Kuntaliitto
Kommunförbundet

Tiedonhallintalain vaikutuksen tietoturvaan

KTM, YTM erityisasiantuntija Tuula Seppo
Kuntaliitto, tietoyhteiskuntayksikkö

@tuula_seppo

Helsingin tietoturvapäivä
22.10.2019 klo 9.30-10.00 Stadin ammatti- ja aikuisopiston auditorio, Mäkelän koulu, Hattulantie 2

- Tietoturvallisuus tiedonhallintalaissa
- Huomioitu myös digipalvelulaki ja tietosuoja-asetus
- VM:n täytäntöönpano ohjeistus
- Mistä lähteä liikkeelle

Sisältö

Kuntaliitto
Kommunförbundet

Vaikutukset tietoturvallisuuteen

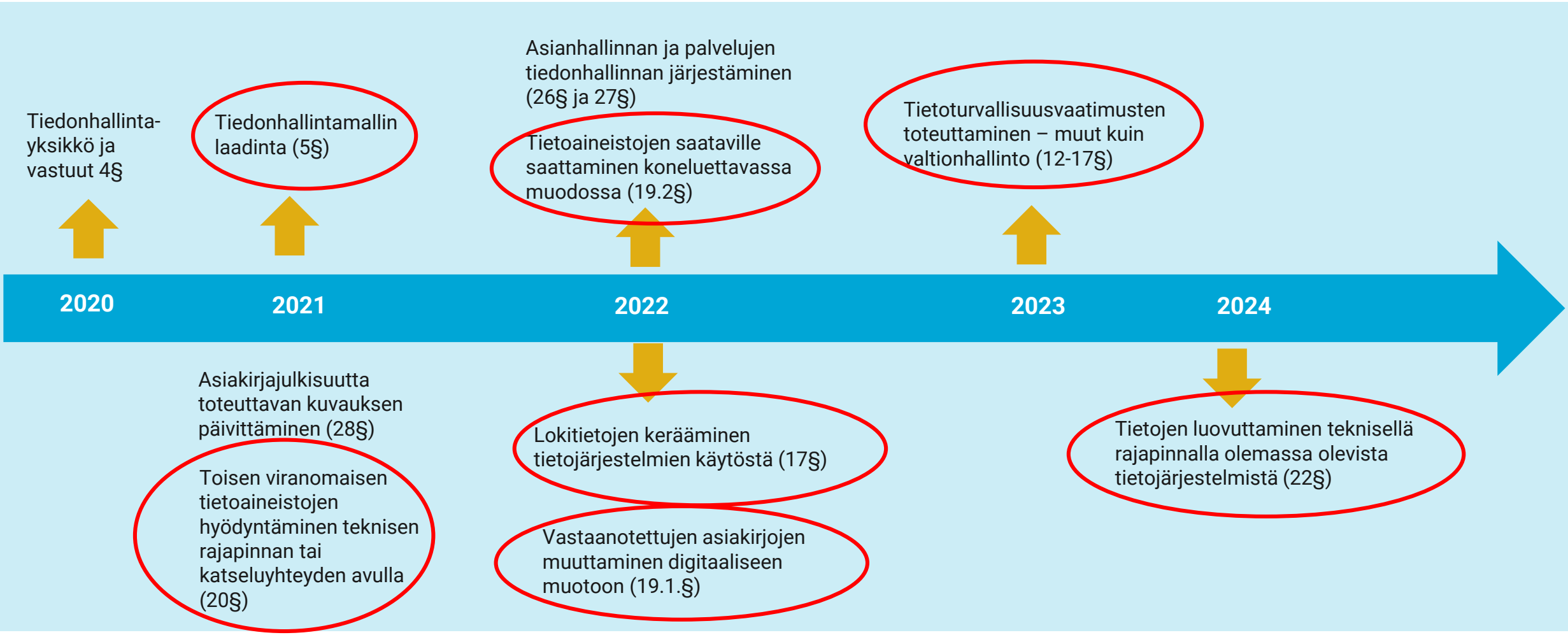
Kohti yhteentoimivaa yhteiskuntaa

Kuntaliitto
Kommunförbundet

- Tietoturvallisuus on huomioitava kaikissa käsittelyvaiheissa; kokonaistietoturvallisuus
- Tietoturvallisuuden merkitys korostuu digitaalisessa tietojenkäsittelyssä
- Tiedonhallintalaki asettaa minimivaatimukset tietoturvallisuudelle; luottamus
- Enemmän rajapintoja ja katseluyhteyksiä ja tiukemmat lokitusmääräykset
- Sääntely ulotetaan myös kunnallisiin viranomaisiin
- Tiedonhallintayksikössä tulee olla ohjeistus mm.:
  - Poikkeusoloihin varautumisesta sekä tietoturvallisuus-järjestelyistä

Siirtymäajat

- Laki tulee voimaan 1.1.2020
- Sisältää useita siirtymäaikoja



Kuntaliitto
Kommunförbundet

Tiedonhallintayksikön johdon vastuulla huolehtia

Kuntaliitto
Kommunförbundet

1. tiedonhallinnan toteuttamiseen liittyvien tehtävien **vastuiden** määrittelystä
2. ajantasaisista **ohjeista** koskien tietoaineistojen käsittelyä, tietojärjestelmien käyttöä, tietojenkäsittelyoikeuksia, tiedonhallinnan vastuiden ja tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuusjärjestelyistä sekä poikkeusoloihin varautumisesta
3. että tarjolla on **koulutusta** henkilöstölle ja tiedonhallintayksikön lukuun toimiville. Tulee olla riittävä tuntemus tiedonhallinnasta, tietojenkäsittelystä sekä asiakirjojen julkisuudesta ja salassapidosta koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista
4. asianmukaisista **työvälineistä**
5. riittävästä **valvonnasta**

Tiedonhallintayksikön johto ja vastuut kunnassa

- Vastuut on määriteltävä
  - tiedonhallintamallin ylläpidon ja
  - tietoaineistojen muodostamisen toteuttamiselle,
  - **tietoturvallisuuden** ja
  - asianhallinnan järjestämiselle,
  - tietojärjestelmien yhteentoimivuuden turvaamiselle sekä
  - tietoaineistojen säilyttämisen järjestämiselle.

- Tehtävien järjestäminen tarkoittaa asiakirjahallinnon ja tietohallinnon sekä muiden toimintojen vastuiden määrittämistä tiedonhallinnan velvollisuuksien ja palvelujen toteuttamiseksi

Tiedonhallintamallissa tietoturvallisuus

Kuntaliitto
Kommunförbundet

Minimisisältö tiedonhallintamallille
Toimintaprosessit (nimikkeet, vastuutaho, tarkoitus, lopputulos, sidokset muihin prosesseihin) kokonaiskuva
Tietovarannot (nimikkeet, kuvaukset tietovarantojen sidoksista niitä käyttäviin prosesseihin ja tietojärjestelmiin, käsittely selostetoimista sisältö (30 art.))
Tietoaineistot (tietoaineiston arkistoon siirtämisestä, arkistointitavasta, arkistopaikasta tai tuhoamisesta)
Tietojärjestelmät (nimikkeet, vastaava viranomainen, käyttötarkoitukset, liittymät muihin tietojärjestelmiin, tiedonsiirtotavat)
Tietoturvajärjestelyt (miten tietoturvallisuus toteutetaan, tekniset ja organisatoriset turvatoimet)

Tiedonhallintamallin tietoturva osio

- Viranomaisen on **suunniteltava ja toteutettava** tietoturvallisuustoimenpiteet siten, että ne kattavat asiakirjan kaikki käsittelyvaiheet sekä menettelytavat
- Tiedonhallintamalliin on sisällytettävät **määritykset** kunkin asiankäsittely- tai palveluprosessin tietoturvallisuusjärjestelyistä sekä tietojärjestelmien rajapinnoista

- Viranomaisen on **tunnistettava** yhteiskunnan toiminnan kannalta keskeisimmät toimintonsa ja niihin liittyvät tiedot sekä suojattavat kohteet, joiden tietoturvallisuudesta huolehtimiseen on kiinnitettävä erityistä huomiota
- Viranomaisen on hallittava häiriötilanteita

Laki digitaalisten palvelujen tarjoamisesta (306/2019)

- Viranomaisen on suunniteltava ja ylläpidettävä digitaaliset palvelunsa siten, että niiden tietoturvallisuus, tietosuoja, löydettävyys ja helppokäyttöisyys on varmistettu

- Lisäksi viranomaisen on varmistettava digitaalisten palvelujensa yhteensopivuus yleisesti käytettyjen ohjelmistojen ja tietoliikenneyhteyksien kanssa

Tietosuoja-asetus tietoturvallisuudesta

Kuntaliitto
Kommunförbundet

- Rekisterinpitäjät – kokonaisvastuu lainmukaisuudesta
- Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan **vaihtelevat riskit** rekisterinpitäjän on toteutettava tarvittavat **tekniset ja organisatoriset** toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä **noudatetaan** asetusta
- Vastuussa myös alihankkijoista – sopimukset ja hankintaketju
- Vaikutustenarviointi, ennakkokuuleminen
- Tietoturvaloukkaukset
- Rekisterinpitäjällä ja henkilötietojen käsittelijällä on oltava käytössään tehokkaat menetelmät, kuten lokitiedot tai muunmuotoinen seloste, jolla osoitetaan käsittelyn laillisuus, mahdollistetaan omaehtoinen valvonta ja varmistetaan tietojen eheys ja tietoturva

Tietoturvallisuus käsitteitä:

- Tietoturvallisuustoimenpiteet:
  - Tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä
  - Tietoturvan järjestelyjä ovat esim. kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä paljomuurin, virustorjuntaohjelman ja varmenteiden käyttö

- Tietoaineisto: asiakirjoista ja muista vastaavista tiedoista muodostuva tiettyyn viranomaisen tehtävään tai palveluun liittyvä tietokokonaisuus

Tietoturvallisuus tiedonhallintalaissa

Kuntaliitto
Kommunförbundet

12 § Henkilöstön ja palvelutuottajien luotettavuuden varmistaminen	On tunnistettava tehtävät, jota edellyttävät luotettavuutta
13 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus	Seuranta, elinkaaren hallinta, kartoitettava riskit, vikasietoisuus, käytettävyys, julkisuus, hankinnat
14 § Tietojen siirtäminen tietoverkossa	Salassapidettävien tietojen siirto suojatulla yhteydellä, vastaanottajan tunnistaminen
15 § Tietoaineistojen turvallisuuden varmistaminen	Muuttumattomuus, suojaus, alkuperäisyys, ajantasaisuus, virheettömyys, saatavuus, käyttökelpoisuus, arkistointimahdollisuus
16 § Tietojärjestelmien käyttöoikeuksien hallinta	Käyttöoikeuksien määrittäminen käyttäjän tehtävien mukaan, ajantasaisuus
17 § Lokitietojen kerääminen	Kerätään tarpeellisia lokitietoja tietojen käytön ja luovutuksen seurantaan sekä virheiden selvittämiseen
18 § Turvallisuusluokiteltavat asiakirjat valtionhallinnossa	Turvallisuusluokittelu ja merkintöjen tekeminen

12§ Henkilöstön ja palvelutuottajien luotettavuuden varmistaminen

- Tunnistettava ne tehtävät, joiden suorittaminen edellyttää luotettavuutta
- Henkilöturvallisuusselvitys turvallisuusselvityslaki (726/2014)
- Työntekijän luottotiedot ja huumausainetestaus, Yksityisyyden suoja työelämässä (759/2004)
- Huomaa, että ed. asiat on käsiteltävä yt-menettelyssä

13§ Tietoaineistojen ja tietojärjestelmien tietoturvallisuus

- Seurattava toimintaympäristön tilaa
- Varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan
  - Tietoturvallisuustoimenpiteet: Tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä
- Selvitettävä ja riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti
- Varmistettava olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys – säännöllinen testaus
- Tietojärjestelmät, tietovarantojen tietorakenteissa ja tietojenkäsittelyssä huomioitava asiakirjojen julkisuuden toteuttaminen, huom. yksityisyyden suoja
- Huomioitava tietojärjestelmien hankinnoissa vaatimukset tietoturvallisuudelle

14§ Tietojen siirtäminen tietoverkossa

- Salassapidettävien tietojen siirto yleisessä tietoverkossa salattua ja muuten suojattua tiedonsiirtoyhteyttä tai –tapaa käyttämällä

- Vastaanottajan tunnistus tai varmistus riittävän tietoturvallisella tavalla

- Digitaalisissa palveluissa käyttäjän sähköinen tunnistaminen vain, jos se on tarpeen palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi ja palvelujen liittyvien oikeusvaikutusten vuoksi (Digipalvelulaki 306/2019)

15§ Tietoaineistojen turvallisuuden varmistaminen

Kuntaliitto
Kommunförbundet

- Tietoaineistojen muuttumattomuuden varmistaminen
- Tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta
- Tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu
- Tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu
- Tietoaineistojen saatavuutta on rajoitettu vain, jos se on laissa erikseen rajoitettu
- Tietoaineistot voidaan tarvittavilta osin arkistoida

- Luottamuksellisuus, eheys ja saatavuus koskee myös toimitiloja, joissa käsitellään ja säilytetään tietoaineistoja

16§ Tietojärjestelmien ja käyttöoikeuksien hallinta

- Viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet
- Käyttöoikeudet on määriteltävä tehtävien mukaisesti
- Käyttöoikeudet on pidettävä ajantasaisina

17§ Lokitietojen kerääminen

- Lokitiedot on kerättävä tarpeelliset lokitiedot tietojärjestelmien käytöstä ja tietojen luovutuksista
  - Jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista
- Lokitietojen käyttötarkoitus on tietojen käytön ja luovutusten seuranta sekä teknisten virheiden selvittäminen
- Sovelletaan 1.1.2020 hankittaviin tietojärjestelmiin
- Ennen lain voimaantuloa hankittuihin tietojärjestelmiin 24 kk:n siirtymäaika

18 § Turvallisuusluokiteltavat asiakirjat valtionhallinnossa

- Valtion virastojen ja laitoksien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskevat merkinnät
- Asiakirjoihin tehtävistä merkinnöistä säädetään julkisuuslaissa 25§
- Erikseen tulossa asetus turvallisuusluokituksesta

Tietosuoja-asetus lokitiedoista

Kuntaliitto
Kommunförbundet

- Lokitiedot on säilytettävä mm. tietojen keräämisestä, muuttamisesta, kyselystä, luovuttamisesta, siirtämisestä, yhdistämisestä tai poistamisesta

- Lokitietoja saa käyttää ainoastaan lainmukaisuuden tarkistamiseen, omaehtoiseen valvontaan, tietojen eheyden ja tietoturvallisuuden varmistamiseen sekä rikosoikeudelliseen menettelyyn

- Omaehtoiseen valvontaan kuuluu myös toimivaltaisen viranomaisen sisäiset kurinpitomenettelyt

VM:n täytäntöönpanon tuki tietoturvallisuudelle

Kuntaliitto
Kommunförbundet

- Tiedonhallintalain täytäntöönpanoa johtaa valtiovarainministeriö. Vuodenvaihteen jälkeen tiedonhallintalautakunnalla tulee olemaan keskeinen rooli täytäntöönpanon varmistamisessa.
- Yksittäisen kunnan kannalta täytäntöönpanoa tukeva informaatio on keskeistä
- Erilaisten verkostojen merkitys kasvaa. Kunnan oma aktiivisuus on tärkeää.
- Tietoturvan osalta kannattaa seurata VRK:n JUDO-hanketta ja VM:n tiedonhallintalain tietoturvallisuuden alatyöryhmää

Lähde: Kirsi Janhunen, VRK, Kuntamarkkinat 2019

Tulossa suosituksia: VAHTI100 kortit

- Tiedonhallintalain 4 luvun säännöksiä avaavia ”soveltamiskortteja” on valmisteltu julkisen hallinnon digitaalisen turvallisuuden toimeenpanohankkeen (JUDO) koordinoimana. Työhön on osallistunut erityisesti VAHTI:n asiantuntijajaokset.
- Myös tiedonhallintalain nojalla annettavan turvallisuusluokitusta käsittelevän asetuksen tueksi laaditaan soveltamiskortteja. Työhön osallistuvat erityisesti turvallisuusviranomaiset.
- Suositukset luovutetaan valmistumisjärjestyksessä VM:n Tietoturvallisuus -alatyöryhmälle jatkokäsittelyyn.
- Suositustyön organisointi tarkentuu osana tiedonhallintalautakunnan tehtävien toteuttamista viimeistään tiedonhallintalautakunnan aloitettua toimintansa.
- Luonnosten valmisteluun voi osallistua kommentoimalla soveltamiskortteja. Lisätietoja digiturva@vrk.fi

Lähde: Kirsi Janhunen, VRK, Kuntamarkkinat 2019

VM:n täytäntöönpanohanke: Ensimmäisenä valmistuvat suositukset ja liitemateriaalit

- 13.2 § riskienhallinta
- 17 § lokitietojen kerääminen,
- 15.1 §, 2 kohta: vahingoilta suojaaminen
- 13.1 § elinkaaren huomioiminen tietojärjestelmissä, tietojenkäsittelyssä
- 13.4 § tietoturvallisuus hankinnoissa
- Turvallisuusluokitteluasetus

Lähde: Kirsi Janhunen, VRK, Kuntamarkkinat 2019

Mistä aloittaa tiedonhallinnan kehittäminen:

1. Tutustu tiedonhallintalakiin ja osallistu koulutuksiin
2. Tee suunnitelma, aikataulu ja budjetti jalkauttamiselle!

   Hyödynnä erilaiset siirtymäajat, priorisoi! Ota huomioon muutokset ja vaatimukset tulevissa hankinnoissa, riskiarviointi, kriittisten järjestelmien tunnistaminen, huomio sopimuksiin ja häiriötilanteiden hallintaan, jatkuvuuden suunnittelu

3. Apuna tietoturvan kehittämisessä, ilmoittaudu mukaan
   1. JUDO hanke (kehitetään digiturvallisuutta, VRK)
   2. KUJA-hanke (kehitetään jatkuvuuden hallintaa, Kuntaliitto),
   3. TAISTO19- harjoitus (mahdollisuus harjoitella tietoturvaloukkauksia, VRK)
4. Kuntaliitolta on tullut yleiskirje, missä pyydetään nimeämään tietoturvasta vastaava(t) sekä perustamaan sähköpostilaatikko muotoon tietoturva@kunta.fi
5. Tee yhteistyötä oman organisaation sisällä sekä ulkopuolisten yhteistyökumppaneiden kanssa!
6. Investointi jatkuvaan tietosuoja- ja –turvatyöhön myös henkilökuntaa kouluttamalla

Kuntaliitto
Kommunförbundet

Kuntaliitto tiedottaa ja auttaa

Kuntaliitto
Kommunförbundet

Kuntaliitto

- https://www.kuntaliitto.fi/

Uutiskirjeet

- Tilaa ainakin Kunnat ja tietoyhteiskunta ja Lakiasiat
- https://www.kuntaliitto.fi/kuntaliitto/uutiskirjeet

Kysymykset palvelusähköpostiin

Tietoyhteiskunta@kuntaliitto.fi

Huom! Kuntaliiton eri yksiköillä on omat palvelusähköpostit

https://www.kuntaliitto.fi/yhteystiedot

Hyvää hallintoa asiakaslähtöisesti, yhdenmukaisesti ja tietoturvallisesti

Erityisasiantuntija, KTM, YTM, Tuula Seppo
0504288255
tuula.seppo[at]kuntaliitto.fi
@tuula_seppo

Kuntaliitto
Kommunförbundet

kuntaliitto.fi
PL 200, 00101 Helsinki
Kuntatalo, Toinen linja 14
00530 Helsinki