

kirjaamo@lvm.fi

tuomas.kaivola@lvm.fi

Asiantuntijalausunto asetus muiden kuin henkilötietojen vapaan liikkuvuuden kehityksestä Euroopan unionissa - vaikutukset Suomessa

Viite: LVM071:00/2018, LVM/1731/03/2018

Kuntaliitto kiittää mahdollisuudesta lausua tietojen vapaan liikkuvuuden kehityksestä Euroopan unionissa ja mitä vaikutuksia sillä on Suomessa. Kuntaliitto on pyytänyt omien asiantuntijoiden lisäksi muutamien kuntien vastuuhenkilöiden näkemyksiä kyseisestä asetuksesta.

Kysymys 1. Onko teillä tiedossa Suomessa olevia tietojen sijaintia koskevia vaatimuksia ja mitkä ne ovat?

Valtiovarainministeriö on 18.1.2019 julkaissut ”Julkisen hallinnon pilvipalvelulinjaukset” (VM julkaisu 35/2018). Myös Kuntaliitto oli mukana työryhmässä, missä nämä linjaukset laadittiin. Raportti sisältää seitsemän pilvipalvelulinjausta sekä suosituksia jatkotoimenpiteiksi. Kunnat ovat tekemässä politiikkoja ja ohjeistuksia tietoturva ja -suoja sekä riskien arviointiin liittyen pilvipalveluiden käyttöönottoon käyttäen apuna muun muassa näitä linjauksia. Muutamilla kunnilla on jo kirjattuja linjauksia, joissa määritellään tiettyjen tietojärjestelmien sijoittamista vain Suomeen. Pilviratkaisujen käyttäminen on selvästi lisääntymässä.

Kysymys 2. Onko teillä tietoa näiden vaatimusten myönteisistä ja kielteisistä vaikutuksista ja onko rajoitus mielestänne perusteltu?

Valtiovarainministeriön linjausraportti on niin tuore, ettei siitä ole kertynyt vielä kokemusta. Yleisesti kunnissa pidetään hyvänä asiana, että tietojen sijaintia ja hallintaa liittyviä asioita linjataan julkishallinnolla yhteisesti. Tarve yhteisiin linjauksiin ja toimintamalleihin on tunnustettu, mutta ne eivät ole vielä toteutuksessa. Vaikutusten arviointi on haasteellista, koska julkishallinnon käytänteet ja kypsyystaso ovat erilaiset. Muun muassa sähköisen asioinnin palveluiden kannalta oleellinen tieto on hajautunutta.

Rajoitukset sijaintia koskevista vaatimuksista sähköisessä muodossa olevalle muulle kuin henkilötiedolle eivät ole kaikilta osin perusteltuja. Lähtökohtaisesti rajaava tekijä pilvipalveluiden ja tietojen sijainnille ei nimenomaan ole henkilötiedot vaan tietojärjestelmien **kriittisyys, vaikuttavuus sekä niiden sidokset palvelun jatkuvuuteen, käytettävyyteen, saatavuuteen, turvallisuuteen ja valmiuslain mukaisiin vaatimuksiin**. Vastuu tietoturvasta on riippuvainen toteutetusta palvelumallista ja toteutustavasta. Riskipohjaisen arvioinnin kannalta pilvipalveluissa hyödynnettävät teknologiat ja palveluntuotantoratkaisut eroavat oman toimintaympäristön suljetuista toteutuksista. Riskit ovat erilaisia ja osittain riippuvaisia toimintaympäristöstä. Riskienhallinnassa asioita tarkastellaan organisaation kannalta kokonaisuutena.

Esimerkiksi riskienhallintamielessä on nykypäivänä hyvinkin mahdollista se, että Suomen ulkomaanyhteydet katkeavat (esim. Itämeren kaapelit katkaistaan terroristien tai jonkun valtion toimesta tai vaikka kansainvälinen DNS-järjestelmä pettää) ja jos näin käy, niin tilanteen korjaaminen voi kestää useampia päiviä, vaikka kotimainen liikenne toimisi. Palvelumalleja ja toteutustapoja arvioitaessa on tunnistettava asiakokonaisuuteen liittyvät tiedot, arvioitava toimintojen ja tietojärjestelmien tärkeys ja kriittisyys sekä tunnistettava riippuvuussuhteet muihin organisaation palvelukokonaisuuksiin. **Tämän vuoksi riskienhallinnan kannalta on järkevää, että kaikki ne tietojärjestelmät, jotka eivät kestä parin päivän alhaalla oloa, sijoitetaan nimenomaan Suomeen.** Kriittiset tiedot pitää olla tallessa, saatavilla ja hallittavissa tilanteessa kuin tilanteessa.

Yleinen turvallisuus ei ole riittävä kriteeri

Eli pelkkä ”yleinen turvallisuus” ei ole riittävä ja ainoa kriteeri, millä järjestelmät voitaisiin sijoittaa Suomeen. Näitä muita kriteereitä voivat olla esimerkiksi tärkeät/kriittiset tekijät, huoltovarmuus (esim. liikenne, energia, vesihuolto) ja metatiedot (niiden hyödyntäminen mm. käyttövaltuus-hallintaratkaisuihin). Jos esimerkiksi järjestelmän alhaalla olo aiheuttaa merkittäviä kustannuksia (vaikka miljoonia muutamassa päivässä) tai jos joku muu yhteiskunnan elintärkeä toiminto jää hoitamatta). Terminä yleinen turvallisuus on aika laava, eli sen tarkempi määrittely on tärkeää, tarkoittaako se spesifisti tietojärjestelmää vai myös siihen liittyviä järjestelmiä tai komponentteja.

Kunnissa on vanhoja tietojärjestelmiä, joiden toiminnallisuudet edellyttävät tietoliikenneyhteyksiltä pieniä viiveitä. Palvelumalliltaan ja toimintatavoiltaan nämä toimivat optimoidusti paikallisissa toimintaympäristöissä. Tämän vuoksi kyseiset tietojärjestelmät on ollut pakko sijoittaa omiin konesaleihin, koska ne eivät yksinkertaisesti toimi muualla olevista konesaleista käsin. Teknisten ratkaisujen ja kokonaisuuden kannalta on tarve huomioida ja arvioida tiedon sijainti. Kuten myös uusien teknologioiden (esim. 5G-pohjaiset toteutukset) mukanaan tuomat vaatimukset niin verkkotopologian kuin tarvittavan tiedon lähteittenkin kannalta. Smart City ja Smart Village - pohjaisten tulokulmien kannalta yhteiskunta on vasta hahmottamassa näitten edellyttämiä rakenteellisia muutoksia ja tiedonsiirron kriittisiä vaatimuksia (latenssi, viive) toteutettaville palveluille ja toiminnoille (esim. liikenne, energia).

Mikäli järjestelmä on herkkä tietoliikenteen viiveille tai järjestelmä jatkuvasti tai hetkellisesti tuottaisi ison datamäärän, on järkevintä toteutuksen kannalta sekä kustannus- tehokkuus huomioiden tallentaa data paikallisesti. Esimerkkinä isosta datamäärästä ja sen paikallisesta tallentamisesta on ison kiinteistön kameravalvonta. Useista kymmenistä tarkoista kameroista syntyy paljon dataa, jota on tarve säilyttää jonkin aikaa. Tätä datamäärää ei ole kaikissa tapauksissa järkevää siirtää ulkomaille, jolloin se veisi merkittävästi kaistaa ensin kiinteistön omasta dataliittymästä ja lisäksi vielä organisaation internet- ja ulkomaankaistasta. Nykyään, kun tallennuslevyt ovat aika edullisia, on tuon datan säilyttäminen kiinteistössä paikallisilla kameratallentimilla kokonaisuuden kannalta usein edullisinta.

Tiedon fyysinen sijainti ei ole itseisarvo

Toinen näkökulma liittyy tiedon fyysiseen sijaintiin. Asetuksen mukaan (4) ”asetuksella ei rajoiteta millään tavalla yritysten vapautta tehdä sopimuksia siitä, missä tietoja säilytetään”. Asetuksella on tarkoitus ainoastaan **suojata** kyseistä vapautta varmistamalla, että säilytyspaikaksi voidaan sopia mikä tahansa paikka unionissa.” Pyrkimyksenä ei siis ole rajoittaa käyttäjäorganisaatioitten lähtökohtia tarkoituksenmukaisten tiedonhallintaratkaisujen toteuttamiseksi. Tämä toki edellyttää riittävää kypsyystasoa ja riskilähtöisyyttä, mikä näkyy muun muassa kehittämisessä, päätöksenteossa ja johtamisessa. Käyttäjäorganisaatio vastaa aina omista tiedoistaan ja niiden oikeellisuudesta - tämä korostuu julkishallinnossa. Sinälläänhan asetus ei keskity tiedon fyysiseen säilytyspaikkaan ... vaan poistamaan rajoitukset (myös kansalliset) markkinatoimijoiden ja palveluntarjoajien tarjoamien ratkaisujen kannalta.

Säilytyspaikka ei sinällään tuo lisäarvoa tiedon vapaalle liikkuvuudelle, jos fyysinen säilytysympäristö- ja paikka tarjoaa tietoihin pääsyn ja mahdollisuuden käsitellä sitä ”automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, **tallentamista**, järjestämistä, jäsentämistä, **säilyttämistä**, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla se muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista tai tuhoamista.” Fyysinen ydintiedon säilytyspaikkaa koskeva asia on vain tallentaminen ja säilyttäminen ja silloinkaan ydintiedon säilytyspaikan rajaaminen ei ole este tiedon hyödyntämiselle toisaalle esim. EU-alueella. Tiedon liikkuvuus ei lähtökohtaisesti edellytä fyysisen sijoituspaikan pakottamista vapaaksi toisin kuin esim. työvoiman liikkuvuus ns. tuotantoaloilla. Se, että tieto tallennetaan EU-alueella ei takaa sen liikkuvuutta.

Kommenttina lausuntopyynnössä olevaan lauseeseen ”Tämän lisäksi asetusta ei sovelleta kansallista turvallisuutta koskeviin tietoihin, eikä tietojenkäsittelyyn, joka tapahtuu julkisen sektorin sisällä ilman maksettua korvauksia yksityisille osapuolille”. Tarkoittaako kyseinen lause sitä, tietojenkäsittely, mitä tehdään kunnassa ilman kaupallisia sovelluksia ja järjestelmiä (koskeeko myös konesalikapasiteettia) ei ole asetuksen piirissä. Eli jos kunta tekee kaikki sovellukset inhouse- toteutuksina niin asetus ei koske niissä olevaa dataa missään muodossa. Näin ollen tämä voi johtaa siihen, että EU-alueella julkinen sektori rakentaa ja investoi tietojärjestelmiä ja päällekkäisyyksiä vain sen takia, että tieto ”pidetään fyysisesti lähellä”.

Kysymys nro 3. Onko teillä muita huomioita, jotka haluaisitte saattaa työryhmän tietoon?

Lopuksi Kuntaliitto haluaa tuoda työryhmän tietoon seuraavat kommentit koskien asetuksen artikloita 4 ja 6.

4. artikla (Tietojen vapaa liikkuvuus unionissa)

3. Jäsenvaltioiden on viimeistään 30 päivänä toukokuuta 2021 varmistettava, ... vastaiset tietojen sijaintia koskevat vaatimukset kumotaan.

... toimenpide on tämän artiklan 1 kohdan mukainen ja voi näin ollen pysyä voimassa, sen on viimeistään 30 päivänä toukokuuta 2021 tiedotettava kyseisestä toimenpiteestä komissiolle ja esitettävä perustelut sen voimassa pitämiseksi.”

Tästä asiasta olisi hyvä käydä laajapohjainen keskustelu, jotta kansalliset tarpeet ja näkökulmat erityisesti julkishallinnosta tulee huomioitua.

4. Jäsenvaltioiden on asetettava yksityiskohtaiset tiedot kaikista alueellaan sovellettavista laeissa, asetuksissa tai yleisluonteisissa hallinnollisissa määräyksissä säädetyistä tietojen sijaintia koskevista vaatimuksista julkisesti saataville kansallisen keskitetyn verkko-tietopisteen kautta ja pidettävä nämä tiedot ajan tasalla tai toimitettava ajan tasalle saatetut tiedot kaikista tällaisista sijaintia koskevista vaatimuksista jollakin toisella unionin säädöksellä perustetulle yhteiselle tietopisteelle."

Yllä oleva vaatimus kaipaa tarkennusta toteutustavasta ja vastuutahosta. Tarkoittaako tämä sitä, että kootut tiedot tulisi huomioida hankintoja ja kilpailutuksia toteutettaessa ja kansallisten hankkeiden kannalta. Edellytetäänkö esimerkiksi kuntia päivittämään muuttuvien käytäntöjensä kautta tiedot kansalliseen keskitettyyn verkkopisteeseen, vai raportoimaan nimetyn viranomaisen kautta (vrt. NIS-direktiivin soveltaminen). On syytä huomioida, että julkishallinnon toimijoiden lukumäärä on yli 500. Lisäksi käynnissä on hankkeita koskien muun muassa alustataloutta ja ekosysteemeitä. Ne merkitsevät muutoksia toimintaympäristöjen rakenteisiin ja toimintatapoihin.

6. artikla (Tietojen siirtäminen)


"2. Komissio varmistaa, että käytännesäännöt laaditaan tiiviissä yhteistyössä kaikkien asiaankuuluvien sidosryhmien, myös pk-yritysten sekä startup-yritysten järjestöjen, käyttäjien ja pilvipalvelujen tarjoajien kanssa"

Myös tätä kohtaa on tarpeellista avata käytännössä. Onko tavoitteena tehdä ohjeistusta EU-laajuisesti, kansallisesti ja miten huomioidaan eri toimintaympäristöjen erityisesti julkishallinnon erilaiset tarpeet, toimintatavat ja kypsyystasot. On huolehdittava vastuiden määrittelystä ja ohjauksesta, jotta kokonaisuuden johtaminen on mahdollista.

Lisätietoja: erityisasiantuntija Tuula Seppo, Kuntaliitto, tuula.seppo@kuntaliitto.fi

050-428 82 55

SUOMEN KUNTALIITTO



Tuula Seppo

erityisasiantuntija

JAKELU: Kuntaliiton kirjaamo