CSC-Tieteen tietotekniikan keskus Oy

Lausunto

01.11.2017

Asia: VM/1709/00.01.00.01/2016 VM098:00/2016

Lausuntopyyntö julkisen hallinnon tiedonhallinnan sääntelyn kehittämistä selvittäneen työryhmän raportista

Yleiset kommentit raportista

Yleiset kommentit raportista

CSC – Tieteen tietotekniikan keskus Oy kiittää mahdollisuudesta saada lausua julkisen hallinnon tiedonhallinnan sääntelyn kehittämistä selvittäneen työryhmän raportista. CSC on suomalainen ammattikorkeakoulujen, yliopistojen ja valtion omistama, erityistehtävää hoitava tietotekniikan

osaamiskeskus, joka tuottaa kansainvälisesti korkeatasoisia ICT-asiantuntijapalveluita tutkimukselle, koulutukselle, kulttuurille, julkishallinnolle ja yrityksille.

CSC toteaa julkisen hallinnon tiedonhallinnan sääntelyn kehittämisen olevan ensiarvoisen tärkeää lainsäädännön saattamiseksi ajan tasalle, hallitusohjelman tavoitteiden saavuttamiseksi sekä digitaalisen, kansalaisia palvelevan yhteiskunnan rakentamiseksi. CSC kiittää työryhmää perusteellisesta työstä ja ansiokkaasta raportista, joka esittää lukuisia kannatettavia ehdotuksia ja toimenpidesuosituksia. Tiedonhallintaa on tarkasteltava koko elinkaaren ajalta, ja CSC kannattaa lämpimästi nykyisten lakien uudistamista digitaalinen toimintaympäristö huomioiden, erityislakien konvergenssia yhdeksi yleislaiksi, sekä nopeaa etenemistä uudistusten toteuttamiseksi, lainvalmistelun tasosta tinkimättä. CSC katsoo, että työryhmän tavoite tuoda keskeinen sääntely julkisen hallinnon tiedonhallinnosta yhteen yleislakiin on kannatettava. Samoin raportissa mainitut tavoitteet elinkaarimallin käytöstä, tiedon kattavammasta hyödyntämisestä sekä käsittelyn yhtenäistämisestä ja yksinkertaistamisesta ovat tarpeellisia.

CSC katsoo, että tiedon luottamuksellisuuden turvaamista ei riittävästi huomioida raportissa, vaikka tiedon eheyden ja saatavuuden edellytysten parantamisella on merkittävä vaikutus tiedon käytettävyyteen. Ruotsin Kuljetushallituksessa tapahtunut ulkoistukseen liittyvä, sinänsä arkipäiväisiltä vaikuttaviin yksityiskohtiin (haltijan henkilötiedot) liittyvä tietovuoto, on hyvä esimerkki riskistä, joka voi toteutua Suomessakin, mikäli tiedon luottamuksellisuuteen tunnistamiseen ja suojaamiseen ei aseteta riittäviä velvoitteita lainsäädännön kautta. Nykyisin käytössä olevat mekanismit luokitella ja suojata luottamuksellista ja ei-julkista tietoa

julkishallinnossa ovat jäykkiä. Siksi näitä mekanismeja tulee uudistaa ja tehostaa tiedon käytettävyyden parantamiseksi.

Uudistuvan lainsäädännön tulee selkeästi ja tehokkaasti ohjata ja tukea henkilötietojen ja rajallisen pääsyn tiedon (ST IV) tunnistamista, luokittelua ja suojaamista julkisessa hallinnossa. Erityistä huomioita tulee kiinnittää siihen, miten tällaista tietoa suojataan silloin, kun tietoa jaetaan rajatusti kansalaisten, sekä toimittajina ja asiakkaina toimivien yritysten välillä. CSC pitää tärkeänä kiinnittää huomiota kansalaisten oikeuksien, kuten sananvapauden ja luottamuksellisten tietojen suojan, turvaamiseen lakimuutoksissa. Lisäksi uudistuksissa on huomioitava muut käynnissä olevat lakimuutokset, kuten esimerkiksi tietosuoja-asetus ja niin sanottu toisiolaki (Hallituksen esitys laiksi sosiaali- ja terveystietojen tietoturvallisesta hyödyntämisestä sekä eräiksi siihen liittyviksi laeiksi) siten, että lait eivät ole keskenään ristiriitaisia. Samoin tulevan lainsäädännön on oltava yhteentoimiva tietosuoja-asetuksen, PSI-direktiivin ja muiden direktiivien kanssa.

CSC suhtautuu varauksella pyrkimykseen liian yksityiskohtaisesta lain- tai asetuksentasoisesta sääntelystä. Tiedonhallinnan alalla on jo olemassa useita vakiintuneita, velvoittavaksi koettuja käytäntöjä, jotka ovat osoittautuneet toimiviksi. Myös nopeasti muuttuva toimintaympäristö on huomioitava sääntelyn tarkoituksenmukaisuuden näkökulmasta. CSC ehdottaa, että lainvalmistelussa selvitetään, mistä asioista on säädettävä lailla tai asetuksella, ja minkä voi mahdollisesti jättää alan itsesäätelyn ja vakiintuneiden parhaiden käytäntöjen varaan.

CSC toivoo, että lainsäädännön uudistamisessa huomioidaan jo käynnissä oleva kansallinen ja kansainvälinen työ ja hankkeet tutkimusdatan alalla. Erityisesti huomionarvoisia ovat Opetus- ja kulttuuriministeriön Avoin tiede ja tutkimus -hanke (ATT), Research Data Alliance (RDA), jonka puitteissa kehitetään tiedonhallinnan yhteentoimivuutta kansainvälisesti FAIR (Findable; Accessible, Interoperable ja Reusable) –periaatteiden mukaisesti, tutkimusdataan liittyviä palveluja kehittävä ja tarjoava EUDAT, sekä tutkimuksen pilvipalvelualoite European Open Science Cloud (EOSC).

Kommentit raportin 5 luvusta

Kommentit osasta 5.1 Tiedonhallintaa koskevan sääntelyn soveltamisaloista

CSC esittää harkittavaksi, että jo soveltamisalaa käsittelevässä osassa todetaan lainsäädännön koskevan myös tietojärjestelmissä tapahtuvaa tiedonhallintaa. CSC kannattaa ajatusta luoda yhtenäinen tietojärjestelmän käsite, joka kattaisi lainsäädäntöä laajasti.

Suomessa tehdään laadukasta rekisteritutkimusta ja maassa on hyvät edellytykset siihen. Rekisterien avulla tehtävä tutkimus on huomioitava uudistettaessa lainsäädäntöä. CSC toivoo, että jatkovalmistelussa huomioidaan rekisterinpitäjän erilaiset roolit ja vastuut. Samoin on huomioitava erilaiset aineistot ja niiden käyttö sekä se, että rekistereihin liittyy erilaisia toimijoita.

Esimerkiksi viranomaisen, yliopiston tai muun tutkimuslaitoksen ja tutkimusryhmän tai yksittäisen tutkijan vastuut on määriteltävä. Tutkimuksen näkökulmasta on huomioitava, että rekisterinpitäjä ei välttämättä ole aineiston omistaja tai rekisterin käsittelijä. Lainsäädännössä tulee eritellä erilaiset aineistot, niiden käyttö ja omistajat, kuten viranomainen, yliopisto ja tutkija. Lakiuudistuksessa tulee myös selvittää yliopiston ja tutkijan suhteet ja vastuut. Rekisterinpitäjän tulee olla organisaatio, eli yliopisto tai tutkimuslaitos, ei yksittäinen tutkija. Toisaalta taas yksittäisellä tutkijalla voi olla salassa pidettäviä aineistoja, joita ei välttämättä voida luovuttaa organisaatiolle. Sääntelyssä on lisäksi huomioitava virastojen, yliopistojen ja muiden, myös yksityisten, tutkimuslaitosten, sekä kaupallisten toimijoiden keskinäiset erot ja toimintaedellytykset.

Muilta osin CSC katsoo, että luku soveltamisalasta on kattava. CSC myös kannattaa lämpimästi pyrkimystä välttää saman tiedon keräämistä tai tallentamista useisiin tietovarantoihin.

Kommentit osasta 5.2 Tiedonhallinnan suunnittelu ja kuvaaminen

CSC on samaa mieltä työryhmän kanssa siitä, että rinnakkaisia suunnitteluvelvollisuuksia tulee yhtenäistää ja selkeyttää. Ongelmana on kuitenkin lisäksi se, että suunnittelu- ja kuvaamisvelvoitteiden toteuttaminen jää usein liian yleisluonteiseksi tai jopa ylimalkaiseksi, millä voi olla negatiivisia vaikutuksia sekä tiedon käytettävyyteen että sen luottamuksellisuuteen.

CSC kannattaa lämpimästi työryhmän toteamusta siitä, että arviointivelvollisuuden tulee palvella niin yksilön ja yhteisöjen oikeuksiin kuin tietoturvallisuuteen sekä henkilötietojen suojaan liittyviä tarpeita sekä viranomaisten ja julkista hallintotehtävää hoitavien toimijoiden tarpeita.

Tietojen luovuttamisen avoimen rajapinnan tai teknisen käyttöyhteyden kautta ei tule olla erityistapaus, vaan normaali käytäntö. Järjestelmien automatisointi ja yhteentoimivuus ovat tässä avainasemassa. Niiden suunnitteluun, toimijoiden koulutukseen, sekä infrastruktuuriin on panostettava.

Myös muiden kuin asiakirjajärjestelmien tietojen elinkaari on suunniteltava. Esimerkiksi arkistoinnin toteuttaminen järjestelmävaihdosten yhteydessä, päivittyvien tietokantojen arkistointi, sekä viranomaisten verkkosivujen arkistointi on suunniteltava etukäteen. Viranomaisen toiminnan laajeneminen sähköisiin kanaviin nostaa esiin uudenlaisia haasteita arkistoitavuudelle ja tiedon säilyttämiselle, ja nämä tulee huomioida myös lainsäädännössä. Esimerkiksi diaarijärjestelmä ei vastaa sosiaalisen median tuomiin haasteisiin: pitääkö esimerkiksi viranomaisen viestintä tai vastaukset kansalaisten kysymyksiin sosiaalisessa mediassa tallentaa ja arkistoida järjestelmällisesti? On myös pohdittava, missä määrin ja missä yhteydessä lainsäädännössä edellytetään arkistointia tai säilyttämistä. Pysyvien tunnisteiden elinkaariin ja niiden käytön ohjeistamiseen on panostettava.

Kommentit osasta 5.3 Tietoturvallisuus

Tietoturvallisuus on olennainen osa tiedonhallintaa. CSC:n näkemyksen ja pitkäaikaisen kokemuksen mukaan nykyinen tietoturvallisuuteen liittyvä lainsäädäntö, ohjeistus ja arviointikäytännöt ovat tehottomia, niiden tulkinta ja soveltaminen on vaikeaa, ja lisäksi ne ovat jatkuvien, vaikeasti ennakoitavissa olevien muutosten alla.

Esimerkiksi luokitellun tiedon suojaamisen arvioinnissa sovelletaan keskenään ristiriitaisia sekä usein ylimalkaisia VAHTI-ohjeita: VAHTI 2/2010, VAHTI 3/2010, VAHTI 3/2011, VAHTI 3/2012, VAHTI 1/2013. VAHTI 2/2012, VAHTI 4/2013 sekä VAHTI 5/2013. Viestintävirasto on soveltanut ohjeistusta siten (Ohje tietoturvallisuuden arviointilaitoksille. 2013. s. 27), että kuutta näistä ohjeista käytetään arvioinnissa, mutta ristiriitatilanteessa siten, että tiukin vaatimus täyttyy. Rinnakkain on myös sovellettu puolustusvoimien ja turvallisuusviranomaisten suosimaa KATAKRI-arviointikriteeristöä.

IT-palveluita kehittävälle ja toimittavalle taholle tämä tarkoittaa, että luottamuksellisen tiedon (ST III) suojaamisessa tulee täyttää noin 1200 eri yleistasoista vaatimusta, joiden pelkkä arviointikin voi kestää useita vuosia. Tämä ei ole tehokas eikä ketterä tapa toteuttaa turvallista tiedonhallintaa. Valitettavasti ohjeistusten uudistaminen on pysähtynyt, ja niin sanotut beta-ohjeet ovat edelleen toistaiseksi saatavissa vasta alustavana jäsentelyversiona: https://beta.vahtiohje.fi/etusivu.

Tiedonhallinnan huonoja ääripäitä ovat toisaalta jäykkä detaljisääntely ja toisaalta hallitsematon vastuun siirto ulkoisille toimijoille, mikä sekään ei ole kestävää tiedonhallintaa. Nyt esitetyt muutokset tiedonhallinnan tietoturvallisuuteen saattavat johtaa tiedonhallinnan hallitsemattomiin ulkoistuksiin esimerkiksi kolmansiin maihin, kuten aiemmin mainitussa esimerkissä Ruotsin kuljetushallituksen tietovuototapauksesta.

CSC on huolissaan siitä, että työryhmän ehdottamat toimenpiteet luokittelun nimellisistä muutoksista (suojatasot, turvallisuusluokka) sekä vaikeasti tulkittava uusi käsite ”tietoturvallisuuden vähimmäistaso” käytännössä heikentävät Suomen kyberturvallisuutta ja entisestään lisäävät turvallisuuden toteuttamisen tulkinnanvaraisuutta. Muutosehdotukset tietoturvallisuussääntelyyn (5.3.3.) tulee valmistella siten, että niiden pohjalta voidaan tuottaa tehokas, ketterä, käyttötoturvallisuutta, turvallisuuden varmistusta sekä tiedon hyödyntämistä toteuttava sääntely julkisen hallinnon tiedonhallintaa varten. CSC osallistuu asiantuntijana mielellään tietoturvallisuussääntelyn jatkokehittämiseen.

Termistön suhteen raportissa olisi hyvä selkiyttää ja määritellä termien "käytettävyys" (usability) ja "saatavuus" (availability) ero. Viimeksi mainittu termi on eräs tietoturvallisuuden perustavoite, jälkimmäinen taas viittaa palvelun laatuun, käyttökokemukseen ja hyötyyn. Saatavuus tarkoittaa, että palvelu on saatavissa, esimerkiksi sovitusti 99,99% palveluaikoina. Tietoturvallisuus ja käytettävyys ovat kaksi usein ristiriitaista tavoitetta, jotka tulee tasapainottaa riskienhallinnan sekä taloudellisten ja strategisten tavoitteiden pohjalta.

CSC ei kannata termin ”harkinnanvaraisesti julkinen” käyttöönottoa, koska käyttöturvallisuuden kannalta termi sisältää lukijalle ristiriitaisen ja vaikeasti tulkittavan viestin. Nyt käytössä oleva termi ”rajattu käyttö” on erinomainen, selkeästi tulkittava ja myös kansainvälisten käytäntöjen ”access restricted” mukainen. CSC ehdottaa, että tätä termiä käytetään myös jatkossa.

Kommentit osasta 5.4 Tietoaineistojen muodostaminen ja vastuut

CSC kannattaa työryhmän ehdotusta siitä, että asiakirjan, tietovarannon, sekä tietojärjestelmän käsitteiden selkiyttämistä lainsäädännössä tulee harkita. Samoin CSC kannattaa pyrkimystä vähentää rinnakkaisia tietoaineistoja ja saman tiedon keräämistä useassa yhteydessä. Avointen rajapintojen ohella myös tietokomponenttien tulee olla jaettuja.

Tietoaineistojen yhteentoimivuus ei ole ainoastaan tekninen kysymys, vaan huomiota on kiinnitettävä myös aineistojen sisällölliseen yhteentoimivuuteen. Sanastot, ontologiat ja koodistot toimivat liimana, jotka mahdollistavat eri tietoaineistojen sisältöjen sisäisen toimivuuden sekä yhteentoimivuuden yhdessä muiden aineistojen ja niiden tietokomponenttien kanssa. Näin ollen tietoaineistojen muodostamisessa on eri tahoilla huomioitava sanastot, ontologiat ja koodistot, joiden laatiminen, ylläpito ja käyttäminen vaatii resursseja. Näillä tulee siksi olla oma vastuutahonsa. Resurssit on suunniteltava siten, että eri tahot voivat vastata asianmukaisesti mahdollisiin uusiin velvoitteisiin. Käyttöönottovaiheessa on erityisesti panostettava käyttäjien ohjeistukseen ja koulutukseen.

Kommentit osasta 5.5 Tietojen ja tietojärjestelmien yhteentoimivuus

Yhteentoimivuus on digitaalisen yhteiskunnan kriittinen kohta. Jos rajapinnat eivät toimi, digitalisaation tavoitteet eivät toteudu. CSC kannattaa lämpimästi raportissa esitettyjä keinoja tietojen ja tietojärjestelmien yhteentoimivuuden parantamiseksi, mutta toivoo, että myös käytännön ohjeistuksille, toimenpiteille ja tuelle määritellään vastuutaho, ja niille osoitetaan tarvittavat resurssit.

Yhteentoimivuus on ensiarvoisen tärkeää sekä kansallisesti että kansainvälisesti. Lainsäädännössä on varmistettava edellytykset kansainväliselle yhteentoimivuudelle. Erityisesti huomioitavia ovat toisiokäyttö ja avoimet standardit. Julkisille toimijoille tulee olla suosituksia kansainvälisesti tunnustettujen avointen standardien ja lisenssien käytöstä.

CSC kannattaa aktiivista sanastotyötä sekä toimia semanttisen yhteentoimivuuden lisäämiseksi. Sanastotyön lisäksi tulee määritellä rakenteita, komponentteja ja koodistoja, ja näin ohjata aktiivisesti yhteentoimivuuden toteutumista. Pelkät rajapinnat eivät riitä, vaan tietokomponenttien tulee olla jaettuja tiedon liikkuvuuden edistämiseksi.

CSC toivoo, että jatkotoimenpiteissä varmistetaan tiedonsaanti ja yhteentoimivuus kaikilta tarvittavilta toimijoilta kaikille tarvittaville aineistoille, niin ettei yhteensopivuus tarkoita ainoastaan yhteensopivuutta viranomaisten välillä. Etenkin tutkimuksen näkökulmasta on huomioitava, että tiedon liikkuvuus kaikkien toimijoiden välillä on ensiarvoisen tärkeää.

CSC kannattaa työryhmän näkemystä, että PSI-direktiivin käsitteistöä tulee käyttää myös kansallisessa lainsäädännössä.

Kommentit osasta 5.6 Tietoaineistojen julkisuus ja salassapito

CSC pitää tärkeänä julkisuuteen ja salassapitoon liittyvän sääntelyn selkiyttämistä ja kannattaa työryhmän ehdotusta siitä, että salassapitoon liittyvä sääntely tulee jäsennellä ja kuvata nykyistä selkeämmin. Myös salassapidon perustelu tulee olla mahdollisimman selkeää ja läpinäkyvää, ja perustua suojattavaan kohteeseen. Tiettyjen tietojärjestelmiin liittyvien tietojen, kuten pääsynhallinnan, turvallisuusjärjestelyiden ja varautumisen, tulee olla mahdollista luokitella rajatulle käytölle. Lisäksi pääsy henkilötietoihin tulee säätää siten, että kansalaisten oikeus tietosuojaan ei vaarannu siinäkään tapauksessa, kun kansalainen asioi viranomaisen kanssa.

Tietoaineiston salassapidon varmistamiseksi kaikkien julkisen hallinnon toimijoille tarkoitettujen tietovarantojen tulee toimia siten, että tiedon hausta jää aina automaattinen lokimerkintä sekä merkintä käsittelyperusteesta. Tietoaineistojen jakamisessa on huomioitava ainakin kaksi tapaustyyppiä: jako viranomaisten välillä, sekä jakaminen kolmansille osapuolille. Tietojen omistajuus- ja vastuukysymykset on selvitettävä omadata-ajattelun mukaisesti, joka korostaa yksilön oikeuksia itse päättää itseään koskevien tietojensa siirtämisestä tai vastaanottamisesta erilaisiin tarkoituksiin. Viranomaisille tulee luoda kannustimia hyväksyä tai ylläpitää tietojenkäsittelyjärjestelmiä, jotka ovat teknisesti yhteensopivia omadata-toimintaan.

Kommentit osasta 5.7 Tiedonsaanti asiakirjoista ja tietoaineistoista

CSC kannattaa erilaisin keinoin ja eri tahoilla tuotetun tutkimus- ja muun tiedon avoimuutta ja hyödyntämistä. CSC näkee merkittäviä hyötyjä datan avaamisessa, mutta katsoo, että ohjeistusta tulee täsmentää erityisesti sen osalta, miten vähäisiä määriä sisältävien henkilötietojen aineistojen luovutus tulee toteuttaa.

CSC katsoo, että rajoite- ja salassapitosäännökset ovat vaikeasti tulkittavissa. Se, että pääsy tietoihin tietojärjestelmien avulla on teknisesti mahdollista, ei muodosta automaattisesti oikeutta tietojen hyödyntämiseen (”tiedonsaantioikeus atk:n avulla talletettuihin viesteihin on monipuolisempi kuin perinteisten asiakirjojen kysymyksessä ollessa”). Rekisterinpitäjän sekä osaltaan myös tiedon käsittelijän tulee varmistua, että pääsy tietoihin on asianmukaisesti rajattu.

CSC on samaa mieltä ehdotuksen kanssa siitä, että jäykkä hallinnollinen menettely ei sinänsä lisää suojattavien tietojen turvallisuutta.

CSC kannattaa tietopyyntöjen käsittelyn merkittävää selkiyttämistä siten, että huomioidaan sekä julkisuusperiaate että suojattavien tietojen käytön rajaaminen.

CSC kannattaa raportissa mainittuja huomioita tutkimustiedon hyödyntämisestä, mutta haluaa lisätä, että sekä akateemisille että kaupallisille tutkimusryhmille tulee tarjota selkeitä ohjeita, vaatimuksia sekä neuvontaa siihen, miten ei-julkinen tieto suojataan. Pelkkä tutkimusryhmän vastuullisen johtajan nimeäminen ei ole riittävä suojaustoimenpide.

Kommentit osasta 5.8 Tietoaineistojen säilyttäminen ja arkistointi

CSC katsoo, että raportissa käsitellään laaja-alaisesti ja kattavasti tietoaineistojen säilyttämistä ja arkistointia. Kuten raportista ilmenee, ovat Kansallisarkiston rooli sekä tietoaineiston säilyttäminen tutkimuskäyttöä varten keskeisiä kysymyksiä, joita on syytä edelleen selventää. Kansallisarkiston ohjaava rooli osaltaan selkiyttää tilannetta. Raportissa on huomioitu kattavasti tietosuoja-asetuksen vaikutuksia säilyttämiseen ja arkistointiin.

CSC yhtyy näkemykseen, että arkistolaki ei tue riittävän kattavasti digitaalisessa muodossa olevien tietoaineistojen säilyttämistä eikä arkistointia.

Raportissa olevat säilyttämiseen ja arkistointiin liittyvät linjaukset ovat CSC:n näkemyksen mukaan kannatettavia. CSC kuitenkin toivoo, että jatkovalmistelussa kiinnitetään huomiota pitkäaikaissäilytyksen (PAS) ratkaisuihin. On harkittava muun muassa, minkälaisia aineistoja halutaan pitkäaikaissäilytykseen, millaisia vaatimuksia PAS-säilytyksen tekniselle toteutukselle asetetaan, ja mitä tapahtuu aineistoille, joita ei pitkäaikaissäilytetä. Muuttuvien aineistojen arkistoinnin kehittämistä tulee edistää, ja siihen tulee varata tarvittavat resurssit. Tieteen ja tutkimuksen olemassa olevaa osaamista (mm. kansalliset ja kansainväliset hankkeet, jotka on mainittu yleisissä kommenteissa) muuttuvista aineistoista ja niiden versioinnista tulee hyödyntää ja kehittää edelleen. Aineistojen ja tietosisältöjen toisteisuutta tulee vähentää kehittämällä datan viittaamiskäytänteitä sekä ontologioita ja niiden arkistointia.

Kommentit osasta 5.9 Tietohallinnon ja tiedonhallinnan ohjaus

CSC:n näkemyksen mukaan julkisen hallinnon tietojärjestelmien yhteentoimivuudessa on edelleen merkittävästi kehitysvelkaa. CSC katsoo, että raportissa kuvatut muutostarpeet on kuvattu oikeansuuntaisesti. Kokonaisarkkitehtuurien merkitys toiminnan kehittämisessä on tärkeää, ja samalla on tunnistettava kokonaisarkkitehtuurimenetelmän ja nykyisen tietohallintalain ongelmat.

Kommentit muutosehdotusten priorisoinnista

Mitä muutosehdotuksia olisi mielestänne priorisoitava valmistelussa?

CSC:n näkemyksen mukaan tärkein muutos- ja kehitystarve raportin osalta on tietoturvallisuuteen sekä tiedon luokitteluun liittyvä sääntely. Nämä tekijät tulee tunnistaa, määritellä ja säännellä selkeämmin ja kestävämmin kuin miten nyt käsillä olevassa versiossa on tehty.

Muut tarpeelliset toimenpiteet

Millä muilla toimenpiteillä, lainsäädännön uudistamisen lisäksi, katsotte olevan merkitystä julkisen hallinnon tiedonhallinnan kehittämisessä?

Raportissa ehdotetaan lukuisia muutoksia, jotka toteutuessaan selkiyttävät nykytilaa ja päivittävät tiedonhallintaa vastaamaan digitaalisen toimintaympäristön vaatimuksiin. CSC arvioi, että mahdollisten muutosten toimeenpano vaatii paljon työtä ja merkittäviä panostuksia sekä tekniikkaan että osaamiseen.

Vaatimusten ja sääntelyn muuttuessa on panostettava koulutukseen viranomaisille ja muille toimijoille, jotka ostavat, suunnittelevat ja käyttävät tietojärjestelmiä.

Vastuuta tiedonhallinnasta ja yhteentoimivuudesta ei saa liikaa ulkoistaa, ja toteutuksessa on suosittava avoimia ratkaisuja toimittaja- tai järjestelmäloukun (vendor lock in) välttämiseksi.

Toteutuksessa on luotava selkeät ja ymmärrettävät ohjeet ja nyrkkisäännöt, sekä hyödynnettävä parhaita käytäntöjä, joita voidaan kerätä ja luoda esimerkiksi erilaisissa laajapohjaisissa asiantuntijaelimissä.

Työryhmän ehdotusten vaikutukset

Yleiset kommentit vaikutuksista

Lainsäädännön selkiyttäminen ja päivittäminen nykyistä toimintaympäristöä vastaavaksi helpottaa organisaatioiden omaa ja niiden välistä toimintaa. Kansalaisen näkökulmasta tämä tarkoittaa parempia viranomais- ja muita palveluita, sekä parempaa oikeusturvaa.

Tietoturvallisuuden osalta nyt ehdotetut muutokset eivät kuitenkaan selkiytä sääntelyä vaan saattavat jopa edelleen hämärtää sitä, mitä tietoturvallisuuden osalta loppujen lopuksi edellytetään.

CSC toivoo, että olemassa olevaa teknistä osaamista esimerkiksi pitkäaikaissäilytysratkaisujen ja aineistojen versiointiin, kuratointiin ja siirtämiseen liittyen hyödynnetään jatkovalmistelussa ja muutosten toteuttamisessa, kansallinen ja kansainvälinen yhteentoimivuus huomioiden.

Taloudelliset vaikutukset

-

Vaikutukset viranomaisten toimintaan

-

Yhteiskunnalliset vaikutukset

-

Kaila Urpo
CSC-Tieteen tietotekniikan keskus Oy