Valtionhallinnon pilvipalvelulinjaukset

Julkisen hallinnon ICT

VALTIOVARAINMINISTERIÖN JjulkaisuJa – 2023:75

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Valtiovarainministeriön julkaisuja 2023:75

Valtionhallinnon pilvipalvelulinjaukset

Valtiovarainministeriö Helsinki 2023

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Valtiovarainministeriö

ISBN pdf: 978-952-367-475-2
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2023

Kuvailulehti

23.10.2023

Valtionhallinnon pilvipalvelulinjaukset

Valtiovarainministeriön julkaisuja 2023:75		**Teema**	Julkisen hallinnon ICT
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Julkisen hallinnon tieto- ja viestintätekninen osasto		
Kieli	suomi	**Sivumäärä**	24

Tiivistelmä

Pilvipalvelulinjauksien tavoitteena on tukea valtionhallinnon sekä soveltuvin osin hyvinvointialueiden ja kuntien päätöksentekoa pilvipalvelujen käytössä. Pilvipalveluja hyödyntämällä voidaan edistää julkisen hallinnon digitalisaatiota ja julkisen hallinnon tuottavuutta. Linjausten tarkoituksena on antaa ohjeita pilvipalvelujen turvallisesta käytöstä ja tukea riskienhallinnan päätöksentekoa sekä tarjota suuntaviivoja pilvipalvelujen toteuttamiseen. Linjauksien tarkoituksena on lisäksi selkeyttää henkilötiedon ja salassa pidettävän tiedon käsittelyyn liittyviä periaatteita. Nämä pilvipalvelulinjaukset ovat päivitys valtiovarainministeriön vuonna 2019 julkaisemiin linjauksiin.

Päivitetyt valtionhallinnon pilvipalvelulinjaukset koskevat seuraavia aihealueita:

1. Ensisijaisesti pilveen (Cloud 1st) strategia
2. Pilvi- ja ekosysteemiratkaisut EU/ETA-alueelta
3. Valtion yhteiset pilvi- ja ekosysteemiratkaisut
4. Kilpailutukset ja hankinnat valtionhallinnon yhteisillä hankintasopimuksilla
5. Pilvipalvelujen hankinta, käyttöönotto ja hyödyntäminen
6. Julkinen tieto julkisessa pilvipalvelussa
7. Salassa pidettävä tieto julkisessa pilvipalvelussa
8. Henkilötieto julkisessa pilvipalvelussa
9. Turvallisuusluokan IV tieto julkisessa pilvipalvelussa

Asiasanat	julkisen hallinnon ICT, digitalisaatio, julkinen hallinto, pilvipalvelut, tietoturva, tietosuoja		
ISBN PDF	978-952-367-475-2	**ISSN PDF**	1797-9714
Asianumero	VN/3115/2023		
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-475-2		

Presentationsblad

23.10.2023

Riktlinjer om molntjänster för statsförvaltningen

Finansministeriets publikationer 2023:75		**Tema**	Offentliga förvaltningens ICT
Utgivare	Finansministeriet		
Utarbetad av	Avdelningen för den offentliga förvaltningens informations- och kommunikationsteknik		
Språk	finska	**Sidantal**	24

Referat

Avsikten med riktlinjerna om molntjänster är att stödja statsförvaltningens samt i tillämpliga delar välfärdsområdenas och kommunernas beslutsfattande i användningen av molntjänster. Genom att utnyttja molntjänster kan man främja digitaliseringen och produktiviteten inom den offentliga förvaltningen. Syftet med riktlinjerna är att ge anvisningar om säker användning av molntjänster och stödja beslutsfattandet om riskhantering samt att ge riktlinjer för genomförandet av molntjänster. Ett ytterligare syfte med riktlinjerna är att förtydliga principerna för behandling av personuppgifter och sekretessbelagd information. Dessa riktlinjer om molntjänster är en uppdatering av finansministeriets riktlinjer från 2019.

De uppdaterade riktlinjerna om molntjänster för statsförvaltningen gäller följande ämnesområden:

1. Molntjänster i första hand (Cloud 1st) som strategi
2. Moln- och ekosystemlösningar från EU/EES-området
3. Statens gemensamma moln- och ekosystemlösningar
4. Konkurrensutsättning och upphandling genom statsförvaltningens gemensamma upphand-lingskontrakt
5. Upphandling, ibruktagande och utnyttjande av molntjänster
6. Offentlig information i en offentlig molntjänst
7. Sekretessbelagd information i en offentlig molntjänst
8. Personuppgifter i en offentlig molntjänst
9. Information av säkerhetsklass IV i en offentlig molntjänst

Nyckelord	offentliga förvaltningens ICT, digitalisering, offentlig förvaltning, molntjänster, informationssäkerhet, dataskydd		
ISBN PDF	978-952-367-475-2	**ISSN PDF**	1797-9714
Ärendenummer	VN/3115/2023		
URN-adress	https://urn.fi/URN:ISBN:978-952-367-475-2		

Description sheet
23 October 2023

Cloud service guidelines for central government

Publications of the Ministry of Finance 2023:75		**Subject**	Public Sector ICT
Publisher	Ministry of Finance		
Group author	Public Sector ICT Department		
Language	Finnish	**Pages**	24

Abstract

The aim of these cloud service guidelines is to support decision-making in central government, and as appropriate, in wellbeing services counties and municipalities, concerning the use of cloud computing services. Cloud services can promote the digitalisation and productivity of public administration. The purpose of these guidelines is to give instructions for the safe use of cloud services, to support decision-making concerning risk management and to provide guidelines for the implementation of cloud services. The purpose of the guidelines is also to clarify the principles for the processing of personal data and non-disclosable information. These cloud service guidelines are an update to the guidelines published by the Ministry of Finance in 2019.

The updated cloud service guidelines for central government cover the following subjects:

1. Cloud 1st strategy
2. Cloud and ecosystem solutions from the EU/EEA area
3. Shared government cloud and ecosystem solutions
4. Calls for tenders and procurement processes using joint central government procurement contracts
5. Procurement, deployment and utilisation of cloud services
6. Public information in public cloud services
7. Non-disclosable information in public cloud services
8. Personal data in public cloud services
9. Security class IV information in public cloud services

Keywords public sector ICT, digitalisation, public administration, cloud services, information security, data protection

ISBN PDF	978-952-367-475-2	**ISSN PDF**	1797-9714
Reference number	VN/3115/2023		
URN address	https://urn.fi/URN:ISBN:978-952-367-475-2		

Sisältö

1 Johdanto

Linjausten tavoitteena on tukea valtionhallinnon ja myös soveltuvin osin hyvinvointialueiden ja kuntien päätöksentekoa niiden suunnitellessa, hankkiessa ja käyttäessä uusia pilvipalveluja.

Tietojärjestelmien ja prosessien uudistamisessa hyödynnetään ja tullaan enenevässä määrin hyödyntämään pilvipalveluteknologiaa ja laajemminkin pilvipalvelujen toimintamallin muutoksia. Pilvipalveluille ominaisia etuja ovat skaalautumiskyky, muuntautumiskykyisyys, joustavuus ja innovatiivisuus. Pilvipalveluilla on saavutettu taloudellisia hyötyjä sekä parannettu tietoturvallisuutta. Pilvipalvelut ja niiden hyödyntäminen ovat keskeinen osa julkisen hallinnon digitalisaation edistämistä ja keino tuottavuuden parantamiseksi. On huomioitava palveluja kehitettäessä ja suunniteltaessa, että pilvipalvelut ja pilvipalveluteknologia ovat jatkossa monissa tapauksissa ainoa vaihtoehtoinen palvelumalli. Monet uudet teknologiat hyödyntävät taustallaan pilvipalveluteknologioita esimerkiksi tekoälyn hyödyntäminen.

Palvelu- ja toteutusmallien eri vaihtoehtojen perusteella saadaan rakennettua erilaisia toteutuksia. Eri toteutustavoissa riskit, riskienhallinnan monimutkaisuus, pilviteknologiasta saatavat hyödyt sekä kokonaiskustannukset vaihtelevat selvästi ja kunkin toteutustavan soveltuvuutta aiottuun tarkoitukseen on arvioitava huolellisesti. Linjausten tarkoituksena on tuottaa tietoa pilvipalvelujen käyttöön liittyvään päätöksentekoon.

Tausta

Valtiovarainministeriö on 19.1.2019 antanut valtionhallinnon pilvipalvelulinjaukset (VM/276/00.01.00.01/2018). Nyt annettavat linjaukset ovat päivitys aiemmin julkaistuihin linjauksiin. Linjaukset määrittävät osaltaan, miten julkisen hallinnon organisaation hallussa olevaa tietoa voidaan käsitellä pilvipalveluissa, ja ohjeistavat organisaatioita pilvipalvelujen käyttöön.

Linjauksien valmistelu on tehty valtiovarainministeriössä, yhteistyössä Valtion tieto- ja viestintätekniikkakeskus Valtorin asiakkaiden pilvipalvelujen sekä kokonaisturvallisuuden yhteistyöryhmien kanssa. Valtorin yhteistyöryhmissä on ollut edustettuna laaja joukko valtion virastojen asiantuntijoita. Linjausluonnoksesta pyydettiin lausuntoja maaliskuussa

2023. Lausuntopalautetta saatiin laajasti valtion virastoilta, yrityksiltä ja yhteisöiltä. Lausuntopalaute on huomioitu linjauksia täsmentämällä ja vastaamalla lausunnonantajien esittämiin huomioihin.

Pääministeri Orpon hallitusohjelman toimeenpanossa digitalisaatio on keskeinen keino kasvun ja tuottavuuden parantamiseksi. Suomi siirtyy asteittain digitaalisten palveluiden ensisijaisuuteen viranomaisasiointikanavana. Digitaalisten palvelujen tuottaminen vaatii jatkossa laajempaa pilvipalvelujen hyödyntämistä. Suomen tavoitteena on tarttua täysimääräisesti uusien teknologioiden ja digitalisaation tarjoamaan potentiaaliin ja pilvipalvelut ovat osa tätä kehitystä. Digitalisaation ja teknologisen kehityksen luonne vaatii, että sääntelyä päivitetään. Hallituksen tavoitteena on vaikuttaa aktiivisesti ja ennakolta siihen, että alustataloutta, tekoälyä, dataa ja digitalisaatiota koskeva EU-sääntely kulkee mahdollistavaan, tasapainoiseen ja Suomen kannalta edulliseen suuntaan, ja minimoi kansallisen lisäsääntelyn. Hallituksen tavoitteena on toteuttaa kansallisen tietosuojalainsäädännön kokonaisuudistus. Kokonaisuudistuksen yhteydessä on tavoitteena kumota tiedon liikkuvuutta, pilvipalveluiden tarkoituksenmukaista käyttöä tai muuten julkisten palveluiden tarkoituksenmukaista järjestämistä haittaavat säädökset ja hyödynnetään tarvittaessa nykyistä laajemmin GDPR:n kansallista liikkumavaraa. Pilvipalvelujen hyödyntämisessä tietosuojalainsäädännön hajanaiset tulkinnat ovat hidastaneet julkisen hallinnon pilvipalvelujen hyödyntämistä. Hallituksen tavoitteena on toteuttaa valtionhallinnon tuottavuusohjelma, jolla tuetaan hallituksen julkisen talouden kestävyystavoitetta. Tuottavuusohjelman toimeenpanossa hyödynnetään erityisesti digitalisaation mahdollisuuksia tehostaa julkisen sektorin toimintaa. Pilvipalvelut ovat keskeinen teknologia digitalisaation edistämisessä.

Tavoite

Linjaukset käsittelevät yleisesti pilvipalvelujen kaikkia palvelu- ja toteutusmalleja.

Linjausten tavoitteena on:

- Tunnistaa pilvipalvelujen käyttöön liittyviä mahdollisuuksia
- Parantaa tuottavuutta edistämällä julkisen hallinnon pilvipalveluja hyödyntämällä
- Antaa tiedonhallintayksiköille yleistä ohjausta reunaehdoista, joita noudattamalla pilvipalveluja voidaan turvallisesti hyödyntää
- Tukea pilvipalvelujen käyttöönottoon ja käyttöön liittyvää riskienarviointia ja -hallintaa ja siihen liittyviä menettelyjen kehittämistä ja sitä kautta mahdollistaa uusien pilvipalvelujen turvallinen käyttöönotto tiedonhallintayksiköissä

- Antaa ohjeellisia suuntaviivoja valtionhallinnon pilvi- ja ekosysteemiratkaisujen toteuttamiseksi
- Mahdollistaa laajemmat pilvipalvelujen käytöstä saatavat hyödyt (toiminnallinen ja taloudellinen hyöty) ja edistää tuottavuutta

Pilvipalvelujen käyttäminen

Pilvipalvelu tarkoittaa palvelumallia, jossa palveluntarjoaja tarjoaa tietojenkäsittely-kapasiteettia tai -palvelua, ja jonka tuottamisessa hyödynnetään tyypillisesti jaettuja ja skaalautuvia resursseja. Pilvipalvelun käyttäminen tapahtuu tietoliikenneverkon yli. Usein pilvipalveluista maksetaan käytön mukaan ja niiden käyttöönotto tai käyttäminen voi olla osin automatisoitua. Pilvipalveluista löytyy erilaisia palvelu- ja toteutusmalleja.

Pilvipalvelujen käyttö tarkoittaa, ettei organisaatiolla ole enää välttämättä suoraa määräysvaltaa tai kontrollia siihen, miten palvelua tuotetaan. Pilvipalvelujen toimitusmallissa pilvipalveluntarjoaja ei välttämättä päästä palvelutuotanto- ja laitetiloihin viranomaisia tai heidän kumppaneitaan tekemään arviointeja. Tilaaja joutuu luottamaan palveluntarjoajaan sekä sopimuksista ja arviointituloksista saatuihin tietoihin riskienhallintaa tehdessään. Loppukädessä tilaaja joutuu varmistumaan palveluntarjoajan luotettavuudesta ja palvelun vaatimuksenmukaisuudesta, ilman perinteistä fyysistä tarkastusta.

Palvelujen tuotannon ja tiedon sijainti

Pilvipalvelut on luontaisesti rakennettu sijaintiriippumattomalla toimintamallilla. Palvelutuotannosta voidaan erottaa maantieteelliseen sijaintiin liittyviä keskeisiä ulottuvuuksia sekä niistä johtuvia sovellettavaan lainsäädäntöön ja oikeuspaikan arviointiin liittyviä seikkoja:

- Palvelutuottajana toimivan yrityksen kotipaikka
- Palvelutuotannossa käytetyn konesalin sijainti
- Palvelussa käytettävien hallinta- ja valvontatoimenpiteiden suorittamisen ja suorittamiseen liittyvän henkilöstön sijainti
- Palvelun käytössä tarvittavien ei-toiminnallisten tietojen (diagnostiikkatieto, lokitieto ja asiakastiedot) sijainti

Pilvipalvelujen globaalissa toimintamallissa on yleensä voitu hajauttaa tiedonkäsittely kaikissa näissä ulottuvuuksissa, johtuen pilvitoimintamallin mahdollisuudesta esimerkiksi hajauttaa hallinta- ja valvontapalvelut toimimaan 24/7-periaatteella globaalisti. Toimintamalli haastaa tiedon suojaamiseen liittyvät nykyiset menetelmät sekä tietoturva- ja järjestelmäarkkitehtuurit uudistumaan. Uudistumisen tarve tuottaa tiedonhallinta-yksiköille tarpeen uudistaa näkemyksiään tietoturva- ja järjestelmäarkkitehtuureista.

Julkisella pilvipalvelulla tarkoitetaan tässä ohjeistuksessa EU/ETA-alueen ulkopuolelta osin tai kokonaan tuotettua pilvipalvelua, joka ei välttämättä ole kaikilta osin Suomen ja EU-lainsäädännön soveltamisen piirissä. Tällöin pilvipalveluun tallennettu tieto kuitenkin sijaitsisi lähtökohtaisesti EU/ETA-alueella tai Suomessa. Julkisen pilvipalvelun hallinta- ja valvontapalvelu voidaan tuottaa kolmansissa maissa. Hallinta- ja valvontapalvelujen toteuttamiseksi voidaan telemetriikka- ja diagnostiikkatietoja siirtää kolmansiin maihin.

Ei-luotetulla verkolla ja pilvipalvelulla tarkoitetaan sellaisia palveluja, joiden tietoturvallisuuden tasoa ei ole määritelty tai se ei vastaa salassa pidettävän tai turvallisuusluokitellun tiedon käsittelylle asetettuja vaatimuksia. Ei-luotettu verkko tai pilvipalvelu voi olla esim. organisaation sisäinen verkko, jota ei ole rakennettu kyseessä olevia tietoturvallisuuden vaatimuksia vastaavaksi.

Yleiset tietoon liittyvät linjaukset ja suositukset

Pilvipalveluissa kuten kaikissa tietojärjestelmien hankinnoissa ja hallinnoinnissa pitää koko elinkaaren noudattaa voimassa olevia säännöksiä ja vaatimuksia. Alla on lisäksi kuvattu käytettävän tiedon sekä hankintojen osalta ensisijaisesti noudatettavat linjaukset:

- Suositus salassa pidettävien asiakirjojen käsittelystä.
- Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä.
- Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa.
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö.
- Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri).
- Suositus tietoturvallisuudesta hankinnoissa.

Linjausten hyödyntäminen

Tilanteissa, joissa useampi kuin yksi seuraavista linjauksista soveltuu, on syytä huomioida kaikki soveltuvat linjaukset. Eli esimerkiksi, mikäli harkitaan salassa pidettävien henkilötietojen viemistä pilvipalveluun, on huomioitava sekä salassa pidettäviä tietoja koskeva linjaus (7.) että henkilötietoja koskeva linjaus (8.).

2 Valtionhallinnon pilvipalvelulinjaukset

Valtionhallinnon pilvipalvelulinjaukset ovat seuraavat:

1. Ensisijaisesti pilveen (Cloud 1st) strategia: Pilvipalvelun tai pilvipalveluteknologian tulee olla ensisijainen valinta, mikäli estäviä perusteita valinnalle ei ole
2. Pilvi- ja ekosysteemiratkaisut tulee tuottaa lähtökohtaisesti EU/ETA-alueelta
3. Valtion yhteisten pilvi- ja ekosysteemiratkaisujen tulee olla ensisijainen valinta, mikäli estäviä perusteita valinnalle ei ole
4. Pilvialustapalveluihin liittyvät kilpailutukset ja hankinnat tulee tehdä ensisijaisesti valtionhallinnon yhteisillä hankintasopimuksilla
5. Pilvipalvelujen hankintaa, käyttöönottoa ja hyödyntämistä tulee käsitellä vastaavasti, kuin mitä tahansa tietojärjestelmän hankintaa tai muutosta
6. Julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä
7. Salassa pidettävää turvallisuusluokittelematonta tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturvallisuus, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä
8. Henkilötietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä
9. Turvallisuusluokan IV tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä

2.1 Ensisijaisesti pilveen (Cloud 1st) strategia

Pilvipalvelun tai pilvipalveluteknologian tulee olla ensisijainen valinta, mikäli estäviä perusteita valinnalle ei ole.

Cloud First -strategialla tarkoitetaan mallia, jossa organisaatio on valinnut ensisijaiseksi tavoitteeksi hyödyntää pilvipalveluja tietojenkäsittelyssään, kuitenkin huomioiden myös muista tavoitteista johtuvat reunaehdot.

Pilvipalvelujen hyödyntäminen on tärkeää, ja tulevaisuudessa jopa välttämätöntä Suomen julkisen hallinnon digitalisaatiolle. Kansainvälisesti pilvipalvelujen hyödyntäminen nähdään yhtenä merkittävimpänä keinona edistää digitalisaatiota ja parantaa tuottavuutta. Pilvipalveluja hyödynnetään jo nyt skaalautuvien infrastruktuuripalvelujen tuottamiseen, kuten laskentakapasiteettiin ja tallennustilaan. Pilvipalvelujen joustavuus, innovatiivisuus ja skaalautuvuus ovat hyödyllisiä erityisesti odottamattomissa olosuhteissa, ja pilvipalvelut ovat omalta osaltaan mahdollistaneet Covid-19-pandemiaan varautumisen sekä valtionhallinnon joustavan siirtymisen monipaikkaiseen työhön. Pilvipalvelujen jatkuva kehittyminen tuottaa nopeampaa ja joustavampaa sovelluskehitystä, joka mahdollistaa nopeamman palvelukehityksen ja julkisen hallinnon palvelujen kehittymisen. Jatkossa pilvipalvelut tulevat olemaan tekoälyn ja koneoppimisen keskeisiä mahdollistajia ja siten digitalisoinnin tuottavuuden työkaluja. Jatkossa myös valmissovellukset siirtyvät tuotettavaksi pilvipalvelumallilla ja käytännössä se tarkoittaa jatkossa sitä, että joitakin uusimpia sovelluksia on tarjolla vain pilvipalveluna.

Pilvipalvelujen hyödyntämisestä saadaan myös tuottavuutta ja sitä kautta kustannussäästöjä. Keskeistä tuottavuuden aikaansaamisessa on pilvipalveluihin liittyvän nopeamman sovelluskehityksen ja valmiiden pilvisovelluksien hyödyntämisen mukanaan tuomat edut. Joiltakin osin on mahdollista saada kustannushyötyjä myös infrastruktuuripalvelujen käytössä muun muassa karsimalla hukkakäytöllä olevaa palvelin- tai tallennuskapasiteettia ja maksamalla vain siitä, mitä kulloinkin käyttää. Useat valtiot ovat laajasti siirtyneet hyödyntämään pilvipalveluja toiminnassaan ja perustaneet pilvimurroksensa Cloud First -strategiaan. Pilvipalvelujen käyttöä estävä peruste voi olla sellainen käyttötapaus, jonka vaatimukset täyttyvät paremmin hyödyntämällä jotakin muuta teknologiaa. Pilvipalvelujen laajamittainen hyödyntäminen ei ole sinällään itseisarvo, vaan pilvipalveluista saatavat hyödyt suhteessa perinteisiin toteutustapoihin.

2.2 Pilvi- ja ekosysteemiratkaisut EU/ETA-alueelta

Pilvi- ja ekosysteemiratkaisut tulee tuottaa lähtökohtaisesti EU/ETA-alueelta.

Henkilötietojen käsittelyyn käytettävien pilvipalvelujen tulisi lähtökohtaisesti olla tuotettuja EU/ETA-alueella. Tiedonhallintayksikön tulee myös muiden kuin henkilötietojen käsittelyyn tarkoitettujen pilviratkaisujen osalta arvioida mahdollisuutta hyödyntää EU/ETA-alueella tuotettuja palveluja lainsäädäntöjohdannaisten riskien vähentämiseksi. Lainsäädäntöjohdannaisilla riskeillä tarkoitetaan esimerkiksi eri maiden lainsäädännössä mahdollisesti olevia säännöksiä, jotka voivat velvoittaa pilvipalveluntuottajaa toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suoran tai epäsuoran pääsyn pilvipalvelun asiakkaiden tietoihin. Tiedon sijainnin lähtökohtaisesta suosituksesta tiedonhallintayksikkö voi poiketa riskiperusteisella päätöksellä, mikäli sijainnista johtuvat riskit on hallittu käyttämällä riittäviä suojauskeinoja.

Euroopan talousalue (ETA) on yhteismarkkina-alue, jolla toteutetaan tavaroiden, palvelujen, pääomien ja työvoiman vapaata liikkuvuutta. Euroopan talousalueeseen kuuluvat Euroopan unionin (EU) jäsenvaltioiden lisäksi Islanti, Norja ja Liechtenstein. Lähtökohtaisesti EU/ETA-alueen maissa on yhtenäistä lainsäädäntöä muun muassa henkilötietojen käsittelystä, minkä takia näissä maissa tuotettuun pilvipalveluun voidaan soveltaa yhtenäisiä käytäntöjä.

Iso-Britannian erotessa EU:sta teki Euroopan komissio kaksi Iso-Britanniaa koskevaa niin kutsuttua tietosuojan vastaavuuspäätöstä EU:n yleisen tietosuoja-asetuksen ja rikosasioiden tietosuojadirektiivin nojalla kesäkuussa 2021. Komission vastaavuuspäätökset ovat ensisijaisia siirtoperusteita, joilla henkilötietoja voidaan siirtää ETA-alueelta Britanniaan. Huomioitavaa on, että kyseiset päätökset ovat voimassa kesäkuuhun 2025 ja Tietosuojavaltuutetun toimisto ilmoittaa toimenpiteistä päätöksen voimassa olon lakkaamisen jälkeen.

Euroopan parlamentin ja neuvoston asetus muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa (2018/1807) on 28.5.2021 jälkeen edellyttänyt jäsenvaltioiden poistavan osaltaan perusteettomat sijaintia koskevat vaatimukset muulle kuin henkilötiedolle. Asetus ei kuitenkaan rajoita esimerkiksi yleisen turvallisuuden perusteella annettuja, suhteellisuusperiaatteen mukaisia kansallisia sijaintivaatimuksia. Asetuksen perusteella ei tulisi olla esteitä tiedon sijoittamiselle EU-alueelle. Tiedonhallintayksikön tulee esim. hankintoja tehdessään huomioida asetuksen vaikutukset tiedon sijoittamiselle. Eli kansallisesti ei saa asettaa asetuksen vastaisia sijaintivaatimuksia tiedolle.

Mikäli tiedonhallintayksikkö harkitsee pilvipalveluratkaisua, jota tuotetaan EU/ETA-alueen ulkopuolelta, on sen kiinnitettävä erityistä huomiota palvelun tuottamiseen liittyviin lainsäädäntöjohdannaisiin riskeihin. Muiden kuin EU/ETA-valtioiden osalta tulee palvelun tuottamiseen liittyvät riskit arvioida ja huomioida käytettävissä suojauskeinoissa. Myös erilaiset maiden tai organisaatioiden väliset sopimukset voivat vaikuttaa sijaintiin liittyviin riskeihin. Henkilötietojen osalta on huomioitava jäljempänä 7. kohdassa esitetty, salassa pidettävien tietojen osalta kohdassa 8. esitetty ja turvallisuusluokitellun tiedon osalta kohdassa 9. esitetty.

Globaalin tuotantomallin pilvipalvelut on yleensä tuotettu tavalla, jossa tiedon sijainti ja sen käsittely tapahtuvat eri maissa ja eri lainsäädännön alla. Näin ollen tiedonhallintayksikön tulee varmistaa palvelun eri toimintojen ja tietojen sijainti koko palvelun elinkaaren ajan, kattaen koko palvelukokonaisuuden tuottajat ja tietovarantojen sijainnit. Riskiarvioinnin lähtökohtana on riittävä selvitys elinkaaren aikaisesta tietojen käsittelystä sekä kussakin tehtävässä ja elinkaaren vaiheessa sovellettava lainsäädäntö.

2.3 Valtion yhteiset pilvi- ja ekosysteemiratkaisut

Valtion yhteisten pilvi- ja ekosysteemiratkaisujen tulee olla ensisijainen valinta, mikäli estäviä perusteita valinnalle ei ole.

Linjauksen tavoitteena on edistää valtion ja muun julkisen hallinnon tiedonhallinnan yhteentoimivuutta. Yhteentoimivuudesta saadaan valtion konsernitavoitteiden mukaisia toiminnallisia ja taloudellisia hyötyjä. Tavoitteena on myös kannustaa tiedonhallintayksiköitä huolehtimaan niiden linjausten, arkkitehtuurien ja hankintamenettelyjen toteuttamisesta yhteentoimivuutta edistävällä tavalla.

Tiedonhallintayksikön tulee suunnitteluvaiheessa selvittää ja arvioida, onko pilvipalveluja hyödyntäviä vastaavia tietojärjestelmiä tai vastaavia tietojärjestelmäkomponentteja jo aiemmin toteutettu valtionhallinnossa sekä voisiko näitä käyttää tiedonhallintayksikön tarpeeseen. Linjauksen tavoitteena on myös, että vältettäisiin pilvipohjaisen tietojärjestelmäkehityksen päällekkäisyyttä valtionhallinnon sisällä. Päällekkäisyyksien poistaminen tehostaa myös pilvipohjaista tietojärjestelmäkehitystä ja jakaa käytön sekä ylläpitovaiheen kustannuksia virastojen kesken.

Suunniteltaessa palvelun tuotantovaihetta tulee valtion viranomaisten ottaa huomioon valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain (1226/2013), jatkossa Tori-laki, 3 §:n mukainen käyttövelvoite koskien laissa tarkoitettuja yhteisiä palveluja. Pääosa tietojärjestelmien alustapalveluista on Tori-lain käyttövelvoitteen

piirissä ja tietojärjestelmien suunnittelussa tulee ottaa huomioon Tori-laissa tarkoitetun palvelutuottajan, Valtorin palvelut, palvelukuvaukset, palveluarkkitehtuurit ja suunnitteilla olevan tietojärjestelmän soveltuvuus käyttöympäristöihin. Yhteisten palvelujen laaja käyttäjäkunta ja palvelukeskuksen yhteisesti sovitut hallintamallit varmistavat palvelujen tasalaatuisuuden, tietoturvallisuuden vähimmäisvaatimukset, jatkuvuuden hallinnan sekä jatkuvan kehittämisen.

Valtion viranomaisten tulisi pilvipalvelujen hyödyntämisessä arvioida mahdollisuuksia rakentaa pilvipalveluja ja niitä hyödyntäviä tietojärjestelmiä yhteisten esim. hallinnonalakohtaisten arkkitehtuurien ja linjausten perusteella. Pilvipalvelun perusominaisuutena on muun muassa koodin uudelleen käytettävyys ja toistettavuus. Ilman laajempaa yhteistyötä ja jo tehtyjen koodien yhteiskäyttöä pilvipalvelujen käytöstä ei saada kaikkia tavoiteltuja hyötyjä. Linjauksen tavoitteena on kannustaa valtion viranomaisia käynnistämään yhteisiä, jopa hallinnonalat ylittäviä, yhteishankkeita, ekosysteemejä ja hankintoja.

2.4 Kilpailutukset ja hankinnat valtionhallinnon yhteisillä hankintasopimuksilla

Pilvialustapalveluihin liittyvät kilpailutukset ja hankinnat tulee tehdä ensisijaisesti valtionhallinnon yhteisillä hankintasopimuksilla.

Tietojärjestelmien hankintaa suunniteltaessa tiedonhallintayksikön tulee ottaa huomioon Valtion talousarviosta annetun lain (423/1988) säädös yhteishankintojen hyödyntämisestä ja huomioida yhteishankintayksikkö Hansel Oy:n kilpailuttamat sopimukset. Linjauksen tarkoitus on muilta osin kannustaa valtion viranomaisia järjestämään pilvipalveluihin liittyvät hankinnat virastojen välisellä yhteistyöllä ekosysteemien rakentamiseksi pilvipalvelujen hyödyntämisessä. Hansel Oy:n toteuttamat yhteishankinnat ovat myös muun julkisen hallinnon käytettävissä ja tulisikin ottaa huomioon, että yhteisten sopimusten käyttäminen tuottaa yhteentoimivuutta myös suhteessa muuhun julkiseen hallintoon. Valtorin tuottamien valtion yhteisten tieto- ja viestintäpalvelujen taustalla olevat Valtorin hankinnat toteuttavat laajan asiakaskunnan tarpeita. Yhteisten hankintavolyymien kautta on mahdollista saada kustannushyötyjä sekä laadukkaampia palveluja. Esimerkiksi Iso-Britanniassa virastoyhteistyö ja valtion yhteiset ekosysteemit ovat merkittävästi parantaneet valtion käytössä olevia kyvykkyyksiä ja tuottaneet taloudellista hyötyä. Valtori hyödyntää omissa palveluissaan Hanselin yhteishankintoja sekä toteuttaa tarvittavia hankintoja omien palvelujensa toteuttamiseksi.

Yhteishankintojen kautta myös palvelujen määrittelyä tehdään laajemmalla asiakaspohjalla, mikä mahdollistaa laaja-alaisemman ja laadukkaamman valmistelun. Yhteisvalmistelu tuottaa yhteishankintaan osallistuvien organisaatioiden yhteisen näkemyksen palvelutarpeesta ja sitä kautta muodostaa hankittavalle palvelulle myös laajemman yhteentoimivuuden sen ja muiden yhteishankinnalla hankittavien palvelujen välillä.

Yhteisten hankintasopimusten kautta voidaan myös sopia palvelutuottajien kanssa yhteisistä sopimusehdoista. Yhteisissä sopimusehdoissa voidaan sopia riittävän laadukkaasti muun muassa tietosuojasta ja tietoturvallisuudesta. Nyt jokainen viranomainen on lähtökohtaisesti sopinut näistä ehdoista erikseen.

2.5 Pilvipalvelujen hankinta, käyttöönotto ja hyödyntäminen

Pilvipalvelujen hankintaa, käyttöönottoa ja hyödyntämistä tulee käsitellä vastaavasti, kuin mitä tahansa tietojärjestelmän hankintaa tai muutosta.

Tiedonhallintayksikön tulee jatkossakin varmistaa huolellisella suunnittelulla pilvipalvelujen käyttöönotto vastaavalla tavalla, kuin myös perinteiset tietojärjestelmien hankinnat ja käyttöönotot on suunniteltu. Linjauksen tarkoituksena on huomioida pilvipalvelujen erilaiset ominaisuudet suhteessa perinteiseen tietojärjestelmäkehitykseen. Pilvipalvelujen tuotantomallit mahdollistavat palvelujen helpon käyttöönoton. Tämä ei kuitenkaan poista tiedonhallintayksikön vastuita palvelun elinkaaren suunnittelun osalta. Tiedonhallintayksikön on huomioitava pilvipalvelun käyttöönoton mahdolliset vaikutukset julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, tiedonhallintalaki) 5 §:n mukaiseen tiedonhallintamalliin ja tarvittaessa tehtävä pykälän 4 momentin mukainen muutosvaikutuksen arviointi. Pilvipalvelujen hyödyntäminen ei poista, vaan muuttaa tiedonhallintayksikön riskejä ja vastuita palvelujen toteuttamisessa. Pilvipalvelujen hyödyntämisessä asiakas ei voi määrittää ja hallita palvelujen yksittäisiä toimintoja, kuin loogisella tasolla, mikä vähentää asiakkaan riskienhallintaan käytettäviä teknisiä keinoja, painopisteen siirtyessä loogisen tason kontrolleihin. Jatkossa toimintatavan muutokseen liittyvät riskit tulee hallita sopimuksilla tai muilla käytettävissä olevilla kontrolleilla, mikä pitää ottaa huomioon myös osaamisen tarpeen kohdentumisena uudella tavalla.

Pilvipalvelujen hyödyntäminen edellyttää uudenlaista osaamista. Osaamisen painopiste siirtyy syvällisestä teknologioiden osaamisesta kohti tietosuojan, tietoturvallisuuden ja riskienhallinnan osaamista. Pilvipalvelujen käyttöönotto edellyttää organisaatiolta riittäviä kyvykkyyksiä.

2.6 Julkinen tieto julkisessa pilvipalvelussa

Julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä.

Julkisen, henkilötietoja sisältämättömän tiedon osalta tietoturvallisuuden osa-alueista tulee luottamuksellisuuden lisäksi arvioida myös tiedon saatavuus ja eheys. Tietosuojan osalta on huomioitava pilvipalvelun käytön elinkaaren ajan, ettei tietoaineistoon sisälly henkilötietoja ja mikäli sisältyy, on huomioitava linjaus 8. Tiedonhallintalain 4 luvussa asetetut tietoturva- ja tiedonhallintavaatimukset koskevat myös julkisen tiedon käsittelyä. Niiden toteutuminen tulee varmistaa myös pilvipalvelujen käytössä. Viranomaisen on esimerkiksi suunniteltava tietojärjestelmänsä ja tietojenkäsittelynsä siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa ja varmistettava, että sen hankkimissa tietojärjestelmissä on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Julkisenkin tiedon osalta tulee kuitenkin huolehtia tiedon saatavuudesta. Tiedonhallintayksikön tulee tiedonhallintalain 4 luvun mukaisten tietoturvavaatimusten toteutumisen lisäksi varmistaa myös valmiuslain 12 §:n mukainen toimintakyky. Viranomaisten tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa. Tämä edellyttää sitä, että yhteiskunnan elintärkeiden toimintojen ja muiden kriittisten tehtävien tarvitsemat tietovarannot ovat käytettävissä myös silloin, kun tietoliikenneyhteydet Suomen rajojen ulkopuolelle ovat poikki. Ulkomailla olevien pilvipalvelujen käyttö edellyttää toimivia tietoliikenneyhteyksiä Suomen ulkopuolelle. Tietoliikenneyhteydet tulee varmistaa pilvipalveluja käytettäessä riittävällä tavalla esimerkiksi yhteyksien moninkertaisella varmistamisella.

Tiedonhallintalain 13 §:n vaatimus tietoaineistojen saatavuuden varmistamisesta koko elinkaaren ajan ja 13 a §:n häiriötilainteisiin varautumisesta edellyttävät saatavuuden uudenlaista arviointia. Lähtökohtana varautumiselle on perinteisesti ollut tiedon sijoittaminen Suomen rajojen sisäpuolelle tai huolehtiminen tiedon siirtämisestä tarvittaessa Suomeen. Viranomaisten ennakollisessa varautumissuunnittelussa on kuitenkin arvioitava myös tarpeet tiedon varmistamisesta ja tarvittaessa sijoittamisesta Suomen rajojen ulkopuolelle.

2.7 Salassa pidettävä tieto julkisessa pilvipalvelussa

Salassa pidettävää turvallisuusluokittelematonta tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturvallisuus, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä.

Linjauksen tavoitteena on mahdollistaa salassa pidettävän turvallisuusluokittelemattoman tiedon käsittely julkisessa pilvipalvelussa. Salassa pidettävien tietojen käsittelylle julkisissa pilvipalveluissa ei ole lähtökohtaisia lainsäädännöllisiä esteitä, kunhan on varmistuttu siitä, että salassa pidettävät tiedot eivät päädy tahoille, joilla ei ole oikeutta käsitellä niitä. Pilvipalvelujen soveltuvuutta arvioitaessa organisaation on kuitenkin selvitettävä pilvipalvelun turvallisuuteen liittyvät riskit, erityisesti riskit, jotka liittyvät tietoaineistojen siirtämiseen tietoverkossa, tiedon tallettamiseen ja käsittelyyn pilvipalvelussa.

Pilvipalvelun hyödyntäminen tulisi arvioida kokonaisvaltaisesti ja riskiperusteisesti osana tiedonhallintayksikön tiedonhallinnan ja tietoturvallisuuden kansallisen lainsäädännön mukaisia vastuita. Tiedonhallintalaki ja laki viranomaisten toiminnan julkisuudesta (621/1999), jatkossa julkisuuslaki asettavat tiedonhallintayksikölle velvoitteita, joita korostavat rikoslain (39/1889) rangaistussäännökset, jotka voivat julkisuuslain 35 §:n mukaisesti tulla sovellettavaksi salassapito- ja vaitiolovelvollisuuden ja hyväksikäyttökiellon rikkomisesta. Tämä edellyttää tiedonhallintayksiköiltä huolellista salassa pidettävän tiedon käsittelyä.

Lisäksi on huomattava, että EU-lainsäädäntö saattaa yksittäistapauksissa asettaa rajoitteita globaalien pilvipalveluratkaisujen käytölle. Esimerkiksi datanhallinta-asetuksen (Euroopan parlamentin ja neuvoston asetus (EU) 2022/868, annettu 30 päivänä toukokuuta 2022, eurooppalaisen datan hallinnoinnista ja asetuksen (EU) 2018/1724 muuttamisesta) mukaista suojattua dataa ei saa siirtää kolmanteen maahan eikä siihen saa päästä käsiksi kolmannesta maasta, jos siirto tai pääsy olisi ristiriidassa unionin lainsäädännön tai kansallisen lain kanssa.

Osana kokonaisarviota on huomioitava tiedon sijaintiin liittyvät lainsäädäntöjohdannaiset ja määräysvaltaan liittyvät riskit. Ulkomaille (mukaan lukien EU/ETA-maat) sijoitettavassa pilvipalvelussa oleva tieto voi olla toisen valtion lainsäädännön piirissä, jolloin mahdollisuudet tiedon suojaamiseen sopimuksilla ovat rajalliset. Useiden valtioiden lainsäädännössä on asetettu kansallisen turvallisuuden varmistamiseksi viranomaisille hyvin laajat tiedonsaantioikeudet kyseessä olevan valtion alueella sijaitseviin tietoihin. Samat laajat tiedonsaantioikeudet voivat ulottua myös kyseessä olevassa valtiossa toimivien yritysten kansainvälisiin tytäryhtiöihin sekä näiden alihankkijoihin. Käytännössä tämä saattaa

tarkoittaa näiden valtioiden viranomaisten mahdollisuutta saada tietoa pilvipalvelusta, jopa ilman tiedon omistajan lupaa tai tietoisuutta tiedon luovuttamisesta kyseessä olevan valtion viranomaiselle. Käytännössä nämä lainsäädäntöjohdannaiset riskit edellyttävät tiedonhallintayksiköltä erityistä huolellisuuttaa tiedon suojaamisen suunnittelussa. Riskejä voidaan vähentää tiedon sijoittamisella sellaiseen pilvipalveluun, johon sovelletaan Suomen lainsäädäntöä, palvelutuottajan yritysturvallisuustodistuksella sekä huolehtimalla tiedon salaamisesta luotettavasti sen elinkaaren ajan.

Tiedonhallintalaki ja turvallisuusluokitteluasetus mahdollistavat salassa pidettävän ja turvallisuusluokitellun tiedon siirtämisen julkisen tai muun ei-luotetun verkon kautta tilanteissa, joissa tieto on riittävän luotettavasti salatussa muodossa. Tiedon salauksen tulee kattaa sekä salauksen toteuttavan ohjelmiston tai laitteiston ja avainhallinnan sijoittaminen ei-luotetun verkon ulkopuolelle. Samaa periaatetta voidaan soveltaa myös tilanteisiin, joissa salassa pidettävää ja turvallisuusluokiteltua tietoa on tarve siirtää tai säilyttää ei-luotetuissa pilvipalveluissa. Periaatteen soveltamisessa tulee kuitenkin aina huomioida, että pilvipalveluntarjoajalla on lähtökohtaisesti aina pääsy palvelussa käsiteltävään tietoon, mikäli tieto on elinkaarensa aikana palvelussa selväkielisessä muodossaan (esimerkiksi asiakkaalle näytettävänä kuvana). Esimerkiksi yleiset omien avainten käyttöön (BYOK, Bring Your Own Keys) tai pilvipalveluntarjoajan fyysiseen konesaliin sijoitettaviin laitteistopohjaisiin turvamoduuleihin (HSM, Hardware Security Module) pohjautuvat ratkaisumallit rajaavat, mutta eivät tyypillisesti estä pilvipalveluntarjoajan pääsymahdollisuuksia palvelussa käsiteltävään tietoon. Salauksen lisäksi voidaan käyttää kuitenkin täydentävänä suojauksena esimerkiksi asiakkaiden tietojen erottelua, suojattavien kohteiden tuhoamisprosessia tai tehtävien erottelua. Salaustuotteiden valinnassa voi käyttää esimerkkinä Traficomin hyväksymiä salaustuotteita kansainvälisen turvallisuusluokitellun tiedon suojaamiseksi Suomessa. Ohjetta sovellettaessa on kuitenkin huomioitava, että kyseinen ohje on tarkoitettu kansainvälisen tietoturvallisuusvelvoitteen kattaman tiedon suojaamiseen eikä sinällään vastaa pilvipalvelujen tarpeisiin. Tiedonhallintayksikön tulee tehdä oma arvionsa käytettävistä salausratkaisuista.

Suunniteltaessa ja arvioitaessa salassa pidettävän turvaluokittelemattoman tiedon käsittelyä pilvipalveluissa voidaan hyödyntää muun muassa seuraavia suosituksia:

- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), sekä siihen sisältyvä käyttötapaus ”SaaS-pilvipalvelun arviointi”, liite 3, luku 2.1.2
- Tiedonhallintalautakunnan suositus salassa pidettävien asiakirjojen käsittelystä pilvipalveluissa (VM 2023:4)
- Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri), s. 13, 15.

Salassa pidettävän tiedon osalta on myös huomioitava mahdollinen kasaumavaikutus. Käytännössä salassa pidettävää tietoa sisältävä tietovaranto, joka sisältää koosteen tietoja, voi kokonaisuutena synnyttää turvallisuusluokiteltavana tietona pidettävän kasauman. Tällainen tilanne voi edellyttää tiedon sijainnin ja suojauksen uudelleenarviointia. Tiedon suuri määrä ei ole lähtökohtaisesti automaattisesti peruste kasaumavaikutukselle. Vastaavasti tietovaranto voi sisältää päällekkäisiä suojaustarpeita edellyttäviä tietoja. Samassa tietovarainnossa voi olla julkista tietoa, salassa pidettävää tietoa, henkilötietoa ja turvallisuusluokiteltua tietoa.

2.8 Henkilötieto julkisessa pilvipalvelussa

Henkilötietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä.

Henkilötietojen käsittelyyn sovelletaan EU:ssa ja Euroopan talousalueella EU:n yleistä tietosuoja-asetusta (EU) 2016/679, jota täydentää Suomessa kansallinen tietosuojalaki (1050/2018). Lisäksi on olemassa asetuksen kansallisen liikkumavaran perusteella annettua erityislainsäädäntöä. Henkilötietojen käsittelyyn rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä sovelletaan henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia (1054/2018). Tietosuojasääntely ei ota suoraan kantaa pilvipalveluihin, mutta asettaa vaatimuksia henkilötiedon käsittelylle toteutustavasta riippumatta.

Yleinen tietosuoja-asetus rajoittaa henkilötietojen siirtoa EU:n ja ETA-alueen ulkopuolelle kolmansiin maihin. Henkilötietojen siirrolle on tällöin oltava tietosuoja-asetuksen V luvussa määritelty siirtoperuste, jonka tehokkuus ja täydentävien suojatoimien tarve on arvioitava tapauskohtaisesti. Henkilötietoja voidaan siirtää kolmansiin maihin, jos Euroopan komissio on antanut päätöksen henkilötietojen suojan riittävyydestä (niin kutsuttu vastaavuuspäätös, tietosuoja-asetuksen 45 artikla) tai toissijaisesti, jos kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet (46 artikla). Joissakin tapauksissa siirto voidaan suorittaa myös perustuen erityistilanteita koskeviin poikkeuksiin (49 artikla), kuten jos siirto on tarpeen tärkeää yleistä etua koskevien syiden vuoksi ja tämä etu tunnustetaan unionin oikeudessa tai sen jäsenvaltion lainsäädännössä, jota rekisterinpitäjään sovelletaan.

Henkilötietojen siirrosta on Euroopan tietosuojaneuvoston mukaan kyse myös silloin, jos henkilötietoja käsitellään EU:n ulkopuolelta etäyhteyden kautta, vaikka tiedot fyysisesti sijaitsisivat EU:n alueella. Vastaavasti kyse on henkilötietojen siirrosta, jos henkilötiedot sijoitetaan esimerkiksi pilvipalveluun, jota tarjotaan EU:n ulkopuolelta. Tiedonhallintayksikön on tapauskohtaisesti arvioitava, missä määrin siirron mahdollisuutta riittää rajaamaan esimerkiksi pilvipalveluntuottajan henkilötiedon käsittelyn rajoittaminen, ja missä määrin rekisterinpitäjän olisi pystyttävä teknisesti estämään kaikki pääsy tietoihin. Teknisillä suojakeinoilla, esimerkiksi teknisesti korkeatasoisella tiedon salaamisella voitaisiin teoriassa toteuttaa ratkaisu, jossa tieto ei siirry julkiseen pilvipalveluun sellaisessa muodossa, että sitä voitaisiin pitää henkilötietona. Tulevaisuudessa on myös mahdollista, että komission vastaavuuspäätöksillä laajennetaan niiden valtioiden joukkoa, joihin siirrot ovat sallittuja, tai tarkennetaan valvovien viranomaisten ohjeistusta.

Useimmat tämän hetken merkittävimmistä pilvipalveluntarjoajista toimivat Yhdysvalloissa. Euroopan komission vastaavuuspäätös Yhdysvaltojen tietosuojan tason riittävyydestä on astunut voimaan 10.7.2023. Komissio katsoo, että Yhdysvallat varmistaa riittävän suojan henkilötiedoille, jotka siirretään EU:sta yhdysvaltalaisille yrityksille, jotka ovat sitoutuneet EU:n ja Yhdysvaltojen välisessä tietosuojakehyksessä (niin kutsuttu EU-U.S. Data Privacy Framework) sovittuihin suojatoimiin. Tietosuoja-asetuksen henkilötietojen siirtoja koskevan etusijajärjestyksen mukaisesti ensisijaisena siirtoperusteena henkilötietoja Yhdysvaltoihin siirrettäessä on käytettävä komission antamaa vastaavuuspäätöstä.

Vastaavuuspäätös laajentaa mahdollisuuksia henkilötietojen siirroille Yhdysvaltoihin. Vastaavuuspäätöstä ja sen toimivuutta arvioidaan komission toimesta säännöllisesti ja vähintään neljän vuoden valein. Kuten muussakin henkilötietojen käsittelyssä, myös henkilötietojen siirroissa on aina varmistuttava siitä, että henkilötietojen käsittely on lainmukaista koko käsittelyn elinkaaren ajan. Tiedonhallintayksikön on siis arvioitava käsittelyn lainmukaisuutta, vaikka se käyttäisi vastaavuuspäätöstä siirtoperusteena.

2.9 Turvallisuusluokan IV tieto julkisessa pilvipalvelussa

Turvallisuusluokan IV tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä.

Linjauksen tarkoituksena on mahdollistaa turvallisuusluokiteltujen turvallisuusluokan IV tietojen käsittely julkisessa pilvipalvelussa. Turvallisuusluokan IV tietojen käsittelyyn pilvipalvelussa ei ole ehdotonta lainsäädännöllistä estettä, mikäli asiakirjojen käsittely ja

säilytys on toteutettu ennakollisesti vaatimusten mukaisesti ja huomioiden muun muassa edellä kuvatut lainsäädäntöjohdannaiset ja toisen valtion määräysvaltaan liittyvät riskit. Turvallisuusluokiteltavan tiedon käsittelyyn pätee, mitä edellä on todettu salassa pidettävän tiedon käsittelystä, minkä lisäksi olisi huomioitava tässä mainitut vaatimukset.

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jatkossa turvallisuusluokitteluasetus, sääntelee turvallisuusluokiteltujen tietojen käsittelyä. Asetuksen 9 §:n mukaan tiedonhallintayksikön on määritettävä tietyt fyysisesti suojatut turvallisuusalueet turvallisuusluokiteltujen asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi asetuksen 10 §:ssä tarkoitetulla tavalla. Käytännössä tämä tarkoittaa velvoitetta sijoittaa turvaluokitellut tietojärjestelmät fyysisesti laissa tarkoitetulle turvallisuusalueelle. Valtionhallinnon ohjeissa turva-alue määritellään tarkemmin julkisen hallinnon tietoturvallisuuden arviointikriteeristössä (Julkri). Käytännössä voidaan katsoa riittävän salauksen olevan riittävä suojauskeino tiedon oikeudettoman käytön estämiseksi. Salauksen voidaan katsoa olevan rinnakkainen suojauskeino turva-alueen kanssa.

Tiedonhallintalain 14 §:ssä ja vastaavasti turvallisuusluokitteluasetuksen 12 §:n 2 momentissa edellytetään tiedon salaamista sen siirtämiseksi tietoverkoissa. Turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on turvallisuusluokitteluasetuksen 11 §:n 1 momentin 1 kohdan mukaan toteutettava siten, että ne erotetaan niissä käsiteltyjen asiakirjojen turvallisuusluokka huomioiden riittävän luotettavasti alemman turvallisuustason tietojärjestelmistä ja tietoliikennejärjestelyistä. Turvallisuusluokitteluasetuksen 11 §:n 1 momentin 7 kohdassa edellytetään salauksen olevan turvallisuusluokka huomioiden riittävän turvallinen. Vaatimusten toteuttamisessa voidaan hyödyntää muun muassa Julkri-kriteeristöä.

Tiedon salaamisessa ja sen siirtämisessä pilvipalveluun tulee huomioida, että tiedon on oltava salattuna koko sen elinkaaren ajan. Kun vaatimukset tiedon salaamisesta ja eriyttämisestä koko elinkaaren ajan, mukaan lukien tietoliikenteessä, on toteutettu vaatimustenmukaisella tavalla voidaan turvallisuusluokiteltua tietoa käsitellä julkisessa pilvipalvelussa. Turvallisuusluokittelusta säädetään tiedonhallintalain 18 §:ssä ja turvallisuusluokitellun tiedon merkitsemisestä ja käsittelystä turvallisuusluokitteluasetuksessa. Asetuksessa on korostettu turvallisuusluokiteltujen asiakirjojen monitasoista suojausta (asetuksen 7 §), ns. need-to-know-periaatetta (asetuksen 8 §) sekä turvallisuusluokiteltujen asiakirjojen suojaamista sivullisilta (asetuksen 10 § 1 mom). Turvallisuussalaisuuden paljastamisen rangaistavuudesta on säädetty rikoslain (39/1889) 12 luvun 7 §:ssä. Turvallisuusluokitellun tiedon käsittely edellyttää tiedonhallintayksiköltä erityistä huolellisuutta.

Julkisuuslain, tiedonhallintalain ja turvallisuusluokitteluasetuksen velvoitteiden täyttyminen tulee tarvittaessa huolellisesti varmistaa tietoturvallisuuden arvioinneilla. Tietoturvallisuuden arviointi voidaan tehdä viranomaisen itsearviointina, ulkoisena arviointina ja

tarvittaessa arviointilaitoksen toimesta, jolloin arvioinnista on mahdollisuus saada todistus. Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) velvoittaa valtion virastoja käyttämään laissa tarkoitettuja arviointilaitoksia tietojärjestelmiensä ja tietoliikennejärjestelyjen arviointiin. Arviointien perusteella vaatimukset täyttävät järjestelmät voivat saada todistuksen vaatimuksenmukaisuudesta. Tällä hetkellä tietoturvallisuuden arviointilaitosten pätevyysalueisiin ei sisälly pilvipalvelujen käyttöä tukevia kriteeristöjä.

Seuraavia turvallisuusluokitellun turvaluokka IV-tiedon käsittelyyn liittyviä ohjeita voidaan hyödyntää palvelujen suunnittelussa:

- Julkisen hallinnon tiedonhallintalautakunnan suositukset: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5), s. 47 ja 64.
- Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa (VM 2022:4)
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), (VM 2023:46), esimerkiksi kriteerit HAL-06.1, HAL-16.1, TEK-04, TEK-07.2, TEK-08, TEK-21.2, VAR-02.1 ja TSU-18.
- Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille (VM 2020:73), s. 87.
- Ohje turvallisuuskriittisiin hankintoihin: Määräysvaltamuutoksiin varautuminen turvallisuuskriittisissä tieto- ja viestintäjärjestelmien sekä -ratkaisujen hankinnoissa (VM 2019:7), s. 11, 12.
- Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri), s. 13, 15.

Lähteet

Liikenne- ja viestintävirasto Traficom, Kyberturvallisuuskeskus 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Traficomin julkaisuja 13/2020. Osoitteessa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf. Viitattu 9.10.2023.

Valtiovarainministeriö 2023. Suositus tietoturvallisuudesta hankinnoissa. Valtiovarainministeriön julkaisuja 2023:57. Valtioneuvoston hallintoyksikkö, Helsinki. Osoitteessa: http://urn.fi/URN:ISBN:978-952-367-645-9. Viitattu 9.10.2023.

Valtiovarainministeriö 2023. Suositus salassa pidettävien asiakirjojen käsittelystä. Valtiovarainministeriön julkaisuja 2023:4. Valtioneuvoston hallintoyksikkö, Helsinki. Osoitteessa: http://urn.fi/URN:ISBN:978-952-367-241-3. Viitattu 9.10.2023.

Valtiovarainministeriö 2023. Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö. Valtiovarainministeriön julkaisuja 2023:46. Valtioneuvoston hallintoyksikkö, Helsinki. Osoitteessa: http://urn.fi/URN:ISBN:978-952-367-458-5. Viitattu 9.10.2023.

Valtiovarainministeriö 2022. Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa. Valtiovarainministeriön julkaisuja 2022:4. Valtioneuvoston hallintoyksikkö, Helsinki. Osoitteessa: http://urn.fi/URN:ISBN:978-952-367-906-1. Viitattu 9.10.2023.

Valtiovarainministeriö 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Valtiovarainministeriön julkaisuja 2021:5. Valtioneuvoston hallintoyksikkö, Helsinki. Osoitteessa: http://urn.fi/URN:ISBN:978-952-367-500-1. Viitattu 9.10.2023.

Valtiovarainministeriö 2020. Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille. Valtiovarainministeriön julkaisuja 2020:73. Valtioneuvoston hallintoyksikkö, Helsinki. Osoitteessa: http://urn.fi/URN:ISBN:978-952-367-503-2. Viitattu 9.10.2023.

Valtiovarainministeriö 2019. Määräysvaltamuutoksiin varautuminen turvallisuuskriittisissä tieto- ja viestintäjärjestelmien sekä -ratkaisujen hankinnoissa. Valtiovarainministeriön julkaisuja 2019:7. Valtiovarainministeriö, Helsinki.Osoitteessa: http://urn.fi/URN:ISBN:978-952-251-988-7. Viitattu 9.10.2023.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-475-2 (pdf)

Lokakuu 2023