Tietotilinpäätös 2021

Sipoon kunta

18.2.2022

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.

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 kriittisten järjestelmien tiedot varmuuskopioidaan säännöllisesti.

Tietojärjestelmien käyttövaltuudet on käyttöoikeusryhmien avulla rajattu siten, että kullakin käyttäjällä on pääsy vain työtehtävissään tarvitsemiinsa tietoihin. Käytönvalvontaa toteutetaan eri tietojärjestelmissä olevilla lokeilla ja tarpeen mukaisilla käyttövaltuuksien auditoinneilla. Kunnassa on käyttöönotettu vuonna 2021 keskitetty identiteetin- ja käyttövaltuushallinnan järjestelmä. Käyttövaltuushallinnan laajentaminen kaikkiin kunnan järjestelmiin on vielä kesken, mutta tarkoitus on saada työ valmiiksi vuoden 2022 aikana. IT-palvelut vastaavat keskitetystä käyttövaltuuksien hallinnasta ja järjestelmien omistajat järjestelmiensä käyttöoikeuksien toteuttamisesta. Identiteetin- ja käyttövaltuushallintaprojektin 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 tietosuojavastaava (lokakuusta 2021 alkaen ulkoinen palvelu Privaon Oy:stä) käsittelee ne määritellyn prosessin mukaisesti. Tämä mahdollistaa yhtenäisen ja asiantuntevan toimenpiteiden suunnittelun, koordinoinnin ja dokumentoinnin. Tarvittaessa IT-palvelut auttaa.

Covid-19-pandemian vuoksi osa kunnan työntekijöistä oli etätyössä suurimman osan vuodesta 2021. 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 keväällä 2021.

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.

Merkittävin kybermaailman uhkatekijä oli edellisten vuosien tapaan myös vuonna 2021 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 2021 aikana taas edellisiä vuosia enemmän. Tämä ilmiö on näkynyt myös valtakunnallisella tasolla, muun muassa Kyberturvallisuuskeskuksen varoituksissa.

Vuonna 2021 jatkuivat 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.

Vuonna 2021 Suomessa levisi laajasti FluBot-haittaohjelma. Ohjelma pyrki leviämään tekstiviestien kautta ja suomalaisille lähetettiin jopa 70 000 haittaohjelmaviestiä vuorokaudessa. Tekstiviestejä tuli myös Sipoon kunnan puhelimiin runsaasti. Toistuva varoittelu kunnan intrassa tehosi melko hyvin ja vain muutama työntekijä avasi viestejä. IT-palvelut pystyi estämään haittaohjelman leviämisen.

Sipoon kunnassa tehdään jatkuvaa ohjeistusta ja viestintää tietojenkalastelun vaaroista, jotta kunnan ympäristön lisäksi työntekijät osaavat suojata henkilötietojaan myös työn ulkopuolisessa arjessa. Kunnassa on jo vuonna 2020 otettu käyttöön monivaiheinen tunnistautuminen (MFA), jolla kyetään pienentämään tuntuvasti tietojenkalasteluun lankeamisen todennäköisyyttä.

Riskikartoituksissa on voitu todeta, että suurin riski on edelleen loppukäyttäjässä. Laitteen tai ohjelmiston virhe on harvinaisempi syy tietoturvaloukkaukseen kuin ihmisen tekemä virhe. Myös rikolliset hyödyntävät tätä haavoittuvuutta. Pääsääntöisesti rikollisten yritykset kohdistuvat siis työntekijöihin ohjelmistoissa mahdollisesti olevien haavoittuvuuksien sijaan. Tietoturvallisuuden kehittämisessä tulee teknisen kyvykkyyden lisäksi näin ollen huomioida myös prosessien turvallisuus sekä haavoittuvuuksien inhimillinen ulottuvuus. Siksi kunta on erityisesti panostanut henkilöstön informointiin, ohjeistuksiin ja koulutuksiin.

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. Jo 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”.

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. Perehdytyksen yhteydessä edellytetään, että tietosuoja ja tietoturvakoulutus on suoritettu ja tietoturvasitoumus allekirjoitettu. Mikäli koulutusta ei suoriteta, työntekijän tai luottamushenkilön käyttäjätunnukset lukitaan. Ennen tunnusten lukitsemista asiasta kerrotaan Intrassa ja annetaan mahdollisuus hoitaa velvoite kuntoon.

Vuoden 2021 aikana lähdettiin etsimään uusia ratkaisuja henkilöstön kouluttamiseen. Aikaisemmat, erittäin laajat koulutukset on koettu raskaiksi ja niiden raportoinnin ominaisuudet on koettu heikoiksi. Tietosuojaan ja tietoturvaan liittyvät asiat myös muuttuvat koko ajan. On todettu, että yksittäistä ja laajaa koulutusta korvaamaan tai tukemaan pitäisi voida henkilöstölle jakaa vuoden aikana päivittyvää opastusta. Uuden ratkaisun etsimisessä on vaatimukseksi nostettu myös kyvykkyys niin sanotun mikro-oppimisen mahdollistamiseen eli siihen, että opastusta voidaan tiivistää ja jakaa tietoiskumaisiin kokonaisuuksiin, joiden omaksuminen voi olla monelle hektisessä arjessa helpompaa kuin pitkien ohjeistusten lukeminen tai webinaarien katsominen, joita jatkossakin toki tarjotaan.

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 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.

2.7 Verkkopalveluympäristöt ja muut ICT-palvelut

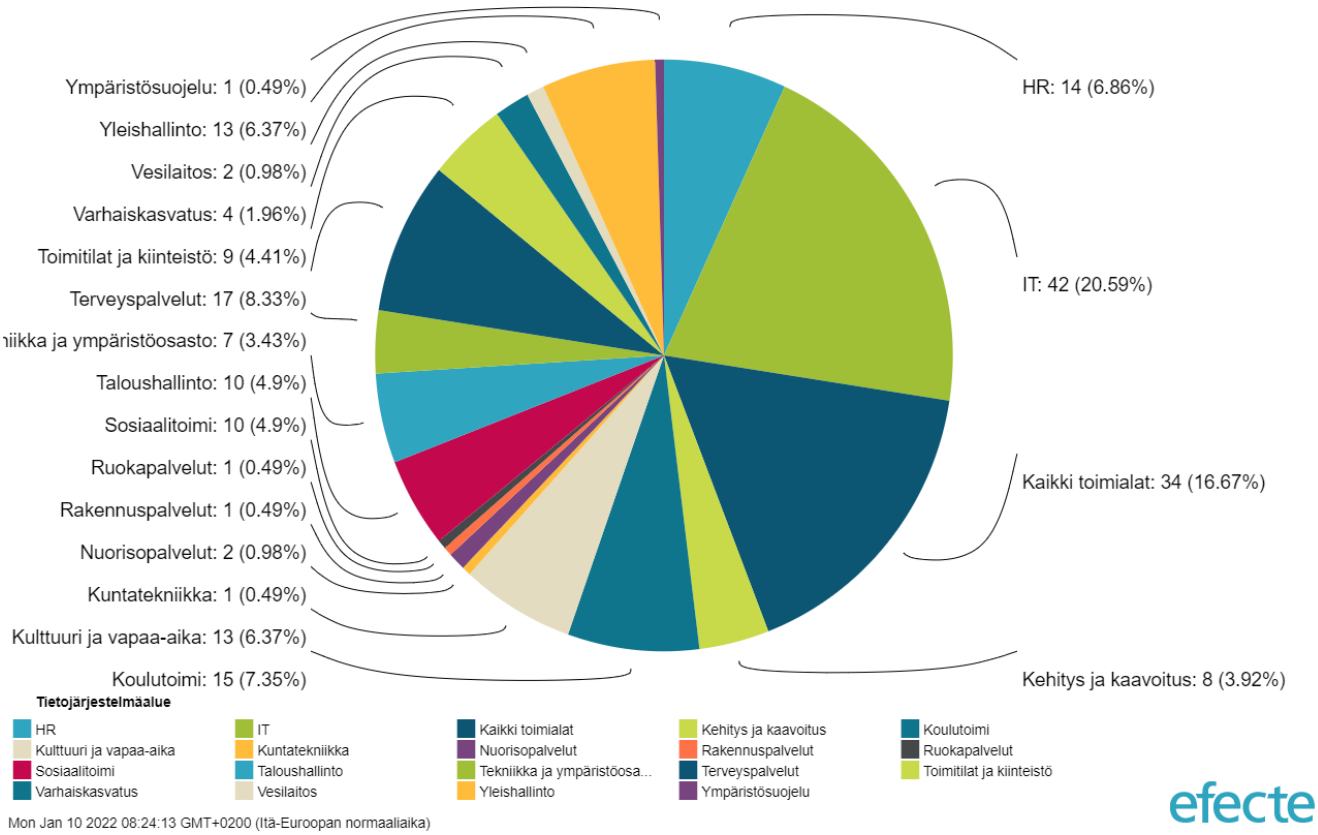
IT- yksikkö tuottaa kunnan toiminnalle välttämättömiä infrapalveluja, kunnan yhteisiä palveluja sekä toimiala- ja/tai tulosyksikkökohtaisia palveluja. Infrapalveluihin kuuluvat kokonaisuudet ovat loppukäyttäjäpalveluita, tietoliikennepalvelut, palvelin- ja kapasiteettipalvelut sekä käyttäjähallinta. 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.



Järjestelmäkartta 2021

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. Myös erilaisten pilviteknologioitten hyödyntäminen on kasvanut. Etenkin pilvipalveluihin siirryttäessä riskienhallinnan merkitys korostuu.

2.8 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.

Hankinnoissa käytetään 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.

Toimittajien sopimuspohjat käydään läpi ja varmistetaan, että niissä on riittävät tiedot kunnan näkökulmasta tietoturvaan ja tietosuojaan liittyen.

Tietosuoja-asetus edellyttää, että henkilötietojen käsittelystä on sovittava sopimuksella tai muulla oikeudellisella asiakirjalla, joka sitoo käsittelijää. Uusi sopimushallinnan ohje valmistui 2021 ja vuoden aikana varmistettiin, että kaikki sopimukset on päivitetty vastaamaan voimassa olevaa lainsäädäntöä.

Syksyllä 2021 Sipoon kunta haki ja sai Valtiovarainministeriöltä digitukirahaa SaaSec-hankkeelle. Hankkeeseen tuli mukaan myös muita KUUMA-kuntia. Hankkeessa tehdään konsepti ja sopimuspohjat SaaS-palveluiden hankintaan ja elinkaareen liittyen, jotta kunnilla olisi tulevaisuudessa määrämuotoinen tapa varmistaa sopimuksissa tietoturvaan ja tietosuojaan liittyvät käytännöt, auditoinnit mukaan lukien. Hanke osallistuu kauden 2021–2023 aikana myös ministeriön koordinoimiin turvallisuuteen liittyviin yhteishankkeisiin.

2.9 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 kuvausten ja ohjeistusten avulla.

Tiedonhallintalaki asettaa viranomaisille velvoitteita kuvausten, sähköisen arkistoinnin sekä tietoaineistojen saatavuuden ja hyödynnettävyyden osalta. Arkistointivelvoitteiden ja eräiden lakisääteisten tiedonvaihtovelvoitteiden vuoksi kunnalla käsitellään kuitenkin yhä paljon paperiaineistoa. Asiakirjojen sähköiseen käsittelyyn siirrytään sitä mukaa kun digitaaliset ratkaisut kehittyvät, tulevat lakisääteisten tehtävien näkökulmasta hyväksyttäviksi sekä sopiviksi kunnan kokonaisarkkitehtuuriin. Myös tietojenkäsittelyn käytänteiden uudistamisessa ja vanhoista tavoista poisoppimisessa on yhä tehtävää.

Rekisterinpitäjänä kunta huolehtii siitä, että käsiteltävät tiedot suojataan asianmukaisesti, olipa kyseessä tietojärjestelmä tai paperiaineisto. 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. Kunnan organisaatiossa monilla osastoilla tietokatkokset, resurssien ja arkistoinnin perustietojen puute sekä jo pitkään jatkunut arkistointikäytäntöjen rapautuneisuus aiheuttavat ongelmia. Monet osastot kuitenkin osoittavat kasvavaa kiinnostusta arkistointikysymyksiin ja pyrkivät parantamaan käytäntöjään.

Asiakirjojen käsittelyn ja arkistoinnin ajantasaisten ja toimivien käytäntöjen tuominen systemaattisesti osaksi osastojen toimintatapoja on pitkän aikavälin tavoite. Vuonna 2021 arkistointiohjeistuksen osastokohtainen pääpaino on ollut sosiaali- ja terveysosastolla, jossa ohjeistus on otettu hyvin vastaan ja monia käytännön parannuksia arkistoinnin perustarpeita ajatellen toteutettu.

Vuodesta 2023 alkaen Sipoon kunnan sosiaali- ja terveyspalvelut siirtyvät Itä-Uudenmaan hyvinvointialueen vastuulle. Sosiaali- ja terveyspalveluiden tiedonhallinnan ja arkistoinnin osalta hyvinvointialueelle siirtymisen valmistelu aloitettiin syksyllä 2021.

Asiakirjahallinto tekee tiedonhallinnan kokonaistavoitteiden saavuttamiseksi jatkuvaa yhteistyötä IT-osaston kanssa. Vuonna 2021 tärkeimmät yhteistyöalueet olivat tiedonhallintamallin laadinta, sähköisen arkistoinnin ja digitoinnin valmistelu sekä tietosuojakysymykset.

Kunnan hallinnon uusiin toimitiloihin muuton yhteydessä 2020 osa seulotusta lähiarkistoaineistosta puhdistettiin ja siirrettiin uusiin toimitiloihin. Päätearkisto sekä osa vanhasta lähiarkistoaineistosta jäi kuitenkin vielä toistaiseksi vanhoihin toimitiloihin odottamaan seulontaa ja mahdollista digitointia. Vuonna 2021 osastot jatkoivat vanhoissa toimitiloissa olevien aineistojensa seulontaa.

Aineistojen mahdollisimman laajamittaiseen digitointiin valmistautuminen on tärkeää, koska pysyvästi säilytettävän paperiaineiston vuosikasvu on jatkuvaa, mutta kunta ei tällä hetkellä investoi uusien arkistotilojen rakentamiseen. On kuitenkin muistettava, että osa päätearkistoaineistosta tullaan jatkossakin säilyttämään myös paperimuodossa kulttuurihistorialliseen arvoon perustuen. Päätearkistoaineiston paperiversioiden hävittämiseen tähtäävä digitointi edellyttää tällä hetkellä voimassa olevien määräysten mukaisesti Kansallisarkiston seulontapäätöstä. Osasta Sipoon kunnan päätearkistoaineistoa tehtiin seulontaesitys Kansallisarkistolle syksyllä 2021 ja seulontapäätöstä odotellaan 2022.

Yksi vuoden 2021 tärkeimpiä päätöksiä arkistoinnin kehittämisen osalta oli päätös kunnan kaikkein toimialojen yhteisen, pysyvästi säilytettävän aineiston yksinomaan sähköisen arkistoinnin mahdollistavan sähköisen arkiston hankinnasta. Sähköinen arkiston käyttöönoton tarkasta ajankohdasta ei kuitenkaan tässä vaiheessa ole vielä tietoa.

Sipoon kunnassa otettiin 1.1.2021 käyttöön prosessien nykytilaa kuvaava ja SÄHKE2-vaatimuksia vastaava tiedonohjaussuunnitelma (TOS) samanaikaisesti asianhallintajärjestelmä Dynasty10 -version käyttöönoton yhteydessä. Tiedonohjaussuunnitelman käyttöönoton myötä Sipoon kunnan monilta osin vanhentuneet ja puutteelliset arkistonmuodostussuunnitelmat (AMS) kumottiin.

Tiedonohjaussuunnitelma ohjaa prosesseja asianhallintajärjestelmän taustalla sekä toimii ajantasaisena ohjeistuksena asiakirjojen säilytysaikoja ja salassapitoa koskevissa kysymyksissä. Tiedonohjaussuunnitelma on myös edellytys sähköiseen arkistointiin siirtymiselle.

Tiedonohjaussuunnitelman ja asianhallintajärjestelmä Dynasty10 -version käyttöönotto on vaatinut organisaatiossa totuttelua, mutta tuonut positiivisia muutoksia. Uuden asianhallintajärjestelmäversion toiminnallisuudesta ja uudistuneesta tehtäväluokituksesta johtuen organisaation asianhallinta on nyt aiempaa jäsennellympää, tiedon löydettävyys on parantunut ja julkisuus- ja salassapitonäkökohdat tiedostetaan aiempaa selvemmin.

Tiedonohjaussuunnitelma pidetään ajan tasalla siten, että osastot ilmoittavat asiakirjahallinnolle päivitystarpeesta. Varsinkin vuoden 2021 alkupuolella päivityksiä tehtiin runsaasti. Jatkossa tiedonohjaussuunnitelmaa päivitetään edelleen osastojen tarpeiden mukaan.
Asiakirjajulkisuuskuvauksen laadinta aloitettiin 2021. Tavoitteena on saada asiakirjajulkisuuskuvaus valmiiksi 2022.

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:

- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- 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 (yleinen Tietosuoja-asetus, artikla 5). Informointivelvoitteen täyttämiseksi käytetään toistaiseksi tietosuojaselosteita. Hyväksytyt ja ajantasaiset tietosuojaselosteet löytyvät kunnan nettisivuilta (yleinen Tietosuoja-asetus, artiklat 13 ja 14).

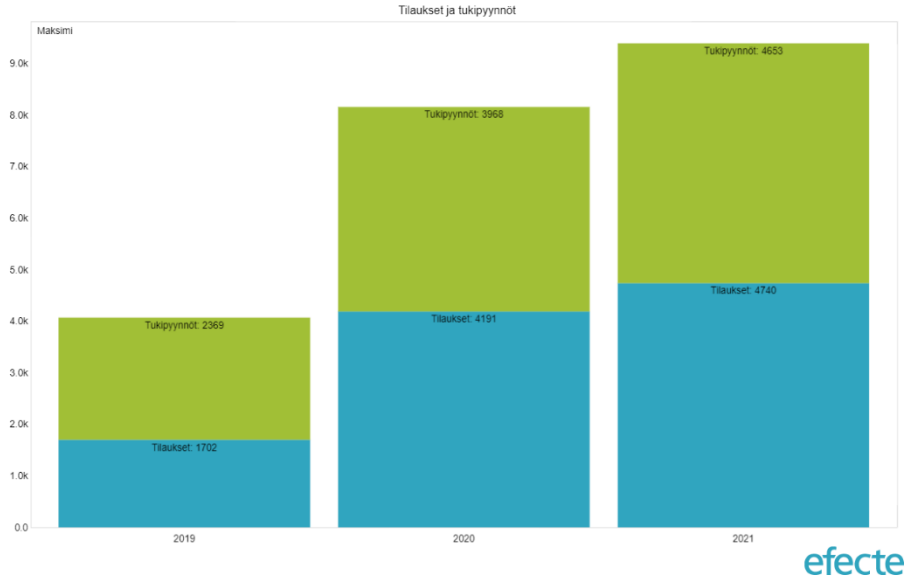
Sipoon kunnan verkkosivuille on avattu Tietosuojasivusto rekisteröidyille asian tiedottamista varten. Verkkosivuilta löytyvät rekisteröityjen oikeuksiin perustuvat tarkastuspyyntö- ja oikaisupyyntölomakkeet (yleinen Tietosuoja-asetus, artiklat 15, 16).

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.

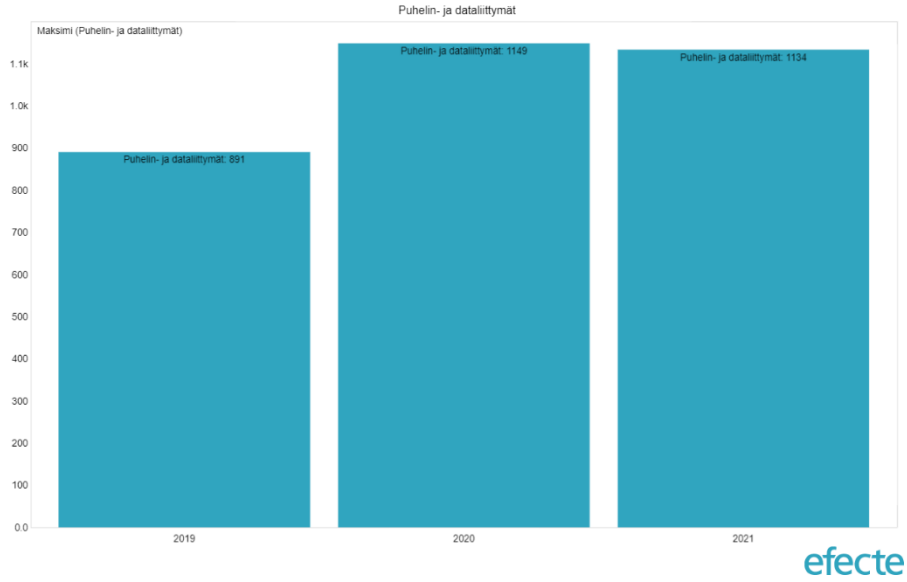
Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta on ilmoitettava rekisteröidylle ilman aiheetonta viivytystä silloin, kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietoturvaloukkauksista ilmoittaminen (artikla 33) tapahtuu tietoturvatiimin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

5 Seuranta ja mittaaminen

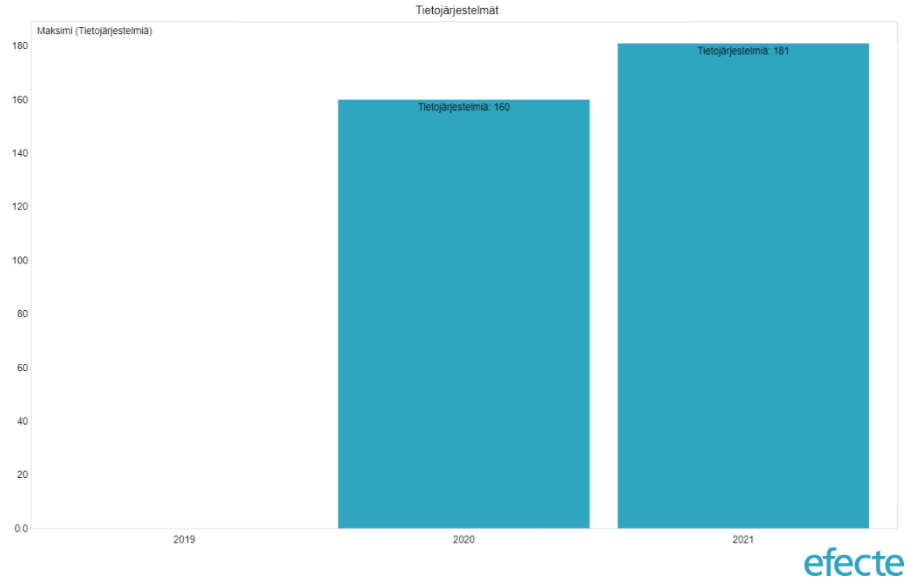
Tietosuojan ja tietoturvan tilaa sekä ICT-ympäristöä vuonna 2021 voidaan kuvata seuraavin tunnusluvuin:



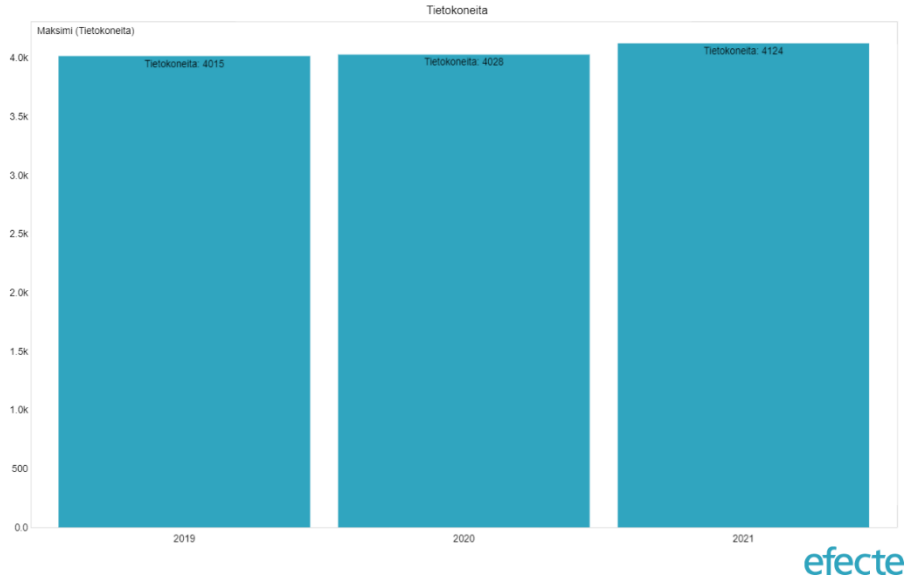
Kuva 1 Tilaukset ja tukipyynnöt



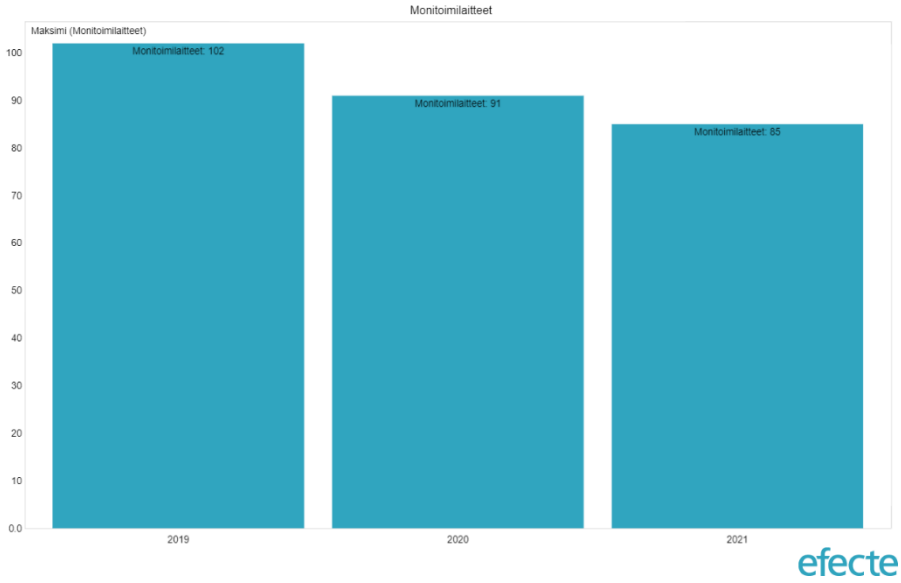
Kuva 2 Puhelin- ja dataliittymät



Kuva 3 Tietojärjestelmät

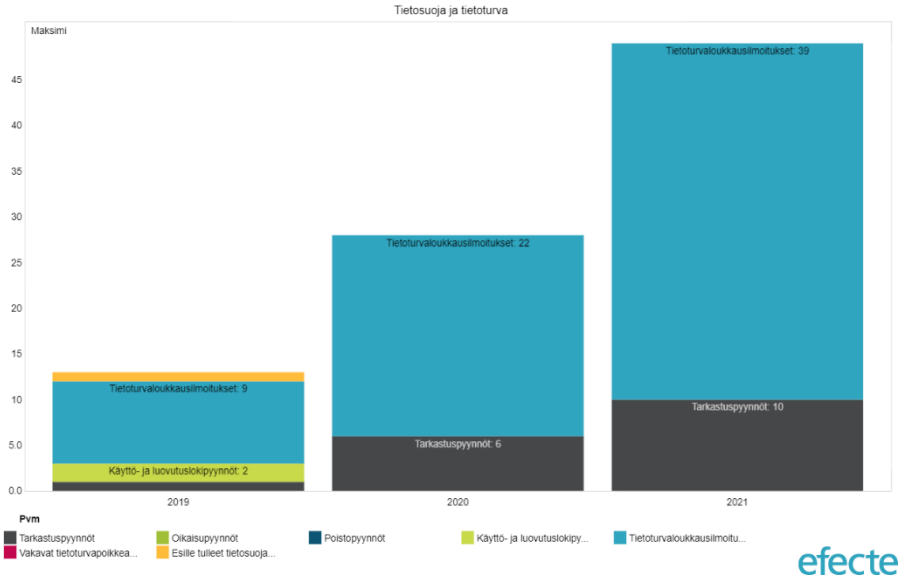


Kuva 4 Tietokoneita sisältäen opiskelijoiden koneet



Kuva 5 Monitoimilaitteet

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



Kuva 6 Tietosuoja ja tietoturva

Vuonna 2021 (kuva 6)
Tietoturvaloukkausilmoitukset 40 kpl
Tietosuojapoikkeamat: 4 kpl
Vakavat tietoturvapoikkeamat: 0 kpl
Esille tulleet tietosuojarikkomukset ja niiden epäillyt: 0 kpl

Koulutusmäärät:

Verkkokoulutuksen koko henkilöstölle on suorittanut noin 95% henkilöstöstä
Esimiesten täydennyskoulutuksen on suorittanut noin 90% esimiehistä
Tietosuojakoulutukset henkilöstölle: 4 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 jälleen edellisistä vuosista, mutta kehittämiskohteitakin löytyy.

Tietoturva- ja tietosuojaryhmä tulee jatkossa koordinoimaan kehittämistä.

6.1 Tietoturva- ja tietosuojaryhmän uudelleenmuodostaminen

Sipoon kunnalla on ollut aiemmin päätoiminen tietosuojavastaava ja osatoiminen tietoturvavastaava, jotka muodostivat yhdessä kunnan Tietoturvatiimin. Tietoturvavastaava irtisanoutui kesällä ja tietosuojavastaava lokakuussa. Lokakuussa kunnanjohtaja ja CDO päättivät ostaa tietosuojavastaavan palvelut Privaon Oy:stä, jotta kunta ei joudu tilanteeseen, jossa tietosuojavastaavaa ei ole ollenkaan. Joulukuun lopussa CDO aloitti uuden tietosuojavastaavan rekrytointiprosessin.

Kunnanjohtaja asetti marraskuussa uuden tietoturva- ja tietosuojaryhmän, johon johtoryhmässä nimettiin jäsenet eri toimialoilta. Ryhmä ei ehtinyt kokoontua enää marras-joulukuun aikana. Tietoturva- ja tietosuojaryhmä tulee seuraamaan tietosuojan toteutumista, tekemään kehitysehdotuksia sekä toimimaan toimialojen tietosuojavastaavien sekä järjestelmien pääkäyttäjien tukena. Ryhmän on tarkoitus raportoida puolivuosittain tietoturvan ja tietosuojan toteutumista kunnan johtoryhmälle.

Osaamista teknisen tietoturvan varmistamiseen ja parantamiseen tullaan jatkossa hankkimaan Tieran kautta.

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.

Tiedonhallintalain mukainen dokumentointi on aloitettu vuonna 2021. Dokumentointi on ollut pirstaleista ja siitä on ollut mahdotonta koostaa tiedonhallintamallia. Helmikuussa 2022 tullaan ottamaan käyttöön uusi Digiturvamalli (www.digiturvamalli.fi), jotta kaikilla toimialoilla päästään kuvaamaan tiedonhallintalain vaatimia kokonaisuuksia helpolla Teams-käyttöliittymällä. Kun kuvausten vähimmäistaso on saatu vietyä malliin, voidaan tiedonhallintamalli ladata palvelusta automaattisesti.

Digiturvamalli tulee sisältämään jatkossa Tiedonhallintamallin lisäksi GDPR-vaatimukset täyttävän dokumentoinnin, joka voidaan julkaista myös www.sipoo.fi-sivustoilla. Digiturvamalliin voidaan julkaista myös uutisia ja ohjeita henkilöstölle Tiedonhallintamalliin, GDPR-asioihin ja yleiseen tietoturvaan ja tietosuojaan liittyen.

Kunta kartoitti vuoden 2021 aikana markkinoilla olevia SIEM-järjestelmiä (Security Information and Event Management). Kartoituksen jälkeen määriteltiin kunnan lokipolitiikan mukaisesti tiedot, jotka siirtyvät keskitettyyn lokitusjärjestelmään. SIEM-järjestelmä ja sen mukana hankittu SOC (Security Operations Center) on hankittu palveluna ja sitä tuottaa kunnalle Insta Defsec. SIEM tarkkailee organisaation tietojärjestelmiä ja -verkkoja sekä hälyttää havaitessaan normaalista poikkeavaa toimintaa. Instan SOC-palvelu suojaa kriittisiä IT-järjestelmiä tunnistamalla vaikeasti torjuttavat hyökkäykset ja muut uhkatilanteet. Kun tunnistaminen tehdään mahdollisimman aikaisessa vaiheessa, poikkeamiin voidaan reagoida nopeasti ja minimoida vahingot.

Identiteetin- ja käyttövaltuushallinnan järjestelmä (Efecte IGA) on käyttöönotettu vuoden 2021 aikana. Työntekijöiden käyttäjätunnuksien ja niihin liitettyjen käyttövaltuuksien hallinta voidaan nyt toteuttaa tiedonhallintalain vaatimalla tavalla. Käyttäjätunnusten ajantasaisuus on varmistettu kytkemällä käyttäjätunnusten voimassaolo työntekijän työsopimukseen. IGA-järjestelmässä käyttöoikeudet toteutetaan työntekijän tehtävien mukaisesti, joko roolin kautta tai erikseen tilaamalla. Vaikka muutosvastarintaa onkin ollut paljon, henkilöstö alkaa vähitellen ymmärtämään, että identiteetin- ja käyttövaltuushallinnan tarkoitus ei ole kiusata henkilöstöä tai vähentää IT-palveluiden töitä vaan kyseessä on lain vaatima, uusi toimintatapa, joka lisää IT-palveluiden ja HR-palveluidenkin työtä. Toinen vaihtoehto hoitaa lain vaatima hallinta olisi ollut se, että jokainen yksikkö olisi itse ylläpitänyt rekisteriä ja lokia jokaisen työntekijän ja järjestelmän käyttöoikeuksista manuaalisesti. Tämä olisi kuitenkin koko kunnan tasolla vienyt työaikaa kymmenkertaisesti eikä prosessia olisi luultavasti koskaan saatu lain vaatimalle tasolle.

Kesällä 2021 asennettiin kuntaan uusi palomuuri ja vanha palomuuri poistettiin käytöstä. Laitteiden asennuksen jälkeen palomuurin asetukset saatiin nopeasti tehtyä. Syksyn aikana palomuuriin määriteltiin uusia suodattimia, joilla estetään Sipoon kunnan verkoista pääsy haitallisille sivustoille internetissä. Pääsy on estetty kokonaan sivustoille, joissa on suomessa laitonta sisältöä kuten lapsiporno, asemyynti ja huumeet. Palomuuri varoittaa käyttäjää sivustoista, jotka eivät ole suoraan laittomia, mutta on luokiteltu esimerkiksi haittaohjelmia sisältäviksi sivustoiksi tai sisällössä on seksiä tai väkivaltaa.

Opetuksen järjestämisessä tulee ottaa huomioon lukuisia ohjeita ja määräyksiä mm. henkilötietojen käyttöön, julkisuuteen ja yksityisyyden suojaan liittyen. Vuonna 2021 Sipoo otti käyttöön Luuppi-tietosuojapalvelun sivistystoimen tietosuojan hallintaan. Palvelun avulla Cloudpoint Oy:n tietosuoja-asiantuntijat tarkastavat, että oppilaitosten käytössä olevat digitaaliset palvelut ovat voimassa olevien tietosuoja-asetusten ja perusopetuslain mukaisia. Palvelulla varmistetaan, että opetuskäytössä ei ole digitaalisia palveluja, joissa on mainontaa tai muutoin asiatonta sisältöä. Kun palvelujen ensimmäinen tarkastus on tehty, Luupilla jatketaan opetuksen järjestäjän käyttämien palvelujen tietosuojan seurantaa, sillä palvelujen tietosuoja-asetukset voivat muuttua.

Suomi.fi-tunnistaminen on lisääntynyt viranomaisjärjestelmissä viime vuonna merkittävästi. Sipoossa linjattiin vuonna 2021, että kunta maksaa DVV:n organisaatiokortit niille työntekijöille, jotka joutuvat jatkuvasti tunnistautumaan eri palveluihin työnsä puolesta. Organisaatiokorttien avulla on mahdollisuus myös sähköiseen allekirjoittamiseen, joka täyttää ylimmän EIDAS-asetuksen tason. DVV kuuluu Traficomin hyväksyttyihin luottamuspalveluiden tarjoajiin. Organisaatiokortin lisäksi operaattorivaihdon myötä otettiin käyttöön myös mobiilivarmenteet. Henkilökohtaisessa käytössä olevien kunnan puhelinten liittymillä on mahdollisuus ottaa käyttöön mobiilivarmenne, jota voi käyttää tunnistautumiseen henkilökohtaisten pankkitunnusten sijaan. Mobiilivarmenteen käyttö on työntekijälle ilmainen. Sen käyttöönotto vaatii vahvan tunnistautumisen, mutta käyttö vaatii vain puhelimen. Organisaatiokorteilla ja mobiilivarmenteilla mahdollistetaan henkilöstön vahva tunnistautuminen ulkoisiin palveluihin.

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.

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.

Asiakkaat ovat koko ajan paremmin tietoisia omista oikeuksistaan heidän tietojensa käsittelyn osalta. Kunta panostaa siihen, että jatkossakin saamme vastattua tietopyyntöihin ja asiakkaiden tietosuojaa koskeviin kysymyksiin mahdollisimman ripeästi ja laadukkaasti.