Kansallinen turvallisuusviranomainen

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)

Kansallinen turvallisuusviranomainen kehottaa varmistamaan, että lakiehdotuksen 2 § sisältää kaikki määritelmät, jotka esiintyvät kautta lakiehdotuksen. Tällä hetkellä lakiehdotuksessa käytetään termiä ”kansainvälinen tietoturvallisuusvelvoite”, mutta sitä ei kuitenkaan ole sisällytetty lakiehdotuksen 2 §:n määritelmiin. Määritelmä tulisi sisällyttää 2 §:ään tarkasti saman sisältöisenä kuin se on määritelty kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004, ”KvTituL”).

Lakiehdotuksen 2 § sisältää tällä hetkellä ”tietovarannon” määritelmän, sekä ”asiakirjan” määritelmän, jonka jälkimmäisen osalta viitataan julkisuuslain (621/1999) mukaiseen ”viranomaisen asiakirjan määritelmään”. Julkisuuslaki erottelee ”asiakirjan” sekä ”viranomaisen asiakirjan” käsitteet. Näyttäisi siltä, että nykyinen julkisuuslain mukainen asiakirjan laaja käsite kattaisi myös uuden, ehdotetun tietoaineiston käsitteen, mutta näiden kahden käsitteen välinen ero ei käy ilmi lakiehdotuksesta, joka saattaa olla omiaan harhaanjohtamaan lainsoveltajaa.

Ainakin lakiehdotuksen 14 §:ssä käytetään asiakirjan elinkaaren määritelmää, mutta ehdotuksen 2 §:ssä ei ole kuitenkaan elinkaarta määritelty. Kumottavaksi ehdotetun tietoturvallisuusasetuksen (681/2010) 6 §:ssä säädetään, että tietoturvallisuustoimenpiteet on suunniteltava ja toteutettava siten, että ne kattavat kaikki käsittelyvaiheet.

Kansallinen turvallisuusviranomainen kiinnittää erityistä huomiota lakiehdotuksen 3 §:n soveltamisalaan. Tässä 3 §:ssä tulisi olla ensiksikin viittaus lakiin kansainvälisistä tietoturvallisuusvelvoitteista (588/2004, ”KvTituL”).

Tämän lisäksi kansallinen turvallisuusviranomainen tuo lainvalmistelijoille esille, että KvTituL:n 3 §:n lain suhdetta muuhun lainsäädäntöön koskevassa pykälässä on säädetty, että erityissuojattavan tietoaineiston julkisuudesta sekä sen käsittelyssä noudatettavasta hyvästä tiedonhallintotavasta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) ja sen nojalla säädetään, jollei KvTituL:ssa toisin säädetä. Julkisuuslain nojalla säädetty valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) ehdotetaan nyt käsillä olevan esityksen yhteydessä samalla kumottavaksi, jolloin samalla tulisi tehdä muutos myös KvTituL:n 3 §:n viittaukseen julkisuuslakiin ja sen nojalla annettuun, kumottavaksi ehdotettuun tietoturvallisuusasetukseen.

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

-

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)

Kansallinen turvallisuusviranomainen katsoo, että esityksen tietoturvallisuutta koskeva 4 luku vaikuttaa jäävän huomattavasti yleisemmälle tasolle kuin kumottavaksi ehdotetussa tietoturvallisuusasetuksessa. Tätä osoittaa muun muassa se, että nykyisen tietoturvallisuusasetuksen 5 §:n mukaisesta tietoturvallisuuden perustasosta on luovuttu. Kansallisen turvallisuusviranomaisen mielestä tulisi varmistaa, että kaikki tarpeelliset tietoturvallisuusvaatimukset edelleen sisältyvät esitykseen. Yleisempi sääntely kyllä jättää enemmän mahdollisuuksia tietoturvallisuustoimien käytännön toteuttamiseen, mutta se voi johtaa erimittaisiin turvallisuustoimiin eri toimijoiden välillä (tässä yhteydessä huomio erityisesti siihen, että jatkossa turvallisuusluokan IV asiakirjoja voisi käsitellä 14 §:n mukaiseen riskiarviointiin perustuen).

Lakiehdotuksen 14 §:n 2 ensimmäisessä momentissa vastuut on annettu tiedonhallintayksikölle, kun taas 3 viimeisen momentin vastuut on säädetty viranomaiselle. Kansallinen turvallisuusviranomainen kehottaa vielä harkitsemaan näiden välistä suhdetta.

Kansallinen turvallisuusviranomainen huomauttaa, että ehdotetussa 15 §:ssä tietojen siirtämiselle tietoverkossa asetettu salausvaatimus on ulotettu koskemaan myös henkilötietoja, joka olisi tiukennus siihen, mitä henkilötietoja koskevassa EU:n yleisessä tietosuoja-asetuksessa nimenomaisesti edellytetään.

Lakiehdotuksen 16 §:n 2 momentissa säädetään, että tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia. Kyseinen säännös ei ota kantaa siihen, kenen vastuulla on määritellä ja hyväksyä toimitilojen turvallisuus? Onko tilaturvallisuutta koskien tarkoitus antaa tarkempia säännöksiä asetuksessa? Asetuksenantovaltuus puuttuu tästä pykälästä.

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

Lakiehdotuksen 19 §:ssä laajennetaan turvallisuusluokiteltavien, julkisuuslain 24 §:n mukaisten tietokategorioiden alaa. 19 § on nyt kirjoitettu velvoittavaan ”on turvallisuusluokiteltava” –muotoon, kun taas tätä pykälää selostavassa yksityiskohtaisessa perustelujaksossa sama on kirjoitettu ”voitaisiin turvallisuusluokitella” –muotoon. Käytännön soveltamisongelmaksi saattaa muodostua se, että jos esimerkiksi poliisin asiakirjat (JulkL 24 § 1 mom 5-kohta) olisi jatkossa pakko turvallisuusluokitella, tulevat ne kansainvälisen tiedonvaihdon näkökulmasta Suomen solmimien kahdenvälisten tietoturvallisuussopimusten (General Security Agreement, GSA) soveltamisalan piiriin. Tällöin niiden sähköinen siirtäminen sopimuspuolten välillä on mahdollista toteuttaa ainoastaan sopimusosapuolten toimivaltaisten viranomaisten keskenään erikseen sopimien järjestelyjen välityksellä. Tällaisia sähköisiä sopimusosapuolten välillä sovittuja kanavia on toistaiseksi käytössä vain muutamia, joka saattaa aiheutua tiedonsiirron nopeuden kannalta huomattavaksi ongelmaksi, mikäli esimerkiksi poliisin asiakirjat olisi jatkossa aina turvallisuusluokiteltu.

Ehdotuksen 21 §:ssä säädetään turvallisuusluokiteltujen asiakirjojen tietoturvallisuusvaatimuksista. Turvallisuusluokan IV osalta säädetään, että tämän turvallisuusluokan tietoa käsitellään ainoastaan riskiarvioon perustuen, jonka osalta on erittäin tärkeää, että esityksen osalta arvioidaan vielä tarkasti, antavatko lakiehdotuksen säännökset riittävän suojan kansainvälisille turvallisuusluokitelluille tiedoille. Suomen solmimista kahdenvälisistä tietoturvallisuussopimuksista johtuvasta turvallisuusluokitellun tiedon suojaamisen vastavuoroisuusperiaatteesta johtuu, että sopimuskumppanivaltion turvallisuusluokiteltuja asiakirjoja suojataan Suomessa samalla tavalla kuin suomalaisia vastaavantasoisia luokiteltuja asiakirjoja. Mikäli suoja ei ole riittävä tai sitä heikennetään aiemmasta, tulisi Suomen tehdä ilmoitukset tästä kansainvälisille sopimusosapuolille, joiden kanssa on tehty tietoturvallisuutta koskeva valtiosopimus.

Ehdotuksen 21 §:n 3 momentissa säädetään, että valtioneuvoston asetuksella säädetään tarkemmin turvallisuusluokan III, II ja I asiakirjojen käsittelystä valtion virastoissa ja laitoksista toimivissa viranomaisissa ja muissa valtion viranomaisissa. Kansallinen turvallisuusviranomainen painottaa, että täsmälliset velvoitteet sisältävän asetuksen on tultava lain kanssa voimaan heti samaan aikaan, sillä muutoin riskinä on, että kahdenvälisten tietoturvallisuussopimusten nojalla Suomen saamat turvallisuusluokitellut tiedot (tasoilla CONFIDENTIAL, SECRET, TOP SECRET) jäävät ilman lainsäädännöllistä suojaa, ja josta seikkatilasta Suomi joutuisi ilmoittamaan sopimusosapuolilleen.

Kansallinen turvallisuusviranomainen huomauttaa erityisesti, että ehdotettu tietoturvallisuuden perustaso, jonka ehdotetaan riittävän myös turvallisuusluokan IV KÄYTTÖ RAJOITETTU käsittelyyn, on matalammalla tasolla kuin esimerkiksi Euroopan Unionin vaatimukset RESTREINT UE/EU RESTRICTED -tason asiakirjoille. Näin ollen Euroopan Unionin turvallisuusluokiteltuja asiakirjoja ei olisi mahdollista käsitellä esimerkiksi tietojärjestelmissä, jotka täyttävät vain perustason vaatimukset. Käytännössä siis kansalliselle KÄYTTÖ RAJOITETTU -luokitellulle asiakirjalle annettaisiin heikompi suoja kuin sitä vastaavalle RESTREINT UE/EU RESTRICTED -tason asiakirjalle.

Lakiehdotuksen 22 §:ssä puhutaan salassapitomerkinnän tai turvallisuusluokitusmerkinnän poistamisesta tai muuttamisesta. Kuitenkaan itse pykälän teksti ottaa kantaa ainoastaan turvallisuusluokitusmerkintään (samoin kuin turvallisuusluokitusta koskeva 4 luku).

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

-

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

-

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

-

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:

Lakiehdotuksen 19 §:ssä laajennetaan turvallisuusluokiteltavien tietokategorioiden alaa, jonka lisäksi turvallisuusluokittelua koskeva kyseinen pykälä on nyt kirjoitettu velvoittavaan ”on turvallisuusluokiteltava” –muotoon. Käytännön soveltamisongelmaksi saattaa muodostua se, että jos esimerkiksi poliisin asiakirjat (JulkL 24 § 1 mom 5-kohta) olisi jatkossa pakko turvallisuusluokitella, tulevat ne kansainvälisen tiedonvaihdon näkökulmasta Suomen solmimien kahdenvälisten tietoturvallisuussopimusten (General Security Agreement, GSA) soveltamisalan piiriin. Tällöin niiden sähköinen siirtäminen sopimuspuolten välillä on mahdollista toteuttaa ainoastaan sopimusosapuolten toimivaltaisten viranomaisten keskenään erikseen sopimien järjestelyjen välityksellä. Tällaisia sähköisiä sopimusosapuolten välillä sovittuja kanavia on toistaiseksi käytössä vain muutamia, joka saattaa aiheutua tiedonsiirron nopeuden kannalta huomattavaksi ongelmaksi, mikäli esimerkiksi poliisin asiakirjat olisi jatkossa aina turvallisuusluokiteltu.

Kansallinen turvallisuusviranomainen painottaa asetuksen antamista turvallisuusluokkien III-I asiakirjojen käsittelystä, sekä korostaa, että asetuksen on erityisen tärkeää tulla voimaan samaan aikaan tiedonhallintalain kanssa. Kun voimassa oleva valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) kumoutuisi käsillä olevan lakiuudistuksen myötä, tarvitaan samalla hetkellä voimaan nykyisen tietoturvallisuusasetuksen kattamat säännökset em. turvallisuusluokkien käsittelystä. Mikäli asetus ei tulisi voimaan, tilanne olisi epätyydyttävä Suomen solmimien kahdenvälisten tie-toturvallisuussopimusten (General Security Agreement, GSA) kannalta, sillä niissä on sovittu, että sopimuskumppanivaltion turvallisuusluokiteltuja asiakirjoja käsitellään Suomessa samalla tavalla kuin suomalaisia vastaavantasoisia turvallisuusluokiteltuja asiakirjoja.

Järvenpää Jesse
Kansallinen turvallisuusviranomainen - Kansallinen turvallisuusviranomainen (NSA)