Tietojärjestelmien tarkastus ja valvonta ry

Lausunto

06.09.2021

Asia: VN/4400/2021

Arviomuistio julkisen hallinnon tietojärjestelmiä koskevan sääntelyn kehittämistarpeista

Lausuntonne arviomuistiosta

1. Kommenttinne arviomuistiossa tehdystä nykytilan kuvauksesta

Nykytilakuvaus ("johdanto") luo hyvän pohjakuvauksen tarpeesta ja merkittävistä syistä itse työlle. Lukijan sekä asiantuntijiden näkökulmasta johdanto ei kuitenkaan selvästi tuo esille mitkä ovat ne konkreettiset syyt tai tavoitteet nykytilan muutokselle. Esimerkkinä tästä on mm. "Osa sääntelystä on uutta ja osa kymmeniä vuosia vanhaa" joka vaatisi selkeät esimerkit sekä vaikutukset mitä esimerkiksi kymmenen vuotta vanhat sääntelyt aiheuttavat. Asiantunitjoille vanhentunut lainsäädäntö sekä muuttunut maailma on selkeää, mutta yhtälössä on monta päättäjää joille nämä asiat eivät ole arkipäivää.

Johdannon loppupuolelle on lisäksi "...kiinteästi tietosuoja-asetuksessa tarkoitetun automatisoidun päätöksenteon...". Mikäli käsitellään vain tietosuojakokonaisuutta jää tavoitteellisesti lausunto tyngäksi. Tietoturvan kokonaisuuden huomioiminen yhdessä tietosuojan näkölulman kannalta olisi pitkäjänteisempää ja merkityksellisempää tavoitteiden kannalta, koska hyvää tietosuojaa ei saavuteta ilman pohjalla olevaa hyvää tietoturvaa. Näitä kahta ei tule sekoittaa toisiinsa, mutta ei myöskään arvioida erikseen, sillä muuten tietosuojan näkökulma jää juridiseksi näkökulmaksi eikä täten vastaa tietosuojan ylläpidon haasteisiin joita tietoturvamekanismit tukevat.

2. Kommenttinne tietojärjestelmistä sääntelykohteena

Kohta on pääosin selkeä ja nostaa esille mm. koko tietojärjestelmä-termin ongelmallisuuden. Tietojärjestelmät tulkitaan turhan usein vain IT eli ns. ATK-laitteiksi, vaikka tänä päivänä tietojärjestelmistä puhuttaessa merkittävän tulevaisuuden vektorin luovat myös erilaiset (äly)laitteet sekä ns. IOT-laitteet. Kappaleessa merkittävä kohta onkin sivulla 16 kohta "Tietojärjestelmiin kohdistuvaa sääntelyä voidaan lähestyä ainakin seuraavista näkökulmista", joka tuo merkityksen esille eli kattavuuden lähes kaikkeen mitä yritykset ja hallinnonalat tänä päivänä tekevät.

Täydennystä ja konkretisointia vaatisi se, että lähes kaikki laitteet (jotka ovat verkotettuna, oli kyseessä sitten tuottava teollisuus taikka terveydenhuolto) tulisi olla tietojärjestelmien sääntelyn alaisuudesta toimialasta taikka laitteen käyttötarkoituksesta riippumatta.

Tietojärjestelmä itsessään liittyy aina johonkin viranomaisen tai yhteisön tuottamaan toimintoon, eikä itse teknistä toteutusta (tietojärjestelmä) tule suoraan lakien kautta säätä. Teknologinen kehitys on huomattavan nopeaa, eikä lainsäädännöllä pystytä vastaavaan sen alati muuttuvaan kenttään. Lainsäädännön tulee luoda puitteet ja velvoitteet, joiden mukaisesti viranomainen toimii, toimintaansa tukevilla tietojärjestelmillä.

3. Millaisia yleisiä vaatimuksia tietojärjestelmien toiminnallisuuksille pitäisi lainsäädännöllä asettaa?

Tämän päivän tietojärjestelmien monimuotoisuus, sisältöpitoisuus ja muuttavat käyttötarkoitukset lisäävät ennakkovastuita ja vaatimuksia niin omistajalle/tilaajalle kuin myös palvelun toimittajalle/ylläpitäjälle/kehittäjälle. Nämä mahdollisuudet ja vastuut tulisi osaltaan koskea myös tietosuoja- ja tietoturvavaatimuksia.

Toiminnallisesta näkökulmasta tietojärjestelmille tulisi pystyä vaatimaan paremmat lähtökohdat tulevaisuuden muutoksille ja kehityksille. Toiminnallisesti yhteiskunnallinen yhteentoimivuus, luotettavasti tiedon siirtäminen (myös turvaluokitellun tiedon) kuin myös ylläpidollisen sitoutumattomuuden pitäisi olla johdetumpaa. vaatimustenmukaisuudella pystytään saavuttamaan jo tiettyjä kokonaisuuksia, mutta käytännöntasolla toiminnassa on vielä merkittäviä heikkouksia. Toiminnallisia vaatimuksia käsitellään liiankin toimintolähtöisesti, ei strategisesti tai mukautuvasti. Tämä näkyy erityisesti kun puhutaan yhteiskunnallisesti kriittisten järjestelmien yhteentoimivuuden näkökulmasta (joka peilautuu myös heikkona tietoturvana ja vaihtelevina käytäntöinä).

Lainsäädännöllä tulee ohjata tietojärjestelmien elinkaarenhallintaa ja määritellä vaatimukset hyvälle tiedonhallintatavalle. Lainsäädännön keinoin vahvistetaan tietojärjestelmien toimintaympäristön ja tiedon hyödyntämisen hallintaympäristöä, ilman että tarpeettomasti rajataan pois teknologian tuomia mahdollisuuksia.

4. Millaisia olennaisia teknisiä vaatimuksia hallintoasioita käsitteleville tietojärjestelmille pitäisi lainsäädännöllä säätää?

Tietojärjestelmiä tai niissä hyödynnettäviä teknologioita ei ole syytä säätää teknisiä vaatimuksia. Lainsäädännön tulee kohdistua tiedon käyttöön, sekä viranomaisen tuottamien palveluiden tuottamiseen. Lainsäädännöllä tulee säätää tiedon- ,sekä tietojärjestelmän elinkaarenhallinnan vaatimukset, jotka pohjautuvat olemassa oleviin ja tunnettuihin kansainvälisiin standardeihin.

Järjestelmien tulisi kasvavassa määrässä hyödyntää esimerkiksi pilvipalveluiden mahdollisuuksia niin lainsäädännön kautta kuin myös prosessien toiminnan näkökulmasta. Koska muutokset toimintaympäristöissä tapahtuvat entistäkin tietojärjestelmä lähtöisesti, on huomioitava että mikä tänään on uutta, on kohta jo vanhentunut. Kansallisesti kriittisten järjestelmien kehitys "kotikutoisesti" ei ole kustannustehokasta ja pyörää ei kannata keksiä uusiksi. Merkittävää onkin varhaisen vaiheen riskienhallinnalliset menetelmät ja balansointi sekä mekanismien rakentaminen jolla a) palveluissa voidaan turvallisesti käsitellä kriittistä informaatiota ja b) vastuut on muutenkin kuin paperilla määritelty.

Ns. toimitusketjujen (lue: IT-kumppanit / vast.) vastuita tulisi kasvattaa kokonaisuudessa ja heiltä tulisi kriittisten järjestelmien osalta vaati laadukkaampaa tietoturvaa/-suojaa. Tekniset vaatimukset koskevat valitettavan usein minimitasoa ja tietoturva/-suoja on kohta jossa leikataan liikaakin tai

oletetaan sen olevan hyvällä tasolla. Auditointi ei ole ratkaisu vaan vain yksi mekanismeista. Sen sijaan kontrollikehys tulisi rakentua aina ideoinnista lähtien rampauttamatta toiminnallisia tavoitteita.

Tekoälyn käyttö päätöksenteossa, edellyttää ensin juridisen yhteisymmärryksen, miten kuka vastaa teköälyn tekemistä päätöksistä ja miten se tulee näkyä päätöksessä. Kun tästä on saatu selkeä tulkinta, niin se vasta avaa mahdollisuudet sen hyödyntämiseen.

Automaattisessa päätöksenteossa tehokkaimmin luottamus saavutetaan mahdollisimman läpinäkyvyydellä ja päätöksenteossa käytetyt algoritmit on mahdollista tieteellisin menetelmin tutkia.

5. Millaisia vaatimuksia, kuten dokumentointivaatimuksia, tietojärjestelmien kehittämiselle pitäisi lainsäädännöllä säätää?

Dokumentaation osalta Suomessa on vielä liiaksi vaatimuksena vain Suomeksi dokumentointi. Tällöin terminologia saattaa poiketa alan standardeista tai dokumentaatiossa uusille teknologioille käytetään soveltuvia termejä. Tämän kaltaiset käytännöt saattavat heikentää ylläpidettävyyttä, kestävyyttä ja ongelmanratkaisua tietojärjestelmän elinkaaren aikana. Erityisesti ongelmia syntyy, jos kumppanit vaihtuvat tietojärjestelmän elinkaaren vaiheissa. Näiden epäselvyyksien kustannusvaikutukset saattavat tuntua ajanhetkellä pieniltä, mutta kasaantumisen vaikutuksesta muuttuvat merkittäviksi. Siksi suotavaa olisikin vaati myös englanniksi olevaa dokumentaatiota (tai jopa vain englanniksi olevaa dokumentaatiota), joka mahdollistaisi laajemmat mahdollisuudet käyttää kansainvälisiä resursseja vastaamaan jo näkyvään resurssiongelmaan mikä alaa koskee.

Toinen merkittävä asia on dokumentaation laatu ja ylläpito mitä tulee kumppaneille asetettaviin vaatimuksiin. Dokumentaatio vaaditaan sopimusteknisesti, jolloin sen vaatimukset laaditaan yleisellä tasolla ja tulkintojen takia siihen ei ole resursoitu/budjetoitu riittävästi resursseja. Tilaajien tulee vaatia dokumentaatiolta hyvä laatua ja tarkoituksenmukaista laajuutta.

6. Miten lainsäädännöllä tulisi varmistua virkavastuun toteutumisesta ja kohdistumisesta, mitä tulee tietojärjestelmien kehittämiseen, käyttöönottoon ja käyttöön, sekä tietovarantojen käyttöön?

Kehittämisen osalta tulisi vaatia myös aiempaa kattavampia tietoturvatoimia. Nykyiset auditoinnit eivät annan todellista kuvaa, ja ns. SDLC/DevSecOps eli kehityksen aikana tapahtuva tietoturvavarmistus on matalalla tasolla. Toimittajilta vaaditaan tietoturvatoimia, mutta näiden toteutuminen ja valvonta on vielä todella vaihtelevalla tasolla. Syitä on mm. resurssipula, osaamattomuus ja epätieto/luotto kumppanin toimiin.

7. Mitä edellytyksiä tietovarannoille, niiden laadulle tai niiden käytölle tulisi lainsäädännössä asettaa, jotta niitä voidaan käyttää osin tai täysin automaattisessa päätöksenteossa?

Turvallisen kehittämisen onnistumisen kannalta vastuuta tulisi olla niin tilaajalla kuin myös kumppanilla joka toteuttaa. Mikäli jompikumpi tahoista karsii kustannussäästösyistä tietoturva/-suoja asioista pitäisi sanktiot/vaikutukset olla nykyistä merkittävämmät.

Tietovarastojen osalta tulisi edellyttää reaaliaikaista tiedon käyttöä nykyisen massakopioinnin sijaan. Tietovaranto toteuttaa tiedon suojaamisen tarkoituksenmukaisella ja tehokkaalla tavalla, jota ei ole mahdollista toteuttaa tiedon hyödyntäjän toimesta. Tiedon laatu myös heikkenee kopioinnissa, eikä tiedon päivitykset välttämättä siirry eri kopioihin.

Tietovarastojen tuottamiseen tai hyödyntämiseen osallistuu myös julkishallinnon ulkopuolisia tahoja, joten omistajuus tulee säilyttää virkavastuulla toimivalla taholla.

Kuten aiemmissa kohdissa jo kommentoitu, laatu ja käytettävyys lähtee jo alkuvaiheen huomioimisesta ja suunnitelmista. Käyttöä tulisi harkita laajemmassa kuin vain oman organisaation kontekstissa, sillä yhteiskunnallinen yhteentoimivuus ja luotettavuus on digitalisoituvassa yhteiskunnassa menestystekijä. Mikäli päätöksiä halutaan automatisoida täysin, on luottamus laatuun oltava merkittävä. Se asettaa reunaehtoja niin teknisesti kuin myös hallinnollisesti. Tietovarantojen vaikeus on niiden monimuotoisuus, jotta automatisointia tai yhteiskäyttöä voisi harkita. Lainsäädännöllisesti tämä voisi tarkoittaa yhtenäistä linjausta tietoaineiston muodosta, tasosta jne. jolla voi olla merkittäviä kustannusvaikutuksia varsinkin ns. legacy-järjestelmät huomioiden.

Tämä kohta saattaa muodostua erittäin haastavaksi vaikka ja siirtymäaika voi olla merkittävä.

8. Miten tietoturvallisuuden arviointia ja arviointijärjestelmää koskevaa lainsäädäntöä tulisi kehittää? Entä erityisesti viranomaisten tietojärjestelmien arvioinnin osalta?

Aiemmissa kohdissa tätä jo kommentoitu laajasti, mutta ns. audit-lähtöinen varmistus ei vastaa enää tämän päivän haasteisiin. Tarkastuksia tullaan tarvitsemaan jatkossakin, mutta ns. kontrollien kautta tehtävä arviointi ei kykene tuottamaan luotettavaa kuvaa kontrollien tehokkuudesta. Tietoturvaa tulisi arvioida ja testata jatkuvasti niin järjestelmänäkökulmasta kuin myös organisaation hallinnollisesta näkökulmasta (=miten johdetaan ja valvotaan, mitataan ja kehitetään). Tarkastus tulee olla yhdenmukaista ja sen tulee kattaa laajasti järjestelmän kyseisen elinkaarivaiheen hallinnan ja teknologian toteutus.

Lisähuomiona tulisi tunnistaa myös toimitusketjujen vastuu. Nykyisellään tarkastukset ovat suhteellisen vähäisiä tai läpinäkymättömiä järjestelmän omistajan suuntaan mitä tulee kumppaneiden vastuisiin. Tekemättä jääneet tietoturvatehtävät tulevat esille vasta ongelmien noustessa esiin, kumppania vaihdettaessa tai hyökkäysten/tietomurtojen tutkinnan yhteydessä. Yhteiskunnallisesti luotetaan liiaksi tilanne raportteihin ja oletuksiin, mutta kattavaa ja tehokasta testausta tulisi vaatia enemmän kumppaneilta. Kumppaneiden tulisi kehityksen aikana toteuttaa tietoturvatyötä ja monitorointia. Eri yhteisöissä tästä on keskusteltu ja esille on nostettu mm. minimibudjettiosa mikä tulisi asettaa tietoturvalle kehitystyössä, joka ei ole liitetty osaksi muuta kustannusta vaan sen pitäisi kohdistua suoraan tietoturva-/tietosuojatyölle osana tietojärjestelmä kehitystä (ja kumppaneilta vaaditaan läpinäkyvyys tähän).

9. Kommenttinne muistiossa todetuista sääntelytarpeista yleensä

Arviointimuistiossa on käytetty pääsääntöisesti tietosuojaa esimerkkinä, johtuen sen asemasta julkishallinnon tehtävissä. Tietosuojalle on olemassa selkeät vaatimukset, joiden toteuttaminen tuottaa yhtenevän ja johdonmukaisen kontrolliympäristön. Tietosuoja on kuitenkin vain yksi tietotyyppi ja vastaavat kontrollit tulee toteuttaa myös muita salassa pidettävän tai turvaluokitellun tiedon hallinnassa. Tämän vuoksi tulisi hyödyntää lähtökohtaisesti yhtenäistä julkishallinnon tietohallintokehystä, jossa hyödynnetään sovelutuvia kansainvälisiä standardeja luomaan auditoitavan toimintaympäristön, joka vastaa eri toimijoiden vaatimuksia ja tukee tiedon hyödyntämisen esteettömyyttä.

Arviointimuistiossa tulee tuoda laajemmin esiin soveltuvia kansainvälisiä standardeja, joiden hyödyntäminen luo tiedonkäsittelyn eri osapuolien välille yhtenäisen tiedonhallintakontrollit.

10. Muut yleiset kommentit arviomuistiosta

Tietojärjestelmien tarkastus ja valvonta ry toimii ISACAn paikallisena Chapterina Suomessa. ISACA ylläpitää useita ammattiosaamista osoittavia henkilösertifikaatteja ja CobIT hallintakehystä. Yhdistyksen jäsenet työskentelevät johtamisen, tietoturvajohtamisen, tarkastuksen ja riskienhallinnan tehtävissä.

Arviomuistiossa käsitellään asiaa laajasti ja useasta näkökulmasta, joka tuottaa huomattavasti paremman kuvan, kuin tavanomainen fokusoitunut tarkastelu. Tällöin hallintakehyksen sekä kansainvälisten standardien merkitys osana julkishallinnon tietojärjestelmäkokonaisuuksien hallintaa kasvaa. Arviointimuistio osoittaa, että käsiteltävä aihe on laaja ja muutokset tulee käsitellä riippuvuuksien vuoksi yhtenä laajana kokonaisuutena.

Tietojärjestelmien tarkastus ja valvonta ry

Lisätietoja antaa:

Pasi Korhonen, puheenjohtaja

pasi.korhonen@isaca.fi

+358 40 591 6497

Korhonen Pasi
Tietojärjestelmien tarkastus ja valvonta ry - Tietojärjestelmien tarkastus ja valvonta ry