Huoltovarmuutta pilvipalveluilla

Liite 3 Juridinen selvitys

Huoltovarmuusorganisaatio

13.2.2023

Pilvipalveluiden juridinen selvitys

Huoltovarmuusorganisaation Digipooli on tilannut FiComilta konsulttityönä pilvipalveluiden juridisen selvityksen osana Pilvipalvelut ja huoltovarmuus -hankettaan.

Sisällys

Koonti havainnoista

Sekä kansallinen että EU-lainsäädäntö asettavat pilvipalveluiden käytölle tiettyjä edellytyksiä, joita valitettavan usein pidetään esteenä pilvipalveluiden hyödyntämiselle. Näitä ovat esimerkiksi yleisen tietosuoja-asetuksen ja muun tietosuojasääntelyn sekä tiettyjen alojen oman säilytettävien tietojen luonteeseen tai vaikkapa tietoturvallisuuteen liittyvän sääntelyn vaatimukset. Myös julkishallinnolle on asetettu esimerkiksi henkilötietoihin ja turvallisuusluokiteltuun tietoon liittyviä omia vaatimuksia, jotka myös julkishallinnolle palveluita tarjoavien yritysten tulee ottaa toiminnassaan huomioon. Sääntelyä on paljon, ja Euroopan unionin alati kehittyvä lainsäädäntö sekä Suomen Nato-jäsenyys lisäävät todennäköisesti myös pilvipalveluiden sääntelyä lähivuosina entisestään.

Pilvipalveluiden käyttö halutaan kuitenkin mahdollistaa, kunhan reunaehdot täyttyvät. Esimerkiksi valtiovarainministeriö on ohjeistuksissaan julkisen hallinnon päätöksentekijöille ja asiantuntijoille suhtautunut pilvipalveluiden käyttöön lähtökohtaisesti myönteisesti. Monissa tilanteissa pilvipalveluiden hyödyt ovat niiden käyttämisestä aiheutuvia velvoitteita suuremmat, ja tietojen hajauttaminen pilveen edistää tietoturvaa.

Pilvipalveluiden käytössä on kuitenkin tärkeää pitää mielessä olemassa oleva säädöskehikko ja seurata sen kehittymistä. Kullakin alalla on omaa erityissääntelyä, jota on mahdoton tässä yleisesityksessä esittää tyhjentävästi. Siksi oman erityisesti oman toimialan sääntelyyn tulee kiinnittää huomiota. Selvityksen tavoitteena on pikemminkin avata pilvipalveluihin liittyvää sääntelyä ja antaa työkaluja yritysten ja julkishallinnon toimijoiden oman toiminnan kannalta relevanttien säännösten ja määräysten tunnistamiseen.

Yleiset lainsäädännön vaatimukset pilvipalveluiden käytölle

Erilaisiin tietoihin kohdistuu erilaisia juridisia velvoitteita, jotka määrittelevät reunaehdot niiden säilyttämiselle. Esimerkiksi henkilötietoja, sähköistä viestintää, maksukorttitietoja ja muita luottamuksellisia tai arkaluonteisia tietoja koskevat merkittävät säilytys- ja turvallisuusvaatimukset. On hyvä huomata, että kaikkiin tietoihin ei kohdistu välttämättä samanlaisia vaatimuksia, mutta kaikkia tietoja voidaan niin halutessa säilyttää yhtä turvallisesti. Lisäksi yrityksen asiakkaiden toimialaan liittyvä lainsäädäntö voi vaikuttaa myös itse yrityksen toimintaan. Kaikella tällä on vaikutusta pilvipalveluiden käyttöön.

Henkilötiedot

Keskeisin pilvipalvelujen käytölle vaatimuksia asettava säädös lienee Euroopan parlamentin ja neuvoston asetus (EU) 679/2016 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/ EY kumoamisesta, joka tunnetaan myös yleisenä tietosuoja-asetuksena (General Data Protection Regulation, GDPR). GDPR:n mukaisesti eurooppalaisten henkilötietojen käsittelyn ja säilyttämisen tulee tapahtua joko Euroopan unionissa tai Euroopan talousalueella (ETA). Euroopan talousalueeseen kuuluvat EU-maiden lisäksi Islanti, Liechtenstein ja Norja. Kun henkilötietoja siirretään Euroopan talousalueen ulkopuolelle, tietosuoja-asetuksen takaama henkilötietojen suojan taso voi heiketä. Asetuksessa on määritelty edellytyksiä henkilötietojen siirrolle, jotta tietosuojan ja tietoturvan riittävästä tasosta voidaan varmistua.

Henkilötietoja ovat yleisen tietosuoja-asetuksen 4(1) artiklan mukaan kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot. Henkilötietojen käsittelyä koskevista periaatteista säännellään asetuksen 5 artiklassa ja turvallisuudesta asetuksen 32 artiklassa. Tietosuoja-asetuksen 35 artiklassa säädetään tilanteista, joissa rekisterinpitäjän tulee tehdä tietosuojaa koskeva vaikutusarviointi. Henkilötietojen siirrosta kolmansiin maihin taas säännellään asetuksen V luvussa, jonka säännöksiä (artiklat 44–50) on sovellettava, jotta varmistetaan, että henkilötietojen suojan tasoa ei vaaranneta. Edellytyksenä on, että henkilötietojen käsittely on sallittua kyseisessä tilanteessa, minkä lisäksi siirrolle on oltava V luvussa määritelty siirtoperuste. Siirtoperusteen tehokkuus ja täydentävien suojatoimien tarve on arvioitava tapauskohtaisesti.[1]

Luvussa V määritellyt siirtoperusteet ovat toisilleen vaihtoehtoisia, joten riittää, että yhden siirtoperusteen edellytykset täyttyvät. Jos minkään siirtoperusteen edellytykset eivät täyty, henkilötietoja ei voida siirtää ETA-alueen ulkopuolelle. Siirtoperusteena voi olla joko

- komission päätös riittävästä tietosuojan tasosta (45 artikla),
- komission hyväksymät vakiolausekkeet (artikla 46:2(c) ja artikla 46:2(d)),
- yritystä koskevat sitovat säännöt (47 artikla),
- hyväksytyt käytännesäännöt (40 artikla ja artikla 46:2(e)) tai
- hyväksytty sertifiointimekanismi (42 artikla ja artikla 46:2(f)) yhdessä sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa,
- viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline (artikla 46:2(a)),
- tietosuojaviranomaisen luvanvaraiset sopimuslausekkeet (artikla 46:3(a)) tai

[1] Henkilötietojen siirrot Euroopan talousalueen ulkopuolelle, Tietosuojavaltuutetun toimisto, https://tietosuoja.fi/henkilotietojen-siirrot-etan-ulkopuolelle, viitattu 13.2.2023.

- viranomaisten tai julkisten elinten välisiin hallinnollisiin järjestelyihin sisältyvät säännökset (artikla 46:3(b)).

Lisäksi luvussa säännellään erityistilanteita koskevista poikkeuksista (49 artikla). Siirtoperusteita sovelletaan sekä rekisterinpitäjään että henkilötietojen käsittelijään, joiden keskinäisestä suhteesta säännellään tietosuoja-asetuksen 28 artiklassa.

Edellytys siirtoperusteesta on muodostunut ongelmaksi erityisesti tietoja Yhdysvaltoihin siirrettäessä. Euroopan unionin tuomioistuimen 16.7.2020 antamalla niin sanotulla Schrems II -tuomiolla (C-311/18) on ollut merkittäviä vaikutuksia ETA-alueen ulkopuolelle tehtäviin henkilötietojen siirtoihin. Tuomiossa täsmennettiin kansainvälisten henkilötietojen siirtojen edellytyksiä, joiden on täytyttävä, jotta henkilötietoja voidaan laillisesti siirtää Euroopan talousalueelta kolmanteen maahan tai kansainväliseen organisaatioon.

Schrems II -ratkaisussa tuomioistuin otti kantaa esimerkiksi Euroopan komission päätöksessään 2010/87/EU vahvistamien vakiolausekkeiden käyttöön tiedonsiirron perusteena. Tuomiossa korostetaan, että rekisterinpitäjien ja henkilötietojen käsittelijöiden on arvioitava tarvetta vakiolausekkeita ja muita tiedonsiirtoperusteita täydentäville suojatoimenpiteille varmistaakseen, että EU:n vaatimuksia vastaavaa tietosuojan tasoa noudatetaan. Tuomioistuin tarkasteli myös ns. Privacy Shield -päätöksen (EU:n ja Yhdysvaltojen välisen Privacy Shield-järjestelyn tarjoaman tietosuojan tason riittävyyttä koskeva päätös 2016/1250) pätevyyttä. Se totesi päätöksen pätemättömäksi, koska tietojen siirtäminen kolmanteen maahan merkitsee merkittävää puuttumista niiden henkilöiden perusoikeuksiin, joiden tietoja siirretään. Taustalla päätöksessä oli Yhdysvaltojen kansallisen lainsäädännön vaatimukset (ulkomaantiedustelun valvonnasta annetun lain [Foreign Intelligence Surveillance Act, FISA] 702 § ja toimeenpanoasetus E.O. 12333) sekä erityisesti tietyt ohjelmat, joiden perusteella Yhdysvaltojen viranomaiset voivat saada käyttöönsä EU:sta Yhdysvaltoihin siirrettyjä henkilötietoja kansalliseen turvallisuuteen liittyviin tarkoituksiin. Nämä vaatimukset koskevat myös yhdysvaltalaisten yritysten pilvipalveluihin siirrettyjä suomalaisten henkilötietoja. [2]

Schrems II -ratkaisun myötä rekisterinpitäjien ja henkilötietojen käsittelijöiden on arvioitava, onko vakiolausekkeita ja muita tiedonsiirtoperusteita täydentäville suojatoimenpiteille tarvetta sen varmistamiseksi, että EU:n vaatimuksia vastaavaa tietosuojan tasoa noudatetaan. Yhdysvaltain presidentti Joe Biden on allekirjoittanut 7.10.2022 uuden transatlanttista datansiirtoa koskevan asetuksen, joka on paraikaa EU:n käsittelyssä. Euroopan komissio julkaisi 13.12.2022 päätösluonnoksen Yhdysvaltojen tietosuojan tason riittävyydestä, joka toimitettiin Euroopan tietosuojaneuvoston arvioitavaksi. Tietosuojaneuvoston arvioinnin jälkeen jäsenmaat ja parlamentti antavat omat näkemyksensä. Tämän jälkeen komissio voi tehdä lopullisen päätöksen tietosuojan riittävyydestä.[3] On kuitenkin erittäin todennäköistä, että myös tästä uudesta datansiirtojärjestelmästä tullaan valittamaan Euroopan unionin tuomioistuimeen ja epävarmuus jatkuu.

[2] Tiedonsiirtovälineitä täydentävät suojatoimet, Tietosuojavaltuutetun toimisto, https://tietosuoja.fi/tiedonsiirtovalineita-taydentavat-suojatoimet, sekä Usein esitettyjä kysymyksiä, jotka koskevat Euroopan unionin tuomioistuimen tuomiota asiassa C311/18 Data Protection Commissioner vastaan Facebook Ireland Ltd ja Maximillian Schrems, Euroopan tietosuojaneuvosto, https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_fi.pdf, viitattu 13.2.2023.

[3] Euroopan komission luonnos Yhdysvaltojen tietosuojan riittävyyttä koskevasta päätöksestä hyväksymismenettelyyn, Tietosuojavaltuutetun toimisto, https://tietosuoja.fi/-/euroopan-komission-luonnos-yhdysvaltojen-tietosuojan-riittavyytta-koskevasta-paatoksesta-hyvaksymismenettelyyn, viitattu 13.2.2023.

Yleistä tietosuoja-asetusta on täsmennetty ja täydennetty Suomessa tietosuojalailla (1050/2018), jossa säännellään esimerkiksi tietyistä tietojenkäsittelyn erityistilanteista. Vastaavasti yksityisyyden suojasta työelämässä annetussa laissa (759/2004, työelämän tietosuojalaki) säädetään muun muassa työntekijää ja eräiltä osin työnhakijan asemassa olevaa henkilöä koskevien henkilötietojen käsittelystä.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on laatinut raportin pilvipalveluiden turvallisuudesta. Sen mukaan ulkomaiset pilvipalveluntarjoajat suosivat oman maansa lainsäädäntöä riitatilanteissa. Näin ollen pilvipalveluja käyttöön ottavan organisaation tulee joko laatia palvelusopimukseen lauseke, jolla sovellettavaksi lainsäädännöksi asetetaan oma kansallinen lainsäädäntö ja määritellään riitatilanteiden varalle toimivaltainen tuomioistuin, tai sen on varauduttava toisen maan lainsäädännön soveltumiseen.[4]

Lainsäädännön lisäksi tietojen käsittelyä pilvipalveluissa voivat määritellä myös erilaiset standardit. Esimerkiksi kansainvälisen standardisoimisjärjestön ISO-standardeista 27000, 27017, 27018, 27701 ja 9001 määrittelevät tietoturvallista tietojenkäsittelyä myös pilvipalveluiden osalta.

Yleisen tietosuoja-asetuksen 40 artiklan mukaan yhdistykset ja muut elimet, jotka edustavat rekisterinpitäjien tai henkilötietojen käsittelijöiden eri ryhmiä, voivat asetuksen säännösten soveltamisen täsmentämiseksi laatia käytännesääntöjä. Pilvipalveluiden osalta tällaisia hyväksyttyjä käytännesääntöjä ovat EU Cloud Code of Conduct sekä CISPE. [5]

Omat vaatimuksensa pilvipalveluiden käytölle asettavat eri laeista tulevat säilytysajat eri asiakirjoille. Tällaisia säännöksiä löytyy henkilötietolain lisäksi esimerkiksi kirjanpitolaista (1336/1997), työaikalaista (872/2019), työsopimuslaista (55/2001), vuosilomalaista (162/2005), ennakkoperintälaista (1118/1996), luottotietolaista (527/2007), laissa sähköisistä allekirjoituksista (14/2003), laista potilaan asemasta ja oikeuksista (potilastietolaki, 785/1992), laista sähköisestä lääkemääräyksestä (61/2007), laista sosiaalihuollon asiakasasiakirjoista (254/2015), laista sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (asiakastietolaki, 784/2021) ja sen nojalla annetussa sosiaali- ja terveysministeriön asetuksessa potilasasiakirjoista (94/2022) sekä arkistolaista (831/1994). Lisäksi esimerkiksi Kuntaliitto on julkaissut omia kunnallisten asiakirjojen säilytysaikaoppaita[6].

Tiettyjen alojen erityssääntely

Yleissääntelyn lisäksi joillain aloilla on omaa erityissääntelyä, joka tulee ottaa huomioon. Esimerkiksi sosiaali- ja terveysalalla asiakastiedot ovat salassa pidettäviä tietoja, joiden luottamuksellinen käsittely täytyy varmistaa myös pilvipalveluja käytettäessä. Tällöin tulee ottaa huomioon esimerkiksi potilastietolaki, asiakastietolaki, terveydenhuoltolaki (1326/2010) sekä sosiaalihuoltolaki (1301/2014). Myös laki sosiaali- ja

[4] Pilvipalveluiden turvallisuus: Mitä organisaatioiden tulisi huomioida pilvipalvelu ja hyödyntäessä, Kyberturvallisuuskeskus, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf, viitattu 13.2.2023.
[5] EU Cloud Code of Conduct, https://eucoc.cloud/en/home, ja CISPE, Cloud Infrastructure Services Providers in Europe, https://www.codeofconduct.cloud/, viitattu 13.2.2023.
[6] Kunnallisten asiakirjojen säilytysajat, Kuntaliitto, https://www.kuntaliitto.fi/tietotuotteet-ja-palvelut/analyysit-ja-tietoaineistot/kunnallisten-asiakirjojen-sailytysajat, viitattu 13.2.2023.

terveystietojen toissijaisesta käytöstä (552/2019) ja tätä ns. toisiolakia tarkentava Sosiaali- ja terveysalan tietolupaviranomainen Findatan määräys 1/2022 muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavista vaatimuksista[7] voi tulla huomioitavaksi sotedatan toisiokäytössä. Samoin EU:n lääkintälaiteasetus MDR:n ((EU) 2017/745) sekä sitä täydentävän kansallisen, lääkinnällisistä laitteista annetun lain (719/2021) mukaisia lääkintälaitteeksi luokiteltuja ohjelmistoja voidaan tuottaa myös pilvipalveluista.[8]

Terveyden ja hyvinvoinninlaitos THL on asiakastietolakiin pohjautuen antanut lisäksi tarkentavia määräyksiä sosiaali- ja terveydenhuollon tiedonhallinnasta ja asiakastietojen sähköisestä käsittelystä. Pilvipalveluiden kannalta relevantteja ovat määräys 3/2021, määräys 4/2021 sekä määräys 5/2021.[9]

Monella alalla ei ole omaa erityislainsäädäntöä tiedon säilyttämisestä eikä siten myöskään pilven käytöstä, mutta jotkut valvontaviranomaiset ovat antaneet asiasta omaa ohjeistustaan. Esimerkiksi Finanssivalvonta on ohjeistanut verkkosivuillaan vakuutusalan toimijoita[10] ja viitannut mm. Euroopan vakuutus- ja lisäeläkeviranomaisen EIOPA:n ohjeistukseen vahinko- ja henkivakuutusyhtiöille toiminnan ulkoistamista pilvipalvelujen tarjoajille[11] sekä Euroopan arvopaperimarkkinaviranomaisen ESMAn antamiin ohjeisiin[12].

Liikenne- ja viestintävirasto Traficom on päivittämässä teletoiminnan tietoturvaa koskevaa määräystään (Viestintävirasto 67 A/2015 M) pilvipalveluiden käytön osalta[13], vaikka telealalla on laissa sähköisen viestinnän palveluista (917/2014) toki omaakin sääntelyä aiheesta. Esimerkiksi SVPL 283 § edellyttää, että kriittinen viestintäverkon järjestelmä sekä sen ohjaus, ylläpito ja hallinta voidaan valmiuslain 60 §:n 1 momentin 8 kohdan mukaista toimivaltuutta käytettäessä viipymättä palauttaa Suomeen ja että teleyrityksen tarjoamaa palvelua tai järjestelmää voidaan ylläpitää mainitun pykälän 1 momentin mukaisessa menettelyssä määritellystä paikasta. Samoin viestintäverkkojen ja -palvelujen varmistamisesta sekä

[7] Sosiaali- ja terveysalan tietolupaviranomaisen määräys 1/2022: Muiden palveluntarjoajien tietoturvallisille käyttöympäristöille asetettavat vaatimukset, Findata, https://findata.fi/palvelut-ja-ohjeet/maaraykset/, viitattu 13.2.2023.

[8] Sosiaali- ja terveysalan lainsäädäntökatsauksen lähteenä käytetty Kuntaliiton ja Alueiden ja kuntien sosiaali- ja terveydenhuollon tietohallintoyhteisfoorumi AKUSTI:n Sote-tietojärjestelmät pilvipalveluina -soveltamisohjetta, https://www.kuntaliitto.fi/julkaisut/2022/2158-sote-tietojarjestelmat-pilvipalveluina, viitattu 13.2.2023.

[9] Määräys 3/2021 - Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista, THL, https://thl.fi/documents/920442/2816495/THL_Maarays_3_2021_Tietoturvasuunnitelman_selvitykset_ja_vaatimukset.pdf/b4f17949-bace-b8d4-0cee-b215c6e5d372, Määräys 4/2021 - Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista, THL, https://thl.fi/documents/920442/2816495/THL-Maarays_4-2021_Sote-tietojarj_Luokittelu-Sertifiointi.pdf/1d2fb82d-5bc1-e6b5-0bbc-803b220a138a, sekä Määräys 5/2021 - Määräys sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista ja tietoturvavaatimuksista, THL, https://thl.fi/documents/920442/2816495/THL_maarays_5-2021_OlennaisetVaatimukset.pdf/6f62b65f-3dc1-f97d-7905-a054bef0584d, viitattu 13.2.2023.

[10] Vakuutustoimintaa pilvessä, Finanssivalvonta, https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/blogit/2020/vakuutustoimintaa-pilvessa/, viitattu 13.2.2023.

[11] Guidelines on outsourcing to cloud service providers, EIOPA, https://www.eiopa.europa.eu/document-library/guidelines/guidelines-outsourcing-cloud-service-providers_en, viitattu 13.2.2023.

[12] Määräykset ja ohjeet 4/2021 ulkoistamisesta pilvipalvelujen tarjoajille, Finanssivalvonta, https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2021/maaraykset-ja-ohjeet-42021-ulkoistamisesta-pilvipalvelujen-tarjoajille/, viitattu 13.2.2023.

[13] Määräyshankepäätös: Määräys teletoiminnan tietoturvasta (TRAFICOM/248815/03.04.05.00/2022), https://www.traficom.fi/fi/ajankohtaista/maarayshankepaatos-maarays-teletoiminnan-tietoturvasta, viitattu 13.2.2023.

viestintäverkkojen synkronoinnista annetun Traficomin määräys tuo omat vaatimuksensa.[14] Telealan sääntely on hyvä esimerkki tilanteesta, jossa alan oma erityissääntely tai viranomaisohjeistukset luovat omat vaatimuksensa ja rajoitteensa pilvipalveluiden käytölle. Tämän vuoksi selvityksessä mainittujen yleisohjeiden lisäksi tulee kullakin alalla huomioida myös alan oma erityissääntely, jota on valitettavasti mahdoton esittää tässä yleisesityksessä tyhjentävästi.

Lisäksi Liikenne- ja viestintävirasto on antanut 27.10.2022 voimaan astuneen uuden ohjeen välitystietojen käsittelyä koskevien tietojen tallentamisesta[15], joka korvaa aiemman Viestintäviraston suosituksen 308/2004 S tunnistamistietojen käsittelyä koskevien tietojen tallentamisesta. Ohjeen aiempi versio pohjautui sähköisen viestinnän tietosuojalain (516/2004) 15 §:ään, jossa tapahtumatietojen tallentaminen ulottui ainoastaan teleyrityksiin. Päivitetyssä ohjeessa on otettu huomioon lainsäädännössä tapahtuneet muutokset sekä tekninen kehitys.

SVPL 145 §:n säätämisen myötä tapahtumatietojen tallennusvelvollisuus laajennettiin teleyrityksistä kaikkiin viestinnän välittäjiin, kuten yhteisötilaajiin, ja samalla säännökseen lisättiin poikkeusmahdollisuus. Yhteisötilaajat tai muut viestinnän välittäjät voivat käyttää apunaan esimerkiksi sähköpostijärjestelmänsä toteuttamisessa lukuunsa toimivia pilvipalvelun tarjoajia (ns. yhteisötilaajan alihankkija), ja jatkossa velvollisuus tapahtumatietojen tallentamiseen koskee viestinnän välittäjiä myös näissä tilanteissa. Uuden ohjeistuksen mukaan pilvipalveluntarjoajan kaupallinen käytäntö ei ole asianmukainen peruste vedota käsittelylokin tallentamisvelvollisuutta koskevaan poikkeusperusteeseen, koska nykyaikaisessa pilvipalvelussa lokitietojen tallentamista ei normaalisti voida pitää teknisesti mahdottomana, eikä lokituksen toteuttaminen aiheuta epätavanomaisia kustannuksia. Lakisääteinen säilytysaika tulee ottaa huomioon myös pilvipalvelun käytön päättymisen yhteydessä.

Lainsäädännön vaatimukset pilvipalveluiden käytölle julkishallinnossa

Henkilötiedot

Viranomaiset ja julkisen sektorin organisaatiot voivat siirtää henkilötietoja kolmansien maiden julkisille elimille tai kansainvälisille järjestöille Euroopan komission hyväksymän tietosuojan riittävyyttä koskevan päätöksen perusteella (45 artikla). Jos siirtoon soveltuvaa päätöstä tietosuojan riittävyydestä ei ole tehty, yleisessä tietosuoja-asetuksessa on kaksi siirtoperustetta viranomaisille ja julkisen sektorin toimijoille: viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline (artikla

[14] Määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista, Traficom/54045/03.04.05.00/2020, https://www.traficom.fi/sites/default/files/media/regulation/Määräys_viestintäverkkojen_ja_-palvelujen_varmistamisesta_sekä_viestintäverkkojen_synkronoinnista.pdf, viitattu 13.2.2023.

[15] Liikenne- ja viestintäviraston ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta, Traficom/376384/03.04.05.01/2022, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Liikenne-%20ja%20viestintäviraston%20ohje%20välitystietojen%20käsittelyä%20koskevien%20tietojen%20tallentamisesta.pdf, viitattu 13.2.2023.

46:2(a)) sekä viranomaisten tai julkisten elinten välisiin hallinnollisiin järjestelyihin sisältyvät säännökset (artikla 46:3(b)).[16]

Euroopan tietosuojaneuvosto käynnisti 15.2.2022 yhteisen toimenpiteen, jossa selvitettiin julkisen sektorin pilvipalveluiden käyttöä[17]. Valvontaviranomaiset selvittivät erityisesti julkisten organisaatioiden pilvipalvelujen käyttöön liittyviä haasteita tietosuoja-asetuksen noudattamisessa. Pyrkimyksenä on edistää parhaita käytäntöjä ja varmistaa tietosuojan riittävä taso pilvipalvelujen käytössä. Euroopan tietosuojaneuvosto julkaisi raporttinsa 18.1.2023[18]. Raportin alkuun (s. 2–3) on koostettu 13 kohdan lista asioista, jotka on syytä huomioida, kun julkishallinto tekee sopimuksia pilvipalveluiden tarjoajien kanssa. Julkishallinnon tulee (EDPB:n suosituksesta vapaasti kääntäen)

- suorittaa tietosuojaa koskeva vaikutustenarviointi (DPIA),
- varmistaa, että osapuolten roolit on määritelty selkeästi ja yksiselitteisesti,
- varmistaa, että pilvipalveluiden tarjoaja toimii vain rekisterinpitäjän puolesta ja julkishallinnon organisaation dokumentoitujen ohjeiden mukaisesti, sekä tunnistaa kaikki mahdollinen henkilötietojen käsittely, jossa palveluntarjoaja voisi toimia rekisterinpitäjänä,
- varmistaa mielekäs tapa vastustaa uutta, alihankintana suoritettavaa tietojen käsittelyä,
- varmistaa, että henkilötiedot määritellään suhteessa niihin tarkoituksiin, joita varten niitä käsitellään,
- edistää tietosuojavastaavan osallistumista,
- tehdä yhteistyötä muiden julkishallinnon organisaatioiden kanssa neuvoteltaessa pilvipalveluiden tarjoajien kanssa,
- tarkastaa, käsitelläänkö tietoja tehdyn vaikutustenarvioinnin mukaisesti,
- varmistaa, että jo hankintamenettelyssä huomioidaan kaikki vaatimukset, joita GDPR:n noudattaminen edellyttää,
- tunnistaa, mitkä tietojen siirrot voivat tapahtua rutiinipalveluiden tarjoamisen yhteydessä ja mitkä pilvipalveluiden tarjoajan käsitellessä henkilötietoja omia liiketoiminnallisia tarkoituksiaan varten, sekä varmistaa, että GDPR V luvun määräyksiä noudatetaan, ottamalla tarvittaessa käyttöön lisätoimenpiteitä,
- analysoida, sovelletaanko kolmansien maiden lainsäädäntöä pilvipalveluiden tarjoajaan ja voiko tämä aiheuttaa pyyntöjä päästä tietoihin, joita palveluntarjoaja säilyttää EU-alueella,
- tutkia asioita tarkasti ja neuvotella tarvittaessa sopimus uudelleen, sekä
- tarkistaa ehdot, joilla julkishallinnon toimija voi osallistua auditointeihin ja varmistaa, että niistä on sovittu.

Tietosuojavaltuutetun toimiston selvitysten käsittely Suomen osalta on tätä selvitystä kirjoitettaessa vielä kesken.[19]

---

[16] Viranomaisten ja julkisen sektorin siirtoperusteet, Tietosuojavaltuutetun toimisto, https://tietosuoja.fi/viranomaisten-ja-julkisen-sektorin-siirtoperusteet, viitattu 13.2.2023.

[17] Tietosuojavaltuutetun toimisto käynnistää selvityksen julkisen sektorin pilvipalvelujen käytöstä osana Euroopan valvontaviranomaisten yhteistä toimenpidettä, Tietosuojavaltuutetun toimisto, https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-kaynnistaa-selvityksen-julkisen-sektorin-pilvipalvelujen-kaytosta-osana-euroopan-valvontaviranomaisten-yhteista-toimenpidetta, viitattu 13.2.2023.

[18] 2022 Coordinated Enforcement Action, use of cloud-based services by the public sector, European Data Protection Board, https://edpb.europa.eu/our-work-tools/our-documents/report/coordinated-enforcement-action-use-cloud-based-services-public_en, viitattu 13.2.2023.

[19] Julkishallinnon pilven käyttö sai uusia suosituksia – tässä 13 kohdan lista, Tivi 25.1.2023, https://www.tivi.fi/uutiset/tv/b7f29a62-2e06-4aed-85d5-fa9e14c0fe24, viitattu 13.2.2023.

Suomen valtion omistama kehitysyhtiö DigiFinland Oy on saanut huhtikuussa 2022 toimeksiannon valtiovarainministeriöltä vastata hankkeesta, jonka tavoitteena on nopeuttaa julkishallinnon pilvisiirtymää vähentämällä ja poistamalla pilvipalveluiden tietosuojaan liittyviä riskejä sekä luomalla julkishallinnon vaatimuksiin yhteensovitetut sopimusehdot. Hankkeen tehtävänä on pilvipalveluiden tietosuojan määrittäminen julkishallinnossa ja niihin liittyvät sopimusehtojen neuvottelut pilvipalveluiden toimittajien kanssa.[20] Hankkeesta järjestettiin lokakuussa 2022 ensimmäinen virallinen verkostotapaaminen, jossa pilvipalvelujen tietosuojan kehittämishanke nimettiin Cirrukseksi. Hanke kestää vuoden 2023 loppuun, ja julkinen sektori tulee hyötymään hankkeesta etenkin yhteneväisten tietosuojan toimintamallien myötä.[21]

Henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä on annettu oma lakinsa (1054/2018), jonka 7 luvussa käsitellään henkilötietojen siirtoja kolmansiin maihin ja kansainvälisille järjestöille. Laissa tarkoitettu toimivaltainen viranomainen saa siirtää henkilötietoja kolmanteen maahan vain tietyissä, lain määrittelemissä tilanteissa. Tämän voidaan katsoa pitävän sisällään myös tietojen tallentamisen kolmansiin maihin sijoittautuneeseen pilvipalveluun.

Muut kuin henkilötiedot

Euroopan parlamentin ja neuvoston asetus (EU) 2018/1807 muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa tuli voimaan joulukuussa 2018. Tämän ns. datan vapaata liikkuvuutta koskevan asetuksen keskeinen vaikutus oli, että jäsenvaltiot eivät voi vaatia sähköisessä muodossa olevaa muuta kuin henkilötietoa säilytettäväksi tai käsiteltäväksi tietyllä alueella, ellei vaatimusta voi perustella yleisellä turvallisuudella. Asetuksen kansallisen täytäntöönpanon yhteydessä liikenne- ja viestintäministeriön asettama työryhmä laati selvityksen muiden kuin henkilötietojen vapaan liikkuvuuden esteistä Suomessa[22]. Selvityksessä löytyi vain yksittäisiä vaatimuksia sisäministeriön hallinnonalalla. Näitä olivat passilain (671/2006) 35 §:n mukainen velvollisuus palveluntuottajalle, jonka tulee suorittaa passin yksilöinti ja passin toimittamista edeltävä laadun ja oikeasisältöisyyden tarkastaminen Suomessa; henkilökorttilain (663/2006) 22 §:n mukainen velvollisuus palveluntuottajalle suorittaa henkilökortin yksilöinti ja henkilökortin toimittamista edeltävä laadun ja oikeasisältöisyyden tarkastaminen Suomessa; sekä ulkomaalaislain (301/2004) velvoite suorittaa ulkomaalaislupia koskeva yksilöinti ja oikeasisältöisyyden tarkistaminen Suomessa (LVM 2019:11, s. 31-33).

Laissa viranomaisten toiminnan julkisuudesta (621/1999) säädetään mm. julkisuusperiaatteesta, viranomaisen tiedon luovuttamisesta sekä salassapidosta. Julkisuuslain 24 §:ssä säädetään salassa pidettävistä viranomaisen asiakirjoista.

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019) säädetään muun muassa viranomaisten tietoaineistojen tietoturvallisesta käsittelystä ja tietoturvallisuustoimenpiteiden toteuttamisesta. Laki

[20] DigiFinland edistämään pilvisiirtymää, DigiFinland Oy, https://digifinland.fi/digifinland-edistamaan-pilvisiirtymaa/, viitattu 13.2.2023.
[21] Cirrus – Julkisten pilvipalveluiden tietosuojan sopimusehtojen kehittämishanke, DigiFinland Oy, https://digifinland.fi/toimintamme/julkisten-pilvipalveluiden-tietosuojan-sopimusehtojen-kehittamishanke/2, sekä Uusi hanke parantaa julkisten pilvipalveluiden tietosuojaa, Valtiovarainministeriö, https://vm.fi/-/uusi-hanke-parantaa-julkisten-pilvipalveluiden-tietosuojaa, viitattu 13.2.2023.
[22] Muiden kuin henkilötietojen vapaan liikkuvuuden esteet Suomessa, Työryhmän selvitys, Liikenne- ja viestintäministeriön julkaisuja 2019:11, http://urn.fi/URN:ISBN:978-952-243-571-2, viitattu 13.2.2023.

velvoittaa julkisen hallinnon tiedonhallintayksiköitä ja viranomaisia sekä julkisia hallintotehtäviä hoitavia yksityishenkilöitä, yhteisöjä ja muita kuin viranomaisina toimivia julkisoikeudellisia yhteisöjä. Tiedonhallintalaissa säädetään muun muassa tietoturvallisuustoimenpiteiden vähimmäistasosta, mutta jätetään tiedonhallintayksiköille riskiperusteista harkintavaltaa toimenpiteiden toteuttamiseksi.

Tiedonhallintalainlain 18 §:n mukaan valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle. Tiedonhallintalakia on täydennetty valtioneuvoston asetuksella asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jossa säädetään asiakirjojen turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokiteltujen asiakirjojen käsittelyä koskevista tietoturvallisuustoimenpiteistä valtionhallinnon viranomaisissa.

Digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) 4 §:n mukaan viranomaisen on suunniteltava ja ylläpidettävä digitaaliset palvelunsa siten, että niiden tietoturvallisuus, tietosuoja, löydettävyys ja helppokäyttöisyys on varmistettu. Viranomaisen on huolehdittava sen vastuulla olevien digitaalisten palvelujen ja muiden viranomaisen käytössä olevien sähköisten tiedonsiirtomenetelmien saatavuudesta muulloinkin kuin viranomaisen asiointipisteiden aukioloaikoina. Viranomaisen on myös varmistettava digitaalisten palvelujensa riittävä yhteensopivuus hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain 3 §:ssä tarkoitettujen tukipalvelujen sekä muiden viranomaisten digitaalisten palvelujen kanssa. Lailla pantiin varsinaisesti täytäntöön julkisen sektorin elinten verkkosivustojen ja mobiilisovellusten saavutettavuudesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/2102, saavutettavuusdirektiivi, mutta viranomaisten digitaalisten palvelujen tietoturvallisuudesta ja tietosuojasta voi tulla velvoitteita myös tietojen säilyttämiselle pilvipalveluissa.

Lailla (1406/2011) säädetään myös viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. Arviointilain mukaan valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden arvioinnissa vain mainitussa laissa tarkoitettua menettelyä taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston (nykyisin Liikenne- ja viestintävirasto Traficom) hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaan.

Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa

Valtiovarainministeriön yhteydessä toimiva julkisen hallinnon tiedonhallintalautakunta, joka on monialaiseen asiantuntijayhteistyöhön perustuva viranomainen, on julkaissut 10.1.2022 suosituksen

turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa[23] (VM 2022:4), joka täydentää aiemmin 18.1.2021 annettua suositusta turvallisuusluokiteltavien asiakirjojen käsittelystä[24] (VM 2021:5). Nämä kaksi suositusta opastavat täyttämään tiedonhallintalain 18 §:n ja sitä täydentävän turvallisuusluokitteluasetuksen vaatimuksia. Tiedonhallintalautakunnan suositukset eivät ole velvoittavia tai sitovia, vaan niissä ohjataan tiedonhallintayksikköjä ja viranomaisia toteuttamaan hyviin käytäntöihin pohjautuen tiedonhallintalaissa säädetyt vaatimukset[25]. Tuoreemmassa julkaisussa tiedonhallintayksiköitä suositellaan valitsemaan pilvipalvelu siinä käsiteltävien turvallisuusluokiteltujen tietoaineistojen tiedonhallinta- ja tietoturvallisuusvaatimusten sekä käsittelyn käyttötapausten perusteella. Pilvipalveluihin liittyvien riskien hallitsemiseksi tiedonhallintayksiköitä suositellaan käyttämään sellaisia pilvipalveluita, joiden turvallisuus ja joiden tarjoajan turvallisuus on arvioitu turvallisuusselvityslain mukaan tehdyissä yritysturvallisuusselvityksissä, tai joille on myönnetty tietoturvallisuuden arviointitoimintaa koskevien säännösten mukainen turvallisuusvaatimustenmukaisuutta osoittava todistus.

Turvallisuusluokiteltavien asiakirjojen käsittelyä pilvipalveluissa on linjattu aiemmassa suosituksessa seuraavasti: ”*Turvallisuusluokan IV asiakirjojen käsittely ja säilytys on mahdollista sellaisissa pilvipalveluissa, joihin ei arvioida kohdistuvan lainsäädäntöjohdannaisia riskejä edellyttäen, että viranomainen on huomioinut myös kaikki muutkin turvallisuusluokitellun tiedon käsittelyyn liittyvät suojaustarpeet ja -velvoitteet. Turvallisuusluokan IV asiakirjojen säilyttäminen muissa pilvipalveluissa on mahdollista vain luotettavasti salatussa muodossa siten, että salausta ei voida purkaa tiedon elinkaaren aikana kyseisessä palvelussa. Siten osa viranomaisen turvallisuusluokitellun tiedon käsittely-ympäristöstä voi olla toteutettu pilviteknologiaa hyödyntäen*” (VM 2021:5, s. 64). Suosituksen mukaan tiedonhallintalain 14 § ja turvallisuusluokitteluasetuksen 11 §:n kohdat 7 ja 12 § mahdollistavat turvallisuusluokitellun tiedon siirtämisen julkisen tai muun ei-luotetun verkon kautta tilanteissa, joissa tieto on riittävän luotettavasti salatussa muodossa.

Suosituksessa turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa (VM 2022:4) kuvataan turvallisuusluokiteltavien asiakirjojen suojaamisen riskienhallintamenettelyä ja riskienhallinnan vaikutusten arviointia. Siinä tarkastellaan myös turvallisuusluokiteltavien asiakirjojen käsittelyssä käytettävien pilvipalveluiden ja niiden tarjoajien luotettavuuden arviointia sekä pilvipalveluja koskevissa palvelusopimuksissa huomioitavia näkökulmia. Lisäksi esimerkiksi tiedonhallintolain 13 §:n mukaista riskienhallintaa on yleisesti käsitelty tiedonhallintalautakunnan suosituskokoelmassa tiettyjen tietoturvallisuussäännösten soveltamisesta (VM 2021:65)[26], yleisimpiin pilvipalvelujen palvelumalleihin (SaaS, PaaS, IaaS ja CaaS) liittyviä riskejä julkisen hallinnon pilvipalvelulinjauksissa (VM 2018:35)[27] sekä

[23] Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa, Valtiovarainministeriön julkaisuja 2022:4, http://urn.fi/URN:ISBN:978-952-367-906-1 (VM 2022:4), viitattu 13.2.2023.
[24] Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä, Valtiovarainministeriön julkaisuja 2021:5, http://urn.fi/URN:ISBN:978-952-367-500-1 (VM 2021:5), viitattu 13.2.2023.
[25] Tiedonhallintalautakunta, https://vm.fi/tiedonhallintalautakunta, viitattu 13.2.2023.
[26] Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta, Valtiovarainministeriön julkaisuja 2021:65, http://urn.fi/URN:ISBN:978-952-367-897-2 (VM 2021:65), viitattu 13.2.2023.
[27] Julkisen hallinnon pilvipalvelulinjaukset, Valtiovarainministeriön julkaisu 35/2018, http://urn.fi/URN:ISBN:978-952-251-982-5 (VM 2018:35), viitattu 13.2.2023.

ohjeessa julkisen hallinnon pilvipalvelujen hyödyntämiseen (VM 2020:66)[28] ja pilvipalveluiden soveltamisohjeessa (VM 2020:73)[29].

Suosituksen mukaan turvallisuusluokitellut asiakirjat ovat yleensä tulkittavissa Suomen kansallisen turvallisuuden piiriin kuuluviksi (VM 2022:4, s. 16). Kansainvälisissä pilvipalveluissa ei suositella käsiteltäväksi sellaisia turvallisuusluokiteltavia asiakirjoja, jotka on rajattu Euroopan parlamentin ja neuvoston muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa annetun asetuksen (EU) 2018/1807 soveltamisalan ulkopuolelle. Asetuksen soveltamisalan tulkintaa on käsitelty aiemmin mainitussa liikenne- ja viestintäministeriön julkaisussa 2019:11.

Julkisuuslain 26 §:n 3 mom. sekä turvallisuusluokitteluasetuksen 6 § ja 8 § edellyttävät turvallisuusluokitellun aineiston käsittelyssä käytettävien pilvipalveluiden ja niiden tarjoajien luotettavuuden arviointia. Suosituksen VM 2022:4 mukaan yksi säännösten mukainen menettely pilvipalvelun tarjoajan luotettavuuden arviointiin on turvallisuusselvityslain (726/2014) mukainen Suojelupoliisin laatima yritysturvallisuusselvitys, jonka osana Traficom laati lain 9 §:n mukaisen ”*tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen*”. Pilvipalvelun ja sen tarjoajan luotettavuutta voidaan suosituksen mukaan arvioida myös arviointilain mukaisilla kriteereillä.

Suomi on lisäksi tehnyt tietoturvallisuussopimuksia useiden valtioiden ja kansainvälisten järjestöjen kanssa, mutta valtioiden välinen turvallisuussopimus ei tarkoita sitä, että sopimuksessa osallisena olevien valtioiden kaupalliset toimijat toteuttaisivat turvallisuussopimuksen velvoitteita. Turvallisuussopimuksen velvoitteet saatetaan koskemaan kaupallisia toimijoita kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitetun yritysturvallisuusselvitysmenettelyn (FSC) avulla (VM 2022:4, s. 20–21).

Tiedonhallintalautakunnan suosituksen (VM 2022:4) mukaan kansainvälisten pilvipalvelujen ja niiden tarjoajan luotettavuuden arvioinnissa on suositeltavaa hyödyntää kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettua yritysturvallisuusselvitysmenettelyä aina, kun se on mahdollista. Tämän vuoksi tiedonhallintayksikön suositellaan olevan yhteydessä kansalliseen turvallisuusviranomaiseen, jos turvallisuusluokiteltavia asiakirjoja on tarkoitus käsitellä kansainvälisissä pilvipalveluissa (VM 2022:4, s. 21). Vastaavasti pilvipalveluiden käyttäminen turvallisuusluokiteltavien asiakirjojen käsittelyssä edellyttää palvelusopimusten jatkuvaa seurantaa, sillä tiedonhallintalain 13 §:n mukaan ”*tiedonhallintayksikön on varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan*”. Tietoturvallisuudesta sopimista on käsitelty kattavammin tiedonhallintalautakunnan suosituskokoelmassa tiettyjen tietoturvallisuussäännösten soveltamisesta (VM 2021:65).

Tuoreimpana tiedonhallintalautakunnan ohjeena huomioitavaksi tulee suositus salassa pidettävien asiakirjojen käsittelystä (VM 2023:4)[30], jossa kuvataan salassa pidettävien asiakirjojen (tietojen) käsittelyä sekä käsittelyä koskevien vaatimusten täyttämistä. Aiemmassa suosituskokoelmassa tiettyjen

[28] Tuottavuutta pilvipalveluilla: Ohje julkisen hallinnon pilvipalvelujen hyödyntämiseen, Valtiovarainministeriön julkaisuja 2020:66, http://urn.fi/URN:ISBN:978-952-367-327-4 (VM 2020:66), viitattu 13.2.2023.
[29] Pilvipalvelujen soveltamisohje - Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille, Valtiovarainministeriön julkaisuja 2020:73, http://urn.fi/URN:ISBN:978-952-367-503-2 (VM 2020:73), viitattu 13.2.2023.
[30] Suositus salassa pidettävien asiakirjojen käsittelystä, Valtiovarainministeriön julkaisuja 2023:4, http://urn.fi/URN:ISBN:978-952-367-241-3 (VM 2023:4), viitattu 13.2.2023.

tietoturvallisuussäännösten soveltamisesta (VM 2021:65) esitettyjä vähimmäisvaatimuksia suositellaan sovellettavaksi myös salassa pidettävien asiakirjojen käsittelyssä, mutta lisäksi uusi suositus tuo uusia huomioitavia seikkoja. Salassa pidettävien tietojen käsittelylle pilvipalveluissa ei suosituksen mukaan ole lähtökohtaisesti lainsäädännöllisiä esteitä, mutta pilvipalveluiden soveltuvuutta arvioitaessa organisaation on kuitenkin selvitettävä pilvipalvelun turvallisuuteen liittyvät riskit sekä palvelun soveltuvuus suunniteltuun käyttötarkoitukseen, ottaen huomioon suosituksessa tarkemmin eritellyt näkökohdat (VM 2023:4, s. 29).

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on julkaissut Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri)[31], jonka tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa. PiTuKri ei ole suoraan velvoittava vaan ohjeluonteinen kriteeristö, joka on tarkoitettu pilvipalvelujen turvallisuuden arviointiin. Vastaavasti ulkoministeriössä toimivan Kansallisen turvallisuusviranomaisen (NSA) julkaisema kansallinen turvallisuusauditointikriteeristö Katakri[32] on auditointityökalu, jota viranomaiset voivat käyttää arvioidessaan kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa.

Tuoreimpana arviointikriteeristönä on tiedonhallintalautakunnan 2.6.2022 julkaisema Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)[33], joka tukee koko julkishallinnon tietoturvallisuuden kehittämisen ja arvioinnin tarpeita. Julkri on PiTuKria ja Katakria laajempi ohjeistus mm. turvallisuusluokittelemattoman tiedon osalta, ja sen kriteeristö jatkuvuuden ja varautumisen näkökulmista ottaa huomioon myös osittain vanhentuneet VAHTI-ohjeistukset.

Kansallinen turvallisuusviranomainen on julkistanut kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohjeen, jossa kuvataan tarkemmin esimerkiksi EU:n, Naton sekä muiden valtioiden ja kansainvälisten järjestöjen tietoaineistojen käsittelyä[34]. Kansainväliseen turvallisuusluokiteltuun aineistoon sovelletaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) erityissäännöstä ehdottomasta salassapitovelvollisuudesta, eikä siihen kohdistu julkisuuslain mukaista salassapidon tapauskohtaista arviointia. Kansainväliset turvallisuusluokitellut tietoaineistot on pidettävä salassa, jollei niitä koskevista sopimuksista tai säännöistä muuta johdu. Esimerkiksi EU:n toimielinten asiakirjojen julkisuutta koskevaan säädökseen, ns. avoimuusasetukseen (Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001), sisältyy yleisiä säännöksiä arkaluonteisten EU-asiakirjojen käsittelystä. Tämän lisäksi neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU) on jäsenvaltioiden kannalta keskeisin EU:n turvallisuusluokiteltujen tietojen suojaamista koskeva säädös.

[31] Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri), https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri, viitattu 13.2.2023.
[32] Katakri – tietoturvallisuuden auditointityökalu viranomaisille, Kansallinen turvallisuusviranomainen NSA, Ulkoministeriö, https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille, viitattu 13.2.2023.
[33] Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö, Valtiovarainministeriön julkaisuja 2022:43, http://urn.fi/URN:ISBN:978-952-367-275-8, viitattu 13.2.2023.
[34] Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje, Kansallinen tietoturvaviranomainen, 2020, https://um.fi/documents/35732/0/KV-TIEDON+KÄSITTELYOHJE+NSA+%28SUOMI%29_CLEAN.pdf/888aeb84-3e23-df3b-1774-a936f29a3fd9?t=1604931832075, viitattu 13.2.2023.

Lopuksi

Alati muuttuva sääntely-ympäristö tekee tästä selvityksestä vanhentuneen valitettavan nopeasti. Kaikki nyt esitelty sääntely ohjeistuksineen on relevanttia jatkossakin, mutta Euroopan unionin lainsäädännöstä sekä Suomen Nato-jäsenyydestä tulee lähivuosina aiheutumaan paljon lisäsääntelyä myös pilvipalveluiden hyödyntämiseen.

Euroopan komissio julkaisi 23.2.2022 ehdotuksensa parlamentin ja neuvoston asetukseksi tietojen oikeudenmukaista saatavuutta ja käyttöä koskeviksi harmonisoiduiksi säännöiksi eli niin kutsutuksi EU:n datasäädökseksi. Suorien datankäsittelyyn liittyvien vaatimusten lisäksi datasäädös sisältää vaatimuksen siitä, että tietojenkäsittelypalveluiden tarjoajien on tehtävä niiden palveluista luopuminen helpoksi, myös yrityskäyttäjille. Datasäädös on vielä muotoutumassa, ja trilogineuvottelut Euroopan komission, parlamentin ja neuvoston välillä alkavat oletettavasti Ruotsin puheenjohtajuuskaudella vuoden 2023 ensimmäisellä puoliskolla. Datasäädös tulee varmasti vaikuttamaan myös pilvipalveluiden käyttöön.

Toinen huomionarvoinen EU-hanke on komission jo vuonna 2017 antama ehdotus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). Tämän ns. ePrivacy-direktiivin korvaavan asetuksen oli alun perin tarkoitus tulla sovellettavaksi samaan aikaan yleisen tietosuoja-asetuksen kanssa, mutta näyttää siltä, että asetusta joudutaan edelleen odottamaan. On kuitenkin selvää, että lisäsääntely sähköisen viestinnän tietosuojasta tulee asettamaan lisävaatimuksia myös pilvipalveluille.

EU:n verkko- ja tietoturvadirektiivi (EU) 2016/1148 edellyttää Euroopan komissiolta yhteiseurooppalaisen pilvipalveluiden kyberturvasertifiointijärjestelmän laatimista. Asiasta vastaava EU-virasto ENISA valmistelee parhaillaan luonnosta EUCS-järjestelmästä (European Cybersecurity Certification Scheme for Cloud Services)[1], minkä jälkeen Euroopan komissio säätää sen laiksi täytäntöönpanosäädöksenä. NIS-direktiiviä ollaan uudistamassa, ja uudistuksessa komissio saa vallan säätää sertifioinnista pakollinen tietyille kriittisille sektoreille. Tämän myötä vielä neuvottelussa olevat EUCS:n suvereniteettivaatimukset voivat vaikuttaa merkittävästi myös Suomen julkipilven käyttömahdollisuuksiin lähivuosina. Sertifikaattien myöntämisen on arvioitu alkavan vuonna 2024.

Suomi on hakenut Pohjois-Atlantin liitto Naton jäsenyyttä, mikä tullee vaikuttamaan myös pilvipalvelujen käyttöön. Aiemman Naton ja Suomen tekemän tietoturvallisuussopimuksen (SopS 7 ja 8/2013) mukaisesti sopimuspuolet suojelevat jo nyt toistensa turvallisuusluokiteltua tietoa, mutta Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohjeen mukaan Natolla on jäsenilleen myös oma erillinen, sisäisesti hyväksytty säännöstö turvallisuusluokitellun tiedon käsittelemisestä.

Kansallisesti oikeusministeriö käynnistänyt keväällä 2022 valmiuslain (1552/2011) kokonaisuudistuksen, jonka tavoitteena on saattaa valmiuslaki vastaamaan nykyaikaista käsitystä yhteiskunnan kokonaisturvallisuudesta ja sitä uhkaavista tekijöistä sekä erilaisten vaikutuksiltaan vakavien uhka- ja häiriötilanteiden tunnistamisesta[35]. Muuttuneessa maailmassa poikkeusoloihin varautuminen voi tarkoittaa

[1] EUCS – Cloud Services Scheme, ENISA, https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme, viitattu 13.2.2023.

[35] Valmiuslain kokonaisuudistus, Oikeusministeriö, https://oikeusministerio.fi/valmiuslaki-uudistuu, viitattu 13.2.2023.

uusia vaatimuksia myös pilvipalveluille. Valmiuslain uudistus kestää 3,5–4 vuotta ja hallituksen esitys on tarkoitus antaa eduskunnalle viimeistään syysistuntokaudella 2025.

Pilvipalveluihin kohdistuvan sääntelyn ei kuitenkaan pidä antaa lannistaa. Sääntely lähtee siitä, että pilvipalveluiden käyttö halutaan mahdollistaa, kunhan tietyt edellytykset täyttyvät. Monissa tilanteissa pilvipalveluiden hyödyt ovat niiden käyttämisestä aiheutuvia velvoitteita suuremmat. On kuitenkin tärkeää pitää mielessä olemassa oleva säädöskehikko ja seurata sen kehittymistä.