Tampereen yliopisto

Alisa Hakkarainen

TURVALLISUUSLUOKITELTAVAT ASIAKIRJAT TIETOJÄRJESTELMISSÄ

Informaatioteknologian ja viestinnän tiedekunta

Kandidaatintutkielma

Toukokuu 2022

TIIVISTELMÄ

Alisa Hakkarainen: Turvallisuusluokiteltavat asiakirjat tietojärjestelmissä
Kandidaatintutkielma
Tampereen yliopisto
Informaatiotutkimus
Toukokuu 2022

Tämä tutkielma tarkastelee turvallisuusluokiteltavien asiakirjojen käsittelyä lainsäädännön näkökulmasta, sekä millaisilla käytännön toimenpiteillä lainsäädännön vaatimuksiin voidaan vastata ja kuinka tietoturvallista työskentelytapaa käytännön työssä voidaan toteuttaa. Uudistuneen lainsäädännön myötä on mielekästä tarkastella, kuinka tietojärjestelmien ja etenkin turvallisuusluokiteltavien asiakirjojen tietoturvallinen käyttö voidaan käytännössä viranomaisen toiminnassa järjestää.

Tutkielman tutkimuskysymykset kuuluvat seuraavasti: 1. Mitä vaatimuksia turvallisuusluokitus luo aineiston käsittelyyn? 2. Millaisia vaatimuksia turvallisuusluokiteltavan aineiston sähköinen käsittely luo tietojärjestelmille ja miten tietoturvallinen työskentelytapa saavutetaan lainsäädännön näkökulmasta?

Tutkielma toteutettiin katsauksena lainsäädäntöön hyödyntäen kuvailevan kirjallisuuskatsauksen menetelmiä soveltamalla. Tutkielman tutkimusaineistoksi valikoitui keskeiset tiedonhallintaan ja turvallisuusluokiteltaviin asiakirjoihin liittyvät lait ja asetukset. Tutkimusaineistossa on lisäksi lainsäädäntöä täydentämään laadittuja suosituksia ja viranomaistyöskentelyyn muodostettu kansallinen turvallisuusauditointikriteeristö.

Tutkielmassa havaittiin, että lainsäädäntö luo runsaasti vaatimuksia tietojärjestelmille ja turvallisuusluokiteltavien asiakirjojen tietoturvalliseen käsittelyyn. Tuloksista huomataan, kuinka ensinnäkin turvallisuusluokitus asettaa vaatimuksia aineiston käsittelylle ja toiseksi, miten tietoturvallisen työskentelyn edistämiseksi voidaan tehdä erilaisia hallinnollisia ja teknisiä toimenpiteitä. Tuloksista käy ilmi myös, kuinka huolellisesti toteutetulla riskienhallinnalla myötä poikkeamatilanteista on mahdollista toipua.

Avainsanat: tiedonhallinta, tietoturvallisuus, tietojärjestelmät, turvallisuusluokitus

SISÄLLYSLUETTELO

1 JOHDANTO

Viime vuosien aikana tehokas tiedonhallinta on kokenut suuria haasteita digitalisaation edetessä ja tietojärjestelmien kehittyessä. Työskentelipä asiantuntija missä tahansa, tiedonhallinnan kentän muutoksilta on ollut vaikea välttyä. Yksi merkittävimpiä tiedonhallinnan aihealueen muutoksia on viime vuosina ollut tiedonhallintaan liittyvän lainsäädännön muutos, jossa aiempaa lainsäädäntöä yhtenäistettiin vastaamaan paremmin nyky-yhteiskunnan vaatimuksiin ja selkeyttämään varsinkin julkisen hallinnon työskentelyä. Hallituksen esityksessä eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi (HE 284/2018) kerrotaan lainsäädännön uudistuksen tavoitteeksi tietoaineistojen yhdenmukainen hallinta sekä tietoturvallinen käsittely, jotta lain viranomaisen toiminnan julkisuudesta (621/1999) mukaista julkisuusperiaatetta voidaan toteuttaa. Esityksen mukaan uudistunut lainsäädäntö ottaa huomioon myös ne muutokset, joita tietotekninen kehitys on luonut tiedonhallinnalle (HE 284/2018). Lainsäädännön uudistustyön tuloksena syntyi laki julkisen hallinnon tiedonhallinnasta (906/2019), joka astui voimaan vuoden 2020 alusta. Samalla kumottiin vanha laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011).

Kun lainsäädäntöä uudistetaan, asettaa se uudenlaisia vaatimuksia tiedon turvalliselle käsittelylle tietojärjestelmissä. On tärkeää ymmärtää, mitä asioita tietoturvallisessa työskentelyssä tulee ottaa huomioon ja kuinka sen merkitys korostuu entisestään, kun kyseessä ovat turvallisuusluokiteltavat asiakirjat.

Tarkastelen kandidaatintutkielmassani turvallisuusluokiteltavien asiakirjojen käsittelyn asettamia vaatimuksia tietojärjestelmille hyödyntäen olennaista lainsäädäntöä sekä niiden tueksi luotuja suosituskokoelmia ja auditointikriteeristöä. Tutkielman tavoite on luoda yleiskatsaus turvallisuusluokiteltavien asiakirjojen käsittelyyn tietojärjestelmissä sekä tietoturvallinen työskentelytapa ottaen huomioon uudistuneen lainsäädännön asettamat vaatimukset.

Tutkielma rakentuu siten, että luvussa 2 käydään läpi tutkielman kannalta keskeiset käsitteet, joiden näkökulmasta tutkielmaa tarkastellaan. Näihin keskeisiin käsitteisiin

lukeutuu lainsäädäntö, turvallisuusluokitus, tietojärjestelmä ja tietoturvallisuus. Luvussa 3 esittelen tutkielman tutkimusasetelman, tutkimuskysymykset sekä tutkimusaineiston. Luvussa 4 tarkastelen lainsäädännön asettamia vaatimuksia asiakirjojen käsittelylle tietojärjestelmissä ensin fyysisen käsittely-ympäristön näkökulmasta ja sen jälkeen tutkin, millaisia tekijöitä tietojärjestelmän turvallisuudessa täytyy ottaa huomioon sisältäen vähimpien oikeuksien periaatteen niin hallinnollisesta kuin teknisestä näkökulmasta sekä salausratkaisut. Luvussa 4 tutustutaan myös riskienhallinnan teemoihin ottaen näkökulmaa henkilöstöturvallisuudesta, tietoriskien hallinnasta sekä poikkeamatilanteista.

2 KESKEISET KÄSITTEET

Tässä luvussa tutustutaan tutkielman kannalta keskeisiin käsitteisiin.

2.1 Lainsäädäntö

Tässä tutkielmassa keskeisimmät tarkasteltavat lait ja asetukset koskettavat tiedonhallintaa ja turvallisuusluokiteltavia asiakirjoja julkisessa hallinnossa. Laki julkisen hallinnon tiedonhallinnasta (906/2019), jatkossa *tiedonhallintalaki* säädettiin mahdollistamaan hyvää hallintotapaa sekä myös selkeyttämään aiempaa osin ristiriitaista lainsäädäntöä (HE 284/2018). Tiedonhallintalaki astui voimaan vuoden 2020 alusta ja sen nojalla valtiovarainministeriön yhteyteen perustettiin tiedonhallintalautakunta viranomaisten tiedonhallinnan toteuttamisen tueksi (Savolainen 2019).

Valtioneuvoston asetuksella asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) säädetään turvallisuusluokiteltujen asiakirjojen luokittelusta, asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokituksen edellyttämistä tietoturvallisuustoimenpiteistä asiakirjoja käsitellessä. Asetuksen sisältö tarkentaa tiedonhallintalain (906/2019) säännöksiä turvallisuusluokiteltavien asiakirjojen käsittelystä (Savolainen 2019).

2.2 Turvallisuusluokitus

Tiedonhallintalain 18 §:n mukaan turvallisuusluokiteltaviin asiakirjoihin on tehtävä merkintä osoittamaan, millaisia tietoturvallisuuden toimenpiteitä niitä käsiteltäessä on noudatettava. Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) määritellään asiakirjojen turvallisuusluokat sen suhteen, kuinka suurta vahinkoa tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa tiedonhallintalain (906/2019) 18 §:n 1 momentissa kuvatulle suojattavalle edulle. Tällä suojattavalla edulla tarkoitetaan käytännössä maanpuolustusta, poikkeusoloihin varautumista, kansainvälisiä suhteita, rikosten torjuntaa, yleistä turvallisuutta tai valtion- ja kansantalouden toimivuutta taikka muulla tavoin niihin rinnastettavaa asiaa Suomen turvallisuudelle.

Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 3 §) asiakirjojen turvallisuusluokitus ja sen yhteydessä käytettävät merkinnät määräytyvät seuraavanlaisesti:

- Asiakirja määräytyy turvallisuusluokkaan I, mikäli sen oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa aiemmin määritellylle suojattavalle edulle. Turvallisuusluokka merkitään asiakirjaan merkinnällä ”ERITTÄIN SALAINEN” ja sen lisäksi voidaan käyttää merkintää ”TL I”.
- Asiakirja määräytyy turvallisuusluokkaan II, mikäli sen oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa aiemmin määritellylle suojattavalle edulle. Turvallisuusluokka merkitään asiakirjaan merkinnällä ”SALAINEN” ja sen lisäksi voidaan käyttää merkintää ”TL II”.
- Asiakirja määräytyy turvallisuusluokkaan III, mikäli sen oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa aiemmin määritellylle suojattavalle edulle. Turvallisuusluokka merkitään asiakirjaan merkinnällä ”LUOTTAMUKSELLINEN” ja sen lisäksi voidaan käyttää merkintää ”TL III”.
- Asiakirja määräytyy turvallisuusluokkaan IV, mikäli sen oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa aiemmin määritellylle suojattavalle edulle. Turvallisuusluokka merkitään asiakirjaan merkinnällä ”KÄYTTÖ RAJOITETTU” ja sen lisäksi voidaan käyttää merkintää ”TL IV”.

Edellä mainituilla turvallisuusluokkamerkinnöillä kerrotaan, millaisia toimenpiteitä asiakirjoja käsitellessä tulee noudattaa. Tietojärjestelmissä tieto turvallisuusluokasta voidaan merkitä esimerkiksi metatietoihin. (Tiedonhallintalautakunta 2020.)

2.3 Tietojärjestelmä

Tässä tutkielmassa tietojärjestelmästä puhuttaessa käytetään tiedonhallintalautakunnan (2021) määritelmää, jossa tietojärjestelmä on järjestelmä, jonka tarkoituksena on tehostaa toimintaa tietoa käsittelemällä. Tietojärjestelmä koostuu määritelmän mukaan ohjelmista, tietovarastoista, laitteista ja palveluista. Tiedonhallintalaki (906/2019 13 §) korostaa tiedonhallintayksikön vastuuta seurata tietoturvallisuuden tilaa koko tietojärjestelmän elinkaaren ajan. Tietojärjestelmän tietoturvallisuuden tilan seuraamiseen

kuuluu olennaisena osana muun muassa riskiarviointi, jonka avulla tarvittavat toimenpiteet turvallisuuden säilyttämiseksi voidaan tehdä (Tiedonhallintalautakunta 2021).

2.4 Tietoturvallisuus

Kyberturvallisuuden sanaston mukaan tietoturvallisuudella tarkoitetaan niitä toimenpiteitä, joilla varmistetaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus, eheys ja luottamuksellisuus ovat yleisesti vakiintuneita termejä tietoturvallisuudesta puhuttaessa. Tiedon saatavuudella tarkoitetaan sitä, että tieto on hyödynnettävissä tarpeen tullen. Tiedon eheydellä tarkoitetaan yhteneväisyyttä alkuperäiseen tietoon verrattuna ja tiedon luottamuksellisuus merkitsee sitä, että sivulliset eivät voi saada tietoa haltuunsa. (Sanastokeskus TSK 2018.) Tietoturvallisuuden ylläpitoon on erilaisia menetelmiä, jotka voivat olla hallinnollisia, fyysisiä tai teknisiä. Hallinnolliset menetelmät sisältävät organisaation johdon valvomia ja järjestämiä toimenpiteitä, kuten käyttöoikeuksien rajaaminen ja henkilöstön kouluttaminen. Fyysisillä toimenpiteillä tarkoitetaan esimerkiksi tietojen käsittelyyn käytettävien työskentely-ympäristöjen rajaaminen rakenteellisin estein. Tekniset ratkaisut sisältävät järjestelmän turvallisuuden toimenpiteitä, kuten haittaohjelmilta suojautuminen ja järjestelmäkovennuksen keinot. (Ulkoministeriö 2020)

3 TUTKIMUSASETELMA

Tässä luvussa käsitellään tutkimusasetelmaa sisältäen tutkimuskysymykset, tutkimusmenetelmä sekä myös tutkimuksessa käytetty aineisto lyhyesti.

3.1 Tutkimuskysymykset

Tutkielman tavoitteena on hahmottaa vaatimuksia turvallisuusluokiteltavien asiakirjojen käsittelystä tietojärjestelmissä lainsäädännön näkökulmasta sekä tutkia, miten lainsäädännön vaatimuksiin voidaan käytännön työssä vastata. Näin tutkimuskysymyksiksi muodostuvat:

1. Mitä vaatimuksia turvallisuusluokitus luo aineiston käsittelyyn?
2. Millaisia vaatimuksia turvallisuusluokiteltavan aineiston sähköinen käsittely luo tietojärjestelmille ja miten tietoturvallinen työskentelytapa saavutetaan lainsäädännön näkökulmasta?

Tutkimuskysymyksiä rajatessa on huomioitu uudistuneen lainsäädännön tuomat muutokset ja sähköisen käsittely-ympäristön jatkuva kehitys. Viranomaistoiminnalle ominainen turvallisuusluokiteltavan aineiston käsittely herättää pohtimaan tietojärjestelmiin kohdistuvia vaikutuksia, sillä niitä kohtaavat riskit voivat syntyä niin käyttäjän huolimattomasta toiminnasta kuin myös pahantahtoisesta hyökkäysyrityksestä.

3.2 Tutkimusmenetelmä- ja aineisto

Tässä tutkielmassa tehdään lakeihin ja asetuksiin perustuva katsaus turvallisuusluokiteltujen asiakirjojen käsittelystä tietojärjestelmissä kuvailevan kirjallisuuskatsauksen keinoin. Tavoitteena on luoda selkeä yleiskatsaus siitä, millaisia tekijöitä tietojärjestelmien suunnittelussa ja käytössä tulee huomioida silloin, kun ne sisältävät turvallisuusluokiteltavia asiakirjoja ja kuinka niistä säädetään laissa. Kuvaileva kirjallisuuskatsaus tutkimusmenetelmänä on omiaan laaja-alaisen kuvan koostamiseen tietystä aihepiiristä (Salminen, 2011).

Tutkielman tutkimusaineistona toimivat keskeiset tiedonhallintaan liittyvät lait, asetukset sekä suosituskokoelmat. Tarkasteluun valikoitui laki julkisen hallinnon

tiedonhallinnasta (906/2019), valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), kaksi tiedonhallintalautakunnan suosituskokoelmaa sisältäen suosituksen turvallisuusluokiteltavien asiakirjojen käsittelystä (2020), sekä suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (2021). Tutkittavaan aineistoon kuuluu myös kansallinen turvallisuusauditointikriteeristö Katakri (Ulkoministeriö 2020).

Laki julkisen hallinnon tiedonhallinnasta (906/2019) sekä valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) on käsitelty aiemmin tutkielman viitekehyksessä, mutta niitä täydentävät muut aineistot esitellään alla.

Tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2020) laadittiin selventämään erityisesti turvallisuusluokan merkitsemiseen, turvallisuusalueisiin ja tietojärjestelmiin liittyvissä kysymyksissä. Suosituksessa korostuvat erityisesti tiedon turvallisen käsittelyn vähimmäisvaatimukset sekä erilaiset turvallisuuden edistämisen keinot.

Tiedonhallintalautakunnan suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (2021) johdattaa viranomaisia tiedonhallintalain (906/2019) mukaiseen tietoturvallisuutta toteuttavaan työskentelyyn. Suosituskokoelmassa huomioidaan koko järjestelmän elinkaari suunnittelusta käytöstä poistoon sekä järjestelmähankinnoissa huomioitavat oleelliset turvallisuutta edistävät asiat.

Kansallinen turvallisuusauditointikriteeristö Katakri (Ulkoministeriö 2020) on tietoturvallisuuden auditointityökalu, joka on kehitetty viranomaisia varten. Ensimmäinen versio siitä julkaistiin vuonna 2009 ja uusin versio on vuodelta 2020. Päivitysten myötä auditointityökalussa on huomioitu muun muassa digitalisaation vaikutukset tietoturvalliseen työskentelyyn. On huomioitava, että itse Katakri ei esitä vaatimuksia tietoturvallisuudelle, vaan päivitystyössä huomioidaan ajantasainen lainsäädäntö ja sen luomat vaatimukset työskentelyyn.

Katakri jakautuu kolmeen osioon, joihin kuuluvat turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus. Tässä tutkielmassa käsitellään ensisijaisesti

teknisen tietoturvallisuuden osiota, sillä siinä tarkastellaan tiedon sähköisen käsittely-ympäristön vaatimuksia niin hallinnollisten ratkaisujen, kuin myös teknisten ratkaisujen näkökulmasta.

4 TULOKSET

Tässä luvussa käsittelen tutkimusaineistoa tarkastellen lainsäädännöstä syntyviä vaatimuksia tietojärjestelmän kontekstissa. Tälle tutkielmalle kiinnostavia näkökulmia ovat fyysisen käsittely-ympäristön asettamat vaatimukset asiakirjojen käsittelylle sekä tietojärjestelmiin kohdistuvat vaatimukset unohtamatta riskienhallintaa. Fyysisen käsittely-ympäristön vaatimuksia käsitellään luvussa 4.1, tietojärjestelmän vaatimuksia käsitellään luvussa 4.2 sekä luvussa 4.3 käsitellään lainsäädännön velvoittamaa riskienhallintaa.

4.1 Fyysinen käsittely-ympäristö

Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 9 §) velvoitetaan tiedonhallintayksikköjä määrittelemään turvallisuusalueet tietoaineistojen suojaamiseksi. Turvallisuusalueet käsittävät hallinnollisen alueen, johon pääsy ilman saattajaa on vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä sekä turva-alueen, jonne kulkua vahditaan henkilökohtaisin tunnistein sekä henkilön luotettavuudesta on varmistuttu. Turvallisuusalueet vaikuttavat siihen, miten turvallisuusluokiteltua tietoa voidaan käsitellä ja säilöä. Seuraavissa kappaleissa tarkastelen, miten hallinnollinen alue ja turva-alue eroavat ominaisuuksiltaan tietojärjestelmien suojaamisessa ja aineistojen käsittelyssä.

Hallinnollisella alueella tarkoitetaan käytännössä viranomaisen tavanomaisimpia työskentelytiloja, kuten esimerkiksi toimistotilaa. Hallinnolliselle alueelle on pääsy vain viranomaisen valtuuttamilla henkilöillä. Turva-alueella tarkoitetaan hallinnollisia alueita paremmin suojattuja tiloja, joissa voidaan käsitellä turvallisuusluokiteltuja asiakirjoja laajemmin kuin hallinnollisella alueella. (Tiedonhallintalautakunta 2020.)

Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 10§) säädetään asiakirjojen käsittelystä ja tietojärjestelmien suojaamisesta turvallisuusalueiden avulla. Asetuksesta käy ilmi, että turvallisuusluokan I mukaisia asiakirjoja saa käsitellä ja säilyttää vain turva-alueella eikä lainkaan hallinnollisella alueella. Myös asiakirjojen käsittelyyn tarkoitetut tietojärjestelmät on sijoitettava turva-alueelle,

mikäli ne sisältävät turvallisuusluokkien II tai III mukaisia asiakirjoja. Mikäli on kyse turvallisuusluokan IV asiakirjoista, tulee niitä sisältävät ja niiden käsittelyyn tarkoitetut tietojärjestelmät sijoittaa turvallisuusalueelle, eli vähintään hallinnolliselle alueelle.

Tiedonhallintalautakunnan suosituksessa turvallisuusluokiteltavien asiakirjojen käsittelystä (2020) selventää turvallisuusluokiteltujen asiakirjojen sähköisen käsittelyn vaatimuksia. Esimerkiksi turvallisuusluokan III mukaisella salausratkaisulla varustettu päätelaite voidaan tarvittaessa väliaikaisesti siirtää turvallisuusalueen ulkopuolellekin, mutta se tulee viipymättä palauttaa säilytykseen turva-alueelle, jotta laitteen tietoturvallisuus ei vahingoitu.

Yhteistä kaikkien turvallisuusluokiteltavien asiakirjojen suojaamiselle turvallisuusluokasta ja turvallisuusalueesta riippumatta on se, että säilytysratkaisujen ja suojaamisen menetelmien täytyy olla sellaisia, että tiedot voidaan suojata sivullisilta. Säilytysratkaisujen arvioinnissa täytyy ottaa huomioon riskit, joita asiakirjojen ja tietojärjestelmien tehokas ja tietoturvallinen suojaaminen voi kohdata. (Tiedonhallintalautakunta 2020.)

4.2 Tietojärjestelmän vaatimukset

Tässä luvussa tarkastellaan tietojärjestelmille asetettuja vaatimuksia sekä keinoja, millä tietojärjestelmien tietoturvallisuus voidaan saavuttaa. Alaluvut käsittelevät vähimpien oikeuksien periaatetta, salausratkaisuja sekä riskienhallintaa. On huomionarvoista, että tietojärjestelmistä puhuttaessa teknisten ratkaisujen lisäksi huomioon täytyy ottaa myös hallinnollisia ratkaisuja.

Niin tiedonhallintalaissa (906/2019) kuin valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) säädetään erilaisista vaatimuksista koskien tietojen käsittelyä tietojärjestelmissä. Tiedonhallintalain (906/2019) tietoturvallisuutta käsittelevä luku 4 sisältää pykälät liittyen muun muassa tietojärjestelmien turvallisuuteen, käyttöoikeuksien hallintaan sekä tietojen turvalliseen siirtämiseen tietoverkossa. Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) tietojärjestelmiä koskevat vaatimukset täydentävät tiedonhallintalakia (906/2019) turvallisuusluokiteltavien asiakirjojen osalta. Näiden lakien

vaatimuksia varten luodut suositukset (Tiedonhallintalautakunta 2020 ja 2021) ja turvallisuuden auditointikriteeristö Katakri (Ulkoministeriö 2020) selventävät lainsäädännön vaatimuksia sekä tarjoavat konkreettisia toimenpiteitä tavoitteiden saavuttamiseksi.

Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 11 §) säädetään fyysisen käsittely-ympäristön lisäksi tietojärjestelmiä koskevista vaatimuksista. Vaatimuksiin sisältyvät muun muassa käyttäjien riittävän luotettava tunnistaminen, tietoturvallisuutta vaarantavia tekijöitä vastaan suojautuminen sekä käytettyjen salausratkaisujen turvallisuus asiakirjan turvallisuusluokitus huomioon ottaen.

4.2.1 Vähimpien oikeuksien periaate

Tietojärjestelmäsuunnittelussa yksi keskeisimpiä periaatteita turvallisuuden kannalta on vähimpien oikeuksien periaate, josta voidaan erotella niin hallinnollinen kuin tekninen näkökulma. Vähimpien oikeuksien periaatteella tarkoitetaan toimintatapaa, jossa oikeudet jonkin toiminnon suorittamiseen myönnetään järjestelmälle tai käyttäjälle vain niissä määrin, kuin sen on tehtävän suorittamisen kannalta tarpeellista (Viega & McGraw 2001). Vähimpien oikeuksien periaatteen laiminlyönti tahallisesti tai tahattomasti voi johtaa vakaviin seurauksiin, mikäli tietoa pääsee vääriin käsiin. Sen vuoksi sekä järjestelmän että käyttäjien osalta tulee varmistua siitä, että vain välttämättömät toiminnallisuudet ja pääsyoikeudet myönnetään. (Anderson & Mutch 2011).

Pääsyä tietojärjestelmiin rajoitetaan ja valvotaan ensisijaisesti pääsyoikeuksien hallinnoinnilla. Varsinkin turvallisuusluokiteltua aineistoa käsitellessä on oleellista, että käyttäjä ei pääse käsiksi muihin kuin työnsä kannalta välttämättömiin asiakirjoihin ja tästä säädetäänkin valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 8 §) toteamalla, että käsittelyoikeuden on oltava perusteltu.

Katakrin (Ulkoministeriö 2020) tietojärjestelmäturvallisuuden osiossa käsitellään vähimpien oikeuksien periaatetta hallinnollisesta näkökulmasta. Tiedonhallintalaissa (906/2019 16 §) todetaan, että viranomaisen on määriteltävä käyttöoikeudet tietojärjestelmiin, joista on vastuussa ja ne on pidettävä ajantasaisina käyttötarpeiden mukaan.

Käytännössä pääsyoikeuksien hallinnointi voidaan toteuttaa niin, että myönnetyistä käyttöoikeuksista pidetään luetteloa ja sen lisäksi tulee niiden ylläpitoon, hyväksymiseen ja poistoon olla kuvattu menettely. Lisäksi käyttöoikeuksien hallinnan tulee keskittyä tehtävään nimetyille vastuuhenkilöille, hallinnan toimenpiteet tulee ohjeistaa ja jokainen myönnetty käyttöoikeus tulee dokumentoida. (Tiedonhallintalautakunta 2021.) Organisaatiossa tulee olla toimiva toimintatapa tapahtuvien muutosten raportointiin käyttöoikeuksista vastaaville tahoille esimerkiksi henkilöstömuutosten tapauksissa (Ulkoministeriö 2020).

Katakrissa (Ulkoministeriö 2020) todetaan, että vähimpien oikeuksien periaatteen mukaisesti tietojärjestelmän käyttö- ja pääsyoikeudet tulee myös katselmoida säännöllisin väliajoin, jotta voidaan varmistua siitä, ettei käyttäjällä ole pääsyä sellaisiin tietoihin, jotka eivät enää ole tehtävien kannalta välttämättömiä. Tällaisia tilanteita voivat olla esimerkiksi työtehtävien muuttuminen tai käyttäjän lähteminen organisaation palveluksesta. Myös käyttö- ja pääsyoikeuksien katselmointi tulee dokumentoida (Tiedonhallintalautakunta 2021).

Hallinnollisen näkökulman lisäksi vähimpien oikeuksien periaatetta voidaan tutkia myös teknisen tietoturvallisuuden näkökulmasta, jolloin tarkasteluun nousee vähimpien oikeuksien lisäksi myös vähimmäistoimintojen konteksti. On yleisesti tiedossa, että tietoturvallisuudessa suurin riski on käyttäjä itse, mutta myös tietojärjestelmien tehokkaalla suunnittelulla voidaan merkittävästi pienentää haavoittuvuuksien riskiä. Haavoittuvuudella tarkoitetaan tietoturvaa vaarantavaa järjestelmän heikkoutta, joka voi olla seurausta virheestä ohjelmassa tai muun toiminnan laiminlyönnistä (Tiedonhallintalautakunta 2021).

Tiedonhallintalaki (906/2019 13 §) määrittelee tietoaineistojen ja tietojärjestelmien tietoturvallisuutta niin, että tiedonhallintayksikön on tunnistettava järjestelmään kohdistuvat riskit ja suoritettava toimenpiteet niiden minimoimiseksi, eli toisin sanoen järjestelmän koventamiseksi. Koventamisella järjestelmän haavoittuvia osia minimoidaan asetuksia muuttamalla (Ulkoministeriö 2020). Lisäksi valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 11 §) määrittää, että

käytetyissä tietojärjestelmissä otetaan käyttöön vain välttämättömät toiminnallisuudet. Vain välttämättömiä toiminnallisuuksia käyttöön ottamalla minimoidaan haavoittuvuuksien riskit, jotka syntyvät ohjelmistokoodin määrän kasvaessa, josta on vaikea tehdä turvallista (Ulkoministeriö 2020).

Koska pääsynhallinta on olennainen osa vähimpien oikeuksien periaatetta, on syytä tarkastella myös käyttäjän tunnistamisen ja kirjautumisen todentamisen suositeltuja menetelmiä. Käyttäjän pääsynhallinnan kannalta suositellaan käytettävän kertakirjautumisen menetelmää, jossa yhdellä kirjautumisella käyttäjä pääsee kaikkiin käyttöoikeuksiensa mahdollistamiin palveluihin ja järjestelmiin. Kertakirjautumisen lisäksi suositellaan käytettävän monivaiheista tunnistautumista, missä hyödynnetään useampaa kuin yhtä todentamismenetelmää. (Tiedonhallintalautakunta 2021.) Monivaiheisen tunnistautumisen yleisimmin käytettävä muoto on kaksivaiheinen tunnistautuminen, jossa käyttäjätunnuksen ja salasanan lisäksi käyttäjä voidaan todentaa käyttämällä esimerkiksi matkapuhelimeen lähetettävää koodia tai käyttäjän yksilöivää ominaisuutta, kuten sormenjälkeä. Saavutettava hyöty on tietojenkalastelun vaikeuttaminen, kun todentamista ei tehdä vain käyttäjätunnuksen ja salasanan yhdistelmällä. (Kyberturvallisuuskeskus 2022.)

4.2.2 Salausratkaisut

Riippuen käytettävästä verkosta liikennöinnissä salausratkaisut voivat usein olla ainoa keino suojata tiedon luottamuksellisuutta ja eheyttä (Tiedonhallintalautakunta 2020). Turvallisuusluokiteltaviin asiakirjoihin liittyy tiedonhallintalaissa (906/2019 18 §) määritelty yleisen edun eli käytännössä valtion turvallisuuden suojaamisen vaatimus, joten niiden suojaamiseen joko tahalliselta tai tahattomalta väärinkäytöltä tulee kiinnittää erityistä huomiota, jolloin salausratkaisujen oikean valinnan tärkeys korostuu (Ulkoministeriö 2020).

Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 11 §) esitetään vaatimus siitä, että käytettyjen salausratkaisujen tulee olla riittävän turvallisia ottaen huomioon käsiteltävien asiakirjojen turvallisuusluokitus.

Myös tiedonhallintalaissa (906/2019 14 §) säädetään tietojen siirtämisestä tietoverkossa esittäen vaatimus tiedonsiirron järjestämisestä niin, että ennen tietojen käsittelyä vastaanottaja tunnistetaan riittävän tietoturvallisella tavalla.

Olennainen kohta tietoturvallisuuden toteuttamisen kannalta on valtioneuvoston asetuksen asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 11 §) mainինta siitä, kuinka tietojärjestelmät tulee toteuttaa niin, että turvallisuusluokiteltavaa tietoa sisältävät osat voidaan erottaa niistä tietojärjestelmän osista, jotka käsittävät alemman turvallisuustason tietoja. Käytännössä tämä voidaan toteuttaa hallintayhteyksien rajaamisella turvallisuusluokittain ja niin, että toimivaltainen viranomainen hyväksyy käytettävät yhdyskäytävä- sekä salausratkaisut (Ulkoministeriö 2020). Yhdyskäytäväratkaisujen tavoitteena on estää korkeamman turvallisuusluokituksen mukaisen tiedon kulkeutuminen ympäristöön, joka on tarkoitettu alemmalle turvallisuusluokalle (Tiedonhallintalautakunta 2020). Yleisimmin käytettyjä yhdyskäytäväratkaisuja ovat menetelmät, jotka mahdollistavat tiedonsiirron vain yhteen suuntaan, eli käytännössä matalammalta tasolta ylemmälle tasolle (Kyberturvallisuuskeskus 2021).

Mikäli turvallisuusluokiteltua tietoa siirretään fyysisten turvallisuusalueiden ulkopuolella, tulee varmistua riittävästä salauksesta. Käytännössä salaus voidaan toteuttaa VPN-ratkaisujen avulla tai esimerkiksi turvapostin ja tiedostosalausratkaisujen avulla. (Tiedonhallintalautakunta 2020.) On huomattava, ettei tavanomainen sähköposti lähtökohtaisesti sovellu turvallisuusluokiteltavan tiedon siirtämiseen sen salauksen riittämättömyyden vuoksi (Tiedonhallintalautakunta 2021). Salausratkaisujen turvallisuuden lisäksi tulee varmistua siitä, että tehtäviä hoitavilla henkilöillä on riittävän asiantuntemus turvallisen työskentelyn mahdollistamiseksi (Ulkoministeriö 2020).

4.3 Riskienhallinta

Tiedonhallintalaissa (906/2019 13 §) velvoitetaan tiedonhallintayksikköä mitoittamaan käytettävät tietoturvallisuustoimenpiteet riskiarvioinnin mukaan. Toimintahäiriön tai poikkeustilanteen yllättäessä viranomaisen toiminnan jatkuvuus on turvattava niin, että mahdolliset vaikutukset turvallisuusluokiteltavaan tietoon ovat mahdollisimman pienet

(Ulkoministeriö 2020). Vaikka edeltävissä luvuissa esitellyt toimenpiteet ovatkin osaltaan osa organisaation riskienhallintaa, on syytä tarkastella sitä, miten lainsäädäntö velvoittaa viranomaisia riskienhallinnan suhteen. Tässä tutkielmassa riskienhallinta jaetaan kolmeen osaan: henkilöstöturvallisuuteen, tietoriskien hallintaan sekä poikkeamatilanteiden hallintaan.

4.3.1 Henkilöstöturvallisuus

Tiedonhallintalaissa (906/2019 4 §) edellytetään tiedonhallintayksikköä tarjoamaan koulutusta henkilöstöltä, jotta voidaan varmistua riittävästä ymmärryksestä, mitä tietojen käsittely tietoturvallisesti edellyttää. Valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 8 §) määrätään, että käsittelyoikeudet voidaan myöntää vain niille henkilöille, joilla on tarvittava tietämys käsittelyn velvoitteista. Organisaation tarjotessa koulutusta se tulee järjestää niin, että myös ajankohtaiset ohjeet huomioidaan henkilön työtehtäviä mahdollisesti kohtaavien riskitekijöiden lisäksi. Koulutuksen osallistujista tulisi pitää listaa sekä huolehtia, että koulutuksia järjestetään säännöllisesti ja niiden sisältö tulisi dokumentoida. (Ulkoministeriö 2020.)

Riskienhallinta henkilöstön osalta tarkoittaa myös sitä, että organisaation on varmistuttava turvallisuusluokiteltavaa tietoa käsittelevien henkilöiden luotettavuudesta, josta myös säädetään tiedonhallintalaissa (906/2019 12 §). Käytännössä tämä tarkoittaa henkilöturvallisuusselvityksen hakemista kyseisestä henkilöstä. Henkilöturvallisuusselvityksen tekemisestä vastaa Suojelupoliisi. Henkilöturvallisuusselvityksen lisäksi työntekijältä voidaan edellyttää salassapito- ja vaitiolosopimusta. (Ulkoministeriö 2020.)

4.3.2 Tietoriskien hallinta

Tietoriskien hallinnalla tarkoitetaan riskienhallintaa, joka keskittyy tietoaineistoihin, tietovarantoihin sekä tietojärjestelmiin (Tiedonhallintalautakunta 2021). Siitä säädetään tiedonhallintalaissa (906/2019 13 §) velvoittamalla tiedonhallintayksiköitä varmistamaan tietojärjestelmien turvallisuus koko niiden elinkaaren ajan. Käytännössä tietoriskien hallinnassa tunnistetaan tietoaineistoa kohtaavat mahdolliset riskit, tehdään toimenpiteitä riskien pienentämiseksi ja sen jälkeen saavutettua turvallisuuden tasoa

ylläpidetään tai sitten hyväksytään jäännösriskit. Jäännösriskillä tarkoitetaan niitä riskejä, joihin ei haluta tai voida vaikuttaa esimerkiksi toimenpiteiden ollessa liian kalliita ottaen huomioon riskin realistiset vaikutukset toiminnalle. (Tiedonhallintalautakunta 2021.)

Organisaatiolla tulee olla tiedonhallintalain (906/2019) mukainen tiedonhallintamalli, josta löytyviä tietovarantojen ja tietoaineistojen tietoja voidaan hyödyntää tietoriskien hallinnassa (Tiedonhallintalautakunta 2021). Tiedonhallintalain (906/2019 5 §) mukaisessa tiedonhallintamallissa kuvataan tiedonhallinnan toimintaympäristöä niin, että se sisältää tietoja muun muassa tietoturvallisuuden toimenpiteistä, tietojärjestelmien käyttötarkoituksesta ja käytettävistä tiedonsiirtotavoista sekä tietojen säilytysajoista. Ajan tasalla olevan tiedonhallintamallin avulla viranomaisen tekemä riskienhallinta helpottuu, kun tiedossa on kaikki tietojärjestelmät, joista viranomainen on vastuussa (Tiedonhallintalautakunta 2021).

4.3.3 Poikkeamatilanteiden hallinta

Tietoturvapoikkeamalla tarkoitetaan tietoturvaa vaarantavaa tapahtumaa, joka voi vaikuttaa organisaation toimintaan negatiivisella tavalla (Sanastokeskus TSK 2018). Sekä tiedonhallintalaissa (906/2019 17 §) että valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 14 §) vaaditaan lokitietojen keräämistä tietojen käsittelyn seuraamiseksi, jotta tapahtumat voidaan tarvittaessa jäljittää. Tapahtumien jäljitettävyydellä varmistetaan toimintojen kirjaaminen niin, että poikkeamatilanteessa tiedetään, kenen toimesta mitäkin toimintoja on tehty (Ulkoministeriö 2020). Lokitietoja kerätään myös normaalitilanteessa, mutta poikkeamatilanteiden selvittämisessä niillä on suuri merkitys (Tiedonhallintalautakunta 2021).

Asiakirjan turvallisuusluokitus muodostaa erilaisia vaatimuksia sille, kuinka niiden käsittelyä seurataan. Turvallisuusluokkien mukaisista käsittelyn rekisteröinnin vaatimuksista säädetään valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 14 §), jossa turvallisuusluokan I-III mukaisen asiakirjan käsittely tulee kirjata esimerkiksi tietojärjestelmään tai sähköiseen lokiin. Asiakirjojen käsittely

voidaan kirjata myös asiarekisteriin, josta säädetään tiedonhallintalain (906/2019 25 ja 26 §) mukaisesti niin, että saapunut asiakirja on viipymättä kirjattava asiarekisteriin ja sille on määriteltävä tietyt yksilöintitiedot.

Organisaatiolla voi olla käytössään useita erilaisia lokeja, joihin voidaan kirjata erityyppisiä tietoja. Esimerkkejä useiden lokien hyödyntämisestä voi olla esimerkiksi pääsynvalvontaan liittyvä loki ja toinen loki, johon rekisteröidään tiedot tietoaineistoon tehdyistä muutoksista. (Tiedonhallintalautakunta 2021.)

Poikkeamien havainnointiin on automatisoituja työkaluja, mutta joskus myös manuaalinen työskentely on tarpeen, jos esimerkiksi poikkeamatilanne vaatii tarkempaa selvitystä tai automatisoidut työkalut eivät ole havainneet poikkeamaa alun perinkään (Ulkoministeriö 2020). Käytännössä julkisessa hallinnossa tapahtuvasta tietoturvapoikkeamasta tulisi tehdä ilmoitus viipymättä, jotta tilanteesta voidaan toipua mahdollisimman nopeasti. Nopealla reagoinnilla voidaan minimoida mahdollisia syntyneitä vahinkoja. (Tiedonhallintalautakunta 2021.) Tehdyistä ilmoituksista voidaan saada myös hyödyllistä tietoa, mikäli kyseessä on esimerkiksi laajamittaisempi tietoturvahyökkäys (Ulkoministeriö 2020).

Poikkeamatilanteesta toipumiseen kuvataan Katakrissa (Ulkoministeriö 2020) erilaisia toimenpiteitä. Mikäli ollaan turvallisuusluokkien IV-II mukaisessa käsittelyn ympäristössä, voidaan toipuminen mahdollistaa toimenpiteillä, jotka sisältävät muun muassa verkkoliikenteen normaalin tilan tuntemisen ja erilaisten poikkeamien havainnoinnin sekä niihin reagoinnin. Tehokkain keino poikkeamista toipumiseen ovat organisaation selkeät valmiit toimintamallit ja menetelmät.

5 POHDINTA

5.1 Johtopäätökset

Tämän tutkielman tavoitteena oli selvittää, millaisia vaatimuksia turvallisuusluokitus luo asiakirjojen käsittelylle etenkin tietojärjestelmissä ja miten lainsäädäntöä voidaan käytännössä toteuttaa sekä turvata työskentelyn tietoturvallisuus. Tutkimuskysymykseni olivat:

1. Mitä vaatimuksia turvallisuusluokitus luo aineiston käsittelyyn?
2. Millaisia vaatimuksia turvallisuusluokiteltavan aineiston sähköinen käsittely luo tietojärjestelmille ja miten tietoturvallinen työskentelytapa saavutetaan lainsäädännön näkökulmasta?

Ensimmäisen tutkimuskysymyksen kohdalla huomaamme, että erilaiset turvallisuusluokitukset luovat hyvinkin erilaisia vaatimuksia aineiston käsittelylle. Yksi merkittävimpiä tekijöitä asiakirjojen turvallisen käsittelyn mahdollistamisessa ovat turvallisuusalueet, joiden tarkoilla omilla vaatimuksilla varmistetaan tietojen oikeellinen käsittely. Aineistosta on mahdollista huomata, miten suuri merkitys myös riskienhallinnan kannalta on varmistua henkilöstön luotettavuudesta ja koulutuksen ajantasaisuudesta. Lyhyesti vastattuna voimme siis todeta, että turvallisuusluokiteltavan aineiston käsittely luo vaatimuksia niin käsittely-ympäristölle kuin aineiston käsittelijälle itselleenkin.

Toinen tutkimuskysymys on kaksiosainen ja hieman haastavampi vastattava. Tietojärjestelmien kehitys on jatkuvaa ja samalla myös niitä kohtaavat riskit kehittyvät. Tutkimusaineistoa tutkimalla kävi ilmi, että tietoturvalliseen työskentelyyn tarjotaan suosituksien ja turvallisuusauditointikriteeristö Katakrin toimesta runsaasti käytännön toimenpiteitä mahdollistamaan lainsäädännön vaatimuksiin vastaaminen. On kuitenkin selvää, että vaikka kyse olisi viranomaisorganisaatiosta, vaatii kehitystyö ja toiminnan ylläpitäminen jatkuvaa huomiota ja useiden asiantuntijoiden työpanosta.

Tutkimuksessa kävi ilmi, että tietoturvallisen työskentelyn mahdollistamiseksi voidaan tehdä niin hallinnollisia kuin teknisiäkin toimenpiteitä. Tehokkaalla riskienhallinnalla

viranomaisen on mahdollista tunnistaa mahdolliset tietoaineistoja ja tietojärjestelmiä kohtaavat riskit sekä tehdä ajoissa toimenpiteet niiden minimoimiseksi.

5.2 Tulevaisuuden tutkimuksesta

Lainsäädännön uudistuminen on suhteellisen tuore asia tiedonhallinnan kentällä ja aiheeseen liittyvää tutkimusta on vielä suhteellisen vähän, joten siitä syystä tämän tutkielman tutkimusaineisto rajautui vain lainsäädäntöön ja sitä tukeviin suosituksiin sekä auditointikriteeristöön. Jatkotutkimuksen kannalta voisi olla mielekästä tutkia, miten suuria muutoksia tietojärjestelmien kehitykseen ja ylläpitoon lainsäädännön uudistuminen on todellisuudessa tuonut ja miten suurilta osin käytössä olevat tietojärjestelmät vastaavat nykyisen lainsäädännön vaatimuksiin. Kiinnostava jatkotutkimuksen kohde olisi myös selvittää, miten paljon aikaa riskienhallinnan suunnitteluun ja kehittämiseen todellisuudessa käytetään ja miten nopeasti poikkeamatilanteista on mahdollista toipua.

LÄHTEET

Anderson, & Mutch, J. (2011). Preventing Good People From Doing Bad Things Implementing Least Privilege (1st ed. 2011.). Apress. https://doi.org/10.1007/978-1-4302-3922-2

HE 284/2018 vp. Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.

Kyberturvallisuuskeskus. (2022) *Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi*. Traficom. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Kyberturvallisuuskeskus. (2021) *Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista.*Traficom. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf

Sanastokeskus TSK. (2018). *Kyberturvallisuuden sanasto*. Huoltovarmuuskeskus. https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Salminen, A. (2011). *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin* (p. 50). http://www.uva.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Savolainen, J. (8.8.2019). *Vuoden 2020 alusta voimaantuleva tiedonhallintalaki edistää viranomaistoiminnan digitalisointia ja tietoturvallisuutta*. EDILEX. https://www-edilex-fi.libproxy.tuni.fi/uutiset/60884?allWords=tiedonhallintalaki&offset=1&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=726838

Tiedonhallintalautakunta. (2021). *Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta.* Valtiovarainministeriö. http://urn.fi/URN:ISBN:978-952-367-897-2

Tiedonhallintalautakunta. (2020). *Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä*. Valtiovarainministeriö. http://urn.fi/URN:ISBN:978-952-367-292-5

Ulkoministeriö. (2020). Katakri – tietoturvallisuuden auditointityökalu viranomaisille.

Viega, & McGraw, G. R. (2001). *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley Professional.

Lait, asetukset ja standardit:

Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906.

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 28.11.2019/1101.

Laki julkisen hallinnon tietohallinnon ohjauksesta (kumottu) 10.6.2011/634.