Suositus tietoturvallisuuden vähimmäisvaatimuksista

Lautakunnat

Valtiovarainministeriön julkaisuja – 2024:

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets nätbokhandel

vnjulkaisumyynti.fi

Publication distribution

Institutional Repository for the Government of Finland Valto

julkaisut.valtioneuvosto.fi

Publication sale

Online bookstore of the Finnish Government

vnjulkaisumyynti.fi

Tuplaklikkaa ja kirjoita ministeriö

ISBN sid. VNK täyttää
ISBN pdf VNK täyttää
ISSN sid. VNK täyttää
ISSN pdf VNK täyttää

Taitto Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2020
Finland (kieliversioissa)
Paino PunaMusta Oy, 2020

Kuvailulehti
xx.xx.2024

Napsauta ja kirjoita julkaisun otsikko

Napsauta ja kirjoita julkaisun alaotsikko

VNK täyttää, sarja ja numero		**Teema**	Napsauta ja kirjoita
Julkaisija	Napsauta ja kirjoita ministeriö		
Tekijä/t	Napsauta ja kirjoita		
Toimittaja/t	Napsauta ja kirjoita		
Yhteisötekijä	Napsauta ja kirjoita		
Kieli	Napsauta ja kirjoita	**Sivumäärä**	VNK täyttää

Tiivistelmä

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019) on säädetty tietoturvallisuustoimenpiteisiin liittyviä vastuita julkisen hallinnon tiedonhallintayksiköille ja viranomaisille sekä yksityisille henkilöille ja yhteisöille taikka muille kuin viranomaisena toimiville julkisoikeudellisille yhteisöille, siltä osin kuin ne hoitavat julkista hallintotehtävää.

Tämä tiedonhallintalautakunnan suositus opastaa tiedonhallintalain asettamien tietoturvallisuuden vähimmäisvaatimusten täyttämisessä**,** jotka kaikkien julkishallinnon organisaatioiden tulee vähintään täyttää. Vähimmäisvaatimusten osana organisaatioiden tulee tunnistaa ja arvioida tietojenkäsittelyyn liittyvät riskit sekä toteuttaa toimenpiteet riskien pienentämiseksi hyväksyttävälle tasolle.

Suositus on tarkoitettu ensisijaisesti tiedonhallintalaissa määritetyille tiedonhallintayksiköille ja viranomaisille, mutta näiden lisäksi tätä suositusta voivat hyödyntää kaikki muutkin toimijat, jotka käsittelevät viranomaisten asiakirjoja.

Tämä suositus korvaa suosituskokoelmat tiettyjen tietoturvallisuussäännösten soveltamisesta (versiot VM 2021:65, VM 2020:61 ja VM 2020:21).

Tiedonhallintalautakunta hyväksyi suosituksen XX.XXXX.

Klausuuli	VNK täyttää		
Asiasanat	lautakunnat, tiedonhallintalautakunta, tiedonhallintalaki, julkinen hallinto, tietoturva		
ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN nid.	VNK täyttää	**ISSN painettu**	VNK täyttää
Asianumero	Napsauta ja kirjoita	**Hankenumero**	Napsauta ja kirjoita
Julkaisun osoite	VNK täyttää		

Presentationsblad
xx.xx.2024

Napsauta ja kirjoita otsikko ruotsiksi

Napsauta ja kirjoita alaotsikko ruotsiksi

VNK täyttää, sarjanimi ja numero		**Tema**	Napsauta ja kirjoita
Utgivare	Napsauta ja kirjoita ministeriö		
Författare	Napsauta ja kirjoita		
Redigerare	Napsauta ja kirjoita		
Utarbetad av	Napsauta ja kirjoita		
Språk	Napsauta ja kirjoita	**Sidantal**	VNK täyttää

Referat

Lagen om informationshantering inom den offentliga förvaltningen (906/2019) finns bestämmelser om ansvar i fråga om informationssäkerhetsåtgärder som gäller informationshanteringsenheter och myndigheter inom den offentliga förvaltningen samt privatpersoner, privaträttsliga sammanslutningar och sådana offentligrättsliga samfund som inte är myndigheter till den del dessa sköter offentliga förvaltningsuppgifter.

Informationshanteringsnämnden godkände rekommendationen den

Klausul	VNK täyttää
Nyckelord	nämnder, informationshanteringsnämnden, informationshanteringslagen, offentlig förvaltning, informationssäkerhet

ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN tryckt	VNK täyttää	**ISSN tryckt**	VNK täyttää
Ärendenr.	Napsauta ja kirjoita	**Projektnr.**	Napsauta ja kirjoita
URN-adress	VNK täyttää		

Description sheet
xx.xx.2024

Napsauta ja kirjoita otsikko englanniksi

Napsauta ja kirjoita alaotsikko englanniksi

VNK täyttää, sarjanimi ja numero		**Subject**	Napsauta ja kirjoita
Publisher	Napsauta ja kirjoita		
Authors	Napsauta ja kirjoita		
Editor	Napsauta ja kirjoita		
Group Author	Napsauta ja kirjoita		
Language	Napsauta ja kirjoita	**Pages**	VNK täyttää

Abstract

The Information Management Board approved the recommendation on

Provision	VNK täyttää
Keywords	board, Information Management Board, Information Management Act, public administration, information security,

ISBN PDF	VNK täyttää	**ISSN PDF**	VNK täyttää
ISBN printed	VNK täyttää	**ISSN printed**	VNK täyttää
Reference no.	Napsauta ja kirjoita	**Project no.**	Napsauta ja kirjoita
URN address	VNK täyttää		

Sisältö

1 Johdanto

Tämä tiedonhallintalautakunnan suositus opastaa tiedonhallintalain tietoturvallisuuden vähimmäisvaatimusten täyttämisessä. Suositus on tarkoitettu ensisijaisesti tiedonhallintalaissa määritetyille tiedonhallintayksiköille ja viranomaisille, mutta näiden lisäksi tätä suositusta voivat hyödyntää kaikki muutkin toimijat, jotka käsittelevät viranomaisten asiakirjoja. Jäljempänä näistä tietoturvallisuussääntelyn kohteista käytetään soveltuvin osin termiä *organisaatio.*

Suosituksessa esitetään tietojen käsittelylle säädetyt tietoturvavaatimukset sekä niihin liittyviä hyviä käytäntöjä. Jokainen luku sisältää lain vaatimuksen, täsmennyksiä lain vaatimukseen, siihen liittyvät suositukset, käytännön esimerkkejä ja viittauksia lisätietoihin. Liitteessä 1 on yhteenveto tiedonhallintalain tietoturvallisuutta koskevista lainkohdista.

Tämä suositus korvaa suosituskokoelmat tiettyjen tietoturvallisuussäännösten soveltamisesta (versiot VM 2021:65, VM 2020:61 ja VM 2020:21). Vähimmäisvaatimussuositus muodostaa yhdessä muiden tiedonhallintalautakunnan tietoturvallisuussuositusten kanssa kokonaisuuden, jota on kuvattu kohdassa 1.3.

1.1 Lainsäädännölliset perusteet

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019), jäljempänä *tiedonhallintalaki* tai *TihL*, on säädetty tietoturvallisuustoimenpiteisiin liittyviä vastuita julkisen hallinnon tiedonhallintayksiköille ja viranomaisille sekä tietyin osin yksityisille henkilöille ja yhteisöille taikka muille kuin viranomaisena toimiville julkisoikeudellisille yhteisöille, siltä osin kuin ne hoitavat julkista hallintotehtävää. Tiedonhallintalakia sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja, jollei muualla laissa toisin säädetä.

Suositus perustuu tiedonhallintalakiin. Lisäksi suosituksen laatimisessa on hyödynnetty sen perustana olevia hallituksen esityksiä[1] sekä hallintovaliokunnan mietintöjä[2].

Tiedonhallintalain 4 luku (pykälät 12–18) sisältää ensisijaiset tietoturvallisuutta koskevat vaatimukset. Lisäksi tietoturvallisuusvaatimuksia asetetaan seuraavissa tiedonhallintalain pykälissä: 4 § (tiedonhallinnan järjestäminen tiedonhallintayksikössä), 5 § (tiedonhallintamalli ja muutosvaikutusten arviointi), 19 § (tietoaineistojen sähköiseen muotoon muuttaminen ja saatavuus), 21 § (tietoaineistojen säilytystarpeen määrittäminen), 22 § (tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä), 23 § (katseluyhteyden avaaminen viranomaiselle) sekä 28 § (kuvaus asiakirjajulkisuuden toteuttamiseksi).

Suosituksessa on huomioitu myös tiedonhallintalakiin [3] lisätty uusi 13 a pykälä häiriötilanteista tiedottamisesta ja varautumisesta häiriötilanteisiin ja uusi 6 a luku automaattisen ratkaisumenettelyn käyttöönotosta ja käytöstä. Luvusta 6 a on tässä suosituksessa huomioitu erityisesti kohdat 28 c § (laadunvalvonta ja virhetilanteiden käsittely) ja 28 f § (tietojen käyttö).[4]

1.2 Vähimmäisvaatimusten merkitys

Tiedonhallintalain tarkoituksena on varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi sekä edistää viranomaisten tietoaineistojen turvallista ja tehokasta sekä tietojärjestelmien ja tietovarantojen yhteentoimivuutta. Suosituksessa kuvatut tiedonhallintalain mukaiset tietoturvallisuuden vähimmäisvaatimukset tukevat tätä lain tarkoitusta ja muodostavat ne vaatimukset, jotka kaikkien julkishallinnon organisaatioiden tulee vähintään täyttää.

[1] HE 284/2018 ja HE 145/2022 vp

[2] HaVM 39/2022 vp ja HaVM 38/2018 vp

[3] Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta (488/2023)

[4] Muutoksia koskevan siirtymäsäännöksen mukaan viranomaisen on saatettava toimintansa 13 a §:n mukaiseksi 18 kuukauden kuluessa lain voimaantulosta eli 31.10.2024 mennessä. Vastaava siirtymäaika koskee 6 a luvun sääntelyä koskien ennen kyseisen lain voimaantuloa käytössä ollutta automaattista ratkaisumenettelyä.

Vähimmäisvaatimuksilla tarkoitetaan yleisiä tai yksityiskohtaisia tietoturvallisuustoimenpiteitä, jotka viranomaisten ja tiedonhallintayksiköiden tulee tiedonhallintalain perusteella tehdä tietoturvallisuuden varmistamiseksi. Yleisiä toimenpiteitä ovat esimerkiksi tietoturvallisuutta koskevien vastuiden määrittely ja riskien tunnistaminen. Esimerkki yksityiskohtaisesta vaatimuksesta on vaatimus lokitietojen keräämisestä. Tämä suositus tukee sekä yleisten että yksityiskohtaisten tietoturvallisuuden vähimmäisvaatimusten tunnistamista ja täyttämistä.

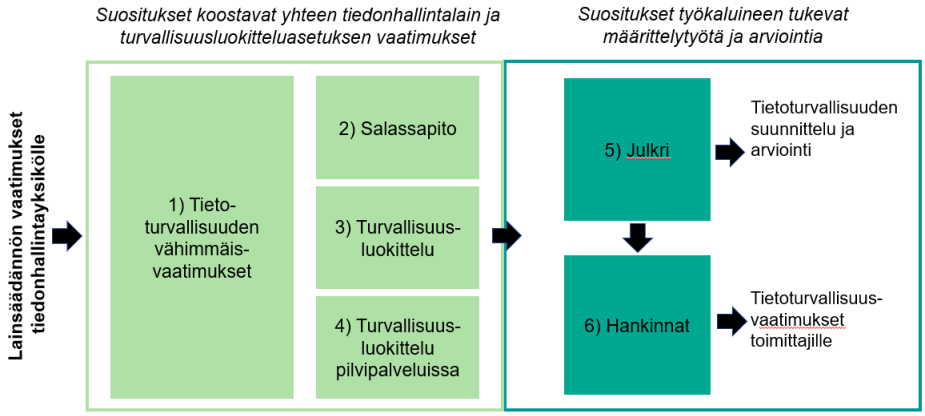
Vähimmäisvaatimusten osana organisaatioiden tulee tunnistaa ja arvioida tietojenkäsittelyyn liittyvät tietoturvallisuusriskit sekä toteuttaa toimenpiteet riskien pienentämiseksi hyväksyttävälle tasolle.

Julkisen hallinnon tietoturvallisuuden arviointikriteeristöä, jäljempänä *Julkri*, suositellaan hyödynnettäväksi tietoturvallisuusvaatimusten täyttämisessä. Julkri sisältää erilaisia tietoturvallisuustoimenpiteitä, joita organisaatio voi toteuttaa tietoturvallisuusriskien pienentämiseksi hyväksyttävälle tasolle. Lisäksi tiedonhallintalautakunta on antanut suosituksen hankintojen tietoturvallisuudesta. Hankintasuositus pohjautuu Julkriin ja se opastaa hankintoihin liittyvien tietoturvallisuusvaatimusten määrittelyssä sekä niiden täyttymisen varmistamisessa.

1.3 Suhde muihin suosituksiin

Tiedonhallintalautakunnan suositukset on laadittu tiedonhallintayksikön ja viranomaisen oman toiminnan kehittämisen tueksi. Suositukset koskevat kaikissa muodoissa olevaa tietoa.

Alla olevassa kuvassa on esitetty tiedonhallintalautakunnan eri suositusten välisiä suhteita. Tiedonhallintalaissa asetetaan viranomaisille vaatimuksia, joiden soveltamisesta tiedonhallintalautakunta antaa suosituksia. Kuvassa on tärkeimmät tietoturvallisuutta koskevat suositukset. Suositus tietoturvallisuuden vähimmäisvaatimuksista muodostaa perustan organisaation tietoturvallisuudelle. Täsmentävät suositukset on laadittu salassa pidettävien ja turvallisuusluokiteltavien asiakirjojen käsittelystä. Suositus tietoturvallisuudesta hankinnoissa ja suositus julkisen hallinnon tietoturvallisuuden arvioinnista (Julkri) sisältävät työkaluja yksityiskohtaisempien tietoturvallisuusvaatimusten määrittelyyn ja niiden toteutumisen arviointiin.



1) Suositus tietoturvallisuuden vähimmäisvaatimuksista (VM 2024: XX)
2) Suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4)
3) Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5)
4) Turvallisuusluokiteltavaien asiakirjojen käsittely pilvipalveluissa (VM 2022:4)
5) Julkisen hallinnon tietoturvallisuuden arviointikriteeristö, Julkri (VM 2023:46)
6) Suositus tietoturvallisuudesta hankinnoissa (VM 2023:57)

Kuvio 1. Tietoturvallisuuden keskeiset suositukset

Tietoturvallisuutta koskevat suositukset toimivat organisaation omien vaatimusten ja toimenpiteiden suunnittelun ja toteuttamisen apuna. Tiedonhallintalautakunnan lisäksi Kyberturvallisuuskeskus, Huoltovarmuuskeskus ja DVV:n Digiturvapalvelut (VAHTI-toiminta) julkaisevat tietoturvallisuuteen liittyviä ohjeita ja hyviä käytäntöjä. Kunkin viranomaisen tulee tapauskohtaisen riskiarvioinnin perusteella valita kuhunkin tapaukseen sopivat, riittävän turvalliset ratkaisut.

1.4 Rajaukset

Tässä suosituksessa ei ole huomioitu alla olevia säädöksiä ja velvoitteita. Organisaation tulee kuitenkin tunnistaa ja ottaa huomioon ne omassa toiminnassaan ja ohjeistuksissaan.

- toimialakohtainen erityislainsäädäntö, kuten sosiaali- ja terveydenhuollon lainsäädäntöön sisältyvät vaatimukset,
- asiankäsittelyssä ja palvelujen tuottamisessa noudatettavat menettelyt,

- salassapito ja tiedonsaantioikeus viranomaisten asiakirjoista,
- asiakirjojen arkistointi,
- henkilötietojen käsittelyä koskeva sääntely,
- laki digitaalisten palvelujen tarjoamisesta (306/2019),
- kansainvälisistä tietoturvallisuusvelvoitteista johtuvat vaatimukset sekä
- sähköisen viestinnän palveluista annettu laki (917/2014), jossa säädetään mm. sähköiseen viestintään liittyvien tietojen salassa pidosta ja käsittelystä.

2 Tehtävät ja vastuut

2.1 Tietoturvallisuusvastuiden määrittely

Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on määritelty tietoturvallisuuteen liittyvät vastuut ja tehtävät.

Tiedonhallintalain 4 §:n 2 momentin 1 kohdan mukaan ”Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on määritelty tässä ja muussa laissa säädettyjen tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut”. Tämä vaatimus koskee myös tietoturvallisuusvastuita.

Tiedonhallintayksikön tulee määritellä ja dokumentoida tietoturvallisuuden hoitamisen tehtävät ja vastuut. Tehtävien ja vastuiden määrittelyssä tulee kuvata konkreettisesti, miten ja kenen vastuulla toteutetaan tiedonhallintalain edellyttämät tietoturvallisuuteen liittyvät tehtävät. Lisäksi on suositeltavaa määritellä organisaation tietojärjestelmien ja tietoaineistojen vastuut. Vastuiden määrittelyssä tulee ottaa huomioon myös palveluntuottajan vastuulla olevat tehtävät.

Vastuut tulisi määritellä esimerkiksi tietoturvallisuusohjeiden ylläpidosta, riskienhallinnasta, varautumisesta sekä turvallisuuskokonaisuudesta (kts. Julkri HAL-osion kriteeri Tehtävät ja vastuut). Tietoturvallisuusvastuut suositellaan määrittelemään rinnakkain muiden organisaation tiedonhallintaan liittyvien vastuiden kanssa sekä riittävällä tarkkuudella suhteessa organisaation tehtävien kriittisyyteen ja tietoaineistoihin kohdistuviin turvallisuusvaatimuksiin. Pilvipalveluita käytettäessä on huomioitava lisäksi erilaiset palvelumallit sekä niihin liittyvät vastuujakojen erot asiakkaan ja palvelun tuottajan välillä.

Tehtävien ja vastuualueiden on oltava eriytettyjä, jotta vähennetään organisaation suojattavan omaisuuden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Vaarallinen työyhdistelmä on esimerkiksi se, että yksi henkilö pääsee muuttamaan sekä tietojärjestelmän tietoja että tietojärjestelmän seurannassa

käytettäviä lokitietoja. Vaaralliset työyhdistelmät on huomioitava myös ulkoistetuissa toiminnoissa.

2.2 Luotettavuutta edellyttävät tehtävät

Tiedonhallintayksikön on tunnistettava erityistä luotettavuutta edellyttävät tehtävät.

Tiedonhallintalain 12 §:n mukaan ”Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta”.

Tiedonhallintayksiköiden tulee arvioida tietoaineistojensa käsittelyyn osallistuvien henkilöiden tehtävät sekä niissä edellytettävä luotettavuus tietoturvallisuuden varmistamiseksi, ottaen huomioon myös organisaation ulkopuolella tehtävät tietojen käsittelytoimet. Erityistä luotettavuutta voivat edellyttää monet erilaiset tietoaineistojen käsittelyyn, tietojärjestelmiin, varoihin, terveydenhuoltoon tai yleiseen turvallisuuteen liittyvät tehtävät sekä pääsyoikeudet tiloihin.

Turvallisuusselvityslain (726/2014) 4 luvussa[5] on määritelty millä edellytyksillä ja minkälaisissa tehtävissä toimivista voi hakea henkilöturvallisuusselvitystä. Lisäksi lain 16 §:n mukaan valtioneuvoston asetuksella voidaan säätää, että valtionhallinnon viranomaisen on hankittava henkilöturvallisuusselvitys tietyin edellytyksin. Myös valtion virkamieslain (750/1994) 8 c § sisältää asetuksenantovaltuuden, jonka mukaan asetuksella voidaan säätää henkilöturvallisuusselvitystodistusta koskevasta vaatimuksesta edellytyksenä virkaan nimittämiselle.

Työnantajan oikeudesta saada ja käyttää tehtävään valittua työnhakijaa koskevia luottotietolain (527/2007) 4 luvussa tarkoitettuja henkilöluottotietoja säädetään

[5] Luettelot yksityiskohtaisemmista tehtävistä 19–21 §

yksityisyyden suojasta työelämässä annetun lain (759/2004) 5 a §:ssä. Työnantajan oikeudesta käsitellä huumausainetestejä koskevia tietoja säädetään lain 3 luvussa.

2.3 Tietoturvallisuus tiedonhallintamallissa

Tiedonhallintayksikön on määriteltävä ja ylläpidettävä tietoja tietoturvallisuustoimenpiteistä tiedonhallintamallissa sekä tehtävä muutosvaikutusten arviointi olennaisten muutosten yhteydessä.

Tiedonhallintalain 5 §:n 2 momentin 5 kohdan mukaan ”Tiedonhallintamallin on sisällettävä tiedot tietoturvallisuustoimenpiteistä”.

Tietoturvallisuuteen liittyvän kuvaamisen tavoitteena on, että viranomaiset suunnittelevat ennakkoon, millä tavoin tietoturvallisuus toteutetaan sekä mitä menettelyitä tietojenkäsittelyn, tietojärjestelmien ja tietoaineistojen turvaamiseksi on toteutettu tai aiotaan toteuttaa, ja miten ne ovat vastuutettu.

Tiedonhallintamallia laadittaessa suositellaan:

- sisällyttämään kuvaukseen, miten tiedonhallintalain edellyttämät tietoturvallisuuden vähimmäisvaatimukset kuten esimerkiksi pääsyoikeuksien hallinta ja tietojen salaus on toteutettu,
- suunnittelemaan kokonaisuutena, miten erilaiset organisaation tietoturvallisuuteen liittyvät ratkaisut, ohjeet, prosessit ja politiikat dokumentoidaan,
- määrittelemään, mitkä tietoturvallisuuteen liittyvät kuvaukset ovat yhteisiä, eli koskevat useita tiedonhallintamallissa esitettyjä kohteita ja mitkä liittyvät yksittäisiin tiedonhallintamallin kohteisiin,
- määrittelemään tiedonhallintamallin tietoturvallisuusasiat viittauksilla erillisiin dokumentteihin sekä
- varmistamaan ylläpidon ja dokumenttienhallinnan avulla, että tiedonhallintamalli sisältää viittaukset aina ajantasaiseen tietoturvallisuutta koskevaan dokumentaatioon.

Tiedonhallintalain 5 §:n 3 momentin mukaan ”Suunniteltaessa tiedonhallintamallin sisältöön vaikuttavia olennaisia hallinnollisia uudistuksia ja tietojärjestelmien käyttöönottoa tiedonhallintayksikössä on arvioitava näihin kohdistuvat muutokset ja niiden vaikutukset suhteessa tiedonhallintalain 4 luvussa säädettyihin tietoturvallisuusvaatimuksiin ja –toimenpiteisiin”.

Tiedonhallintayksikön on tehtävä tiedonhallinnan muutosvaikutusten arviointi tiedonhallintamalliin olennaisesti vaikuttavista tietojärjestelmien käyttöönotoista. Erityistä huomioita tulee kiinnittää tietoturvallisuuteen automatisoiduissa toimintaprosessien toteuttamisessa, koska niissä käsitellään ja tuotetaan mahdollisesti suuriakin määriä erilaisia tietoja.

Muutosvaikutusten arvioinnilla tarkoitetaan riskiarviota, jossa selvitetään, minkälaisia riskejä muutos voi aiheuttaa tiedonhallinnalle, tietojenkäsittelylle, tietojärjestelmille ja tietoaineistoille. Riskikartoituksen perusteella tulee suunnitella toimenpiteet, joilla riskit voidaan minimoida. Ennakollisen suunnittelun tarkoituksena on varmistaa tietojen saanti ja viranomaisen toiminta lakisääteisten tehtävien hoitamiseksi ja palvelujen tuottamiseksi. Muutostarpeen arvioinnissa ja tietoturvallisuustoimenpiteiden mitoittamisessa voi hyödyntää Julkri-arviointikriteeristöä.

2.4 Tietojen luokittelu ja turvallisuusluokittelu

Organisaatioita suositellaan luokittelemaan tietoaineistot sekä tietojärjestelmät luottamuksellisuuden, eheyden ja saatavuuden näkökulmista. Luokittelu mahdollistaa tietoturvallisuustoimenpiteiden suunnittelun ja toteuttamisen sekä tukee lakisääteistä turvallisuusluokittelua.

Tiedonhallintalaissa ei ole yleistä tietojen ja tietoaineistojen luokittelua koskevaa vaatimusta. Käytännössä tietoaineistojen sekä niiden käsittelyssä käytettävien tietojärjestelmien luokittelu on kuitenkin edellytys useiden tiedonhallintalaissa edellytettyjen tietoturvallisuustoimenpiteiden suunnittelulle ja toteuttamiselle.

Organisaation tietojärjestelmien tietoturvallisuusvaatimusten sekä tietoturvallisuusohjeiden räätälöinti erikseen kaikille yksittäisille tietoaineistoille ei ole käytännössä mahdollista. Sen sijaan organisaatioita suositellaan määrittelemään tietoturvallisuusvaatimukset eri luokille sekä hyödyntämään näitä vaatimuksia tietoturvallisuustoimenpiteiden suunnittelussa ja eri luokkiin kuuluvien tietoaineistojen käsittelyssä.

Tiedot suositellaan luokittelemaan luottamuksellisuuden, eheyden, saatavuuden ja niiden sisältämien henkilötietojen näkökulmista. Aineistoja luokiteltaessa suositellaan huomioimaan mahdollinen kasautumisvaikutus (Julkri HAL-osion kriteeri Suojattavat kohteet-kasautumisvaikutus).

Julkri-suosituksen luvussa Luokittelutasot, on kuvattu luokittelun eri näkökulmat sekä niihin sisältyvät luokittelutasot. Organisaatioita suositellaan täsmentämään ja ohjeistamaan omassa toiminnassa käytettävät luokittelutasot Julkrissa olevan kuvauksen pohjalta.

Tiedonhallintalain 18 §:n 1 momentin mukaan ”Valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan”.

Tietoaineistojen yleinen luokittelu tukee tämän lakisääteisen turvallisuusluokittelua koskevan vaatimuksen noudattamista valtionhallinnossa. Lisätietoja turvallisuusluokittelusta löytyy turvallisuusluokiteltavien asiakirjojen käsittelyä koskeva suosituksesta.[6]

Luokittelun apuna voi käyttää myös DVV:n Digiturvapalveluiden julkaisua kriittisten kohteiden luokittelusta.

[6] Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5)

2.5 Riskienhallinta

Tiedonhallintayksiköiden on selvitettävä olennaiset tietoturvallisuuteen kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Lisäksi organisaatioita suositellaan käyttämään dokumentoitua riskienhallinnan menetelmää ja ohjeistamaan sen soveltaminen tietoturvallisuusriskien hallinnassa.

Tiedonhallintalain 13 §:n 1 momentin mukaan ”Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti”. Lisäksi tiedonhallintalain 13 a §:ssä, 28 c §:ssä ja 28 f §:ssä edellytetään riskienhallintaa. Näihin lainkohtiin liittyviä riskienhallinnan vaatimuksia on kuvattu tarkemmin tämän suosituksen luvuissa 2.7 Varautuminen häiriötilanteisiin, 2.8 Häiriötilanteista tiedottaminen ja 4.8 Tietoturvallisuus automaattisessa ratkaisumenettelyssä.

Tiedonhallintalaissa edellytetään tietoaineistojen luottamuksellisuuteen, eheyteen ja saatavuuteen sekä tietojärjestelmien käyttöön ja vikasietoisuuteen liittyvien olennaisten riskien säännöllistä arviointia koko niiden elinkaaren ajan. Olennaisilla riskeillä tarkoitetaan riskejä, jotka voivat vaikuttaa viranomaisen toimintaan tai hallinnon asiakkaan toimintaan haittaavalla tai vahingoittavalla tavalla. Lisäksi viranomaisilta edellytetään automaattiseen päätöksenteon virheettömyyteen liittyvien riskien hallintaa.

Tiedonhallintayksiköiden tulee mitoittaa tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Tietoturvallisuustoimenpiteillä tarkoitetaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Tietoturvallisuustoimenpiteet on suhteutettava riskienhallinnan keinoin muun muassa uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

Tietoturvallisuustoimenpiteiden suunnittelussa ja jäännösriskien arvioinnissa on suositeltavaa huomioida eri turvallisuustoimenpiteiden muodostama kokonaisuus. Esimerkiksi käsiteltäessä salassa pidettäviä tai turvallisuusluokiteltuja tietoja etäkäytössä, on käyttäjien vahva tunnistaminen perusteltu vaatimus. Jos

käsittely tapahtuu turvallisissa toimitiloissa, joihin pääsy sivullisilta on estetty, voi käyttäjätunnukseen ja salasanaan perustuva tunnistaminen riittää.

Riskienhallinta on kokonaisuus, johon kuuluu riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen. Riskienhallinta ei ole kertaluonteista, vaan jatkuvaa toimintaa, jossa muun muassa arvioidaan suunnitelmien toteutumista ja toteutettujen tietoturvatoimenpiteiden vaikuttavuutta.

Tietoturvallisuuteen liittyvien riskien hallinnassa on suositeltavaa hyödyntää dokumentoitua ja ohjeistettua riskienhallintamenetelmää, joka varmistaa yhdenmukaiset tulokset arvioijasta ja riskien tyypistä riippumatta. Esimerkki riskienhallinnan menetelmästä löytyy Riskienhallinnan käsikirjasta[7].

Lisäksi organisaatiot voivat toteuttaa seuraavia toimenpiteitä laadukkaan tietoturvallisuusriskien hallinnan varmistamiseksi:

- varmistaa, että tietoturvariskien tunnistamisen lähtötietoina ovat ajantasaiset kuvaukset organisaation käsittelemistä tietoaineistoista, käsittelyprosesseista ja käsittelyssä hyödynnettävistä tietojärjestelmistä sekä niiden vastuista, (ajantasainen tiedonhallintamalli voi toimia tällaisena lähtötietona)
- suunnitella ja priorisoida tietoaineistojen luokittelun perusteella tietoturvallisuusriskien tunnistamiseen ja arviointiin liittyvät toimenpiteet,
- ohjeistaa tietoturvallisuuteen liittyvien riskien arvioinnin perusteet sekä riskien todennäköisyyden että vaikutusten osalta[8],
- määritellä tietoturvallisuusriskien hyväksymiskriteerit ja menettelyt, joiden mukaisesti jäännösriskit hyväksytään sekä
- viedä ylikorkeat jäännösriskit organisaation johdon päätettäväksi.

Tietoturvallisuusriskien arvioinneissa voidaan hyödyntää Julkrin HAL-osion kriteerejä Riskienhallinta sekä Riskienhallinta – lainsäädäntöjohdannaiset riskit.

[7] Riskienhallinnan käsikirja valtionhallinnon toimijoille (VM 2023:54)
[8] Ohjeen pohjana voi hyödyntää Riskienhallinnan käsikirjan luvussa ”Riskien merkityksen arviointi” olevia taulukoita, mutta niitä on suositeltavaa täydentää konkreettisilla organisaation tietoturvallisuusriskienhallintaa tukevilla esimerkeillä.

2.6 Ohjeet ja koulutus

Organisaatiolla tulee olla ajantasaiset ohjeet tietoturvallisuudesta sekä tarjolla koulutusta niiden riittävän tuntemisen varmistamiseksi.

Tiedonhallintalain 4 §:n 2 momentin mukaan ”Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on

2) ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta;
3) tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja tiedonhallintayksikön lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista”.

Ohjeissa tulee huomioida seuraavat näkökohdat:

- miten tietoaineistoja käsitellään toimintaprosesseissa,
- miten tietojärjestelmiä käytetään tietoturvallisella tavalla lainmukaisiin käyttötarkoituksiin,
- miten tietojenkäsittelyoikeudet määritellään tietojärjestelmiin ja niillä operoitaviin tietovarantoihin sekä niissä oleviin tietoaineistoihin,
- määritellä, millä perusteella ja kenen toimesta käyttöoikeuksia myönnetään,
- miten organisaation sisäisen tehtäväjaon mukaiset tietoturvallisuuden vastuut toteutetaan käytännössä,
- miten ja kenen vastuulla on tietopyyntöihin vastaaminen ja millä tavalla pyydetyt tiedot annetaan sekä
- varautuminen poikkeaviin tilanteisiin, kuten esimerkiksi tietoliikennehäiriöön tai tietojärjestelmässä olevan käyttökatkoon.

Koulutuksiin ja perehdytyksiin kohdistuvat seuraavat vaatimukset:

- organisaation tulee tarjota mahdollisuus koulutukseen tai muuhun perehdytykseen tietoturvallisuuteen liittyvistä menettelytavoista, määräyksistä ja ohjeista,

- koulutusten ja perehdytysten tulee sisältää tietoja sovellettavasta lainsäädännöstä, mukaan lukien asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä sekä
- koulutusta tulee järjestää henkilöstölle ja muille tiedonhallintayksikön lukuun toimiville, kuten sidosryhmien asiantuntijoille.

Suosituksia yleisistä toimenpiteistä, joita organisaatio voi toteuttaa:

- laatia selkeät ohjeet kuinka eri luokkiin kuuluvia tietoja tulee käsitellä,
- varmistaa ohjeiden ymmärrettävyys henkilöillä, jotka eivät ole tietoturva-asiantuntijoita,
- jakaa ohjeet riittävän pieniin kokonaisuuksiin, joista on nopeasti löydettävissä ohjeen pääasiallinen sisältö,
- käyttää tehostekeinoja, jotka korostavat ohjeen pääasiallista sisältöä,
- varmistaa, että ohjeen otsikko ja sisältö vastaavat toisiaan,
- toteuttaa hakupalvelut, joiden avulla ohje on helposti löydettävissä,
- linkittää ohjeet niihin tilanteisiin, joissa niitä todennäköisesti tarvitaan,
- koota ajantasaiset tietoturvaohjeet yhteen paikkaan, josta organisaation käyttäjien on helppo löytää ne,
- viestiä ohjeista sekä niihin tehdyistä muutoksista,
- huolehtia, että tietoturvallisuutta koskevat koulutukset ovat saatavilla myös verkon kautta ajankohdasta riippumatta sekä
- varmistaa, että ohjeisiin on tutustuttu ja keskeinen sisältö on ymmärretty.

2.7 Varautuminen häiriötilanteisiin

Tiedonhallintayksikön on selvitettävä toiminnan jatkuvuuteen kohdistuvat olennaiset riskit ja huolehdittava etukäteisvalmisteluin toiminnan mahdollisimman häiriöttömästä jatkumisesta sekä normaaliolojen häiriötilanteissa että poikkeusoloissa.

Tiedonhallintalain 13 a §:n 3 ja 4 momentin mukaan ”Tiedonhallintayksikön on selvitettävä sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvat olennaiset riskit. Tiedonhallintayksikön on riskiarvioinnin perusteella valmiussuunnitelmin ja häiriötilan-

teissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä huolehdittava, että sen tietoaineistojen käsittely, tietojärjestelmien hyödyntäminen ja niihin perustuva toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa.

Viranomaisten yleisestä varautumisvelvollisuudesta poikkeusoloihin sekä valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tietoturvallisuuden järjestämisestä poikkeusoloissa säädetään valmiuslaissa".

Tiedonhallintayksikön on varauduttava toiminnassaan siihen, että tietojärjestelmät vikaantuvat tai niiden toiminta muusta syystä estyy. Tietojärjestelmien mahdollisimman häiriötön toiminta tulee pyrkiä turvaamaan kaikissa tilanteissa. Lisäksi tulee varautua turvaamaan tietojen käsittelyn ja toiminnan jatkuvuus myös tilanteissa, joissa tietojärjestelmää ei voida käyttää.

Tiedonhallintayksikön on selvitettävä olennaiset toiminnan jatkuvuuteen kohdistuvat riskit. Riskejä ovat tietojärjestelmän vikaantumisen lisäksi esimerkiksi riippuvuudet muiden hallinnassa olevista tietoaineistoista ja –järjestelmistä, häiriöt sähkönsyötössä tai viestintäverkkojen ja -palvelujen toiminnassa, sekä toimitusketjujen kriittisyys ja niiden varautumisen taso. Toiminnan jatkuvuuteen liittyvät näkökohdat on huomioitava myös toimittajien kanssa tehtävissä sopimuksissa. Riskiarvioinnissa tulee ottaa huomioon tietoaineistojen ja tietojärjestelmien kriittisyys, jatkuvuuden turvaamisen mahdollisuudet ja eritasoisten jatkuvuutta turvaavien toimenpiteiden kustannukset.

Viranomaisen on suunniteltava ennalta, miten se tiedottaa muille viranomaisille häiriötilanteissa. Suunniteltaessa tulee erityisesti kiinnittää huomiota niille viranomaisille tiedottamiseen, joiden toiminta on riippuvaista viranomaisen tietojärjestelmän toiminnasta. Lisäksi viestinnän suunnittelussa on otettava huomioon digitaalisten palvelujen ja tietoaineistojen saatavuuden osalta tiedottaminen yleisölle tarjottavien palvelujen järjestelyistä.

Häiriötilanteisiin varautumiseksi suositellaan:

- toteuttamaan teknisiä ja rakenteellisia etukäteisvalmisteluja sekä tilojen ja kriittisten resurssien varauksia,
- varmistamaan henkilöstön osaaminen ohjeistamalla ja kouluttamalla sekä häiriötilanteiden harjoittelulla,
- suunnittelemaan sijaisjärjestelyt,

- varautua ottamaan käyttöön vaihtoehtoisia asiointimuotoja, mikäli automatisoitua toimintaprosessia ei voida hyödyntää,
- toteuttamaan olosuhdehälytyksiä ja seurantaa, joilla varmistetaan nopea tiedonsaanti tietojärjestelmien häiriötilanteista,
- varmistamaan tehonsyöttö sekä toteuttamaan vaihtoehtoiset tietoliikenneyhteydet,
- varmistamaan tietojen saanti ulkoisista tietovarannoista, jos toiminta tai automaattinen päätöksenteko edellyttävät sekä
- sopimaan menettelyt, joilla tietojärjestelmät pystyvät toimimaan tietojen saantiin liittyvissä häiriötilanteissa tai vähintään saamaan ilmoituksen niistä.

2.8 Häiriötilanteista tiedottaminen

Viranomaisen on viipymättä tiedotettava häiriötilanteista sen tietoaineistoja hyödyntäville. Viranomaisia suositellaan suunnittelemaan etukäteen, miten häiriötilanteista tiedotetaan.

Tiedonhallintalain 13 a §:n 1 momentin mukaan ”Viranomaisen on viipymättä tiedotettava sen tietoaineistoja hyödyntäville, jos sen tiedonhallintaan kohdistuu häiriö, joka estää tai uhkaa estää viranomaisen tietoaineistojen saatavuuden. Viranomaisen on tiedotettava häiriön tai sen uhkan arvioidusta kestosta, mahdollisuuksien mukaan korvaavista tavoista hyödyntää viranomaisen tietoaineistoja sekä häiriön tai uhkan päättymisestä”.

Tapa, jolla käyttökatkoista ja palvelun saatavuudesta tiedotetaan, jää viranomaisen harkintaan. Tiedottaminen on mahdollista esimerkiksi viranomaisen yleisillä verkkosivuilla tai asiayhteyteen muuten olennaisesti liittyvällä muulla verkkosivulla. Tiedottamisen tapaan vaikuttaa se, kenelle tiedotetaan. Vakiintuneille yhteistyötahoille ja viranomaisen tietoaineistoista keskeisesti riippuvaisille tiedottaminen voi olla kohdennetumpaa kuin yleisölle suunnattu tiedottaminen. Viranomaisen on myös tiedotettava mahdollisuuksien mukaan korvaavista tavoista hyödyntää viranomaisen tietoaineistoja sekä kertoa häiriön arvioitu kesto.

Häiriötilanteista tiedottamiseen suositellaan:

- suunnittelemaan etukäteen, miten ja kenelle häiriötilanteissa tiedotetaan,
- määrittelemään tiedottamisen vastuut sekä
- varmistamaan tiedon nopea perillemeno ja ymmärrettävyys.

Lisäksi digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) 4 §:n 2 momentin mukaan viranomaisen on tiedotettava digitaalisten palvelujensa ja muiden tiedonsiirtomenetelmien käyttökatkoista sopivalla tavalla ennalta yleisölle. Viranomaisen on myös julkaistava käyttökatkon ajaksi ohjeet, miten jokainen saa asiansa hoidetuksi vaihtoehtoisella tavalla.

2.9 Valvonta

Tiedonhallintayksikön johdon on huolehdittava, että yksikössä on järjestetty riittävä valvonta tietoturvallisuutta koskevien säädösten, määräysten ja ohjeiden noudattamisesta ja että henkilöstöllä on riittävä osaamistaso.

Tiedonhallintalain 4 §:n 2 momentin 5 kohdan mukaan tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta.

Tiedonhallintayksikössä on oltava riittävät valvontamenettelyt, joilla varmistetaan tietoturvallisuutta koskevien laeissa säädettyjen vaatimusten sekä tiedonhallintayksikön sisäisten määräysten ja ohjeiden noudattaminen. Valvontaan sisältyy myös henkilöstön tietoturvaosaamisen riittävyyden valvonta. Valvonnan järjestäminen on osa sisäisen valvonnan järjestelyjä ja tietoturvallisuustoimenpiteiden toteuttamista.

Valvonnan toteuttamiseksi organisaatio voi toteuttaa seuraavia toimenpiteitä:

- dokumentoida, miten valvontavastuu on jaettu johdolle ja esimiehille,
- laatia valvontasuunnitelma, johon on kuvattu ja aikataulutettu valvontatoimenpiteet,

- järjestää testejä tietoturvallisuusosaamisesta ja määräysten tuntemisesta,
- toteuttaa tietojärjestelmiin automaattisia valvontakontrolleja,
- kuvata, miten valvonnan toimivuutta arvioidaan ja kehitetään sekä
- raportoida määräajoin johdolle tietoturvallisuuden valvonnan tuloksista.

3 Tietoaineistot

3.1 Tietoaineistojen tietoturvallisuus

Viranomaisten on varmistettava tarpeellisin tietoturvallisuustoimenpitein tietoaineistojen turvallisuus ottaen huomioon tiedonhallintalain 15 §:ssä eritellyt vaatimukset.

Yksittäisten tietoturvallisuustoimenpiteiden määrittely tulee tehdä riskiarvion perusteella

Tiedonhallintalain 15 §:n 1 momentin mukaan ”Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen:

1. tietoaineistojen muuttumattomuus on riittävästi varmistettu;
2. tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;
3. tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu;
4. tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu;
5. tietoaineistojen saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu;
6. tietoaineistot voidaan tarvittavilta osin arkistoida.”

Edellä oleva pykälä sisältää luettelon pakollisista vaatimuksista tietoaineistojen tietoturvallisuustoimenpiteiden toteuttamiseksi.

Viranomaisten on varmistettava tietoaineistojen muuttumattomuus tarvittavassa laajuudessa. Tietoaineistojen muuttumattomuus on osassa tietoaineistoja tärkeää niiden todistusvoimaisuuden kannalta. Muuttumattomuus tulee varmistaa erityisesti tietoaineistoissa, joilla määritellään yksilöiden ja yhteisöjen etuja, oikeuksia ja velvollisuuksia. Viranomainen voi harkita, miten muuttumattomuus varmistetaan.

Tietoaineistot tulee suojata teknisiltä ja fyysisiltä vahingoilta. Vaatimus koskee muun muassa tietojärjestelmien ja niihin liittyvien palvelimien säilytystiloja sekä paperimuotoisten tietoaineistojen säilytyspaikkoja.

Alkuperäisyys, ajantasaisuus ja virheettömyys ovat tärkeitä viranomaistoiminnan asianmukaisuuden sekä hallinnossa työskentelevien ja hallinnon asiakkaiden oikeusturvan varmistamiseksi.

Viranomaisten toiminta on tietointensiivistä ja riippuvaa viranomaisten tietovarannoissa olevista tietoaineistoista. Asianmukaisen viranomaistoiminnan varmistamiseksi on varmistettava, että tiedot ovat saatavissa käyttökelpoisessa muodossa.

Pääsyä julkisiin tietoaineistoihin ei tule rajoittaa tarpeettomasti. Pääsyn rajoittaminen henkilötietoihin ja salassa pidettäviin tietoihin perustuu lakiin.

Tietoaineistot on voitava arkistoida tarpeellisilta osin. Arkistoituihin tietoaineistoihin sovelletaan tiedonhallintalain tietoturvallisuussäännöksiä, ellei muualla ole toisin säädetty. Arkistoinnista on säädetty erikseen arkistointia koskevissa säädöksissä, joista keskeisimpiä ovat arkistolaki (831/1994), EU:n yleinen tietosuoja-asetus ((EU) 2016/679), jäljempänä *tietosuoja-asetus* sekä tietosuojalaki (1050/2018).

Lisäksi organisaation tulee riskiarvion perusteella määritellä tietoaineistoihin, niiden käsittelyssä käytettäviin tietojärjestelmiin sekä tietoaineistojen käsittelyprosesseihin kohdistuvat yksityiskohtaiset tietoturvallisuustoimenpiteet, kuten tämän suosituksen luvuissa 2.5 Riskienhallinta ja 4.1 Tietojärjestelmien tietoturvallisuus on kuvattu. Yksittäisten tietoturvallisuustoimenpiteiden suunnittelussa voi hyödyntää Julkri-arviointikriteeristöä.

3.2 Toimitilaturvallisuus

Tietoaineistoja on käsiteltävä ja säilytettävä niiden eheyden, saatavuuden ja luottamuksellisuuden kannalta riittävän turvallisissa toimitiloissa. Turvallisuuden varmistamiseksi suositellaan toteuttamaan riskiperusteisesti ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä.

Tiedonhallintalain 15 §:n 2 momentissa todetaan, että ”Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia”.

Säännös korostaa sitä, että tietoaineistojen säilyttämisessä käytettävissä toimitiloissa on huomioitava kaikki tietoaineistojen säilytystä koskevat tietoturvallisuusvaatimukset. Toimitilaturvallisuuden varmistamiseksi suositellaan toteutettavaksi ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä turvallisuutta vaarantavien tekojen havaitsemiseksi, jäljittämiseksi sekä turvallisuustason palauttamiseksi.

Toimitilaturvallisuus perustuu riskien arviointiin ja monitasoiseen suojaukseen. Siten joissakin tilanteissa voidaan riskien arviointiin perustuen joko hyväksyä puutteita yksittäisissä suojaustoimenpiteissä tai edellyttää normaalia korkeampia toimenpiteitä.

Osana toimitilaturvallisuuden suunnittelua on suositeltavaa määritellä ja ohjeistaa, millä edellytyksillä tietoja voi käsitellä ja säilyttää etätöissä sekä yhteiskäyttöisissä toimitiloissa.

Toimitilojen suojaamisessa on suositeltavaa hyödyntää Julkri-kriteeristöä sekä siellä määriteltyjä turvallisuusalueita ja fyysisen turvallisuuden kriteereitä.

Toimitilaturvallisuuden varmistamiseksi organisaatio voi toteuttaa seuraavia toimenpiteitä:

- huolehtia tilojen lukituksista sekä pääsyoikeuksien ja avainten hallinnasta,
- ottaa käyttöön kulunvalvontajärjestelmä,

- jakaa toimitilat tarvittaessa erillisiin turvallisuusalueisiin ja toteuttaa ylimääräisiä tietoturvallisuustoimenpiteitä alueilla, joissa käsitellään tietoja, joihin kohdistuu korkeampia turvallisuusvaatimuksia,
- sijoittaa työpisteet siten, että salakatselu ei ole mahdollista sekä hankkia salakatselun estäviä suojia,
- huolehtia tilojen äänieristyksistä siten, että salassa pidettävistä tiedoista on mahdollista keskustella turvallisesti sekä
- huolehtia, että vierailijoilla on saattajat.

3.3 Tekniset rajapinnat ja katseluyhteys

Viranomaisen tulee varmistaa teknisesti luovutettavien henkilötietojen ja salassa pidettävien tietojen tapauskohtainen tarpeellisuus, rajata katseluyhteydet vain tarpeellisiin tietoihin kohdistuviin yksittäisiin hakuihin, selvittää tietojen hakemisen yhteydessä tietojen käyttötarkoitus sekä tunnistaa automaattisesti poikkeava tietojen hakeminen.

Tiedonhallintalain 22 §:n 2 momentin mukaan ”Sen lisäksi, mitä 4 luvussa (tietoturvallisuus) säädetään, tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä siten, että teknisesti varmistetaan luovutettavien tietojen tapauskohtainen tarpeellisuus tai välttämättömyys tietoja saavan viranomaisen tehtävien hoitamiseksi, jos luovutettavat tiedot ovat henkilötietoja tai salassa pidettäviä tietoja”.

Tiedonhallintalain 23 §:n mukaan ”Sen lisäksi, mitä 4 luvussa (tietoturvallisuus) säädetään, edellytyksenä katseluyhteyden avaamiselle on, että:

1) katselumahdollisuus on rajattu vain yksittäisiin hakuihin, jotka voivat kohdistua tiedonsaantioikeuden mukaisesti tarpeellisiin tai välttämättömiin tietoihin; sekä
2) tietojen hakemisen yhteydessä selvitetään tietojen käyttötarkoitus.

Viranomaisen on toteutettava katseluyhteys siten, että katseluyhteyden mahdollistava tietojärjestelmä tunnistaa automaattisesti poikkeavan tietojen hakemisen”.

Säännös teknisistä rajapinnoista koskee tilanteita, joissa viranomainen luovuttaa toiselle viranomaiselle säännöllisesti tietovarannostaan tietoja toisen viranomaisen lakiin perustuvia tietotarpeita varten. Teknisen rajapinnan avulla luovutettavien tietojen tietopyynnön lähettävässä tietojärjestelmässä tulee olla suojaukset, joilla varmistetaan, että pyydetyt tiedot ovat tarpeellisia. Esimerkiksi terveydenhuollossa ennen potilasrekisterien välillä tapahtuvaa tietoluovutusta on tietoteknisesti varmistettava hoitosuhde potilaaseen.

Katseluyhteyden avaamisen yleisenä edellytyksenä on laissa säädetty tiedonsaantioikeus katseluyhteyden kautta saataviin tietoihin. Katseluyhteys tulee rajata vain ennalta tehdyn arvioinnin perusteella viranomaiskohtaisesti määriteltyihin tehtävien hoitamiseksi tarpeellisiin tietoihin. Lisäksi katselumahdollisuus tulee rajoittaa yksittäisiin hakuihin siten, että katselumahdollisuuden avulla ei ole mahdollisuutta saada toisen viranomaisen tietovarannon tietoja rajoituksetta.

Tietojen hakemisen yhteydessä tulee selvittää tietojen käyttötarkoitus. Käytännössä tämä voidaan toteuttaa esimerkiksi siten, että tietoja haettaessa tietojen hakijan pitää antaa tietojen hakemisen peruste.

Poikkeavan tietojen hakemisen estämiseksi katseluyhteyksiin on toteutettava riittävät suojaukset, joilla estetään massamuotoinen tietojen hakeminen toisen viranomaisen tietovarannosta. Esimerkiksi tietojärjestelmä voi tunnistaa poikkeukselliset tietohaut tietyn rekisteröidyn tietoihin tai tietyn käyttäjän poikkeavat tietohaut niiden lukumäärän perusteella.

Tiedonhallintalautakunnan suositus teknisistä rajapinnoista ja katseluyhteyksistä[9] sisältää yksityiskohtaisempia suosituksia teknisen rajapinnan ja katseluyhteyden avaamisen edellytyksistä.

[9] Suositus teknisistä rajapinnoista ja katseluyhteyksistä (VM 2021:21)

3.4 Tietoturvallinen arkistointi ja tuhoaminen

Tiedonhallintayksikön on huolehdittava tietoaineistojen arkistoinnista tai tuhoamisesta tietoturvallisella tavalla.

Tiedonhallintalain 21 §:n 2 momentin mukaan ”Säilytysajan päättymisen jälkeen tietoaineistot on arkistoitava tai tuhottava viipymättä tietoturvallisella tavalla”.

Kaikkia tietoaineistoihin kohdistuvia tietoturvallisuusvaatimuksia sovelletaan myös tietoaineistojen arkistoinnissa. Arkistoinnin edellytyksistä ja arvon määrityksestä saa lisätietoja Kansallisarkistosta [10]. Suosituksia tietoaineistojen säilytysajoista ja toimenpiteistä säilytysajan päätyttyä löytyy tiedonhallintalautakunnan suosituksesta (VM 2022:54).

Tietoaineistojen tuhoamisella tarkoitetaan sitä, että tietoaineisto on poistettava käytöstä siten, ettei sitä enää voida palauttaa uudelleen käyttöön. Tuhoaminen voidaan tehdä erilaisilla teknisillä toimilla, kuten esimerkiksi kovalevyjen päällekirjoittamisella tai fyysisellä murskaamisella tai sulattamalla. Paperiaineistojen tuhoaminen tapahtuu puolestaan esimerkiksi polttamalla tai silppuamalla. Säännöksellä korostetaan sitä, että aineistot on tuhottava tosiasiallisesti, kun säilyttämiselle ei ole perusteita tai ellei tietoaineistoa siirretä erikseen säädetyn perusteella arkistoon.

Tietoaineistojen tietoturvallisen tuhoamisen varmistamiseksi organisaatio voi toteuttaa seuraavia toimenpiteitä:

- huomioida tuhoamismenettelyn valinnassa tietoaineiston luottamuksellisuus,
- ohjeistaa tuhoaminen osana laitteiden elinkaaren hallintaa mukaan lukien oheislaitteet ja muistivälineet,
- sisällyttää laitteistojen osien (kuten kiintolevyt, muistit ja muistikortit) sisältämän tiedon luotettava tuhoaminen osaksi käytöstä poiston, huoltoon lähetyksen ja uusiokäytön prosesseja sekä

[10] Arkistoinnin ohjaus | Kansallisarkisto

- ohjeistaa ja varmistaa sopimuksissa pilvipalveluissa olevan tiedon tuhoaminen asianmukaisesti.

Sähköisessä muodossa olevien tietojen tuhoamisen menetelmiä on kuvattu Julkrin TEK-osion kriteerissä Sähköisessä muodossa olevien tietojen tuhoaminen ja sen alikriteereissä. Tietojen fyysisen tuhoamisen menetelmiä on kuvattu tarkemmin Julkrin FYY-osion kriteerissä Tietojen fyysinen tuhoaminen ja sen alikriteereissä.

4 Tietojärjestelmät

4.1 Tietojärjestelmien tietoturvallisuus

Tiedonhallintayksikön on seurattava toimintaympäristön tietoturvallisuutta ja varmistettava tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan riskien arviointiin perustuvilla tietoturvallisuustoimenpiteillä.

Yksittäisten tietoturvallisuustoimenpiteiden tunnistamisessa ja valinnassa suositellaan hyödyntämään Julkri-suositusta.

Tiedonhallintalain 13 §:n 1 momentin mukaan "Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti”.

Tietojärjestelmä on laaja kokonaisuus, johon voi tapauskohtaisesti kuulua laaja joukko erilaisia tietojenkäsittelyyn liittyviä ratkaisuja ja palveluita sekä organisaation sisällä että sen ulkopuolella. Esimerkiksi ulkoistettu pilvipalvelu voi olla tietojärjestelmä tai sen osa, jonka tietoturvallisuus tulee varmistaa. Tarkastelussa tulee huomioida koko palvelun toimitusketju sisältäen myös mahdolliset toimittajan alihankkijoiden vastuulla olevat palvelut.

Toimintaympäristön tietoturvallisuuden tilan seurannassa suositellaan:

- suunnittelemaan ja kohdistamaan seurannan toiminnan luonteen ja kriittisyyden mukaan,
- sisällyttämään seurantaan myös organisaation ulkoisen toimintaympäristön,
- seuraamaan kriittisten tietojärjestelmien kuormitusta ja käyttöhäiriöitä,
- seuraamaan korkeaa luottamuksellisuutta vaativien tietojen käyttöä ja siinä havaittavia poikkeavuuksia sekä
- seurata haavoittuvuuksia ja huolehtia niiden nopeasta korjaamisesta.

Lisätietoja seurannan toteutuksesta eri turvallisuuden tasoilla löytyy Julkrin TEK-osion kriteereistä Turvallisuuteen liittyvien tapahtumien jäljitettävyys, Poikkeamien havainnointikyky ja toipuminen sekä niiden alikriteereistä.

Tietoturvallisuustoimenpiteet voivat vaihdella hyvinkin paljon tietojärjestelmän ja siinä käsiteltävien tietojen luonteen perusteella. Tiedonhallintalaissa on määritelty vaatimuksia tietoturvallisuustoimenpiteille esimerkiksi käyttöoikeuksien hallinnan ja tietojen siirtämisen osalta. Tällaisia vaatimuksia on käsitelty myöhemmin tässä luvussa.

Pääosa tietojärjestelmiin kohdistuvista tietoturvallisuustoimenpiteistä tulee määritellä riskiarvioinnin perusteella. Erilaisia tietoturvallisuustoimenpiteitä on paljon ja niiden yksityiskohdat vaihtelevat käsiteltävien tietojen luonteen mukaan. Tämä suositus ei ota kantaa yksittäisiin tietoturvallisuustoimenpiteisiin, mutta niiden tunnistamisessa voi hyödyntää Julkria, joka sisältää työkaluja sekä tarvittavien tietoturvallisuustoimenpiteiden tunnistamiseen että niiden asettamiseen sopivalle vaatimustasolle. Tietoturvallisuustoimenpiteiden määrittelyn perusteena olevaa riskienhallintaa on käsitelty tämän suosituksen luvussa 2.5.

Tietojärjestelmien koko elinkaaren ajan kestävä tietoturvallisuuden varmistaminen edellyttää toimenpiteitä tietojärjestelmien hankinnasta niiden käytöstä luopumiseen asti. Tämä edellyttää, että tietoturvallisuuden tilan seuranta, tietojärjestelmiin kohdistuva riskien arviointi sekä niiden perusteella tehtävä tietoturvallisuustoimenpiteiden ylläpito on suunnitelmallista ja jatkuvaa toimintaa.

4.2 Tietojärjestelmien hankinnat

Hankinnoissa on varmistettava, että tietojärjestelmä täyttää käsiteltävien tietoaineistojen mukaiset tietoturvallisuusvaatimukset ja on käyttökelpoinen viranomaisen tehtävien hoitamiseksi.

Tiedonhallintalain 13 §:n 4 momentin mukaan ”Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet”.

Viranomaisten tietojenkäsittely tapahtuu pääsääntöisesti tietojärjestelmissä. Hankinnoissa on varmistettava, että hankittava tietojärjestelmä täyttää käsiteltävien tietoaineistojen mukaiset tietoturvallisuusvaatimukset ja että tietojärjestelmä on käyttökelpoinen viranomaisen tehtävien hoitamiseksi tuloksekkaasti ja tehokkaasti.

Tiedonhallintalautakunnan suositus tietoturvallisuudesta hankinnoissa (VM 2023:57) sisältää ohjeita tietoturvallisuuden varmistamiseksi tietojärjestelmähankinnoissa sekä liitteitä, joita voi hyödyntää tarjouspyynnöissä ja sopimuksissa. Suosituksessa kuvattu prosessi kattaa vaiheet, joiden avulla suunnitellaan ja varmistetaan hankinnan tietoturvallisuus sekä huolehditaan tietoturvallisuuden säilymisestä koko elinkaaren ajan.

4.3 Vikasietoisuus ja toiminnallinen käytettävyys

Viranomaisen tulee testata säännöllisesti olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys.

Tiedonhallintalain 13 §:n 2 momentin mukaan ”Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti”.

Viranomaisen olennaisten tietojärjestelmien vikasietoisuus tulee testata säännöllisesti toiminnan jatkuvuuden varmistamiseksi ja tietoturvallisuustoimenpiteiden ajan tasalla pitämiseksi. Olennaisilla tietojärjestelmillä tarkoitetaan tietojärjestelmiä, jotka ovat kriittisiä viranomaisen lakisääteisten tehtävien toteuttamisen kannalta erityisesti hallinnon asiakkaille palveluja tuotettaessa.

Tietojärjestelmien toiminnallinen käytettävyys tulee varmistaa testauksen avulla niin hankintavaiheessa kuin merkittävien ylläpitotoimien yhteydessä. Toiminnallisella käytettävyydellä tarkoitetaan sen varmistamista, että tietojärjestelmä on helposti opittava, sen toimintalogiikka on helposti muistettava, sen toiminta tukee

niitä työtehtäviä, joita käyttäjän pitää tehdä tietojärjestelmällä ja tietojärjestelmä edistää sen käytön virheettömyyttä.

Vikasietoisuuden ja toiminnallisen käytettävyyden varmistamiseksi suositellaan seuraavia toimenpiteitä:

- luokittelemaan tietojärjestelmät niiden toiminnallisen kriittisyyden mukaan,
- laatimaan suunnitelma vikasietoisuuden ja toiminnallisen käytettävyyden testaamisesta ja sisällyttämään se tietoturvallisuuden vuosikelloon,
- parantamaan olennaisten tietojärjestelmien vikasietoisuutta erilaisin keinoin kuten kahdentamalla, hajauttamalla tai varajärjestelmillä,
- ottamaan varmistuksia tiedoista riittävän usein,
- testaamaan, että tietojen palautus varmuuskopioista onnistuu,
- testaamaan toiminnallinen käytettävyys yhdessä järjestelmän varsinaisten käyttäjien kanssa sekä
- suunnittelemaan tietojärjestelmään virheentarkastusmenettelyt sekä käyttäjien syöttämille että ulkopuolisista lähteistä siirrettäville tiedoille.

4.4 Salassa pidettävien tietojen siirtäminen yleisissä tietoverkoissa

Viranomaisen on suojattava salassa pidettävien tietojen siirto yleisissä tietoverkoissa. Lisäksi tietojen vastaanottaja on varmistettava riittävän tietoturvallisella tavalla ennen pääsyä salassa pidettäviin tietoihin.

Tiedonhallintalain 14 §:n mukaan ”Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja”.

Viranomainen voi harkita, miten salassa pidettävien tietojen suojaaminen yleisessä tietoverkossa toteutetaan. Yhteys voi olla suojattu esimerkiksi salauksella

tai tiedot voidaan siirtää ilman tietoliikenneyhteyden suojaustakin, jos tiedot ovat salattuna siirrettävässä tiedostossa ja salaus voidaan purkaa vain erillisellä PIN-koodilla tai muulla salasanalla. Lisätietoja löytyy tiedonhallintalautakunnan suosituksesta salassa pidettävien asiakirjojen käsittelystä sekä Julkrin TEK-osion kriteeristä Tiedon salaaminen.

Vaatimus salassa pidettävien tietojen suojaamisesta yleisessä tietoverkossa koskee sekä viranomaisten välistä tietoliikennettä että yleisölle tarjottavia digitaalisia palveluita. Vaatimusta ei sovelleta viranomaisen sisäisessä verkossa tapahtuvaan tietojen siirtämiseen, koska viranomaisen sisäisessä tietoverkossa tietojen siirtoon liittyvät riskit eivät ole vastaavia kuin yleisessä tietoverkossa.

Vastaanottajan varmistaminen tietojärjestelmien välillä voidaan toteuttaa esimerkiksi palvelinvarmenteita käyttämällä. Jos salassa pidettävien tietojen vastaanottaja on luonnollinen henkilö, tulee hänet tunnistaa jollakin luotettavalla menetelmällä, kuten vahvaa sähköistä tunnistusmenetelmää käyttämällä.

Vaatimus salassa pidettävien tietojen vastaanottajan tunnistamisesta ja varmistamisesta koskee esimerkiksi viranomaisten välistä viestintää sähköpostin avulla sekä viranomaisten tietojärjestelmien välistä viestintää rajapintojen avulla. Vastaanottajan tunnistamista koskevista vaatimuksista yleisölle tarjottavissa digitaalisissa palveluissa on säädetty erikseen digitaalisten palvelujen tarjoamista koskevassa laissa (306/2019).

4.5 Käyttöoikeuksien hallinta

Viranomaisen tulee varmistaa, että tietojärjestelmiin pääsevät vain ne henkilöt, joilla on oikeus käsitellä tietoaineistoja tietojärjestelmässä ja vain siltä osin kuin heidän tehtäviinsä perustuvat tietoaineistojen käyttötarpeet sitä edellyttävät. Käyttöoikeudet tulee pitää jatkuvasti ajan tasalla.

Tiedonhallintalain 16 §:n mukaan ”Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina”.

Käyttöoikeudet on määriteltävä ennalta kullekin tietojärjestelmän käyttäjälle käyttäjän tyypillisten työtehtävien mukaisesti. Käyttöoikeudet on pidettävä ajantasaisena, jotta tarpeellinen tietoihin pääsy voidaan varmistaa ja toisaalta estää vanhentuneiden käyttöoikeuksien perusteella tiedonsaanti laajemmin kuin käyttäjän tehtävät edellyttävät.

Käyttöoikeuksien hallinnan vastuut tulee määritellä osana tiedonhallintamallia siten, että tiedetään, kenen vastuulle käyttöoikeuksien määrittely ja ylläpito kuuluvat. Tietojärjestelmästä vastuussa oleva viranomainen ei välttämättä ylläpidä käyttöoikeuksia, vaan tietojärjestelmää käyttävä viranomainen voi olla vastuussa käyttöoikeuksien ajan tasalla pitämisestä. Esimerkiksi palvelukeskus voi määritellä käyttöoikeudet tietojärjestelmän vastuuviranomaisena, mutta tietojärjestelmää käyttävät viranomaiset huolehtivat käyttöoikeuksien ajantasaisuudesta.

Käyttöoikeuksien oikeellisuuden ja ajantasaisuuden varmistamiseksi organisaatio voi:

- määritellä prosessin, jonka mukaisesti käyttöoikeudet eri tietojärjestelmiin hyväksytään ja ylläpidetään,
- määritellä kunkin tietojärjestelmän käyttöoikeuksien hallinnan vastuut,
- uudelleenarvioida ja päivittää käyttöoikeudet työntekijöiden tehtävämuutosten yhteydessä,
- sisällyttää käyttöoikeuksien poistamisen työsuhteiden ja palvelusopimusten päättymisprosesseihin,
- varmistaa käyttöoikeuksien ajantasaisuuden määräajoin tehtävillä tarkastuksilla,
- välttää yhteiskäyttötunnuksien käyttöä ilman pakottavaa perusteltua syytä,
- käyttää kertakirjautumista mahdollisimman laajasti,
- ottaa käyttöön monivaiheisen tunnistautumisen erityisesti kirjauduttaessa palveluihin suojatun ympäristön ulkopuolelta sekä
- huomioida käyttöoikeuksissa tietojen luokittelun ja sopimusten asettamat vaatimukset.

Lisätietoja käyttöoikeuksien hallintaan löytyy Julkrin HAL-osion kriteeristä Käyttö- ja käsittelyoikeudet sekä TEK-osion kriteereistä Hallintayhteydet, Pääsyoikeuksien hallinnointi sekä Tietojenkäsittely-ympäristön toimijoiden tunnistaminen.

4.6 Lokitietojen kerääminen

Viranomaisen tulee kerätä tarpeelliset lokitiedot tietojärjestelmän käytöstä ja tietojen luovutuksista erityisesti, jos tietojärjestelmässä käsitellään salassa pidettäviä tietoja tai henkilötietoja.

Tiedonhallintalain 17 §:n mukaan ”Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista”.

Lokitietojen keräämisen tarkoituksena ja perusteena on toteuttaa viranomaisten tietojärjestelmien tietoturvallisuutta siten, että lokitietojen perusteella voidaan selvittää virhetilanteita ja valvoa tietojärjestelmien käyttöä muun muassa oikeusturvan toteuttamiseksi ja virkavastuun todentamiseksi.

Jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, tulee luovuttavassa järjestelmässä kerätä luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen peruste.

Käyttölokitietoja kerätään tietojärjestelmien käytöstä, jolla tarkoitetaan tietojen tallentamista, muuttamista, poistamista, katselua tai muuta tietoihin kohdistuvaa toimenpidettä. Käyttölokitiedot tulee kerätä esimerkiksi tietojärjestelmistä, joissa käsitellään salassa pidettäviä tietoja ja henkilötietoja. Muissa tapauksissa käyttölokitietojen tarpeellisuus tulee arvioida sillä perusteella, onko niillä merkitystä virheiden selvittelyn, yksilön oikeusturvan, virkavastuun todentamisen tai henkilötietojen suojaamisen näkökulmista.

Viranomaisen tulee määritellä lokitietojen säilytysajat tarpeellisuuden perusteella. Yleisesti lokitietojen säilytysaika on vähintään viisi vuotta viranomaistoiminnassa rikosoikeudellisten vanhentumisaikojen vuoksi, mutta erityislainsäädännön perusteella voi olla pidempiäkin säilytysaikoja.

Lokitiedot ovat salassa pidettäviä, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna tietojärjestelmien tietoturvajärjestelyjä. Lokitiedot ovat myös pääosin henkilötietoja, joiden käsittelyssä tulee huomioida tietosuoja-asetuksen vaatimukset.

Lokitietojen keräämisen lainmukaisuuden ja tehokkuuden varmistamiseksi suositellaan:

- määrittelemään tarpeelliset lokitiedot tietojärjestelmittäin,
- määrittelemään sekä koko organisaation lokitietojen hallinta että kunkin yksittäisen tietojärjestelmän lokitietojen vastuut,
- suunnittelemaan ja ohjeistamaan lokitietojen keruu ja käsittely sekä niissä noudatettavat tietoturvamenettelyt,
- ottamaan käyttöön keskitetty lokienhallintajärjestelmä, jos organisaatiossa kerätään paljon lokitietoja,
- suunnittelemaan ja toteuttamaan lokitietoihin perustuva tietojen luovutusten ja käytön seurannan sekä
- ottamaan käyttöön määrämuotoinen lokitietojen poistamisprosessi.

Lisätietoja lokitietojen keruusta ja käytöstä löytyy Julkrin TEK-osion kriteeristä Turvallisuuteen liittyvien tapahtumien jäljitettävyys sekä HAL-osion kriteeristä Seuranta ja valvonta. Lisäksi lokien käytöstä lisäohjeita saatavilla Traficom ohjeessa ”Näin keräät ja käytät lokitietoja”[11].

4.7 Asiakirjajulkisuuden suunnittelu

Viranomaisten tulee suunnitella tietojärjestelmänsä siten, että viranomaisten tehtävien hoitamisen ja toiminnan julkisuuden toteutumisen kannalta tarpeelliset

[11] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

tiedot ovat saatavilla. Samalla tulee varmistaa, että salassa pidettävien tietojen luottamuksellisuus ei vaarannu.

Tiedonhallintalain 13 §:n 3 momentin mukaan ”Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa”.

Vaatimuksen tavoitteena on tietojen saatavuuden varmistaminen viranomaisten tehtävien hoitamiseksi ja viranomaisen toiminnan julkisuuden toteuttamiseksi siten, että salassa pidettävien tietojen salassapito ei vaarannu. Vaatimus kohdistuu tietojärjestelmien, tietovarantojen tietorakenteiden ja niihin liittyvän tietojen käsittelyn suunnitteluun.

Tietojärjestelmät ja niissä käsiteltävät tiedot tulee suunnitella siten, että tietojärjestelmien hakutoiminnot mahdollistavat asiakirjajulkisuuden toteuttamisen ja tietojen saamisen viranomaisen tehtävien hoitamiseksi.

Asiakirjojen julkisuuden mahdollistamiseksi viranomaiset voivat toteuttaa seuraavia toimenpiteitä:

- selvittää eri tietovarantoihin kohdistuvat tiedonsaantivaatimukset sekä viranomaisen toiminnan julkisuuden että eri viranomaisten tehtävien hoitamisen osalta,
- tunnistaa tietovarantoihin sisältyvät julkiset ja salassa pidettävät tiedot,
- suunnitella miten tietovarannon tietoihin kohdistuvat erilaiset saatavuustarpeet voidaan täyttää vaarantamatta salassapitoa,
- suunnitella tietojärjestelmien hakutoiminnot ottaen huomioon salassapitovaatimukset,
- varmistaa tietojen saatavuus myös hankittaessa valmisjärjestelmiä sekä
- dokumentoida tietojärjestelmät ja tietovarannot siten, että tiedonhallintalain 28 §:ssä edellytetty kuvaus asiakirjajulkisuuden toteuttamiseksi voidaan laatia.

Tiedonhallintalautakunta on antanut erillisen suosituksen asiakirjajulkisuuskuvaksen laatimisesta.[12]

[12] Suositus asiakirjajulkisuuskuvauksen laatimisesta (VM 2020:22)

4.8 Tietoturvallisuus automaattisessa ratkaisumenettelyssä

Viranomaisen on dokumentoitava automaattisen ratkaisumenettelyn käsittelysäännöt, varmistettava automaattisen ratkaisumenettelyn laatu sekä huolehdittava automaattisessa ratkaisemisessa hyödynnettävien tietojen ajantasaisuudesta ja virheettömyydestä.

Tiedonhallintalain 28 c §:n 1 momentin mukaan ”Viranomaisen on valvottava automaattisesti ratkaistavien asioiden laatua ja sisällöllistä virheettömyyttä sekä hallittava automaattiseen ratkaisumenettelyyn liittyviä riskejä käyttöönoton jälkeen”. Tiedonhallintalain 28 f §:n mukaan ”Viranomaisen on riskiarvioinnin perusteella varmistettava, että automaattisessa ratkaisemisessa hyödynnettävien tietojen ajantasaisuus ja virheettömyys varmistetaan asianmukaisin teknisin toimenpitein”. Lisäksi tiedonhallintalain 6 a luvussa on säädetty muista automaattisen ratkaisumenettelyn käyttöönottoon ja käyttöön liittyvistä vaatimuksista.

Laki edellyttää tietoturvallisuuden näkökulmasta tarkasteltuna erityisesti tehtäväjaon ja käsittelysääntöjen dokumentointia, automaattisesti ratkaistavien asioiden laadun ja virheettömyyden valvontaa, muodollisia käyttöönottopäätöksiä ennen automaattisen ratkaisumenettelyn käyttöönottoa ja muutoksia sekä riskiarvioinnin perusteella tehtävää automaattisessa ratkaisemisessa hyödynnettävien tietojen ajantasaisuuden ja virheettömyyden varmistamista. Lisäksi ratkaisemisessa käytetyt käsittelysäännöt tulee säilyttää vähintään viiden vuoden ajan asian ratkaisemisesta.

Automaattisen ratkaisumenettelyn tietoturvallisuuden varmistamiseksi suositellaan seuraavia toimenpiteitä:

- suunnittelemaan ja dokumentoimaan automaattiseen ratkaisumenettelyyn liittyvät tietoturvallisuusvastuut,
- tunnistamaan automaattiseen ratkaisumenettelyyn liittyvät riskit sekä varmistamaan ratkaisujen virheettömyys ja havaittujen virheiden korjaaminen,
- määrittelemään miten, kenen toimesta ja kuinka säännöllisesti automaattisen ratkaisumenettelyn virheettömyyttä seurataan,

- määrittelemään, millä toimenpiteillä automaattisessa ratkaisemisessa hyödynnettävien tietojen ajantasaisuus ja virheettömyys varmistetaan sekä
- suojaamaan automatisoidussa toimintaprosessissa käytetyt käsittelysäännöt oikeudettomalta muuttamiselta ajantasaisen ja suunnitelmallisen käyttöoikeuksien hallinnan avulla.

Automaattisen ratkaisumenettelyn käyttöönottoon ja käyttöön liittyvistä yksityiskohtaisista vaatimuksista tietoa tiedonhallintalautakunnan suosituksessa automaattisesta ratkaisumenettelystä.[13]

[13] Linkki APT:n suositukseen

Sanasto

Termi	Määritelmä	Lähde
ajantasaisuus	tietoaineiston ominaisuus, joka ilmentää sitä, missä määrin aineiston tiedot vastaavat nykyhetken todellisuutta	Geoinformatiikan sanasto http://uri.suomi.fi/terminology/geoinfsan/c321
alkuperäisyys; aitous	ominaisuus, joka ilmentää tiedon eheyttä ja sitä, että tiedon alkuperäinen lähde on se, joka sen väitetään olevan	Tiivis tietoturvasanasto (TSK 31, 2004)
eheys; muuttumattomuus	tiedon ominaisuus, joka ilmentää sitä, että tietoa ei ole muutettu luvatta, ettei se ole tahattomasti muuttunut ja että mahdolliset muutokset voidaan todentaa ja jäljittää	Tietotermit (2018)
hallinnollinen alue	viranomaisen normaaliin työskentelyyn tarkoitettu alue tai tila, jonka osalta aluetta tai tilaa hallitseva toimija varmistaa, että siihen on itsenäinen pääsy ainoastaan viranomaisen ennalta valtuuttamilla henkilöillä Hallinnollinen alue tai tila voi olla esimerkiksi toimistotila, useista eri toimistotiloista muodostuva kokonaisuus, palvelintila, konesali tai jonkin yrityksen tai muun yhteisön tila.	TLA 9 § 1 kohta

	Turvallisuusluokitusasetuksessa hallinnollinen alue on turvallisuusluokiteltujen asiakirjojen suojaamiseksi määritelty alue, jolla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa.	
jäännösriski	riskin käsittelyn jälkeen jäljellä oleva riski	Digi- ja väestötietovirasto.Sanastot.suomi.fi: Tunnus: jäännösriski. VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön. Yhteentoimivuusalusta (suomi.fi) http://uri.suomi.fi/terminology/digiriski/concept-3
käsittely	asiakirjan vastaanottamista, laatimista, tallentamista, katselua, muuttamista, luovuttamista, kopiointia, siirtoa, välittämistä, tuhoamista, säilyttämistä ja arkistointia sekä muita asiakirjaan kohdistuvia toimenpiteitä	TLA 2 §
käyttökelpoisuus	tiedon ominaisuus, joka ilmentää tiedon laatua sekä sitä, että tieto on käsiteltävissä yleisesti käytössä olevalla tietojärjestelmällä	HE 284/2018
luokittelu	tietojen ja tietojärjestelmien ryhmittely luokkiin niiden luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvien vaatimusten perusteella	Suositus tietoturvallisuuden vähimmäisvaatimuksista (VM 2024: XX)
luottamuksellisuus	tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä eikä se paljastu muille	Tietotermit (2018)

muuttumattomuus	kts. eheys	
riskiperusteisuus	riskien suuruuden ja niiden hyväksyttävyyden arviointia sekä riskien suuruuden suhteuttamista riskien pienentämisen kustannusiin osana tietoturvallisuuteen liittyvää päätöksentekoa	Suositus tietoturvallisuudesta hankinnoissa (VM 2023:57)
saatavuus	tiedon ominaisuus, joka ilmentää sitä, miten tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla	Tietotermit (2018)
saavutettavuus	periaatteet ja tekniikat, joita on noudatettava digitaalisten palvelujen suunnittelussa, kehittämisessä, ylläpidossa ja päivittämisessä, jotta ne olisivat paremmin käyttäjien, erityisesti vammaisten henkilöiden, saavutettavissa	Laki digitaalisten palvelujen tarjoamisesta 2 §
tietoaineisto	asiakirjoista ja muista vastaavista tiedoista muodostuva, tiettyyn viranomaisen tehtävään tai palveluun liittyvä tietokokonaisuus	TihL 2 §
tietojärjestelmä	tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuva kokonaisjärjestely Tietojärjestelmiä ovat esimerkiksi erilaiset pilvipalvelut ja ohjelmistojen käsittelyyn käytettävät päätelaitteet.	TihL 2 §
tietoturvallisuustoimenpiteet	tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistaminen hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä	TihL 2 §

tietoturva; tietoturvallisuus	järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus	Kyberturvallisuuden sanasto (TSK 52, 2018)
toimintaympäristö	fyysinen tai digitaalinen ympäristö, jossa organisaation tai henkilön toiminta tapahtuu	Sisäisen turvallisuuden sanasto (Sisäministeriö, 29.6.2023)
turva-alue	alue, joilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle	TLA 9 § 2 kohta
turvallisuusalue	käsite, joka sisältää hallinnolliset alueet ja turva-alueet	TLA 9 §
turvallisuusluokiteltu asiakirja	asiakirja, johon valtionhallinnon viranomaisen toimesta on tehty turvallisuusluokkaa koskeva merkintä Asiakirja on turvallisuusluokiteltava, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten	TihL 18 § JulkL 24 §

	torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.	
varautuminen	toiminta, jolla varmistetaan tehtävien mahdollisimman an häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa	Kokonaisturvallisuuden sanasto (TSK 50, 2017)

Liite 1: Kooste tiedonhallintalain tietoturvallisuusvaatimuksista

Tiedonhallintayksikön tulee täyttää tietoturvallisuutta koskevat vähimmäisvaatimukset.

Julkisessa hallinnossa noudatettavat tietoturvallisuuden vähimmäisvaatimukset on koottu alla olevaan luetteloon. Vaatimukset perustuvat pääosin tiedonhallintalain tietoturvallisuutta koskevaan lukuun 4 sekä soveltuvin osin tiedonhallinnan järjestämistä, tietoaineistojen muodostamista ja automaattista ratkaisumenettelyä koskeviin lukuihin.

1. Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on. TihL 4 § 2 mom

    a. määritelty tietoturvallisuuden vastuut,
    b. ajantasaiset tietoturvallisuutta koskevat,
    c. tarjolla koulutusta tietoturvallisuudesta;
    d. tietoturvalliset työvälineet;
    e. riittävä tietoturvallisuuden valvonta.

2. Tiedonhallintayksikössä ylläpidettävän tiedonhallintamallin on sisällettävä tiedot tietoturvallisuustoimenpiteistä sekä arvioitava näihin kohdistuvat muutokset olennaisten muutosten yhteydessä. TihL 5 §

3. Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. TihL 12 §

4. Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. TihL 13 § 1 mom

5. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. TihL 13 § 1 mom

6. Viranomaisen on varmistettava tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys riittävällä testauksella säännöllisesti. TihL 13 § 2 mom

7. Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa. TihL 13 § 3 mom

8. Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. TihL 13 § 4 mom

9. Viranomaisen on viipymättä tiedotettava sen tietoaineistoja hyödyntäville, jos sen tiedonhallintaan kohdistuu häiriö, joka estää tai uhkaa estää viranomaisen tietoaineistojen saatavuuden. TihL 13 a § 1 mom

10. Tiedonhallintayksikön on selvitettävä tietojen käsittelyyn kohdistuvat olennaiset riskit sekä riskiarvioinnin perusteella huolehdittava, että tietoaineistojen käsittely, tietojärjestelmien hyödyntäminen ja toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä poikkeusoloissa. TihL 13 a § 3 mom

11. Viranomaisen on toteutettava salassa pidettävien tietojen siirto yleisessä tietoverkossa salattuna tai muuten suojattuna sekä varmistettava vastaanottaja riittävän tietoturvallisella tavalla. TihL 14 § 1 mom

12. Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein tietoaineistojen: TihL 15 § 1 mom

    a. muuttumattomuus;
    b. suojaus teknisiltä ja fyysisiltä vahingoilta;
    c. alkuperäisyys, ajantasaisuus ja virheettömyys;
    d. saatavuus ja käyttökelpoisuus;
    e. saatavuuden rajoittaminen vain, jos laissa on erikseen rajoitettu;

f. arkistoitavuus.

13. Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia. TihL 15 § 2 mom

14. Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja pidettävä ne ajantasaisina. TihL 16 §

15. Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. TihL 17 §

16. Valtionhallinnon viranomaisen on tarvittaessa turvallisuusluokiteltava asiakirjat. TihL 18 § (JulkL 24 §)

17. Viranomaisen on varmistettava teknisesti tietojen tapauskohtainen tarpeellisuus luovuttaessaan henkilötietoja tai salassa pidettäviä tietoja teknisten rajapintojen avulla viranomaisten välillä. TihL 22 § 2 mom

18. Luovuttaessaan tietoja muulle kuin toiselle viranomaiselle, on viranomaisen lisäksi varmistettava, että vastaanottaja noudattaa tietojen käsittelyssä tiedonhallintalain vaatimuksia sekä vastaanottajan laissa säädetty tiedonsaantioikeus. TihL 24 §

19. Viranomaisen on rajattava katselumahdollisuus yksittäisiin hakuihin, selvitettävä tietojen käyttötarkoitus, tunnistettava automaattisesti poikkeava tietojen hakeminen sekä noudatettava muita tietoturvallisuuden vähimmäisvaatimuksia avatessaan katseluyhteyden tietovarantoon muille viranomaisille. TihL 23 §

20. Tiheästi päivittyvän julkisen tiedon on pyynnöstä oltava saatavilla teknisten rajapintojen avulla heti tiedon keräämisen jälkeen ja tarvittaessa useana kerralla ladattavana tiedostona. Jos tämän noudattaminen aiheuttaa kohtuutonta vaivaa, tiedon on oltava saatavilla sellaisin tilapäisin rajoituksin, jotka eivät tarpeettomasti haittaa sen hyödyntämistä. TihL 24 a §

21. Arvokkaiden tietoaineistojen, joihin tiedon saajalla on erikseen laissa säädetty tiedonsaantioikeus, on pyynnöstä oltava saatavilla teknisten rajapintojen avulla. Tiedon on tarvittaessa oltava saatavilla myös useana kerralla ladattavana tiedostona. TihL 24 b § 2 mom

22. Viranomaisen on dokumentoitava automaattisen ratkaisumenettelyn käsittelysäännöt, varmistettava automaattisen ratkaisumenettelyn laatu sekä huolehdittava automaattisessa ratkaisemisessa hyödynnettävien tietojen ajantasaisuudesta ja virheettömyydestä. 28 a-g §

Lähteet

Säädökset

Arkistolaki (831/1994). https://www.finlex.fi/fi/laki/ajantasa/1994/19940831.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI.

Laki digitaalisten palvelujen tarjoamisesta (306/2019). Laki digitaalisten palvelujen tarjoamisesta 306/2019 - Ajantasainen lainsäädäntö - FINLEX ®

Laki julkisen hallinnon tiedonhallinnasta (906/2019). Laki julkisen hallinnon tiedonhallinnasta 906/2019 - Ajantasainen lainsäädäntö - FINLEX ®

Laki viranomaisen toiminnan julkisuudesta (621/1999). https://finlex.fi/fi/laki/ajantasa/1999/19990621.

Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi (HE 284/2018 vp). https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_284+2018.pdf

Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi (HE 145/2022 vp). https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_145+2022.pdf

Hallintovaliokunnan mietintö koskien hallituksen esitystä eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi. (HaVM 38/2018 vp). HaVM 38/2018 vp (eduskunta.fi)

Hallintovaliokunnan mietintö koskien hallituksen koskien hallituksen esitystä eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi (HaVM 39/2022 vp). HaVM 39/2022 vp (eduskunta.fi)

Laki sähköisen viestinnän palveluista (917/2014). Laki sähköisen viestinnän palveluista 917/2014 - Ajantasainen lainsäädäntö - FINLEX ®

Laki yksityisyyden suojasta työelämässä (759/2004). Laki yksityisyyden suojasta työelämässä 759/2004 - Ajantasainen lainsäädäntö - FINLEX ®

Tietosuojalaki (1050/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181050?search%5Btype%5D=pika&search%5Bpika%5D=tietosuojalaki.

Turvallisuusselvityslaki (726/2014). Turvallisuusselvityslaki 726/2014 - Ajantasainen lainsäädäntö - FINLEX ®

Valtion virkamieslaki (750/1994). Valtion virkamieslaki 750/1994 - Ajantasainen lainsäädäntö - FINLEX ®

Valmiuslaki (1552/2011). Valmiuslaki 1552/2011 - Ajantasainen lainsäädäntö - FINLEX ®

Tiedonhallintalautakunnan suositukset

Tiedonhallintalautakunta 2020. Suositus asiakirjajulkisuuskuvauksen laatimisesta. Valtiovarainministeriön julkaisuja 2020:22. http://urn.fi/URN:ISBN:978-952-367-304-5

Tiedonhallintalautakunta 2023. Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö. Valtiovarainministeriön julkaisuja 2023:46. http://urn.fi/URN:ISBN:978-952-367-458-5

Tiedonhallintalautakunta 2020. Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa. Valtiovarainministeriön julkaisuja 2020:18. http://urn.fi/URN:ISBN:978-952-367-288-8

Tiedonhallintalautakunta 2020. Suositus tiedonhallinnan muutosvaikutusten arvioinnista. Valtiovarainministeriön julkaisuja 2020:53. http://urn.fi/URN:ISBN:978-952-367-318-2

Tiedonhallintalautakunta 2020. Suositus tiedonhallintamallista. Valtiovarainministeriön julkaisuja 2020:29. http://urn.fi/URN:ISBN:978-952-367-328-1

Tiedonhallintalautakunta 2022. Suositus tietoaineistojen säilytysajasta ja toimenpiteistä säilytysajan päätyttyä. Valtiovarainministeriön julkaisuja 2022:54. http://urn.fi/URN:ISBN:978-952-367-220-8

Tiedonhallintalautakunta 2023. Suositus tietoturvallisuudesta hankinnoissa. Valtiovarainministeriön julkaisuja 2023:57. http://urn.fi/URN:ISBN:978-952-367-645-9

Tiedonhallintalautakunta 2023. Suositus salassa pidettävien asiakirjojen käsittelystä. Valtiovarainministeriön julkaisuja 2023:4. http://urn.fi/URN:ISBN:978-952-367-241-3

Tiedonhallintalautakunta 2021. Suositus teknisistä rajapinnoista ja katseluyhteyksistä. Valtiovarainministeriön julkaisuja 2021:21. http://urn.fi/URN:ISBN:978-952-367-489-9

Tiedonhallintalautakunta 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Valtiovarainministeriön julkaisuja 2021:5. http://urn.fi/URN:ISBN:978-952-367-500-1

Tiedonhallintalautakunta 2022. Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa. Valtiovarainministeriön julkaisuja 2022:4. http://urn.fi/URN:ISBN:978-952-367-906-1

Ohjeet ja muut materiaalit

Valtiovarainministeriö 2023. Riskienhallinnan käsikirja valtionhallinnon toimijoille (2023:54). http://urn.fi/URN:ISBN:978-952-367-633-6. Viitattu 11.9.2023.

Digi- ja väestötietovirasto (2022). Kriittisten kohteiden luokittelu. (11.3.2022). Haku: vuosi 2022 Oppaat ja hyvät käytännöt Kriittisten kohteiden luokittelun menetelmäkuvaus. Digiturvajulkaisut | Digi- ja väestötietovirasto (dvv.fi). Viitattu 11.9.2023.

Kansallisarkisto. Arkistoinnin ohjaus. Verkkosivusto. Arkistoinnin ohjaus | Kansallisarkisto Viitattu 12.9.2023.

Liikenne- ja viestintävirasto. Traficom. Näin keräät ja käytät lokitietoja. Verkkosivusto. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja?toggle=Lokeja%20eri%20tarkoituksiin. Viitattu 14.9.2023.