus
- Tallennatko tiedostot oikeaan paikkaan?

2.4 Kunnan tietosuojakoulutukset

Henkilöstön osaamisen seuranta ja kehittäminen on avainasemassa, sillä globaalisti on arvioitu, että 50 % tietoturvapoikkeamista johtuu inhimillisistä virheistä. Koulutuksilla ja tietoisuuden lisäämisellä voidaan kustannustehokkaasti vähentää tällaisia poikkeamia. Henkilöstölle on järjestetty tietosuojasta ja tietoturvasta yleiskoulutuksia sekä yksikkökohtaisia koulutuksia. Koulutukset on järjestetty kustannustehokkaasti yhteistyössä KUUMA-kuntien kanssa.

Sipoon kunnassa on käytössä tietosuojan ja tietoturvan verkkokoulutus, joka on otettu käyttöön jo vuonna 2018 koko henkilöstölle ja luottamushenkilöille. Koulutus on kaikille työntekijöille ja luottamushenkilöille pakollinen. On todettu, että raportointi on tällä hetkellä vaikeaa ja työläistä. Seuraavalla raportointikaudella tulemme tekemään muutoksia verkkokoulutusta koskevaan prosessiin. Jatkossa perehdytyksen yhteydessä edellytetään, että tietosuoja ja tietoturvakoulutus on suoritettu sekä tietoturvasitoumus allekirjoitettu. Mikäli koulutusta ei suoriteta, työntekijän tai luottamushenkilön käyttäjätunnukset lukitaan. Ennen tunnusten lukitsemista asiasta kerrotaan hyvissä ajoin Intrassa. Käyttäjätunnusten lukitsemisen ajankohdan lisäksi kehotetaan työntekijöitä suorittamaan koulutukset ja hyväksymään tietoturvasitoumus.

2.5 Kunta osallistuu JUDO-hankkeeseen

Digi- ja väestötietoviraston Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma, JUDO-hanke, kehittää julkisen hallinnon digiturvan johtamista ja hallintaa, henkilöstön digiturvaosaamista sekä tarjoaa tukea turvallisempien palveluiden kehittämiseksi. Digitaalinen turvallisuus käsittää viisi osa-aluetta: riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvallisuuden, kyberturvallisuuden sekä tietosuojan. JUDO-hanke tukee julkista hallintoa turvallisten ja luotettavien palveluiden kehittämisessä vuosina 2019–2021. Sipoon kunta osallistuu tähän hankkeeseen, jonka kautta saamme käyttöömme nykyaikaisia menetelmiä, työkaluja ja malleja digiturvallisuuden johtamisen ja hallinnan kehittämisen tueksi.

2.6 TAISTO- harjoitukset

Sipoon kunta osallistui valtakunnalliseen TAISTO19-harjoitukseen marraskuussa 2019. Harjoituksen perusteella havaittuja haasteita on kartoitettu ja niille on etsitty ratkaisuja vuoden 2020 aikana. Vuoden 2020 Taisto-harjoituksen ilmoittautumisen ollessa ajankohtainen, päätti kunnan johtoryhmä, että Sipoon kunta ei osallistu vuoden 2020 Taisto-harjoitukseen, jonka aiheena oli tietovuodon käsittely. Harjoittelun sijaan päätettiin varmistaa, että edellisen harjoituksen perusteella saadut kehittämiskohteet saadaan tehtyä ja harjoittelun sijaan käytettiin aikaa siihen, että käytiin läpi kunnassa tosielämässä tapahtunut tietovuoto-tapaus.

Tähän kunnan itse järjestämään tapahtumaan osallistui edustus kunnan johdosta, tietosuojasta, tietoturvasta, IT-palveluista ja viestinnästä. Sipoossa tapahtuneen tapauksen käsittely koettiin hyödylliseksi ja havainnot on viety kehittämiskohteiksi ja ne on aikataulutettu.

2.7 Mistä henkilötiedot saadaan ja mihin niitä siirretään?

Henkilöstön, kuntalaisten ja eri sidosryhmiin kuuluvien henkilötiedot saadaan pääsääntöisesti rekisteröidyiltä itseltään tai eri viranomaisilta.

Henkilötietoja voidaan siirtää kunnan sisäisiin palveluihin, esim. työsuhteen hoitamiseksi käsiteltäviä henkilötietoja ja työntekijöiden henkilötietoja voidaan siirtää kunnan eri järjestelmien välillä. Henkilökunnan henkilötietoja luovutetaan toisille rekisterinpitäjille ainoastaan asianomaisen suostumuksella tai lainsäädännön perusteella.

Lähtökohtaisesti kunta ei siirrä henkilötietoja EU:n tai ETA:n ulkopuolelle lukuun ottamatta tiettyjä palveluiden toteuttamisen kannalta tarpeellisia henkilötietoja (mm. käyttäjätunnus, sähköpostiosoite ja nimi). Henkilöstön tiedot ovat nähtävillä kunnan julkisilla verkkosivuilla, joita voi katsoa myös EU-alueen ulkopuolelta.

Henkilötietojen siirrot on tarkemmin kuvattu tietosuojaselosteissa, jotka löytyvät Sipoon kunnan verkkosivuilta.

2.8 Verkkopalveluympäristöt ja muut ICT-palvelut

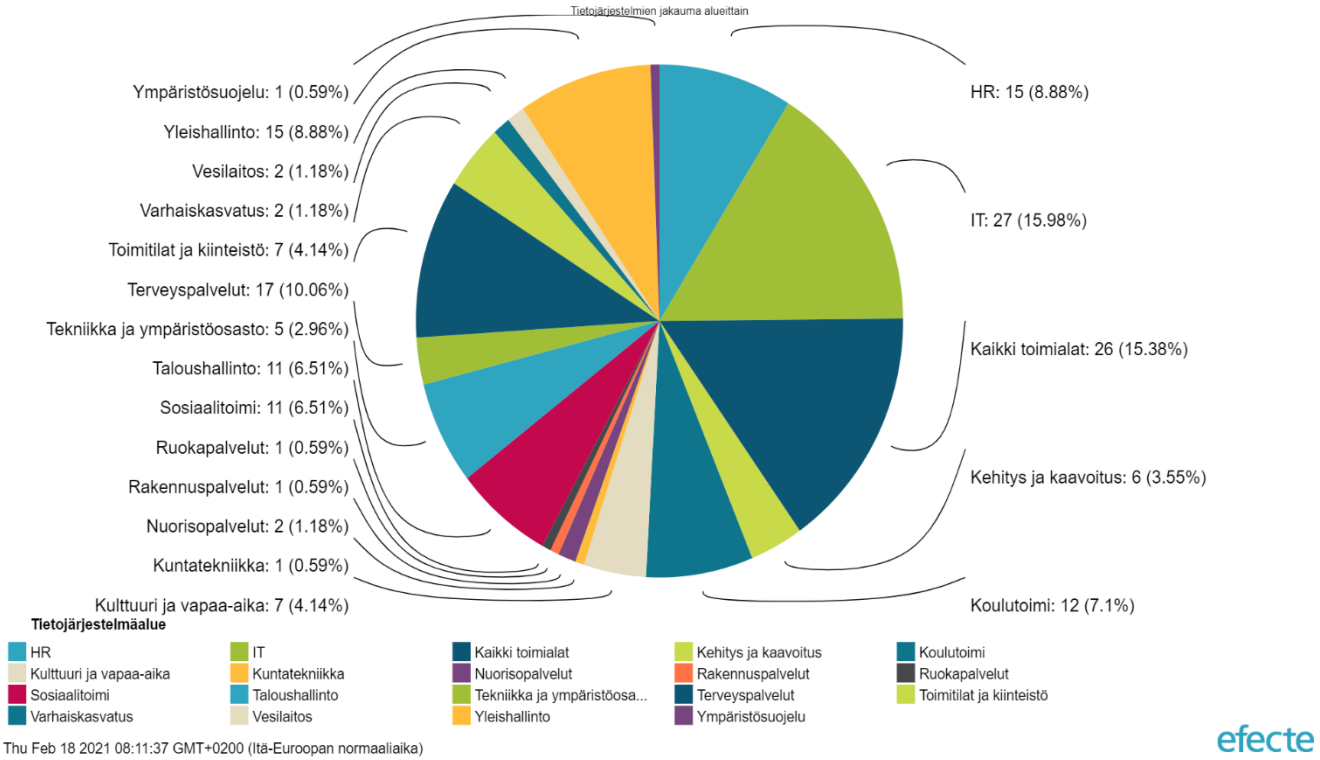
IT- yksikkö tuottaa kunnan toiminnalle välttämättömiä infrapalveluja, kunnan yhteisiä palveluja sekä toimiala- ja/tai tulosyksikkökohtaisia palveluja. Infrapalveluihin kuuluvat kokonaisuudet ovat loppukäyttäjäpalveluita, tietoliikennepalvelut, palvelin- ja kapasiteettipalvelut sekä käyttäjähallinta. Yhteiset ja toimiala tai tulosyksikkökohtaiset palvelut pitävät sisällään sovellukset sekä järjestelmät.

Tietotojärjestelmät on hankittu eri aikoina eri toimittajilta, eivätkä ne siksi muodosta arkkitehtuuriltaan yhtenäistä kokonaisuutta. Sipoossa käytettävät tietojärjestelmät luokitellaan niiden vaikuttavuuden ja vaativuuden perusteella. Luokituksessa vaikuttavuuteen liittyvät kriteerit liittyvät suoraan kunnan prosessien kriittisyyteen.

Järjestelmän kriittisyys:

Kriittinen: Järjestelmän toimimattomuus haittaa merkittävästi palvelutoimintaa tai estää sen kokonaan
Tärkeä: Järjestelmän toimimattomuus haittaa palvelu- tai tukitoimintaa
Hyödyllinen: Järjestelmän toimimattomuus haittaa vähäisesti palvelu- tai tukitoimintaa
Vähäinen: Apu- tai tukijärjestelmä, järjestelmä tehostaa työtä, mutta toimimattomuudesta ei ole sanottavaa haittaa.

Tietojärjestelmien kriittisyysluokka ei korreloi automaattisesti henkilötiedon käsittelyn laajuutta tai järjestelmän sisältämää henkilötiedon määrää tai laatua. Se on henkilötiedon käsittelyyn liittyen suuntaa antava ja kuvastaa tietojärjestelmien suhdetta prosessien kriittisyyteen jatkuvuuden hallinnan näkökulmasta.



Rekisteriin liittyvät tietojärjestelmät määritellään tietosuojaselosteessa. Ne tietokokonaisuudet ja tietovarannot, joita käsitellään tietosuojaselosteessa määritellyllä tavalla, muodostavat rekisterin. Rekisteri on teknologiariippumaton, ja se voi käsittää useita tietovarantoja. Esimerkiksi henkilöstötietoja käsittävä rekisteri voi muodostua HR-tietokannasta, paperiarkistoissa olevista työsopimuksista ja vaikkapa sisäisistä työvuorolistoista; määräävää on se, että rekisterissä tiedot esitellään jäsennellyssä muodossa ja että rekisterin eri ilmentymissä henkilöstötietoja käsitellään samalla, tietosuojaselosteessa määritellyllä, tavalla.

Kunta käyttää paljon ulkoistettuja palveluja palvelutuotannossaan sekä erilaisten pilviteknologioitten hyödyntäminen on kasvanut. Etenkin pilvipalveluihin siirryttäessä riskienhallinnan merkitys korostuu.

2.9 Hankinnat ja sopimusten tietosuoja

Sipoo solmii sopimustoimittajiensa kanssa määrämuotoisia sopimuksia, joissa huomioidaan tietoturvaan, tietosuojaan ja jatkuvuuden hallintaan liittyvät kokonaisuudet. Riippuen tuotettavan palvelun laadusta, kriittisyydestä ja arvosta, sopimusehtoja ja liitteitä tarvittaessa tarkennetaan.

Kaikissa hankinnoissa käytetään ensisijaisesti kunnan omia sopimusmalleja ja kulloinkin voimassa olevia julkishallintoon soveltuvia yleisiä ehtoja. Mikäli toimittaja käsittelee kunnan salassa pidettävää tietoa, edellytetään erillisen turvallisuussopimuksen tekemistä. Mikäli toimittaja käsittelee henkilötietoja kunnan puolesta tai lukuun, sopimukseen tulee liitteeksi EU:n tietosuoja-asetukseen pohjautuvat erityisehdot, joka on Kuntaliiton suosittelema liite henkilötietojen käsittelystä.

Tietosuoja-asetus edellyttää, että henkilötietojen käsittelystä on sovittava sopimuksella tai muulla oikeudellisella asiakirjalla, joka sitoo käsittelijää. Tämän vuoksi sellaiset sopimukset, joissa kunta oli ulkoistanut henkilötietojen käsittelyä palveluntuottajalle, oli päivitettävä vastaamaan asetuksen vaatimuksia. Sopimusten päivittäminen oli yksi EU:n tietosuoja-asetuksen tärkeimmästä kohdista. Strategiaksi valittiin riskiperusteinen lähestymistapa: kaikkein arvokkaimmat sopimukset päivitettiin ensimmäiseksi. Etusijalle asetettiin myös sellaiset sopimukset, joihin liittyi korkean riskiluokan tiedon käsittelyä. Sopimusten päivittäminen oli vielä vuoden 2019 Tietotilinpäätöksessä tunnistettu kehittämiskohde. Vuonna 2020 varmistettiin vielä, ettei meillä ole päivittämättömiä sopimuksia esimerkiksi siitä syystä, että ne puuttuvat asianhallintajärjestelmästä. Tämän lisäksi uutta sopimushallinnan ohjeistusta on valmisteltu ja ohjeistuksen odotetaan valmistuvan alkuvuodesta 2021.

2.10 Asiakirjahallinto ja arkisto

Organisaation on lainsäädännön mukaan tiedettävä, mitä tietoja sillä on hallussaan. Oikeusturvan ja julkisuusperiaatteen toteuttamiseksi organisaation on kuvattava, mitä tietoja sillä on hallussaan ja mitä käsittelysääntöjä tietoon liittyy. Kokonaisvaltaisella tiedonhallinnan suunnittelulla varmistetaan tiedon käytettävyys, eheys, laatu ja tietosuoja. Tiedonhallintaa toteutetaan tiedonohjaussuunnitelman (TOS), tiedonhallintamallin sekä asiakirjahallinnon ja arkistoinnin ohjeistusten avulla.

Arkistointivelvoitteiden ja eräiden lakisääteisten tiedonvaihtovelvoitteiden vuoksi kunnalla käsitellään yhä paljon paperista aineistoa. Asiakirjojen sähköiseen käsittelyyn siirrytään sitä mukaa, kun digitaaliset mahdollisuudet kehittyvät ja ne ovat lakisääteisten tehtävien näkökulmasta hyväksyttäviä sekä sopivat kunnan kokonaisarkkitehtuuriin. Suurin muutos kunnassa on tietojenkäsittelyn käytänteiden uudistamisessa ja vanhoista tavoista poisoppimisessa.

Rekisterinpitäjänä kunta huolehtii siitä, että käsiteltävät tiedot suojataan asianmukaisesti, olipa kyseessä tietojärjestelmä tai paperinen aineisto. Tallennettuja tietoja, käyttöoikeustietoja, sekä muita turvallisuuden kannalta kriittisiä tietoja käsitellään luottamuksellisesti ja vain niiden työntekijöiden toimesta, joiden työnkuvaan se kuuluu.

Sisäisessä arvioinnissa on todettu, että arkistoinnin tilassa on kehittämistä. Asiakirjahallinto pyrkii ohjeistamaan osastoja aineistojen käsittelyssä ja arkistoinnissa sekä päivittämään ohjeistuksia entistä säännöllisemmin. Organisaatiossa monilla osastoilla tietokatkokset, resurssien ja arkistoinnin perustietojen puute sekä jo pitkään jatkunut arkistointikäytäntöjen rapautuneisuus aiheuttavat ongelmia ja ohjeistamisessa on paljon tehtävää. Monet osastot ovat kuitenkin alkaneet osoittaa kasvavaa kiinnostusta arkistointikysymyksiin ja ohjeistukset pyritään ottamaan vastaan ja käytäntöjä parantamaan. Asiakirjojen käsittelyn ja arkistoinnin ajantasaisten ja toimivien käytäntöjen tuominen systemaattisesti osaksi osastojen toimintatapoja on pitkän aikavälin tavoite.

Asiakirjahallinto tekee tiedonhallinnan kokonaistavoitteiden saavuttamiseksi jatkuvaa yhteistyötä IT-osaston kanssa. Arkistoasioiden yhteistyöverkostona osastojen kesken toimii Arkistointiryhmä, joka kokoontuu tarvittaessa.

Alkuvuodesta 2020 tapahtunut kunnan hallinnon muutto uusiin toimitiloihin edellytti ratkaisuja myös arkistoaineistojen osalta. Muuton yhteydessä lähiarkistojen aineistoa on hävitetty paljon, mutta aineistojen seulonta ja hävittäminen jatkuu johtuen aineiston suuresta määrästä. Osa seulotusta lähiarkistoaineistosta puhdistettiin ja siirrettiin uusien toimitilojen arkistotiloihin. Päätearkisto sekä osa vanhasta lähiarkistoaineistosta jäi kuitenkin vielä toistaiseksi vanhoihin toimitiloihin odottamaan seulontaa ja mahdollista digitointia.

Sipoon kunnassa on tarkoitus ottaa käyttöön prosessien nykytilaa kuvaava ja SÄHKE2-vaatimuksia vastaava tiedonohjaussuunnitelma (TOS) vuoden 2021 alussa. Tiedonohjaussuunnitelma ohjaa prosesseja asianhallintajärjestelmän taustalla sekä toimii ajantasaisena ohjeistuksena asiakirjojen säilytysaikoja ja salassapitoa koskevissa kysymyksissä. Tiedonohjaussuunnitelma on myös edellytys sähköiseen arkistointiin siirtymiselle.

Vuoden 2020 aikana on laadittu prosessikuvaukset osastojen substanssiosaajien kanssa työpajoissa siten, että projektiryhmä on vetänyt, ohjannut ja opastanut työtä. Prosessikuvausten yhteydessä on käyty läpi myös prosesseihin liittyvät kehittämistarpeet.
Tiedonohjaussuunnitelmaa tulee pitää jatkuvasti ajan tasalla siten, että osastot ilmoittavat asiakirjahallinnolle päivitystarpeesta. Tiedonohjaussuunnitelman käyttöönoton myötä Sipoon kunnan monilta osin vanhentuneet ja puutteelliset arkistonmuodostussuunnitelmat (AMS) ovat lakanneet olemasta voimassa.

3 Tietojenkäsittelyyn vaikuttava lainsäädäntö

Sipoon kunnassa on ollut henkilötietolain mukaiset rekisteriselosteet kaikista eri käyttötarkoituksen omaavista henkilörekistereistä. Tietosuoja-asetus ei edellytä rekisterikohtaisia selosteita, vaan selosteet rekisterinpitäjän käsittelytoimista sekä läpinäkyvää informointia henkilötietojen käsittelystä.

Kunnassa on laadittu sisäiseen käyttöön tietosuoja-asetuksen artiklan 30 mukainen seloste käsittelytoimista ja sen lisäksi kuvaukset henkilötietojen käsittelystä on julkaistu/ollaan julkiasemassa kunnan kotisivuilla.

Henkilötietojen käsittelyä ohjaavat mm. seuraavat dokumentit:

- Tietosuoja- ja tietoturvapolitiikka
- Riskienhallintapolitiikka
- Tietoturvasäännöt ja -ohjeet
- Tietosuojaselosteiden mallipohjat
- Vaikutustenarvioinnin ohjeet ja mallipohjat
- Tietopyyntöohjeet ja lomakkeet
- Henkilökunnalle tarkoitetut tiedotteet ja ohjeistukset Intrassa

Henkilötietojen käsittelyyn kunnassa vaikuttava keskeinen lainsäädäntö:

- Kuntalaki (410/2015)
- Hallintolaki (434/2003)
- EU:n yleinen tietosuoja-asetus (EU 2016/679)
- Tietosuojalaki (1050/2018)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki sähköisen viestinnän palveluista (917/2014)
- Laki tietoyhteiskuntakaaren muuttamisesta (68/2018)
- Laki julkisen hallinnon tiedonhallinnasta 906/2019
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Arkistolaki (831/1994)
- Hankintalaki (1397/2016)
- Kirjanpitolaki (1336/1997)
- Työsopimuslaki (55/2001)
- Työturvallisuuslaki (738/2002)
- Yhdenvertaisuuslaki (1325/2014)
- Laki naisten ja miesten välisestä tasa-arvosta (609/1986)
- sekä toimialakohtaiset erityislait

Tässä luvussa kuvataan, miten lainmukaisuus, kohtuullisuus ja läpinäkyvyys tietosuojaperiaatteina toteutuvat Sipoon kunnan toiminnassa.

4 Rekisteröidyn oikeudet ja niiden toteuttaminen

Sipoon kunta kerää ja käsittelee asiakkaidensa henkilötietoja vain siinä määrin kuin se on tarpeellista palvelun tuottamiseksi. Henkilötietoja käsitellään rekisterin käyttötarkoituksen mukaan. Rekistereistä on laadittu EU:n yleisen tietosuoja-asetuksen mukaiset tietosuojaselosteet. Asiakkaalla on oikeus tietää, mitä tietoja hänestä kerätään. Jos tiedoissa on virheitä tai tiedot ovat epätarkkoja, asiakas voi vaatia niiden oikaisemista.

Jos tiedonkeruu perustuu suostumukseen, asiakas voi milloin tahansa peruuttaa antamansa suostumuksen ja vaatia tietojensa poistamista. Kunnan palveluista suurin osa perustuu kuitenkin lakisääteisen velvoitteen noudattamiseen tai julkisen vallan käyttämiseen tai yleisen edun toteuttamiseen (usein mm. arkistointi, tilastointi, kehittämishankkeet). Asiakas ei voi niihin liittyvissä tapauksissa vaatia tietojensa poistamista.

Sipoon kunta pyrkii noudattamaan henkilötietojen käsittelyssä läpinäkyvyyttä ja tietojen täsmällisyyttä asetuksen mukaisesti (artikla 5). Informointivelvoitteen täyttämiseksi käytetään toistaiseksi tietosuojaselosteita. Hyväksytyt ja ajantasaiset tietosuojaselosteet löytyvät kunnan nettisivuilta (artiklat 13 ja 14).

Sipoon kunnan verkkosivuille on avattu Tietosuojasivusto rekisteröidyille asian tiedottamista varten. Verkkosivuilta löytyvät rekisteröityjen oikeuksiin perustuvat tarkastuspyyntö- ja oikaisupyyntölomakkeet (artiklat 15, 16).

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille 72 tunnin kuluessa. Vuoden 2020 aikana tehtiin kaksi (2) ilmoitusta tietosuojavaltuutetulle.

Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta on ilmoitettava rekisteröidylle ilman aiheetonta viivytystä silloin, kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietoturvaloukkauksista ilmoittaminen (artikla 33) tapahtuu tietoturvatiimin harkinnan mukaan. Rekisteröityihin tietosuojavastaava on yhteydessä kirjeitse tai puhelimitse. Mikäli tietoturvaloukkaus koskee isoja määriä rekisteröityjä, asiasta tiedotetaan myös kunnan verkkosivuilla.

5 Seuranta ja mittaaminen

Tietosuojan ja tietoturvan tilaa vuonna 2020 voidaan kuvata seuraavin tunnusluvuin:

Perustietotekniikka ja puhelimet:

- Tietojärjestelmiä 160 kpl
- Tietokoneita 4028 kpl sisältäen opiskelijoiden koneet (muutos edelliseen vuoteen +13 kpl)
- Monitoimilaitteet 91 kpl (muutos edelliseen vuoteen -11 kpl)
- Puhelin- ja dataliittymiä 1149 kpl (vuonna 2019 tavallisia puhelinliittymiä 891 kpl)
- ICT-tikettien määrät: Tikettejä yhteensä 8 159 kpl (muutos edelliseen vuoteen +2 489 kpl) Näistä tukipyytöjä 3 968 kpl (muutos +1 599 kpl) ja tilauksia 4 191 kpl (muutos +890 kpl)

Yleisen tietosuoja-asetuksen perustella saapuneet henkilötietojen tarkastus-, oikaisu- ja poistopyynnöt:

Tarkastuspyynnöt: 6 kpl
Oikaisupyynnöt: 0 kpl
Poistopyyntö: 0 kpl
Käyttö- ja luovutuslokipyynnöt: 0 kpl

Tietoturvapoikkeamat:

Tietoturvaloukkausilmoitukset 22 kpl
Vakavat tietoturvapoikkeamat: 0 kpl
Esille tulleet tietosuojarikkomukset ja niiden epäillyt: 0 kpl

Koulutusmäärät:

Verkkokoulutus koko henkilöstölle ovat suorittaneet n. 90-95% henkilöstöstä
Luottamusmiesten koulutus ovat suorittaneet 96% luottamusmiehistä
Esimiesten täydennyskoulutus on suorittaneet 90% esimiehistä
Tietosuojakoulutukset henkilöstölle: 3 kpl

6 Todennetut kehittämiskohteet ja katsaus tulevaisuuteen

EU Yleinen tietosuoja-asetus on otettu organisaatiossamme vastaan kiitettävästi ja organisaatio pyrkii vastaamaan asetuksen tuomiin haasteisiin, joskin monella osa-alueella on vielä kehitettävää. Keskeisenä ohjaavana dokumenttina toimii jo edellä mainittu tietosuojapolitiikka ja tietoturva.

Itsearviointi osoittaa, että monella osa-alueella asetuksen vaatimuksenmukaisuus on parantunut viime vuodesta, mutta kehittämiskohteitakin löytyy.

6.1 Tietoturva- ja tietosuojaryhmän uudelleenmuodostaminen

Sipoon kunnalla on päätoiminen tietosuojavastaava ja osatoiminen tietoturvavastaava, jotka muodostavat yhdessä kunnan Tietoturvatiimin. Tietoturva- ja tietosuojaryhmä kokoontui 8 kertaa vuonna 2018, mutta henkilöstömuutoksien takia ryhmä ei kokoontunut vuonna 2019. Uusi ryhmä oli tarkoitus perustaa vuoden 2020 aikana, mutta kunnassa ei ole vuoden aikana perustettu tietoturva- ja tietosuojaryhmää kunnanjohtajan toimesta.
Kunnanjohtaja asettaa vuoden 2021 aikana ryhmän seuraamaan tietosuojan toteutumista, tekemään kehitysehdotuksia sekä toimimaan toimialojen tietosuojavastaavien sekä järjestelmien pääkäyttäjien tukena. Toimialoja ja avainyksiköitä tullaan pyytämään nimeämään edustajat ryhmään. Tavoitteena on saada ryhmään laaja kattaus eri alojen asiantuntijoita tietosuojasta, tietoturvasta, riskienhallinnasta, ICT:stä ja juridiikasta. Ryhmän on tarkoitus raportoida puolivuosittain tietoturvan ja tietosuojan toteutumisesta kunnan johtoryhmälle.

6.2 Uudistetun lainsäädännön vaatimuksiin vastaaminen

Tiedonhallintalaki astui voimaan 1.1.2020. Laissa säädetään muun muassa julkisen hallinnon yleisistä velvoitteista tiedonhallintaan, julkisen hallinnon tiedonhallinnan yleisestä ohjauksesta, tietoaineistojen muodostamisesta ja sähköisestä luovuttamisesta, julkisen hallinnon tietoturvallisuuden perusteista, teknisten rajapintojen hyödyntämisestä sekä asianhallinnasta ja tietoaineistojen säilyttämisestä. Kuntasektorin näkökulmasta on merkittävää, että lain on tarkoitus kumota valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010), jolloin tietoturvalle asetettavat vaatimukset tulevat jatkossa tietohallintalaista ja ne ovat velvoittavia kuntatoimijoille.

Ensimmäisessä vaiheessa tiedonhallintamallin olisi pitänyt olla valmis vuoden 2021 alussa. Pandemian aiheuttaman työtaakan vuoksi, osa työstä on jäänyt tekemättä. Sipoon kunnassa on tiedonhallinnan kehittämisen työlistalla tulevina vuosina muun muassa
- lokitietojen kerääminen
- asianhallinta
- asiarekisteri ja tietoturvallisuusvaatimukset
- tietoturva- ja tietosuoja-asioiden riskien- ja vaikutusarvioinnin kehittäminen
- tietoturva- ja tietosuoja-asioiden korostaminen pakollisena vaatimuksena järjestelmähankinnoissa

Digitaalisen tiedon määrä kasvaa jatkuvasti kiihtyvällä vauhdilla. Kunnan toiminnassa digitaalista tietoa syntyy mm. erilaisista palvelutapahtumista, liikkumisesta tai vaikkapa rakennuksista. Kasvava tietomäärä mahdollistaa täysin uudenlaisten palveluiden kehittämisen, mutta se myös asettaa kasvavia vaatimuksia tiedonhallinnalle ja tietojenkäsittelylle.

Valmisteilla oleva, kuntia velvoittava lainsäädäntö esimerkiksi avoimen datan osalta tulee haastamaan kuntaa sekä taloudellisesti että resursoinnin osalta.

Tiedonhallintalain suositukset ovat tietoturvallisuuden kannalta haasteellisia, koska ne nojaavat jo vanhentuneeseen Vahti-ohjeistukseen ja siksi velvoitteet ovat osittain epäselviä. Vaatimuksiin liittyvät kansalliset palvelut eivät ole valmistuneet aikataulussaan, joten näiltä osin haasteet koskevat kaikkia kuntia.

Digitalisoinnilla ja datan turvallisella hyödyntämisellä pyritään rakentamaan kuntalaisille asiakaslähtöiset, luotettavat ja kustannustehokkaat palvelut. Tämä kaikki edellyttää, että tietosuojasta ja tietoturvasta huolehditaan riittävällä tasolla. Tietosuoja- ja tietoturvaperiaatteet tulee siis konkretisoida käytännön tasolle ja istuttaa osaksi organisaation toimintaa.

Kunta kartoittaa vuoden 2021 aikana markkinoilla olevia lokitusjärjestelmiä (SIEM) ja kartoituksen jälkeen kunnan lokipolitiikka määrittelee tiedot, jotka siirtyvät keskitettyyn lokitusjärjestelmään. Kunta seuraa tiedonhallintalautakunnan suosituksia lokitietojen keräämiseen.

Käyttäjähallinnan osalta kunta on hankkinut vuonna 2020 Efecten IGA-järjestelmän, jonka avulla kunnalla on valmius toteuttaa käyttäjienhallintaa tiedonhallintalain puitteissa vuoden 2021 aikana. Käyttäjätunnusten ajantasaisuus varmistetaan kytkemällä käyttäjätunnusten voimassaolo työntekijän työsopimukseen. IGA-järjestelmässä käyttöoikeudet toteutetaan työntekijän tehtävien mukaisesti.

Tietojen siirtämiseen on panostettu päivittämällä yhteydet salatuiksi. Kunnan ICT on teettänyt vuonna 2020 ISO-27001 auditoinnin tietoturvallisuuden osalta. Auditoinnin perusteella tehdään kehittämistoimenpiteitä jo vuoden 2021 aikana. Yleisellä tasolla voidaan mainita, että auditoinnin perusteella Sipoota suositeltiin kehittämään tietoturvallisuuteen liittyvät strategiat ja linjaukset ja varmistamaan riittävät henkilöstöresurssit ICT:n ja tietoturvallisuuden kehittämiseen.

Suomi.fi-tunnistaminen on lisääntynyt viranomaisjärjestelmissä viime vuonna merkittävästi. Sipoossa on selvitetty erilaisia vaihtoehtoja henkilöstön tunnistamiseen, jotta henkilökohtaisia tunnisteita ei tarvitsisi käyttää työssä. Kuntaan on päätetty hankkia DVV:n organisaatiokortit, joilla voidaan vahvasti tunnistautua järjestelmiin, jotka hyödyntävät suomi.fi-tunnistautumista. Organisaatiokorttien avulla on mahdollisuus myös sähköiseen allekirjoittamiseen, joka täyttää ylimmän EIDAS-asetuksen tason. DVV kuuluu Traficomin hyväksyttyihin luottamuspalveluiden tarjoajiin.

6.3 Harjoitustoiminnan kehittäminen

Harjoitusten kautta opitaan toimimaan turvallisemmin. Henkilöstön osaamisen kehittäminen harjoitustoiminnan kautta (esimerkiksi Taisto-harjoitukset) on tehokasta ja samalla jatkuvuuden hallinta turvataan. Siksi on järkevää kehittää kunnan harjoitustoimintaa seuraavalla raportointikaudella. Tämä vaatii budjetointia ja henkilöstöresursointia. Jotta saamme myös palveluntuottajamme osallistumaan harjoitustoimintaan, tulee sitoutuminen tähän vaatia jo kilpailutuksissa ja sopimuksissa. Harjoitustoiminnan pitkäjänteinen suunnittelu on välttämätöntä organisaation toiminnan jatkuvuuden turvaamiseksi.

6.4 Jatkuvuuden hallinta

Jatkuvuudenhallinnalla tarkoitetaan toimintamallia, jolla organisaatio rakentaa valmiuden ja kyvyn hoitaa keskeisimmät tehtävät kaikissa tilanteissa. Jatkuvuudenhallinta on prosessi, jolla tunnistetaan toiminnan uhat ja niiden vaikutukset sekä luodaan kattava malli toimintakyvyn hallinnalle. Jatkuvuuden hallinta pitää sisällään kriisinhallinnan, jatkuvuus- ja toipumissuunnittelun.

Jatkuvuuden hallintaa voidaan kuvata myös seuraavilla toimenpiteillä:
- Tunnistaa toimintansa uhkat, riskit, häiriötilanteet ja riippuvuudet
- Arvioi uhkien vaikutukset organisaatiossa ja sen toimijaverkostossa
- Organisoi ja toteuttaa menettelytavat häiriötilanteiden varalle
- Varmistaa kriittisten kumppaneidensa kyvyn toimia häiriötilanteissa
- Suojaa ydintoimintansa intressit ja arvontuotantokykynsä.

Kunnan tulee pystyä hoitamaan kriittiset tehtävänsä ja turvata asukkaiden hyvinvointi ulkoisen tai sisäisen toimintaympäristön häiriöistä, uhkista ja riskeistä huolimatta. Sipoossa jatkuvuuden hallintaa ohjataan ydintoiminnoista sekä niistä prosesseista, joilla voi olla vaikutuksia asiakkaiden terveydelle tai hyvinvoinnille, alkaen. Jatkuvuuden hallintaa ei ole järkevää ulottaa joka tasolle, mutta edelleen tulee tulevana raporttikautena panostaa sopimusten kautta varmistamaan, että jatkuvuuden hallinta on otettu huomioon. Muuttuvassa digitalisoituvassa maailmassa jatkuvuuden hallinta on jatkuvasti ns. agendalla.

6.5 Tietosuojan merkitys kasvaa

Tietosuojan merkitys kasvaa jatkuvasti digitalisoituvassa ja verkottuvassa maailmassa. Digitalisaation myötä henkilötietoja halutaan hyödyntää yhä laajemmin. Informaatioteknologia ja digitalisoituminen vaikuttavat keskeisesti siihen, miten henkilötietoja käsitellään ja miten kunkin yksilön ja organisaation tulisi omassa toiminnassaan tähän suhtautua. Joudumme lähes päivittäin tekemään päätöksiä siitä, mihin annamme tai emme anna itseämme koskevia tietoja. Henkilötiedot ovat nykypäivänä maksuväline, joten ne ansaitsevat huolellista käsittelyä samalla tavalla kuin raha. Henkilötietoja käytetään maksuvälineenä internetissä ja niitä myydään ja ostetaan eri toimijoiden toimesta.

Tietovuotoja havaitaan jatkuvasti. Vuoden 2020 eniten julkisuutta herättänyt tapaus lienee Vastaamo. Monissa kunnissakin identiteettivarkauksia on tapahtunut, vaikka niitä ei julkisuudessa usein noteeratakaan. Työntekijän sähköisen identiteetin suojaaminen on tänä päivänä yhtä tärkeää kuin henkilökohtaisen identiteetinkin suojaaminen.

Lainsäädäntöä tarvitaan turvaamaan yksilön oikeuksia ja vapauksia. Henkilötietoja käsiteltäessä ja uusia toimintoja suunniteltaessa tulee aina huolehtia siitä, ettei yksilön oikeudet, vapaudet eikä oikeusturva vaarannu. Tällä rakennetaan myös luottamus kunnan ja kuntalaisten välille. Kuntalainen voi luottaa siihen, että hänen henkilötietojaan käsitellään lainmukaisesti ja tietoturvallisesti. Pääsy hänen tietoihinsa on vain henkilöillä, jotka tarvitsevat hänen tietojaan työtehtävien hoitamiseen.

Johdon vahva sitoutuminen henkilötietojen käsittelyn kehittämiseen ja parantamiseen on välttämätöntä. Resursointi tulee olemaan tärkeää ja esim. koko henkilöstölle suunnatut koulutukset tulee jatkuvasti kehittää ja olla tarjolla muuttuvassa digitalisoituvassa maailmassa.

Henkilötietojen käsittelyyn ja hallintaan on Sipoon kunnalla kiinnitetty entistä enemmän huomiota. Tietotilinpäätös kertoo henkilötietojen käsittelyn nykytilanteen ja sen pohjalta on hyvä lähteä kehittämään entistä parempaa henkilötietojen käsittelyä Sipoossa.