Oulun yliopisto

Lausunto

01.10.2018

Asia: VM183:00/2017 ja VM/1631/03.01.00/2018

Luonnos hallituksen esitykseksi eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

---

2. Arvionne lukuun 2 Nykytila

---

3. Arvionne lukuun 3 Esityksen tavoitteet ja keskeiset ehdotukset

---

5. Kommentit ja huomiot lakiehdotuksen lukuun 1 yleiset säännökset (pykälät 1-4 ja niiden yksityiskohtaiset perustelut)

---

6. Kommentit ja huomiot lakiehdotuksen lukuun 2 Julkisen hallinnon tiedonhallinnan yleinen ohjaus (pykälät 5-9 ja niiden yksityiskohtaiset perustelut)

Lakiehdotuksen luku 2

5 §. Tietovarantojen yhteentoimivuuden ohjaus

Lakiesityksessä tavoitellaan tietovarantojen yhteentoimivuutta ja sen ohjausta. Lakitekstiä tulisi tarkastella siitä näkökulmasta, miten tarkasti kuvauksissa käytettävistä tavoista ja välineistä on syytä määrätä, jotta em. tavoite todella saavutetaan.

7. Kommentit ja huomiot lakiehdotuksen lukuun 3 Tiedonhallinnan suunnittelu ja kuvaaminen (pykälät 10-12 ja niiden yksityiskohtaiset perustelut)

---

8. Kommentit ja huomiot lakiehdotuksen lukuun 4 Tietoturvallisuus (pykälät 13-18 ja niiden yksityiskohtaiset perustelut)

Lakiehdotuksen luku 4

Yleisesti luvun 4 vaatimukset on otettu huomioon tietojärjestelmänhankintaan liittyvissä tietoturvavaatimuksissa tai palvelu -tai tietoturvasopimuksissa, joten vaatimukset vastaavat pitkälti jo nykyisiä yliopistojen tieturvantasoja:

- Henkilöstön ja palveluntuottajien luotettavuuden varmistaminen – salassapitosopimukset/ NDA:t, hankintasopimukset
- Tietoaineistojen ja tietojärjestelmien tietoturvallisuus - Luokitteluohjeet, järjestelmien tärkeysluokitus
- Tietojen siirtäminen tietoverkossa – tietoliikenteen ja tiedon suojaaminen
- Tietoaineistojen turvallisuuden varmistaminen - Tietoaineistojen käsittely ja luokitteluohjeet
- Tietojärjestelmien käyttöoikeuksien hallinta - käyttöoikeudet ja niiden laajuudet annetaan vain niitä tarvitseville
- Lokitietojen kerääminen – SOC tai vastaavat ratkaisut

Nämä toimet tulee kuitenkin kohdentaa tietojärjestelmän/palvelun ja sen sisältämän tietosisällön kriittisyyden huomioiden. Palveluiden ”kriittisyys”- näkökulma olisi hyvä lisätä lukuun 4.

Kertaluonteisten ja jatkuvien kustannusten määrä on arvioitu liian alhaisiksi. Lain vaatimusten toteuttaminen edellyttää myös teknisiä ratkaisuja, joiden hankinta- ja jatkuvien kustannusten arviointi on vaikeaa. Lisäksi kilpailutus vie aikaa ja teknisten ratkaisujen implementointiin menee useita kuukausia. Vain yhtenä esimerkkinä mainittakoon keskitetyn lokienhallinnan ratkaisu. Teknisen infrastruktuurin toteuttamisprojekti maksaa minimissään miljoona euroa. Karkean arvion mukaan noin 1 TB päivittäisellä lokimäärällä vuosittaiset kustannukset nousevat minimissään 400.000 euroon. Lisäksi tarvitaan lokienhallinnan infrastruktuurin ylläpitohenkilöstöä ja seurantatoimintoon ammattitaitoista lisähenkilöstöä poikkeamien analysointiin ja käsittelyyn. Minimissään näistäkin syntyy vuositasolla 4 henkilötyövuoden kustannukset.

Muutoksien toteuttaminen johtaisi luonnollisesti parempaan ”tiedonhallinnan” laatuun yliopistojen tiedonhallinnan prosesseissa, mutta resurssit eivät todennäköisesti riitä näiden vaatimusten täyttämiseen.

13 § Henkilöstön ja palveluntuottajien luotettavuuden varmistaminen

Yliopistojen osalta koko palvelutuotannon ja yhteistyökumppaneiden kaikkien työntekijöiden ja työnhakijoiden luotettavuuden selvittäminen turvallisuusselvityslaissa tarkoitetulla tavalla aiheuttaa lisäkustannuksia ja ylimääräistä työtä. Turvallisuusselvityksen kohdentaminen on syytä tehdä vain tiettyihin erikseen määriteltyihin työtehtäviin ja turvallisuusselvityksen kohdennus riskiarvioon perustuen tarpeellisiin tehtäviin ja palveluihin, kuten IT-palvelutuotannossa, turvallisuustehtävissä tai vastaavissa työskenteleville henkilöille. Lisäksi turvallisuusselvitys antaa kuvan vain henkilön

luotettavuudesta selvityshetkellä. Kriittisten palvelujen osalta voitaisiin pohtia turvallisuusselvitysten voimassaolon säännöllistä seuraamista.

14 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus

14 §:ssä on kirjoitettuna auki tietoturvallisuuden parhaita käytäntöjä. Riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella ja korjaavien toimenpiteiden toteuttaminen on aina osa ammattimaisesti toteutettua tietoturvallisuuden hallintaa koko tietojärjestelmän elinkaaren ajan.

Tietoturvallisuuden toteuttamisen erityisvaatimuksissa on korostettu hyvin tietojärjestelmien käytettävyyden varmistamista etukäteen tehtyjen testausten kautta.

Tietojen riittävä suojaaminen voidaan toteuttaa suunnittelemalla ja rakentamalla tietojärjestelmät sellaisiksi, että väärinkäytökset havaitaan sekä toteutetaan riittävien lokitietojen kerääminen ja analysointi tietojärjestelmissä tehdyistä toimenpiteistä. Tekninen seuranta on tehokkaampi ratkaisu kuin turvallisuusselvityksen teettäminen, mutta teknisten ratkaisujenkin tulee kohdistua riskiperusteisesti oikeisiin kohteisiin.

Tietojärjestelmien koko elinkaaren aikainen tietoturvallisuus on otettava huomioon jo hankintavaiheessa, tämä on erittäin olennainen ja kannatettava kokonaisuus. Tämä edellyttää tietoturvavaatimusten asettamista suojattavan kohteen vaatimalle turvatasolle ja vaaditun tason säännöllistä todentamista koko elinkaaren ajan. Ennen tietojärjestelmän käyttöönottoa tehty työ on oleellista, vaatimusten ja toteutuksen korjaaminen myöhemmin on vaikeaa ja kallista. Tätä asiaa ei voi liikaa korostaa. Vaatimus käsittelyn suunnittelusta siten, että julkinen ja salassa pidettävä voidaan erottaa vaivatta toisistaan, on hyvä ominaisuus.

Sellaiset viranomaisella olevat tai syntyvät tietoaineistot, jotka eivät toteuta viranomaisen asiakirjan määritelmää tulee käsitellä viranomaisen omaan riskiarvioon pohjautuvan luokittelun mukaisesti. Kaikki tietoaineistoon kuuluvat materiaalit eivät välttämättä ole asiakirjan määrittelyn mukaisesti asiakirjoja. Näiden materiaalien käsittely tulee myös olla riskiarvioon pohjautuvaa. Tällaista tietoa syntyy tai käsitellään muun muassa yliopistojen tutkimustoiminnassa, jota tämä laki koskee.

15 § Tietojen siirtäminen tietoverkossa.

On hyvä huomioida, että EU:n yleisestä tietosuoja-asetuksesta seuraa se, että tiedonsiirtoyhteys tai tiedonsiirtotapa on toteuttava tietoverkossa salattua tai muuta suojattua tiedonsiirtoyhteyttä tai tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä tai henkilötietoja.

Myös vastaanottajan tunnistaminen tai varmentaminen riittävän tietoturvallisella tavalla sisältyy oletusarvoisesti EU:n yleiseen tietosuoja-asetukseen.

Tietojen siirtämisen teknisten turvamekanismien ja niihin kohdistuvien uhkien kenttä on jatkuvassa muutoksessa. Suojautumisessa tulee huomioida elinkaariajattelu ja mukautuminen tulevaisuuteen siten, että esimerkiksi salausmenettely on päivitettävissä.

16 § Tietoaineistojen turvallisuuden varmistaminen.

Tietoturvallisuuden hallintajärjestelmän prosessien avulla varmistetaan tietoaineistojen tietoturvallisuus, huomioiden samalla tietojärjestelmän sisältämän tietosisällön mukainen suojaamistarve. 16 § velvoitteiden ulottaminen koskemaan myös yliopistoja kaikkien tietojärjestelmien ja toimitilojen osalta on osittain ylimitoitettua eikä sellaisenaan sovellu yliopistojen toiminannan luonteeseen, mutta kokonaisuutena 16 § velvoitteet ovat kannatettavia.

Pykälä 16 § pitää luettelon niistä teknisistä, toiminnallisista ja hallinnollisista toimenpiteistä, joilla tietoaineistojen tietoturvallisuus varmistetaan kaikissa tiedonhallintayksiköissä ja niissä toimivissa viranomaisissa. Vastaavanlaisia velvoitteita sisältyy oletusarvoisesti myös EU:n yleiseen tietosuoja-asetukseen.

Tietoaineistojen käsittelyä tulee ohjata riskiarvioinnin kautta ja mitoittaa käsittely siltä osin riskiarvioon pohjautuen, jossa käsittelyssä on hyvä huomioida 14 § linjaukset.

17 § Tietojärjestelmien käyttöoikeuksien hallinta.

Tietojärjestelmien käyttöoikeuksien hallinnan järjestäminen siten, että tietojärjestelmiin on pääsy vain henkilöillä, joilla on oikeus käsitellä tietojärjestelmän tietoaineistoja ja pääsy vain sellaiseen tietoon mitä käyttäjän työtehtäviin sidotut käyttötarpeet edellyttävät, on parhaita käytäntöjä, jotka toteutetaan uusissa tietojärjestelmissä.

Vanhoissa tietojärjestelmissä voi olla tietojärjestelmän teknisistä rajoituksista tai puutteellisista vaatimuksista johtuen työtehtäviin nähden tarpeettoman laajoja käyttöoikeuksia, mutta tilanne saadaan yleensä korjattua vasta järjestelmän uusimisen yhteydessä.

On syytä huomioida, että järjestelmätason käyttöoikeudet ovat nykyisin erillään palvelutason käyttöoikeuksista. Tämä eroavaisuus on hyvä tuoda esiin. Vaatimuksen sisällyttämisellä lakiin voi olla suuria kustannusvaikutuksia.

Tietoaineistoihin pääsyä rajoitetaan jo nyt toimitiloissa. Tietojärjestelmien palvelimet, levyjärjestelmät sekä muut laitteistot on sijoitettu konesaleihin, joihin pääsy on rajattu vain työtehtävien mukaan pääsyä tarvitseville. Mielestämme näiden parhaiden käytäntöjen kirjoittaminen lakiin näin yksityiskohtaisesti ei ole tarpeen.

18 § Lokitietojen kerääminen

Lokitietojen kerääminen virhetilanteiden selvittämiseksi, tietojärjestelmän käytön valvonnan järjestämiseksi sekä tietojärjestelmästä otettavien tietojen selvittämiseksi on hyvä kirjata lakiin. Lokitietojen kerääminen tietojärjestelmistä ja keskitetyn lokienhallinnan automatisoitu järjestäminen on ainoa tapa muodostaa organisaation tietoturvan tilannekuvaa. Lokitietojen kerääminen tulee järjestää lokisisällön riskiarvioon pohjautuen. Keskitetty, yksittäinen lokienkeruu ei ole välttämätön, kunhan tilannekuva pystytään muodostamaan. Tämän vuoksi ehdotamme lakiin lisättäväksi, että lokien hallinta tulee järjestää siten, että tietojenkäsittelyssä tapahtuneet poikkeamat havaitaan eri tyyppisten hälytysjärjestelyjen avulla.

9. Kommentit ja huomiot lakiehdotuksen lukuun 5 Turvallisuusluokittelu (pykälät 19-22 ja niiden yksityiskohtaiset perustelut)

---

10. Kommentit ja huomiot lakiehdotuksen lukuun 6 Asian ja palvelujen tiedonhallinta (pykälät 23-26 ja niiden yksityiskohtaiset perustelut)

Lakiehdotuksen luku 6

24 § Rekisteröinti asiarekisteriin

Lakiesityksessä on ehdotettu menettelytavaksi käyttää lähettävän tiedonhallintayksikön asiatunnusta ensisijaisena asiatunnuksena silloin kun asia liittyy toisessa viranomaisessa käsiteltävänä olevaan asiaan. Esitetty menettelytapa voi johtaa tilanteeseen, missä eri tiedonhallintayksikköjen tiedonohjaussuunnitelmien edellytetään olevan samanlaisia. Tämä ei ole järkevää yliopistojen muista viranomaisista poikkeavien toimintaympäristöjen kannalta. Jo nyt asianhallinnassa on tapana merkitä viitetiedoksi lähettävän viranomaisen asiatunnus, jonka avulla saapunut asiakirja voidaan tunnistaa.

11. Kommentit ja huomiot lakiehdotuksen lukuun 7 Tietoaineistojen muodostaminen ja sähköinen luovutustapa (pykälät 27-31 ja niiden yksityiskohtaiset perustelut)

Lakiehdotuksen luku 7

27 § Tietoaineistojen sähköinen muoto ja sen saatavuus

Paperisten asiakirjojen muuntaminen sähköiseen muotoon on kannatettavaa. Kuitenkin yliopistoissa tulee tulevaisuudessakin olemaan paljon hyvin lyhyen aikaa säilytettäviä paperisia asiakirjoja, esim. tenttivastaukset. Sähköistämisvaatimuksen tulisi koskea vain pidemmän aikaa (esim. yli 1 vuosi) säilytettäviä asiakirjoja, kaiken paperimateriaalin digitointi elektronisesti säilytettävään muotoon voi olla työlästä, kun siihen liittyy vielä validointiprosessi.

12. Kommentit ja huomiot lakiehdotuksen lukuun 8 Tietoaineistojen säilyttäminen ja arkistointi (pykälät 32-38 ja niiden yksityiskohtaiset perustelut)

Lakiehdotuksen luku 8

34 § Kansallisarkiston lausunto arkistoinnista

Lakiesityksen mukaan yliopistoilla tulisi tulevaisuudessa olemaan oikeus itse päättää tietoaineistojensa pysyvästä säilytyksestä ja arkistoinnista niiltä osin kuin lainsäädäntö ei tätä määrittele. Tämä toteuttaa yliopistojen itsehallintoa. Kansallisarkiston asiantuntijatuki tunnistettaessa merkittäviä kansalliseen kulttuuriperintöön kuuluvia tietoaineistoja tulee olla yliopistoille saatavilla tulevaisuudessakin.

37 § Tieteellisten tutkimusaineistojen arkistointi

Tieteellisten tutkimusaineistojen arkistointi: Aineiston elinkaaren vaiheen transitiosta voi tulla hankala prosessi yliopistoille. Lisäksi tutkijaa ei velvoiteta luovuttamaan aineistoa yliopistolle vaan se tapahtuu sopimusperusteisesti, tähän liittyen tutkija on aineistonsa rekisterin pitäjä mutta luovuttaessaan sen yliopistolle, yliopistosta tulee rekisterinpitäjä. Aineiston käsittelyn johdosta pitäisi varmistaa, että jo alun perin tutkija on toiminut asianmukaisesti rekisteriä perustaessaan. Tämä voi olla kuitenkin haasteellista.

13. Kommentit ja huomiot lakiehdotuksen lukuun 9 Erinäiset säännökset (pykälät 39-40 ja niiden yksityiskohtaiset perustelut)

---

14. Muut huomiot

Vaikutusten arviointi

Tiedonhallinnan suunnittelu ja kuvaaminen:

Tietoturvallisuus:

Asian ja palvelujen tiedonhallinta:

Tietoaineistojen luovuttaminen ja sähköinen luovutustapa:

Tietoaineistojen säilyttäminen ja arkistointi:

Muuta huomioitavaa:

4. Arvio lukuun 4 Esityksen vaikutukset

4.4 Vaikutukset yliopistojen ja korkeakoulujen talouteen

Lakiesityksen kustannusvaikutusten arviointi on yliopistojen osalta puutteellista.

Koulutus- ja muut henkilöstökustannukset: suunnittelu- ja kuvaustehtäviin arvioidaan kuluvan 1-2 htv ja lisäksi asiantuntijapalvelujen hankintaan noin 20 000–40 000 eurolla. Kuvausten ylläpitoon arvioidaan menevän noin 0,25 htv. Esitetyt työmäärät vaikuttavat pienehköiltä.

6.6 Muuta huomioitavaa:

Erityisen hyvää lakiehdotuksessa on pyrkimys moninkertaisen ja päällekkäisen sääntelyn poistamiseen.

Kansallisarkiston rooli muuttuu lausujaksi, se ei enää voi velvoittaa yliopistoja. Lisäksi Kansallisarkistolle säädetään vähimmäisaika, jossa se joutuu antamaan lausuntonsa aineiston arkistoinnista.

Lakiesityksessä esitetyt siirtymäajat vaikuttavat hyvin lyhyiltä. Erityisesti tiedonhallintamallin laatiminen ja ylläpito edellyttävät usean erilaisen jo olemassa olevan mallin yhteensovittamista sekä mahdollisesti myös uusien kuvausten ja mallien luomista. Esitetyt siirtymäajat vaikuttavat lyhyiltä tämänkaltaisen kokonaisuuden luomiseen, testaamiseen ja käyttöönottoon. Kiireinen aikataulu kasvattaa riskiä sille, että yliopiston niukat resurssit suunnataan lain vaatiman tiedonhallintamallin laatimiseen ja itse yhteentoimivien prosessien sekä palvelujen edistäminen viivästyy.

Nylund Päivi
Oulun yliopisto