Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Suositus teknisistä rajapinnoista ja katseluyhteyksistä (22§ ja 23§)	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä
Viranomaisten on toteutettava säännöllisesti toistuva ja vakiosisältöinen sähköinen tietojen luovuttaminen tietojärjestelmien välillä teknisten rajapintojen avulla, jos vastaanottavalla viranomaisella on tietoihin laissa säädetty tiedonsaantioikeus. Säännöllisesti toistuva ja vakiosisältöinen tietojen sähköinen luovuttaminen voidaan toteuttaa muulla tavalla, jos teknisen rajapinnan toteuttaminen tai käyttö ei ole teknisesti tai taloudellisesti tarkoituksenmukaista. Viranomainen voi avata teknisen rajapinnan tiedonsaantiin oikeutetulle viranomaiselle myös muissa tilanteissa. Asiakirjojen ja tietojen antamisesta muulla tavalla säädetään erikseen.

Sen lisäksi, mitä 4 luvussa 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.

Teknisen rajapinnan avulla luovutettavien tietojen tietorakenteen kuvauksen määrittelee ja sitä ylläpitää tiedot luovuttava viranomainen. Suunniteltaessa usean viranomaisen välistä tietojen luovuttamista teknisten rajapintojen avulla, on tietorakenteen kuvaus määriteltävä ja ylläpidettävä toimialasta vastaavan ministeriön johdolla.

23 § Katseluyhteyden avaaminen viranomaiselle
Viranomainen voi avata katseluyhteyden toiselle viranomaiselle tietovarannon sellaisiin tietoihin, joihin katseluoikeuden saavalla viranomaisella on tiedonsaantioikeus. Sen lisäksi, mitä 4 luvussa säädetään, edellytyksenä katseluyhteyden avaamiselle on, että:

1) katselumahdollisuus on rajattu vain tiedonsaantioikeuden mukaisiin 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.

Hallituksen esitys HE 284/2018
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Johdanto
Tiedonhallintalain 22-24 §:ssä on säädetty yleiset vaatimukset teknisten rajapintojen ja katseluyhteyksien käyttämisestä. Tämän suosituksen tarkoituksena on esittää suositukset siitä, miten tiedonhallintalaissa säädetyt vaatimukset teknisten rajapintojen ja katseluyhteyksien käytöstä voidaan toteuttaa. Tämä ohje ei ole velvoittava, vaan siinä esitetään ratkaisuja, joilla voidaan toteuttaa tekniset rajapinnat ja katseluyhteydet tiedonhallintalain edellyttämällä tavalla. Teknisiä rajapintoja ja katseluyhteyksiä koskeva sääntely korvaa teknisten käyttöyhteyksien käyttöön liittyvän sääntelyn. Tiedonhallintalain 22-24 §:n säännöksiä sovelletaan, kun erityislainsäädännöstä on kumottu teknisiä käyttöyhteyksiä koskevat säännökset. Tiedonhallintalain teknisten rajapintojen ja katseluyhteyksien käyttöä koskevaa sääntelyä sovelletaan vain, jos muualla ei ole näihin tiedon sähköisiin luovutustapoihin liittyen säädetty toisin.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Suositus teknisistä rajapinnoista ja katseluyhteyksistä (22§ ja 23§)	versio 0.9/01.11.2019

Vakiosisältöisten tietojen sähköinen luovuttaminen

Teknisen rajapinnan käyttöä koskevia säännöksiä sovelletaan tilanteissa, joissa tiedonvaihto tapahtuu automaattisesti kahden tietojärjestelmän välillä. Teknisiä rajapintoja koskevia säännöksiä ei sovelleta, jos tietoja tallennetaan tietojärjestelmään esimerkiksi käyttäjän täyttäessä jotain sähköistä lomaketta tai digitaalista palvelua käyttämällä, jolloin tietojen tallentaminen tai siirtäminen tapahtuu sähköistä tiedonsiirtomenetelmää käyttämällä. Teknisen rajapinnan toiminta perustuu tietojärjestelmän tekemään tekniseen tietopyyntöön toiselle tietojärjestelmälle tietyn tietokokonaisuuden luovuttamiseksi.

Tiedonhallintalain 22.1 §:n mukaan viranomaisten on toteutettava säännöllisesti toistuva ja vakiosisältöinen sähköinen tietojen luovuttaminen tietojärjestelmien välillä teknisten rajapintojen avulla, jos vastaanottavalla viranomaisella on tietoihin laissa säädetty tiedonsaantioikeus. Säännös on viranomaisia velvoittava. Kun viranomaisten välillä tapahtuu säännöllisesti toistuva tietojen luovuttamista sähköisessä muodossa, on tällainen tietojen luovuttaminen toteutettava tietojärjestelmien välillä sähköisten rajapintojen avulla. Säännöllisesti toistuvaa tietojen luovuttamista voi tapahtua päivittäin tai viikoittain. Tiedonhallintalaissa ei ole säädetty mitä säännöllisesti toistuvalla tietojen luovuttamisella tarkoitetaan, joten säännöllisesti toistuva tietojen luovuttaminen voi tapahtua myös kerran vuodessakin tietojärjestelmien välillä.

Lisäksi, jotta säännös on velvoittava, on tietojen luovuttamisen oltava vakiosisältöistä. Teknisiä rajapintoja hyödyntämällä tietojen luovuttamista ei voida toteuttaa, jos tietojen luovuttamiseen liittyy luovuttavalle viranomaiselle harkintamahdollisuus, mitkä ovat välttämättömiä tietoja viranomaisen tiedonsaantioikeuden ja tiedon käyttötarpeen näkökulmasta. Silloin, kun tiedot saavan viranomaisen tiedonsaantioikeus rajautuu vain välttämättömiin tietoihin, on erikseen selvitettävä, liittyykö tietojen antamiseen tapauskohtaista harkintaa, jolloin luovutettava tietosisältökään ei ole vakiomuotoista. Siten mitä tahansa tietoa ei voida luovuttaa tietojärjestelmien välillä teknisten rajapintojen avulla automaattisesti.

Teknisten rajapintojen rakenteet määrittelee luovuttava viranomainen, jolla on myös toimivalta päättää tietojen luovuttamisesta. Tiedot luovuttava viranomainen määrittelee siten käytännössä ne tilanteet, joissa rajapinta voidaan avata toiselle viranomaiselle ottaen huomioon, mitä laissa on säädetty tietojen luovuttamismahdollisuudesta ja velvollisuudesta tietojen luovuttamiseen teknisten rajapintojen avulla.

Teknisten rajapintojen käyttöön ja tiedon luovuttamiseen liittyviä poikkeuksia

Tiedonhallintalaissa säädetty velvollisuus teknisten rajapintojen käyttöön sisältää joitakin poikkeuksia. Säännöllisesti toistuva ja vakiosisältöinen tietojen luovuttaminen voidaan toteuttaa ilman teknisten rajapintojen käyttöä, jos teknisen rajapinnan toteuttaminen tai käyttö ei ole teknisesti tai taloudellisesti tarkoituksenmukaista. Poikkeus voi tulla kysymykseen tilanteissa, joissa käytettävät tietojärjestelmät ovat elinkaarensa loppuvaiheessa, jolloin teknisistä tai taloudellisista syistä rajapintojen toteuttamisen vanhaan tietojärjestelmään ei ole tarkoituksenmukaista. Viranomaisen on kuitenkin arvioitava näissä tilanteissa perusteet sille, miksi tietojen luovuttamista ei voida toteuttaa tiedonhallintalaissa säädetyn velvoitteen mukaisesti. Arviointi on sisällytettävä osaksi tiedonhallintalain 5 §:ssä säädettyä tiedonhallinnan muutosvaikutusarviointia, jos teknistä rajapintaa ei toteuteta tiedonhallintaan liittyvän muutoksen tai uuden tietojärjestelmän käyttöönoton yhteydessä.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Suositus teknisistä rajapinnoista ja katseluyhteyksistä (22§ ja 23§)	versio 0.9/01.11.2019

Tietoja voidaan luovuttaa viranomaisten tietojärjestelmien välillä sähköisesti myös tilanteissa, joissa tietojen luovuttaminen ei ole säännöllistä, jos luovutettavat tiedot ovat vakiosisältöisiä. Kuitenkin tällöin tietojen luovuttamiseen voi olla käytössä taloudellisesti ja teknisesti tarkoituksenmukaisempia keinoja yksittäisten tietoluovutusten toteuttamiseen. Tällöin tietojen luovuttaminen voi olla tehokasta käyttämällä jotain digitaalista palvelua, turvasähköpostia tai muuta sähköistä tiedonsiirtomenetelmää.

Tietojen luovuttamisesta päättää se viranomainen, jonka asiakirjoihin tai tietoihin tekninen rajapinta avataan. Siten tietojärjestelmän teknisestä ylläpidosta vastaava toimija, kuten palvelukeskus, ei päätä teknisen rajapinnan avaamisesta. Päätettäessä avata tekninen rajapinta toiselle viranomaiselle, ei tiedot luovuttava viranomainen voi asettaa sellaisia ehtoja tietojen luovuttamiselle, joista on säädetty tiedonhallintalaissa tai muussa laissa tai ehdot eivät voi olla ristiriidassa laissa säädetyn kanssa. Tiedot luovuttava viranomainen voi asettaa ehtoja tietoluovutuksille siltä osin kuin ne tarkentavat tiedonhallintalain 4 luvussa olevia tietoturvallisuusvaatimuksia. Teknisen rajapinnan avaamista koskevasta päätöksestä on ilmettävä mihin käyttötarkoitukseen tietoja luovutetaan ja minkä laissa säädetyn tiedonsaantioikeuden perusteella tietojen luovuttaminen tapahtuu.

Kortti 22 § Suositus teknisistä rajapinnoista viranomaisten välillä
Kortti 23 § Katseluyhteyden avaaminen viranomaiselle
Kortti 22 § ja 23 § yhteydessä sovellettavat luvun 4 tietoturvavaatimukset

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen toteuttaminen	
Kortti 22 § Suositus teknisistä rajapinnoista viranomaisten välillä	versio 0.9/01.11.2019

	22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä 1 mom , tiedonsaantioikeuden mukaisen pääsyn toteuttamisesta Viranomaisten on toteutettava säännöllisesti toistuva ja vakiosisältöinen sähköinen tietojen luovuttaminen tietojärjestelmien välillä teknisten rajapintojen avulla, jos vastaanottavalla viranomaisella on tietoihin laissa säädetty tiedonsaantioikeus.
	Lain perustelu https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut
	Tietoja luovuttavan viranomaisen tulee selvittää vastaanottavan viranomaisen tiedonsaantioikeudet, vakiosisältöisesti luovutettavat tiedot sekä säännöllisen tietojen luovuttamisen frekvenssi. Selvityksen perusteella tietoja luovuttava viranomainen määrittelee vastaanottajakohtaisesti rajapinnan tietorakenteet, mikäli eri viranomaisten tiedonsaanti poikkeaa toisistaan. Käyttöoikeudet määritellään tiedot pyytävään järjestelmään. Käyttöoikeusmäärittely luovuttavaan tietojärjestelmään tarkoittaa lähinnä tiedot saavan tietojärjestelmän käyttöoikeuden määrittelyä, joka tapahtunee ainakin osittain rajapintakuvauksen perusteella tehdyn toteutuksen kautta. Tietoja luovuttava viranomainen määrittelee tiedonsaantioikeuksiin perustuvien rajapinnan tietorakennekuvausten perusteella vastaanottavan viranomaisen tiedonsaantioikeuksiin perustuvat käyttöoikeudet ja myöntää ne tietoja vastaanottavaan tietojärjestelmään. Käyttöoikeuksien myöntämisessä tulee noudattaa lain 16 §:ssä kuvattuja vaatimuksia.
	Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset Kortti 13 § 2 Riskienhallinta Kortti 16 § Käyttöoikeuksien hallinta

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen toteuttaminen	
Kortti 22 § Suositus teknisistä rajapinnoista viranomaisten välillä	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä 2 mom, tekniset kontrollit tapauskohtaisen tarpeen ja välttämättömyyden varmistamiseksi

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.

Julkisuuslaki

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Salassa pidettävien tietojen tai henkilötietojen luovuttamisen tarpeen tai välttämättömyyden tapauskohtainen varmistaminen voidaan toteuttaa esimerkiksi siten, että haettaessa toisen tietojärjestelmän sisältämiä tietoja rajapinnan avulla reaaliaikaisesti, kontrolloi tiedot pyytävä tietojärjestelmä käyttäjän toimintaa. Kontrolleina on suositeltavaa käyttää seuraavia:

- Tiedot pyytävä tietojärjestelmä informoi käyttäjää siitä, mihin tarkoitukseen tietoja voidaan käyttää ja
- pyytämällä käyttäjän yksilöimään ennalta määritellyistä käyttötarkoituksista sen, johon tietoja pyydetään luovuttamaan, jos tietoja voidaan käyttää useisiin käyttötarkoituksiin. Prosessiohjatuissa tietojärjestelmissä käyttötarpeen selvittäminen ei ole tarpeen, koska rajapinta on avattu toiseen tietojärjestelmään vain tiettyä yksittäistä käyttötarkoitusta varten, jolloin käyttötarkoitus ilmoitetaan osana käyttäjälle annettavaa informointia.
- Tietojen saantia koskeva peruste sisällytetään osaksi sekä tiedot luovuttavan että tiedot vastaanottavan tietojärjestelmän luovutuslokitietoja.

Jos tietojen luovuttaminen tapahtuu automaattisesti viranomaisten tietojärjestelmien välillä säännöllisin väliajoin, kuten eräajopohjaisissa tai muissa tiedostopohjaisissa tietoluovutuksissa, lain vaatimukset voidaan täyttää esimerkiksi rekisteröimällä luovutuslokiin tiedot siitä, mitä tietoja on luovutettu ja mihin käyttötarkoitukseen tiedot on luovutettu. Näissä tilanteissa luovutuksen teknisessä toteutuksessa on kiinnitettävä huomiota siihen, että luovutettavat tiedot ovat tapauskohtaisesti tarpeellisia tai välttämättömiä, jolloin erityisesti on teknisin kontrollein varmistettava, että luovutuksen saavalla viranomaisella on edelleen jatkuva tarve saada toiselta viranomaiselta asiakasta tai muuta asianosaista koskevia tietoja.

Tästä syystä teknisiä rajapintoja käytettäessä ei riitä, että tiedot toimitetaan automaattisesti luovuttavasta tietojärjestelmästä säännöllisin väliajoin. Tiedot saavan viranomaisen tietojärjestelmän on tehtävä jokaisen tietojenluovutuksen osalta tekninen tietopyyntö luovuttavalle tietojärjestelmälle, jos asiankäsittelyt perustuvat siihen, että asiakassuhde ja tiedonsaantitarve ovat määräaikaisia. Tapauskohtainen arviointi voi tapahtua myös siten, että tiedot luovuttava tietojärjestelmä tunnistaa asiakkaiden tiedoissa olevat muutokset ja välittää ne edelleen automaattisesti tiedot vastaanottaviin järjestelmiin.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen toteuttaminen	
Kortti 22 § Suositus teknisistä rajapinnoista viranomaisten välillä	versio 0.9/01.11.2019

	22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä 3 mom, teknisen rajapinnan tiedonsiirtoyhteyden toteuttaminen muiden viranomaisten kanssa yhteentoimivalla tavalla Teknisen rajapinnan avulla luovutettavien tietojen tietorakenteen kuvauksen määrittelee ja sitä ylläpitää tiedot luovuttava viranomainen.
	Lain perustelu https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut
	Yhteentoimivuuteen liittyvät vaatimukset teknisten rajanpintojen osalta edellyttävät yhteentoimivuuden huomioimista ja varmistamista niin teknisen toteutuksen (rajapinta ja tiedonsiirtoyhteys), kuin semanttisen toteutuksen (sanastot ja koodistot) sekä tietomallinnuksen (metatiedot ja rakenteisuus) osalta. Yhteentoimivuuden edistämiseksi suositellaan käytettäväksi Digi- ja väestötietoviraston (DVV) ylläpitämää Yhteentoimivuusalustaa. Siinä on työkalut terminologisten sanastojen, koodistojen ja tietomallien laatimiseen ja julkaisuun. Kun tietovarannoista ja tietovirroista liikkuvista tiedoista tuotetaan tietomalleja Yhteentoimivuusalustalle, niin näiden kuvauksissa voidaan hyödyntää aiemmin toteutettuja käsitteiden, koodistojen ja tietomallien kuvauksia. Tämä tekee järjestelmäkehityksestä kustannustehokasta ja parantaa yhteentoimivuutta muiden toimijoiden järjestelmien kanssa.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Katseluyhteyksien toteuttaminen	
Kortti 23 § Katseluyhteyden avaaminen viranomaiselle	versio 0.9/01.11.2019

	23 § Katseluyhteyden avaaminen viranomaiselle 1 mom, tiedonsaantioikeuden mukaisen pääsyn toteuttaminen Viranomainen voi avata katseluyhteyden toiselle viranomaiselle tietovarannon sellaisiin tietoihin, joihin katseluoikeuden saavalla viranomaisella on tiedonsaantioikeus.
	Lain perustelu https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut
	Tietoja luovuttavan viranomaisen tulee käydä läpi vastaanottavan viranomaisen kanssa tiedonsaantioikeudet. Tiedonsaantioikeuksien perusteella määritellä katseluyhteyden näkymä, joka perustuu kunkin viranomaisen tiedonsaantioikeuksiin ja voi siten olla erilainen kunkin viranomaisen osalta. Käyttöoikeudet myönnetään vastaanottavalle viranomaiselle tiedonsaantioikeuksien ja –tarpeen perusteella. Viranomainen, jolle käyttöoikeudet myönnetään, vastaa siitä, ettei käyttöoikeuksia ja niihin liittyviä tunnuksia luovuteta oikeudettomille henkilöille ja että käyttöoikeuksia käytetään vain siihen tarkoitukseen, johon ne on myönnetty. Lisäksi viranomaisen tulee ilmoittaa käyttäjien virkoihin liittyvistä muutoksista käyttöoikeudet myöntäneelle viranomaiselle siltä osin, kuin ne vaikuttavat käyttöoikeuksien hallintaan, kuten oikeuksien muuttamiseen, jäädyttämiseen tai poistamiseen. Käyttöoikeudet myöntäneen viranomaisen vastuulla on varmistaa käyttöoikeuksien ajantasaisuus ja käyttöoikeuksien mukaisen pääsyn toteutuminen. Käyttöoikeuksien myöntämisessä tulee noudattaa lain 16 §:ssä kuvattuja vaatimuksia.
	Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset Kortti 16 § Käyttöoikeuksien hallinta

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Katseluyhteyksien toteuttaminen	
Kortti 23 § Katseluyhteyden avaaminen viranomaiselle	versio 0.9/01.11.2019

23 § Katseluyhteyden avaaminen viranomaiselle 1 mom kohta 1, 1) katselumahdollisuus on rajattu vain tiedonsaantioikeuden mukaisiin tarpeellisiin tai välttämättömiin tietoihin
Lain perustelu https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut
Katseluyhteyttä tarjoavan viranomaisen tulee toteuttaa järjestelmä niin, että se tukee katselumahdollisuuden rajaamista vain tiedonsaantioikeuden määrittämiin tarpeellisiin tai välttämättömiin tietoihin. Katseluyhteyttä tarjoava viranomainen voi toteuttaa tämän arvioimalla ja dokumentoimalla katselumahdollisuuden saavan viranomaisen tehtävien hoitamisen kannalta tarpeelliset tai välttämättömät tiedot. Katseluyhteyttä tarjoava viranomainen voi toteuttaa järjestelmän teknisesti siten, että katselumahdollisuus rajataan tietotarpeen/ välttämättömien tietojen perusteella viranomais- tai käyttäjäkohtaisesti.
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset Kortti 16 § Käyttöoikeuksien hallinta

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Katseluyhteyksien toteuttaminen	
Kortti 23 § Katseluyhteyden avaaminen viranomaiselle	versio 0.9/01.11.2019

23 § Katseluyhteyden avaaminen viranomaiselle 1 mom kohta 2, 2) tietojen hakemisen yhteydessä selvitetään tietojen käyttötarkoitus.
Lain perustelu https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut
Katseluyhteyttä tarjoavan viranomaisen tulee toteuttaa katseluyhteys siten, että tietoja voidaan hakea ainoastaan yksittäisinä hakuina. Tällöin hakukriteerien on oltava sellaisia, että niiden perusteella ei voida hakea suurta määrää useita henkilöitä koskevia tietoja, vaan haku rajautuu pääsääntöisesti yhden tai muutamaan kriteerit täyttävän henkilön tietotoihin. Vaatimus voidaan saavuttaa toteuttamalla katseluyhteys teknisesti siten, että sen kautta voidaan tehdä kerrallaan vain yksittäisiä hakuja. Vaatimusta voidaan myös edesauttaa toteuttamalla katseluyhteys tietoteknisesti esimerkiksi siten, että tietoja haettaessa käyttäjä syöttää tai valitsee valikosta tai muusta vastaavasta tietojen hakemisen perusteen. Peruste käyttäjätietoineen jää katseluyhteyden avulla kerättäviin luovutuslokitietoihin, jolloin jälkikäteen voidaan todentaa kunkin katseluyhteyden avulla tehdyn haun käyttötarkoitus ja lainmukainen oikeusperuste käsittelylle. Tämä menettely pakottaa käyttäjän arvioimaan kullakin hakukerralla ennen haun tekemistä, onko haku virka- tai työtehtävien hoitamisen kannalta tarpeen. Tällä pyritään estämään osaltaan myös se, ettei hakuja voida tehdä automaattisesti esimerkiksi hakurobotin avulla.
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset Kortti 13 § Riskienhallinta Kortti 17 § Lokitietojen kerääminen

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Katseluyhteyksien toteuttaminen	
Kortti 23 § Katseluyhteyden avaaminen viranomaiselle	versio 0.9/01.11.2019

23 § Katseluyhteyden avaaminen viranomaiselle 2 mom

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

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Katseluyhteyttä tarjoavan viranomaisen tulee toteuttaa katseluyhteys tietovarantoon niin, että katseluyhteyden mahdollistava tietojärjestelmä tunnistaa automaattisesti poikkeavat tietohaut, pyrkii estämään niiden jatkumisen ja hälyttää määritellyn prosessin mukaisesti oikeille tahoille. Valittavan ratkaisun tulee täyttää lain asettamat vaatimukset ja se tulee suunnitella riskiperusteisesti vaatimusmäärittelyn kautta niin, että hallintakeinojen asettamisesta aiheutuvat kustannukset ovat perusteltuja suhteessa riskiin.

Poikkeavilla tietohauilla tarkoitetaan esimerkiksi seuraavaa:

1. Käyttäjä hakee selvästi sellaisia tietoja, joihin hänellä ei oletetusti ole oikeutta tai hän tekee lyhyen ajan sisään poikkeavan paljon hakuja. Riskiä voidaan hallita laatimalla erilaisia hälyttimiä poikkeavan käytön tunnistamiseen. Esimerkiksi hälytin tekee varoituksen tilanteissa, joissa haut kohdistuvat selvästi käyttäjän tehtävien ulkopuolelle hakujen tietosisällön tai maantieteellisen sijainnin osalta, tai haut tapahtuvat tavallisesta poikkeavaan ajankohtaan.
2. Jotain yksittäistä tietoa tai jonkin yksittäisen henkilön tietoja haetaan tavallista enemmän.
3. Käyttäjä syöttää hakukenttään tavanomaisesta poikkeavia hakusanoja tai erikoismerkkejä, tai käyttäjän toiminta viittaa selvästi tavallisesta poikkeavaan toimintaan, jonka tarkoituksena on murtaa järjestelmän suojaukset. Tätä riskiä voidaan hallinta suorittamalla järjestelmälle asianmukainen tietoturvatestaus ennen käyttöönottoa, jossa huomioidaan esimerkiksi SQL-injection –tyyppisiltä hyökkäyksiltä suojautumisen tarpeet. Lisäksi sellaisten hakusanojen tai -merkkien syöttäminen, joita ei oletetusti tarvitse käyttää, tulee estää.

Mikäli jokin asetetuista hälyttimistä hälyttää, niin järjestelmä voi esimerkiksi ilmoittaa tästä käyttäjälle, sulkea käyttäjän käyttöoikeudet ja päättää käyttäjän katseluyhteyden sekä kertoa mihin voi olla yhteydessä käyttäjätunnusten aktivoimiseksi uudelleen. Lisäksi hälytystapahtuman tulee toimia käynnistimenä tätä varten suunnitellulle tietoturvapoikkeamien selvitysprosessille.

Poikkeavien tietohakujen automaattinen tunnistus voidaan toteuttaa usealla tavalla ja teknologialla. Toteuttamiseen löytyy niin avoimeen lähdekoodiin perustuvia kuin kaupallisia ratkaisuja. Yksinkertaisimmillaan toteutuksessa voidaan käyttää järjestelmää, jonka toiminnallisuudet mahdollistavat poikkeavan toiminnan havaitsemisen ja siitä hälyttämisen esimerkiksi lokien analysoinnin ja asetettujen sääntöjen perusteella. Sääntöpohjaiset järjestelmät eivät kuitenkaan tunnista kaikkea poikkeavaa toimintaa, vaan ainoastaan sääntöihin määritellyn poikkeavan toiminnan. Ne edellyttävät täten myös sääntöjen toimivuuden jatkuvaa arviointia ja kehittämistä. Poikkeavan toiminnan tunnistamista voidaan edelleen parantaa hyödyntämällä mm. koneoppimista ja muuta edistynyttä analytiikkaa sääntöjä täydentävänä osana toimintamallia.

Tietoturvapoikkeamatilanteiden hallinta, VM julkaisuja 8/2017
http://julkaisut.valtioneuvosto.fi/handle/10024/79258

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Katseluyhteyksien toteuttaminen	
Kortti 23 § Katseluyhteyden avaaminen viranomaiselle	versio 0.9/01.11.2019

Vahti 3/2012 Teknisen ympäristön tietoturvataso-ohje, soveltuvin osin
https://www.vahtiohje.fi/web/guest/3/2012-teknisen-ympariston-tietoturvataso-ohje

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom

Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään.

23 § Katseluyhteyden avaaminen viranomaiselle, mom 1

Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään.

12 § Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen

Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Turvallisuusselvitysten tekemisestä säädetään turvallisuusselvityslaissa (726/2014) ja muusta henkilöarvioinnista yksityisyyden suojasta työelämässä annetussa laissa (759/2004).

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Turvallisuusselvityslaki (726/2014)

Laki yksityisyyden suojasta työelämässä (759/2004)

Huomioitava eri ammattialoja koskeva erityislainsäädäntö

Viranomaisen on arvioitava, tuleeko teknisen rajapinnan ja katseluyhteyden kautta tietoja vastaanottavalta viranomaiselta edellyttää erityistä luotettavuutta ja sen varmistamista. Luotettavuus voidaan varmistaa edellyttämällä turvallisuusselvitysten tekemistä. Viranomainen voi harkita turvallisuusselvitysten teettämisen edellyttämistä tietoja vastaanottavista viranomaisista mikäli:

- tietoja vastaanottavilta viranomaisen tietojärjestelmän käyttäjiltä edellytetään erityistä luotettavuutta,
- turvallisuusselvityksen tekemiselle on turvallisuusselvityslain mukaan peruste ja
- se on viranomaisen harkinnan mukaan tarpeellista.

Esimerkiksi turvallisuusluokiteltavien tietojen osalta turvallisuusselvitysten teettäminen on yksi keino tietojen luottamuksellisuuteen kohdistuvien riskien hallitsemiseksi.

https://www.supo.fi/turvallisuusselvitykset

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom

Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään.

23 § Katseluyhteyden avaaminen viranomaiselle, mom 1

Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään.

13 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus 2 mom, riskienhallinta

Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Viranomaisen tulee arvioida teknisten rajapintojen ja katseluyhteyksien toteuttamiseen liittyvät riskit sekä suunnitella toimenpiteet riskien hallitsemiseksi siten, että sähköiset tiedonsiirtomenetelmät voidaan toteuttaa ja niitä voidaan käyttää turvallisella tavalla. Riskien arvioinnissa ja hallitsemisessa tulee huomioida tiedonhallintalain 4 luvussa määritellyt tietoturvallisuuden vähimmäisvaatimukset. Perusrekistereitä ylläpitävien, terveystietoja välittävien sekä muiden teknisten rajapintojen kautta tavallista enemmän tietoa luovuttavien viranomaisten on hyvä laatia kattava riskienarviointi. Riskiarviointia suositellaan tehtäväksi yhteistyössä tietoja luovuttavien ja vastaanottavien toimijoiden kanssa, sekä toisaalta yhdessä muiden samoja tai samankaltaisia tehtäviä hoitavien viranomaisten kanssa. Näin mahdollistetaan riskien ja hyvien käytänteiden jakaminen toimijoiden kesken.

Teknisten rajapintojen ja katseluyhteyksien toteuttamiseen ja käyttämiseen liittyvässä riskienarvioinnissa tunnistetaan olennaiset riskit, jotka voivat vaikuttaa kyseisten rajapintojen ja katseluyhteyksien käytettävyyteen ja saatavuuteen tai niissä käsiteltävien tietoaineistojen tietoturvallisuuteen. Riskejä voivat aiheuttaa esimerkiksi puutteet liittyen hyökkäysmenetelmiltä suojautumiseen, avaintenhallintaan, lähetettävän tiedon laatuun, tiedonsiirron automaatioon tai muut tiedonsiirtomenetelmien turvallisuusongelmat.

Lisäksi riskejä voi aiheuttaa vastaanottavan viranomaisen osaamattomuus liittyen sähköisten tiedonsiirtomenetelmien tai lähdejärjestelmän käyttämiseen, vastaanotettavien tietojen käsittelyyn tai puutteet tietojenkäsittely-ympäristössä.

Näitä riskejä voidaan pyrkiä hallitsemaan varmistamalla tietoja vastaanottavien viranomaisten tai järjestelmien käyttäjien tietoturvaosaaminen liittyen kyseisen järjestelmän erityispiirteisiin sekä käsiteltäviin tietoihin. Tällä tarkoitetaan sitä, että tietoja luovuttavan viranomaisen tulee ohjeistaa ja tarvittaessa varmistaa osaaminen esimerkiksi kouluttamalla:

- Miten sähköistä tiedonsiirtomenetelmää ja tietojärjestelmää tulee käyttää, jotta käyttäjä kykenee välttämään riskialttiita ja tietoturvallisuutta vaarantavia käyttötapoja?
- Miten järjestelmän sisältämiä tietoja tulee käsitellä, jotta niiden luottamuksellisuus, eheys ja saatavuus eivät vaarannu?
- Käyttöperusteiden dokumentointi, esimerkiksi dokumentoitu tieto siitä, millä tavoin palveluun liittyvät tietopyynnöt käsitellään, kenelle ne tulee ohjata ja kuinka pitkän ajan tietoja on mahdollista pyytää ilman erillisiä kustannuksia.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

Ohjeistuksen ja koulutuksen lisäksi käyttäjien huolimattomuudesta tai kiireestä aiheutuvia riskejä voidaan hallita muistuttamalla käyttäjiä näistä aina kirjautumisen yhteydessä. Esimerkiksi niin, että kirjautumisen yhdessä muistutetaan, mihin tietoja saa käyttää, millä tavoin ne on luokiteltu ja mitä käsittelysääntöjä tulee noudattaa.

Vastaanottavan viranomaisen tietojenkäsittely-ympäristöön liittyviä riskejä voidaan esimerkiksi pyrkiä hallitsemaan edellyttämällä tarvittavia teknisiä toimenpiteitä, selvityksiä tai kolmannen osapuolen suorittamia tietoturva-auditointeja, joilla varmistetaan tietojen käsittelyltä edellytettävät tietoturvallisuusvaatimukset.

Tiedon minimointi
Tietoja luovuttava viranomaisen tulee huolehtia tietojen minimoimisesta ennen niiden luovuttamista. Tällä tarkoitetaan sitä, että viranomainen luovuttaa vain niitä tietoja, joita vastaanottava viranomainen perustellusti tarvitsee tehtävänsä hoitamiseen. Tietoja luovuttavan viranomaisen tulee varmistaa, ettei luovutettavien tietojen mukana luovuteta sellaista tietoa, jota vastaanottava viranomainen ei ole pyytänyt, jota se ei tarvitse, tai johon sillä ei ole tiedonsaantioikeutta. Tämä riski saattaa korostua etenkin luovutettavissa tietoaineistossa olevien metatietojen osalta, jotka tietoja luovuttavan viranomaisen tulisi kartoittaa ja varmistaa, ettei metatietoihin ole tallennettu sellaisia tietoja, joita ei ole syytä luovuttaa. Tietojen minimointiin kuuluu myös tarpeettomien yksilöllisten identifioivien tunnisteiden poistaminen luovutettavista tiedoista silloin, kun niiden toimittaminen ei ole erikseen perusteltua.

Jo suunnitteluvaiheessa on otettava huomioon mahdolliset tietojen luovuttamisen käytännöt. Järjestelmän siirroissa voi kulkea salaamattomana (tai ylipäätään) tietoa, jota ei ole lupa luovuttaa joko lain perusteella tai tietosuojasäädösten vuoksi. Esimerkkinä on henkilötunnus, jota on aikaisemmin käytetty paljonkin tunnisteena järjestelmissä. Kuitenkin on turha siirtää tunnistetietoja datan mukana, vaikka henkilötunnusta käytettäisiinkin haussa. Tällöin siirrettävä data on vain se data, mitä haettiin. Samoin loppuasiakkaalle mahdollisen tulosteen ottamisessa on tarkistettava, ettei turhaan tositteelle tai viranomaisen asiakirjalle tallennu asiakkaan tai pyydetyn tiedon tietosuojan alaisia tietoja tai muita erityissuojattavia tietoja.

Tekoäly ja koneoppiminen
Tekoälyn ja koneoppimisen hyödyntämiseen tietojen käsittelyssä liittyy riskejä, kuten se, että tekoäly oppiikin vahingossa tai tarkoituksellisen vihamielisen toiminnan seurauksena väärin tai sen ratkaisut eivät ole eettisesti kestävällä pohjalla. Ennen tekoälyn ja koneoppimisen käyttöönottoa tulee suunnitella ja määritellä tarkkaan, mitä niillä halutaan saavuttaa ja millä tavoin niiden halutaan toimivan.

Kortti 13 § Elinkaaren huomioiminen tietojen käsittelyssä

Kortti 13 § Elinkaaren huomioiminen tietojärjestelmissä

Kortti 13 § Riskienhallinta

Kortti 13 § Tietoturvallisuus hankinnoissa

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom

Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään.

23 § Katseluyhteyden avaaminen viranomaiselle, mom 1

Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään.

13 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus 2 mom, Vikasietoisuus ja toiminnallinen käytettävyys

Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti.

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Viranomaisen tulee laatia arvio ja varmistaa onko lähdejärjestelmä oleellinen sitä käyttävien tahojen toiminnan luonteen näkökulmasta. Lisäksi viranomaisen tulee varmistaa järjestelmään tehtävien teknisten rajapintojen ja katseluyhteyksien vikasietoisuus ja toiminnallinen käytettävyys riittävällä testauksella säännöllisesti. Oleellisella järjestelmällä tarkoitetaan järjestelmää, josta sitä käyttävien viranomaisten toiminta on riippuvaa. Vikasietoisuus tulee mitoittaa sen perusteella, kuinka kriittinen järjestelmä on toiminnan kannalta ja kuinka pitkään toimintaa voidaan jatkaa, vaikka järjestelmä ei olisi käytettävissä.

Arvioinnissa tulee myös huomioida järjestelmien käytettävyysvaatimusten muuttuminen eri ajankohtina. Esimerkiksi järjestelmä saattaa olla kriittinen vain kuun vaihteessa tai tiettyyn aikaan vuodesta. Kriittisyyttä arvioitaessa on lisäksi huomioitava lakisääteiset tehtävät sekä riippuvuus muista järjestelmistä (oman organisaation sisällä sekä viranomaisten kesken).

Vikasietoisuus ja toiminnallinen käytettävyys tulee määritellä ennen teknisten rajapintojen ja katseluyhteyksien toteuttamista. Tekniset rajapinnat ja katseluyhteydet tulee toteuttaa määriteltyjen vaatimusten mukaisesti noudattaen turvallisen sovelluskehityksen hyvä käytänteitä ja ohjeita. Teknisten rajapintojen ja katseluyhteyksien vikasietoisuus ja toiminnallinen käytettävyys tulee varmistaa säännöllisellä testauksella. Testaus tehdään vaatimusmäärittelyn mukaisesti ja testauksen säännöllisyys mitoitetaan niin, että sillä voidaan varmistaa kriittisyyden perusteella edellytettävä vikasietoisuus ja toiminnallinen käytettävyys.

Sähköisten palveluiden toiminnallista käytettävyyttä toteutettaessa pitää huomioida myös EU:n saavutettavuusdirektiivi ((EU) 2016/2102) ja sitä seuraava kansallinen lainsäädäntö (Laki digitaalisten palveluiden tarjoamisesta 306/2019). Saavutettavuusdirektiivin soveltamisalaan kuuluvat julkisen hallinnon ja julkista hallintotehtävää hoitavien organisaatioiden verkkosivustot ja mobiilisovellukset sekä lähes kaikki näiden sisällöt.

Katseluyhteyksien toteuttamisen osalta suositellaan noudatettavaksi Sähköisen asioinnin tietoturvallisuus -ohjetta (Valtiovarainministeriön julkaisuja 25/2017)
http://julkaisut.valtioneuvosto.fi/handle/10024/80012

Teknisten rajapintojen ja katseluyhteyksien sovelluskehityksessä ja tietoturvallisuuden testaamisessa suositellaan noudatettavaksi Väestörekisterikeskuksen julkaisemaa turvallisen sovelluskehityksen käsikirjaa.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

https://vrk.fi/documents/2252790/13063677/Tukimateriaali_VRK_turvallisen+sovelluskehityksen_k%C3%A4sikirja.docx

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom

Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään.

23 § Katseluyhteyden avaaminen viranomaiselle, mom 1

Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään.

14 § Tietojen siirtäminen tietoverkoissa 1 mom, tietojen siirron turvallisuus

Viranomaisen on toteutettava tietojensiirto tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä.

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Viranomaisen on toteutettava teknisten rajapintojen ja katseluyhteyksien kautta tapahtuva tietojensiirto tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Tietojen siirtämisessä tietoverkossa on otettava huomioon tiedon eheys, luottamuksellisuus ja saatavuus. Tämän saavuttamiseksi on otettava huomioon niin tekniset kuin hallinnolliset ratkaisut. Siirrettäessä salassa pidettävää tietoa julkisen verkon kautta, tietoaineisto tai tietoliikenneyhteys suojataan riittävän turvallisella salauksella kuten turvapostilla tai käyttämällä TLS-salausta asiointipalvelun ja loppukäyttäjän välisen liikenteen suojaamiseen. Julkisia verkkoja ovat esimerkiksi Internet ja operaattorien tarjoamat MPLS-verkot.

Käytännön toteutustapoja turvalliselle salaukselle ovat esimerkiksi:

- käyttäjien päätelaitteiden ja viranomaisen tietojärjestelmien väliset VPN-ratkaisut,
- asiointipalvelun ja loppukäyttäjän välisen liikenteen TLS-salaus,
- organisaatioiden verkkojen välinen IPSec-salaus, sekä
- loppukäyttäjille tarjottavat turvaposti- ja tiedostosalausratkaisut.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom

Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään.

23 § Katseluyhteyden avaaminen viranomaiselle, mom 1

Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään.

14 § Tietojen siirtäminen tietoverkoissa 2 mom, vastaanottajan varmistaminen ja tunnistaminen

Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Laki digitaalisten palvelujen tarjoamisesta 306/2019

Tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. Käyttäjien tunnistamisessa voidaan käyttää henkilökohtaisia käyttäjätunnuksia ja salasanoja. Siirrettäessä salassa pidettäviä tietoaineistoja, käyttäjät tunnistetaan ja todennetaan käyttäen tunnettua ja turvallisena pidettyä tekniikkaa. Tällaisia tekniikoita ovat esimerkiksi kertakirjautuminen ja monivaiheinen tunnistautuminen. Tunnistamistapa ja -vahvuus on arvioitava tapauskohtaisesti kunkin palvelun sekä siinä käsiteltävien tietojen ja niiden paljastumiseen liittyvien riskien perusteella.

Digipalvelulaki 6.2 § sekä Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016) 3 § 4) luonnollisen henkilön tunnistuspalvelu, joka tunnistaa julkisen hallinnon sähköisiä palveluja käyttävän luonnollisen henkilön vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa (533/2016) tarkoitetun tunnistuspalvelun tarjoajan palvelua käyttäen, hallinnoi tunnistustapahtumaa sekä luovuttaa väestötietojärjestelmästä henkilön yksilöintiä koskevat tiedot käyttäjäorganisaatiolle.

Digipalvelulain kortti 6 § 1-2 mom. Käyttäjän sähköinen tunnistaminen

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom

Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään.

23 § Katseluyhteyden avaaminen viranomaiselle, mom 1

Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään.

15 § Tietoaineistojen turvallisuuden varmistaminen, 1 mom, 1 kohta, Muuttumattomuus

Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen:
1) tietoaineistojen muuttumattomuus on riittävästi varmistettu;

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Muuttumattomuuden varmistamisella tarkoitetaan sitä, ettei tietoaineistoa voi muuttaa oikeudetta, tahattomasti tai hallitsemattomasti missään tiedon elinkaaren vaiheessa ilman, että muutos voidaan havaita. Tietoaineiston muuttumattomuuden varmistaminen riippuu tietoaineiston luonteesta ja tarpeelliset tietoturvallisuustoimenpiteet määritellään tapauskohtaisesti.

Muuttumattomuutta uhkaava riski voi realisoitua esimerkiksi tiedon siirron tai säilytyksen aikana. Tähän liittyvää riskiä voidaan hallita esimerkiksi valvomalla tiedon muuttumattomuutta hyödyntäen tiivistefunktioita, tarkistussummia ja lohkoketjua. Lohkoketju muodostuu dataa sisältävistä lohkoista, joista jokaisella on oma yksilöllinen tiivistefunktio. Edellisen lohkon tiiviste on aina tallennettu aina lohkoon. Näin lohkoista muodostuu ketju. Yhden lohkon muuttaminen katkaisee ketjun ja näin ollen tiedon eheyden menettäminen tulee esiin. Lohkoketjuja on toistaiseksi hyödynnetty lähinnä varmistamaan virtuaalivaluutan siirtojen eheyttä, mutta käytännössä sitä voidaan aukottomasti soveltaa minkä vaan siirrettävän tiedon eheyden ja muuttumattomuuden varmistamiseen. Muuttumattomuuden varmistamiseen on myös teknisiä ratkaisuja, joiden kautta voidaan asettaa hälytyksiä ilmoittamaan esimerkiksi tarkistussummien rikkoontumisesta.

Tarpeellisia hallintatoimia muuttumattomuuden varmistamiseksi voivat olla esimerkiksi: Hallintaoikeuksien rajaaminen, kirjoitusoikeuksien rajaaminen käyttövaltuuksien avulla, tapahtumien lokittaminen ja lokitietojen muokattavuuden sekä poistamisen estäminen, lokiarkistojen pääsyoikeuksien rajaaminen ja varmuuskopiointi sekä muut tietoturvaa edistävät tekniset toimenpiteitä. Teknisillä toimenpiteillä tarkoitetaan esimerkiksi palomuureja, salausmenetelmien käyttöä ja järjestelmien kovennuksia. Teknisillä tietoturvallisuustoimenpiteillä ehkäistään tietojen tahallista ja tahatonta muuttamista. Lisäksi teknisten toimenpiteiden avulla ehkäistään ulkopuolisten pääsyä tietoon sekä estetään heidän mahdollisuutensa muokata tietoa luvattomasti.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

	22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään. **23 § Katseluyhteyden avaaminen viranomaiselle, mom 1** Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään. **15 § Tietoaineistojen turvallisuuden varmistaminen mom 2, teknisiltä ja fyysisiltä vahingoilta suojaaminen** Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen: 2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta
	Lain perustelu https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut
	Lähdejärjestelmä sekä teknisten rajapintojen ja katseluyhteyksien kautta siirrettävät tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta. Tämä voidaan toteuttaa esimerkiksi estämällä luvaton fyysinen pääsy tietoaineistoja käsitteleviin laitteisiin esimerkiksi kulunhallinnan avulla. Lisäksi tiloissa, joissa siirrettäviä tietoaineistoja käsitellään, tulee huolehtia riittävistä paloturvallisuuteen liittyvistä kontrolleista sekä viemäröinnistä.
	Kortti 15 § Vahingoilta suojaaminen

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom

Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään.

23 § Katseluyhteyden avaaminen viranomaiselle, mom 1

Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään.

15 § Tietoaineistojen turvallisuuden varmistaminen § 1 mom 3 kohta alkuperäisyyden, ajantasaisuuden ja virheettömyyden varmistaminen

Viranomaisen on varmistettava tarpeellisin teknisin, toiminnallisin ja hallinnollisin toimenpitein sille muodostuvien tietoaineistojen käsittely ja säilyttäminen siten, että
3) tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu.

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Tiedon todistusvoimaisuuden ollessa keskeistä, tiedon käsittelyvaiheet on suunniteltava, toteutettava ja käsittelytoimenpiteitä valvottava siten, ettei tieto pääse muuttumaan tahallisesti tai tahattomasti tiedon käsittelyn elinkaaren aikana. Näin varmistetaan käsittelyhetken käsittelytarpeisiin riittävä tiedon eheys, virheettömyys, muuttumattomuus ja kiistämättömyys.

Tiedon käsittelyä suunniteltaessa, määriteltäessä ja muutettaessa on tarpeen tunnistaa tiedon käsittelyn elinkaaren eri vaiheet ja näissä käsittelytoimet tai tapahtumat, joihin voidaan suunnitella riittävät kontrollit tiedon kiistämättömyyden ja eheyden varmistamiseksi sekä tahattomien ja tahallisten virheiden havaitsemiseksi.

Esimerkkejä suunniteltavista ja seurattavista kontrolleista: Tiedon syöttämisen muoto- ja sisältötarkastukset, tiedon eheyden tarkistaminen siirron ja säilytyksen aikana esimerkiksi tarkistussummien avulla, käyttäjien vahva tunnistaminen, käyttöoikeuksien rajaaminen vain tarpeelliseen sekä käsittelytoimenpiteiden riittävä kirjaaminen lokiin. Edellä mainittuihin voidaan käyttää erilaisia teknisiä ratkaisuja kuten suunnitelmien perusteella toteutettavia tarkistustoimenpiteitä- tai -palveluja, raja-arvoja, aikaleimoja, määrityksien tai valintojen pakollisuuksia sekä tiivisteitä.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom

Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään.

23 § Katseluyhteyden avaaminen viranomaiselle, mom 1

Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään.

16 § Tietoaineistojen turvallisuuden varmistaminen 1 mom 4 kohta, tietoaineistojen saatavuuden ja käyttökelpoisuuden varmistaminen

Viranomaisen on varmistettava tarpeellisin teknisin, toiminnallisin ja hallinnollisin toimenpitein sille muodostuvien tietoaineistojen käsittely ja säilyttäminen siten, että
4) tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu.

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Tietojen ja tietoaineistojen saatavuuden tarve, käyttökelpoisuus sekä näihin liittyvät vaatimukset tulee arvioida toiminnallisesta näkökulmasta esimerkiksi keskeytysvaikutusanalyysin (BIA), tietoriskianalyysin tai yhtenäisen kriittisyys- ja tärkeysluokittelun avulla, jotta tietojen ja tietoaineistojen merkitys toiminnalle on tunnistettu ja arvioitu. Riittävät kontrollit saatavuuden turvaamiselle perustuvat aina tietojen ja tietoaineistojen kriittisyyteen näiden hyödyntäjille.

Kun tiedot ja tietoaineistot ja niitä käsittelevät toiminnot ja mahdolliset tietojärjestelmät luokitellaan kriittisiksi, esimerkiksi yhtenäisellä kriittisyys- ja tärkeysluokittelulla, on niiden saatavuuteen kiinnitettävä erityistä huomioita ja käsittelytoimien suunnittelussa on huomioitava myös erityis- ja poikkeustilanteet.

Esimerkkejä suunniteltavista ja seurattavista kontrolleista: Tietojärjestelmien ja tietoliikenneyhteyksien kahdennukset ja segmentoinnit, riittävän tai tarpeen mukaan säädettävän tiedonsiirtomäärän (”kaistanleveys”) varmistaminen, palvelunestohyökkäyksiin varautuminen, riittävät valvonta ja reagointivalmiudet poikkeamien havaitsemiseen ja torjuntaan sekä riskiperusteinen varautuminen, sekä valmistautuminen poikkeamien pikaiseen selvittämiseen joko omien tai ulkoisten resurssien tuella.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

22 § Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä, 2 mom

Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään.

23 § Katseluyhteyden avaaminen viranomaiselle, mom 1

Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään.

16 § Tietojärjestelmien käyttöoikeuksien hallinta

Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja ne on pidettävä ajantasaisina.

Lain perustelu
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut

Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet myös teknisten rajapintojen ja katseluyhteyksien osalta. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja ne on pidettävä ajantasaisina.

Asianmukaisen pääsynhallinnan ja käyttäjienhallinnan avulla mahdollistetaan tietojen luvallinen käyttö ja estetään niiden luvatonta käyttöä. Ainoastaan valtuutetuille käyttäjille sekä järjestelmille myönnetään pääsy- ja käyttöoikeudet ja niiden hallinnan tulee noudattaa vähimpien oikeuksien periaatetta. Vähimpien oikeuksien periaate tarkoittaa, että käyttäjälle annetaan tietojärjestelmiin vain sellaiset käyttöoikeudet ja -valtuudet, jotka ovat työn suorittamiseksi välttämättömiä. Käyttäjätilien hallintaa ja käyttöä seurataan ja valvotaan poikkeamien ja uhkien havaitsemiseksi sekä niihin reagoimiseksi. Lisäksi olemassa olevat käyttövaltuudet tulee arvioida säännöllisesti niiden tarpeellisuuden ja ajanmukaisuuden näkökulmasta. Käyttövaltuudet tulee näiden arviointien jälkeen päivittää vastaamaan nykytilan käyttövaltuustarpeita.

Lisäksi viranomaisen tulee laatia käyttöoikeuksiin sidottu hallinnollinen määräys teknisen käyttöyhteyden sallitusta käytöstä niin, että siinä kerrotaan yksiselitteisesti, mihin käyttötarkoitukseen järjestelmää saa käyttää ja mihin ei.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät **Käyttötarkoitus:** Sähköisten rajapintojen ja katseluyhteyksien toteuttaminen	
Kortti 22§ ja 23§ yhteydessä sovellettavat Tiedonhallintalain 4 luvun tietoturvavaatimuksien soveltamissuositukset	versio 0.9/01.11.2019

	22 § 2 mom Tietojen luovuttaminen teknisen rajapinnan avulla viranomaisten välillä Tietojen luovuttaminen teknisten rajapintojen avulla on toteutettava tietojärjestelmien välillä kuten 4 luvussa säädetään. **23 § mom 1 Katseluyhteyden avaaminen viranomaiselle** Edellytyksenä katseluyhteyden avaamiselle on noudattaa, mitä 4 luvussa säädetään. **17 § Lokitietojen kerääminen** Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.
	Lain perustelu https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx#PerusteluOsaYksityiskohtaisetPerustelut
	EU yleinen tietosuoja-asetus ja tietosuojalaki
	Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Tiedonhallintayksikön on määriteltävä lokien käyttötarkoitus ja tietosisältö, samoin se miten niitä kerätään, käsitellään ja säilytetään. Lokitietoihin pääsy tulee sallia oikeutetuille tahoille ja tällöinkin mahdollisuus muuttaa lokitietoja tulee estää.
	Kortti 17 § Lokitietojen kerääminen Vahti 3/2009, Lokiohje https://www.vahtiohje.fi/web/guest/3/2009-lokiohje