Laki julkisen hallinnon tiedonhallinnasta Suosituskortti	B
13 § 3 mom Tietorakenteet	versio 0.9/16.4.2021

13 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus
4 luvun 13 § 3 mom

Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa.

Perustelumuistio
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Tietojen erottelun periaate

Tietovarantojen tietorakenteet on suunniteltava niin, että tietovarannossa olevat asiakirjat ja muut tieto-objektit pystytään erottelemaan julkisiin, harkinnanvaraisesti julkisiin ja salassa pidettäviin luokkiin.

Erottelun toteuttaminen edellyttää, että:

1) **Tietovaranto sisältää tietomallin, joka määrittää asiakirjojen ja tieto-objektien julkisuusluokan niiden koko elinkaaren ajan.** Asiakirjojen ja tiedon julkisuuteen tai salassapitoon liittyy useita säädöksiä ja asetuksia, jotka voivat muuttua ajan kuluessa. Järjestelmän toteutusvaiheessa on syytä muodostaa tiedon kulkua kuvaava tietomalli, jonka avulla tiedon käsittelyyn liittyviä vaatimuksia voi hallita.
2) **Tietovarannon asiakirjoihin ja muihin tieto-objekteihin liittyy riittävästi metatietoa, joiden perusteella yksittäisten asiakirjojen ja tieto-objektien julkisuusluokka voidaan määritellä tietomalliin perustuen riittävän helposti.** Asiakirjojen julkisuusluokka pitää olla koodattuna määrämuotoisesti asiakirjan metatietoihin. Pelkästään asiakirjan sisällä oleva merkintä salassapidosta, tai tiedostonimeen liitetty suojaustasomerkintä eivät mahdollista tiedon tehokasta automaattista erottelua.
3) **Asiakirjojen ja tieto-objektien julkisuustieto on helposti saatavilla.** Tieto asiakirjan julkisuusluokasta pitää olla kuitenkin sellainen, että myös loppukäyttäjä pystyy helposti määrittämään tiedon luokittelun.
4) **Syntyvien asiakirjojen ja tieto-objektien oletusluokitus ei voi olla julkinen, ellei voida varmistua siitä, että niiden sisältämä tieto on julkista.** Tiedon luokittelua ei yleensä pystytä automatisoimaan kuin yksinkertaisissa, määrämuotoista tietoa sisältävissä tapauksissa. Yleensä luokittelun määrittely vaatii tiedon käsittelijän toimia.

Tietojärjestelmän vaatimukset

Jotta asiakirjojen julkisuus voidaan toteuttaa asianmukaisesti ja vaivatta, tulisi näitä käsittelevissä tietojärjestelmissä huomioida seuraavat vaatimukset

- Julkisuus- tai salassapito-olettaman tai ehdottoman salassapidon määrittäminen tietovarastolle tai asiakirjatyypille
- Salassapitoperusteen tai luovutuskiellon määrittäminen tietovarastolle ja/tai asiakirjalle
- Asiakirjan mahdollinen salassapito- tai turvallisuusluokitus
- Tiedot turvallisuusluokituksen tehneestä viranomaisesta
- Merkintä ja peruste sellaiselle tiedolle, joka ei muodosta viranomaisen asiakirjaa (luonnos, muistiinpano, sisäinen viestintä, tms.)

- Ajanhetki, jolloin ei-julkinen asiakirja muuttuu julkiseksi (esim. hankinta-asiakirjat)
- Tiedot henkilörekisteristä, johon asiakirjat mahdollisesti kuuluvat (jotta voidaan varmistaa vastaanottajan käsittelyoikeus tai poistaa henkilötiedot)
- Toiminnallisuus, jolla asiakirjasta voidaan maskata tai poistaa henkilötunnus ja valinnaisesti muut henkilön tunnistetiedot
- Toiminnallisuus, jolla asiakirjasta voidaan maskata tai jättää pois salassa pidettävät tiedot sen julkisen osuuden luovuttamista varten

Tietojen käyttö

Tietojen käytössä joudutaan yhdistämään asiakirjojen ja tieto-objektien julkisuusluokka tietojen käyttäjän oikeuksiin. Yhdistämisessä tärkeintä on se, että ei-julkista ja salassa pidettävää aineistoa ei anneta vahingossa taholle, jolla ei ole siihen oikeutta. Asiakirjojen ja käyttöoikeuksien yhdistäminen tulee pyrkiä tekemään mahdollisimman yksinkertaisesti ja ymmärrettävästi, jotta oikeuksien varmentaminen on mahdollista.

Erityistä huomiota tulee kiinnittää:

- Hakutoiminnallisuuteen; haku tai hakuindeksi ei saa vahingossa paljastaa ei-julkista tai salassa pidettävää tietoa esimerkiksi asiakirjan metatiedoista.
- Oikeuksien muutoksiin ja muutoshistoriaan; käyttäjien muuttuneet oikeudet eivät saa johtaa tilanteeseen, jossa käyttäjä käyttöoikeudet menetettyään pääsee käsiksi aineistoon, johon hänellä ei enää ole oikeutta.
- Järjestelmien välisiin liitoksiin ja rajapintoihin.

Tietojen luovuttaminen järjestelmän ulkopuolelle

Järjestelmän toiminnan pitäisi olla niin luotettavaa ja ymmärrettävää, että käyttäjän ei tarvitse pelätä tietojen luovutuksessa vahingossa luovuttavansa ei-julkista tai salassa pidettävää tietoa.

Tiedon luokittelua koskeva merkintä pitää tehdä viimeistään silloin kun tietoa luovutetaan viranomaisen ulkopuolelle. On kuitenkin huomattava, että mikäli järjestelmän toiminta perustuu siihen, että tiedot luokitellaan niiden luovutuksen yhteydessä, muodostaa tämä hidasteen tietojen luovutukselle. Lisäksi tietojen luokittelu vasta luovutuksen yhteydessä lisää riskiä tietojen väärälle tai epäjohdonmukaiselle luokittelulle.

Kun tietoja luovutetaan, pitää huolehtia siitä, että samassa yhteydessä ei vahingossa luovuteta mitään ylimääräistä tietoa. Tällaista tietoa voi olla esimerkiksi asiakirjoissa oleva meta- tai historiatieto (erityisesti Office-dokumentit). Jos asiakirjasta poistetaan tietoa, pitää poisto tehdä niin, että sitä ei voi perua meta- tai historiatietoja käyttäen.