CSC:n vastaus lausuntopyyntöön tiedonhallintalain tiedonhallinnan kuvausten suosituksista

4.12.2019

Tiedonhallintamallin suositus

Palaute tiedonhallintamallia koskevasta suosituksesta. *Palaute voi kohdistua suosituksen sisältöön tiedonhallintamallin tarkoituksen, sen laatimisen tai sen hyödyntämisen näkökulmista; suosituksen rakenteeseen tai tarkkuustasoon tai suosituksen eri käyttäjäryhmien tarpeisiin. Palautteessa voit tuoda esiin esimerkiksi lain soveltajan kannalta hyödyllisiä lisäyksiä.*

CSC:n vastaus:

CSC pitää tiedonhallintamallia koskevaa suositusta hyvänä ja kannatettavana. Johdon selkeä vastuuttaminen on tärkeää ja mallissa hyvin muotoiltu. Julkisuuslaki toimii tärkeänä pohjana mallille (esitetty hyvin kuvassa 7).

Maksimaalisen hyödyn saavuttamiseksi CSC ehdottaa, että jo kuvausten tasolla pyritään yhteentoimivuuteen. Tämä tapahtuu varmistamalla, että käytetty terminologia on yhtenäistä. Esimerkiksi tietovarantojen kuvauksessa on varmistettava, että sanastot ovat riittävän kattavat. Sopiva paikka kommentoida tätä olisi luku 7.

Tiedonhallintamalliin tulee myös sisällyttää riittävät tunnistepolitiikat. Tunnisteiden elinkaari ja hallinta tulee ottaa osaksi asiankäsittelyprosessien kuvausta. Tästä on hyvä mainita ainakin luvussa 8.

Tietoturvallisuuden suositukset

Palaute tietoturvallisuutta koskevasta suosituskokonaisuudesta, joka koostuu seitsemästä kortista. *Palaute voi kohdistua suositusten sisältöön, rakenteeseen tai tarkkuustasoon tai suositusten eri käyttäjäryhmien tarpeisiin. Palautteessa voit tuoda esiin esimerkiksi lain soveltajan kannalta hyödyllisiä lisäyksiä.*

CSC:n vastaus:

Huomioita suosituskortista ”Suositukset tietoturvallisuudesta”:

Tietoaineistojen ja tietojärjestelmien tietoturvallisuutta koskien tulee nykyistä selkeämmin korostaa aineiston ja järjestelmien omistajan vastuuta tunnistaa vaatimukset ja hyväksyä toteutetut toimenpiteet. Lisäksi suosittelemme muuttamaan muotoilua ”viranomaisen on hyvä arvioida” selkeämmäksi, esimerkiksi muotoon ”viranomaisen tulee arvioida”.

Huomioita suosituskortista 13 § Riskienhallinta:

Suosituskortin maininta ”kaikissa organisaatioissa tietoturvariskit on käsiteltävä johdon sisäisen valvonnan ja riskienhallinnan arviointi- ja vahvistuslausumassa kerran vuodessa” on erinomainen ja selkeästi ilmaistu vaatimus. Vaatimus riskien omistajuudesta tulee kuitenkin määritellä selkeämmin, esimerkiksi muuttamalla sivulla kaksi oleva maininta kohteen omistajasta (”tietoriskin arvioinnin kohteen omistaja päättää…”) kohteen johtajaksi.

CSC – TIETEEN TIETOTEKNIIKAN KESKUS OY
Keilaranta 14 • PL 405 • 02101 Espoo
Puh. (09) 457 2001 • Fax (09) 457 2302 • Y-tunnus 0920632-0 • www.csc.fi

CSC – IT CENTER FOR SCIENCE LTD.
Keilaranta 14 • P.O. BOX 405 • FI-02101 Espoo • Finland
Tel. +358(0)9 457 2001 • Fax +358(0) 9 457 2302 • VAT number FI09206320 • www.csc.fi

Huomioita suosituskortista 17 § Lokitietojen kerääminen:

Kortti on hyvin jäsennelty ja muodostaa tasapainoisen kokonaisuuden. Suosituksen tavoitetaso on kannatettava, mutta melko kunnianhimoinen. Suosituksessa olisi tärkeää ottaa huomioon kaupallisten ja avointen valmisohjelmistojen lokien muodostaminen, johon yleensä voidaan vaikuttaa vain rajallisesti.

Lokiaineistojen kuvaamisessa käyttötarkoituksen, tietotyyppien ja henkilötietojen kuvaaminen on hyvä tavoite. Lokiaineistojen kuvaaminen tarvitsee kuitenkin erillisen yksityiskohtaisemman suosituksen ja menetelmän, jolla eri tiedonhallintayksiköt voivat tuottaa yhteismitallisia ja laadukkaita kuvauksia lokiaineistojen tietosisällöistä. Lokiaineistojen kuvaamisessa voidaan hyödyntää Suomi.fi -yhteentoimivuusalustaa. Kortin lopussa olevista määritelmistä tulee muodostaa sanasto sanasto.suomi.fi -palveluun. Henkilötietotyypeistä, salassa pidettävistä tietoalkioista ja salassapitoperusteista voidaan muodostaa koodisto. Käsitteiden keskinäiset suhteet voidaan mallintaa tietomallit.suomi.fi -palvelussa. Lisäksi yhteentoimivuuden välineiden pohjalta voidaan rakentaa menetelmä ja työväline lokikuvausten laatimiseen tiedonhallintayksiköissä.

Suosituksessa todetaan, että lähtökohtaisesti henkilötunnuksia ei tulisi tallentaa lokeihin. Suosituksen tulee määrittää, kuinka henkilöt yksilöidään lokiaineistoissa, mikäli henkilötunnusta ei suositella käytettävän. Tässä on syytä ottaa huomioon lokien ja lokijärjestelmien tekniset rajoitteet, ja että relaatio-operaatiot ja lokivirtojen mielivaltaiset transformaatiot (pseudonymisointi) eivät ole aina mahdollisia. Henkilön yksilöivä ja yhteismitallinen tunniste on tärkeä käsiteltäessä tietopyyntöjä ja lokiselvityksiä. Tilattomissa palveluissa (esimerkiksi tunnistuspalvelut), loki itsessään voi olla ainoa pysyvä tallenne jota palvelu käsittelee.

Suositusten toteuttaminen konkreettisissa tietojärjestelmissä ei ole suoraviivaista, vaan vaatii merkittävästi suunnittelutyötä. Viranomaisen hyväksymät yksityiskohtaiset lokipalvelujen ratkaisuarkkitehtuurimallit tukisivat suositusten jalkauttamista ja tehostaisivat toteutustyötä tiedonhallintayksiköissä.

Asiakirjajulkisuuden suositus

Palaute asiakirjajulkisuuskuvausta koskevasta suosituksesta. *Palaute voi kohdistua suosituksen sisältöön asiakirjajulkisuuskuvauksen tarkoituksen, sen laatimisen tai sen hyödyntämisen näkökulmista; suosituksen rakenteeseen tai tarkkuustasoon tai suosituksen eri käyttäjäryhmien tarpeisiin. Palautteessa voit tuoda esiin esimerkiksi asiakkaan kannalta tai lain soveltajan kannalta hyödyllisiä lisäyksiä.*

CSC:n vastaus:

-

Suositukset teknisistä rajapinnoista ja katseluyhteyksistä

Palaute teknisiä rajapintoja ja katseluyhteyksiä koskevista suosituksesta. *Palaute voi kohdistua teknisiä rajapintoja ja katseluyhteyksiä koskevien suositusten sisältöön, rakenteeseen*

tai tarkkuustasoon tai suositusten eri käyttäjäryhmien tarpeisiin. Palautteessa voit tuoda esiin esimerkiksi lain soveltajan kannalta hyödyllisiä lisäyksiä.

CSC:n vastaus:

Suosituksen 22 § 2 momentissa todetaan seuraavasti: ”…teknisesti varmistetaan luovutettavien tietojen tapauskohtainen tarpeellisuus tai välttämättömyys tietoja saavan viranomaisen tehtävien hoitamiseksi, jos luovutettavat tiedot ovat henkilötietoja tai salassa pidettäviä tietoja.” Kohtaa on syytä selventää, sillä muotoilu on hieman epäselvä ja lisäksi herää kysymys, miten tämä on käytännössä mahdollista varmistaa tapauskohtaisesti, eli aina kun tulee tietotarve.

Myös suosituksen 22 § 3 momentti vaatii selvennystä seuraavan kohdan osalta: ”Teknisen rajapinnan avulla luovutettavien tietojen tietorakenteen kuvauksen määrittelee ja sitä ylläpitää tiedot luovuttava viranomainen.” Suositus ei määrittele selvästi, miten toimitaan, jos tiedot ovat kolmannen osapuolen (palveluntarjoajan) hallussa viranomaisen puolesta. On epäselvää, määritelläänkö kolmas osapuoli tällaisessa tapauksessa viranomaiseksi tai sen nimissä toimivaksi, ja onko viranomaisella velvollisuus olla käyttämänsä palveluntarjoajan tietorakenteet kuvattuna.

23 § 2 momentin kohdan "2) tietojen hakemisen yhteydessä selvitetään tietojen käyttötarkoitus” tarpeellisuutta voisi selventää. Kohdassa 1) on jo todettu, että viranomainen saa katselumahdollisuuden vain tiedonsaantioikeuden mukaisiin tarpeellisiin ja välttämättömiin tietoihin. Lisäksi tulisi selventää, miten tietojen käyttötarkoitus käytännössä selvitetään.

Tiedonhallinnan kuvausten tuottamista opastavat mallit

Arvioi tarvetta tiedonhallinnan kuvausten tuottamista konkreettisesti opastaville taulukkomuotoisille malleille tai vastaaville.

CSC:n vastaus:

CSC pitää tiedonhallinnan kuvausten tuottamista opastavien mallien luomista hyvänä ajatuksena. Kuvauksia luodessa on tärkeää huomioida tunnisteiden käyttö sekä yhteisten tietokomponenttien ja käsitteiden käyttö (semanttinen yhteentoimivuus).