Valtionhallinnon pilvipalvelulinjaukset

Julkisen hallinnon ICT

VALTIOVARAINMINISTERIÖN JjulkaisuJa – 2024:49

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Valtiovarainministeriön julkaisuja 2024:49

Valtionhallinnon pilvipalvelulinjaukset

Julkisen hallinnon ICT

Valtiovarainministeriö Helsinki 2024

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Valtiovarainministeriö
CC BY-NC 4.0

ISBN pdf: 978-952-367-844-6
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2024

Kuvailulehti
1.11.2024

Valtionhallinnon pilvipalvelulinjaukset

Valtiovarainministeriön julkaisuja 2024:49		**Teema**	Julkisen hallinnon ICT
Julkaisija	Valtiovarainministeriö		
Tekijät	Tommi Kangasaho, Esko Kaarlonen, Santtu Viiman, Jyri Vuorikallio, Juha Vuojärvi		
Kieli	suomi	**Sivumäärä**	28

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. Tässä teknisessä päivityksessä julkaistaan täsmennyksiä vuonna 2023 julkaistuihin 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

Sivua 9 on päivitetty 1.11.2024 ja aineisto korvaa aikaisemmin, 24.9.2024 julkaistun version.

Asiasanat julkisen hallinnon ICT, digitalisaatio, julkinen hallinto, pilvipalvelut, tietoturva, tietosuoja

ISBN PDF	978-952-367-844-6	**ISSN PDF**	1797-9714
Asianumero	VN/19802/2024	**Hankenumero**	-
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-844-6		

Presentationsblad
1.11.2024

Riktlinjer om molntjänster för statsförvaltningen

Finansministeriets publikationer 2024:49		**Tema**	Offentliga förvaltningens ICT
Utgivare	Finansministeriet		
Författare	Tommi Kangasaho, Esko Kaarlonen, Santtu Viiman, Jyri Vuorikallio, Juha Vuojärvi		
Språk	finska	**Sidantal**	28

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. I denna tekniska uppdatering publiceras preciseringar av de riktlinjer som publicerades 2023.

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 upphandlingskontrakt
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

Sidan 9 har uppdaterats 1.11.2024 och materialet ersätter den version som publicerats 24.9.2024.

Nyckelord offentliga förvaltningens ICT, digitalisering, offentlig förvaltning, molntjänster, informationssäkerhet, dataskydd

ISBN PDF	978-952-367-844-6	**ISSN PDF**	1797-9714
Ärendenummer	VN/19802/2024	**Projektnummer**	-
URN-adress	https://urn.fi/URN:ISBN:978-952-367-844-6		

Description sheet
1 November 2024

Cloud service guidelines for central government

Publications of the Ministry of Finance 2024:49		**Subject**	Public Sector ICT
Publisher	Ministry of Finance		
Authors	Tommi Kangasaho, Esko Kaarlonen, Santtu Viiman, Jyri Vuorikallio, Juha Vuojärvi		
Language	Finnish	**Pages**	28

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 a technical update to the guidelines published by the Ministry of Finance in 2023.

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

Page 9 was updated on 1 November 2024 and this version replaces the previous one published on 24 September 2024.

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

ISBN PDF	978-952-367-844-6	**ISSN PDF**	1797-9714
Reference number	VN/19802/2024	**Project number**	-

URN address https://urn.fi/URN:ISBN:978-952-367-844-6

Sisältö

1 Johdanto 7

2 Valtionhallinnon pilvipalvelulinjaukset 12
2.1 Ensisijaisesti pilveen (Cloud 1st) strategia 13
2.2 Pilvi- ja ekosysteemiratkaisut EU/ETA-alueelta 14
2.3 Valtion yhteiset pilvi- ja ekosysteemiratkaisut 15
2.4 Kilpailutukset ja hankinnat valtionhallinnon yhteisillä hankintasopimuksilla 17
2.5 Pilvipalvelujen hankinta, käyttöönotto ja hyödyntäminen 18
2.6 Julkinen tieto julkisessa pilvipalvelussa 19
2.7 Salassa pidettävä tieto julkisessa pilvipalvelussa 20
2.8 Henkilötieto julkisessa pilvipalvelussa 22
2.9 Turvallisuusluokan IV tieto julkisessa pilvipalvelussa 24

Lähteet 28

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. Palveluja kehitettäessä ja suunniteltaessa on huomioitava, että pilvipalvelut ja pilvipalveluteknologia ovat jatkossa monissa tapauksissa ainoa vaihtoehtoinen palvelumalli. Monet uudet teknologiat, kuten tekoälyyn perustuvat teknologiat hyödyntävät taustallaan pilvipalveluteknologioita.

Palvelu- ja toteutusmallien eri vaihtoehtojen perusteella voidaan rakentaa 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

Pilvipalvelulinjaukset ovat valtionvarainministeriön suositus pilvipalvelujen hyödyntämisestä. Linjaukset annetaan valtiovarainministeriön toimialaan ja tehtäviin kuuluvana yleisenä ohjauksena. Linjausten tarkoituksena on antaa suosituksia valtionhallinnon ja soveltuvin osin julkisten pilvipalvelujen käytön yleisiksi perusteiksi. Valtiovarainministeriö on 19.1.2019 antanut ensimmäisen version julkisen hallinnon pilvipalvelulinjauksista (VM/276/00.01.00.01/2018). Voimassa olevat linjaukset on julkaistu uudistettuna 25.10.2023. Nyt julkaistavassa linjausten teknisessä päivityksessä on huomioitu nykyisen version julkaisun jälkeen havaittuja epätarkkuuksia, oikaistu tulkinnavaraisia kohtia ja selkeytetty erityisesti turvallisuusluokka IV

tiedon käsittelyyn liittyviä periaatteita. Päivityksen muutosten valmistelu on tehty valtiovarainministeriössä, yhteistyössä Valtion tieto- ja viestintätekniikkakeskus Valtorin pilvipalvelujen sekä kokonaisturvallisuuden yhteistyöryhmien kanssa. Valtorin yhteistyöryhmissä on ollut edustettuna laaja joukko valtion virastojen asiantuntijoita. Lisäksi muutoksia on käsitelty Traficomin Kyberturvallisuuskeskuksen kanssa. Päivityksessä ei muuteta nykyisiä linjauksia keskeisiltä osiltaan. Myöskään linjauksiin vaikuttavaa sääntelyä ei ole edellisen julkaisun jälkeen muutettu.

Hallitusohjelman tavoitteet ja toimeenpano

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 johdosta myös lainsäädäntöä tulee uudistaa. 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. Hallitusohjelman mukaan kokonaisuudistuksen yhteydessä on tavoitteena kumota tiedon liikkuvuutta, pilvipalveluiden tarkoituksenmukaista käyttöä tai muuten julkisten palveluiden tarkoituksenmukaista järjestämistä haittaavat säädökset ja hyödyntää tarvittaessa nykyistä laajemmin GDPR:n kansallista liikkumavaraa. Tietosuojalainsäädännön tulkintaan liittyvät epäselvyydet ovat hidastaneet julkisen hallinnon pilvipalvelujen hyödyntämistä. Hallitusohjelman toteuttamiseksi valtiovarainministeriö on valmistellut valtionhallinnon tuottavuusohjelman toimeenpanoa. Talouspoliittinen ministeriövaliokunta on 7.2.2024 linjannut valtionhallinnon tuottavuusohjelman toimeenpanon tavoitteista ja asettanut tavoitteita tehostaa julkisen sektorin toimintaa digitalisaatiota hyödyntämällä. 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 pilvipalvelujen hyödyntämistä
- Antaa tiedonhallintayksiköille yleistä ohjausta reunaehdoista, joita noudattamalla pilvipalveluja voidaan turvallisesti hyödyntää
- Tukea pilvipalvelujen käyttöönottoon ja käyttöön liittyvää riskienarviointia ja -hallintaa ja siihen liittyvien 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 tietojenkäsittelykapasiteettia 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 niiden kumppaneita tekemään arviointeja. Tilaaja joutuu luottamaan palveluntarjoajaan sekä sopimuksista ja arviointituloksista ilmeneviin tietoihin riskienhallintaa tehdessään. Loppukädessä tilaaja joutuu varmistumaan palveluntarjoajan luotettavuudesta ja palvelun vaatimuksenmukaisuudesta ilman perinteistä fyysistä tarkastusta.

Tiedonhallintayksikön tehtävät ja vastuut pilvipalvelujen hyödyntämisessä

Tiedonhallintalaissa lähtökohtana on tiedonhallintayksikön harkintaan perustuva vapaus valita tiedonkäsittelyn keinot ja menettelyt toimintaan sovellettavan lainsäädännön asettamissa puitteissa. Pilvipalvelujen käyttö on noussut keskeiseksi keinoksi tietojenkäsittelyn tehostamisessa. Tiedonhallintayksiköllä on vastuu huolehtia tietojärjestelmien toteuttamisesta tarkoituksenmukaisella ja taloudellisella tavalla. Vastaavasti tiedonhallintayksiköillä on vastuu varmistaa pilvipalvelujen olevan vaatimustenmukaisia toiminnassaan tarvittavien tietojen käsittelemiseksi. Myös EU-sääntelyssä korostuu riskiperusteinen tiedon suojaaminen ja riskienhallinta. Vastuu erilaisten ratkaisujen käyttämisestä on tiedonhallintayksiköllä ja tätä vastuuta ei voida siirtää muille viranomaisille esimerkiksi vain noudattamalla tarjolla olevia ohjeita tai suosituksia.

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 esimerkiksi tarpeesta hajauttaa hallinta- ja valvontapalvelut toimimaan 24/7-periaatteella globaalisti. Toimintamalli haastaa tiedon suojaamiseen liittyvät nykyiset menetelmät sekä tietoturva- ja järjestelmäarkkitehtuurit uudistumaan. Uudistumisen tarve tuottaa tiedonhallintayksiköille tarpeen uudistaa näkemyksiään tietoturva- ja järjestelmäarkkitehtuureista.

Julkisella pilvipalvelulla tarkoitetaan tässä ohjeistuksessa julkisesti tarjolla olevaa ja kaikkien toimijoiden hankittavissa olevaa pilvipalvelua, joka tuotetaan EU/ETA-alueella tai sen ulkopuolelta osin tai kokonaan. Tässä tarkoitettu julkinen pilvipalvelu ei välttämättä ole kaikilta osin Suomen ja EU-lainsäädännön soveltamisen piirissä. Pilvipalveluun tallennettu tieto kuitenkin sijaitsisi lähtökohtaisesti EU/ETA-alueella tai Suomessa. Julkisen pilvipalvelun hallinta- ja valvontapalvelu voidaan tuottaa joiltakin osin kolmansissa maissa. Hallinta- ja valvontapalvelujen toteuttamiseksi voidaan telemetriikka- ja diagnostiikkatietoja siirtää kolmansiin maihin.

Näitä linjauksia voidaan hyödyntää silloin, kun on kyse julkisen, henkilötietoja sisältävän, salassa pidettävän, tai korkeintaan turvallisuusluokan IV tietojen käsittelystä. Linjauksissa ei käsitellä turvallisuusluokan I-III tietojen tai kansainvälisen tietoturvallisuusvelvoitteen mukaisesti turvallisuusluokitellun tiedon käsittelyä. Näiden turvallisuusluokkien käsittelyyn pilvipalveluissa liittyviä vaatimuksia tulee vielä selvittää. Myös tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiin liittyvää lainsäädäntöä on tarkoitus tulevaisuudessa selventää osana pääministeri Orpon hallituksen digitalisaation esteiden purkamisen tavoitetta.

Yleiset tietoon liittyvät linjaukset ja suositukset

Pilvipalveluissa, kuten kaikissa tietojärjestelmien hankinnoissa ja hallinnoinnissa, on koko elinkaaren noudatettava voimassa olevia säännöksiä ja vaatimuksia. Alla on lisäksi listattu suosituksia ja kriteeristöjä, joita voidaan hyödyntää pilvipalvelujen käytössä ja hankinnoissa:

- Tiedonhallintalautakunnan suositus salassa pidettävien asiakirjojen käsittelystä.
- Tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä.
- Tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa.
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Tiedonhallintalautakunnan suositus ja kriteeristö.
- Tiedonhallintalautakunnan 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.).

Tietovaranto voi sisältää tietoja, joihin kohdistuu useista velvoittavista säännöksistä johtuvia päällekkäisiä suojaustarpeita. Samassa tietovarannossa voi olla julkista tietoa, salassa pidettävää tietoa, henkilötietoa ja turvallisuusluokiteltua tietoa. Näihin tietoluokkiin sisältyviä tietoja voidaan tiedon luottamuksellisuuden varmistamiseen liittyvien vaatimusten puolesta pääsääntöisesti käsitellä turvallisuusluokan IV-vaatimukset täyttävissä palveluissa. Tiedonhallintayksikön on kuitenkin aina arvioitava myös mahdolliset tiedon eheyteen ja saatavuuteen liittyvät tarpeet.

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 tietoturvallisuus, 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 tietoturvallisuus, tietosuoja ja jatkuvuudenhallinta on vaatimustenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai viraston johdon riskiperusteisella päätöksellä
9. Turvallisuusluokan IV tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturvallisuus, 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 1st -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 1st -strategiaan. Pilvipalvelujen käyttöä estävä peruste voi olla sellainen käyttötapaus, jonka vaatimukset täyttyvät paremmin hyödyntämällä jotakin muuta teknologiaa. Pilvipalvelujen laajamittainen hyödyntäminen ei ole sinällään itseisarvo, mutta pilvipalveluista saatavat hyödyt suhteessa perinteisiin toteutustapoihin ovat niin merkittäviä, että niiden käytön edistämistä voidaan pitää perusteltuna.

2.2 Pilvi- ja ekosysteemiratkaisut EU/ETA-alueelta

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

Henkilötietojen käsittelyyn käytettävien pilvipalvelujen tulisi lähtökohtaisesti olla tuotettu EU/ETA-alueella silloin kun se on mahdollista. 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 olevia säännöksiä, jotka voivat velvoittaa pilvipalveluntuottajaa toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy 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, Euroopan komissio teki kaksi Iso-Britanniaa koskevaa niin kutsuttua tietosuojan vastaavuuspäätöstä EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 ja rikosasioiden tietosuojadirektiivin (EU) 2016/680 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 (EU) 2018/1807 on 28.5.2021 jälkeen edellyttänyt jäsenvaltioiden poistavan osaltaan perusteettomat sijaintia koskevat vaatimukset myös muulle kuin henkilötiedolle. Asetus ei kuitenkaan rajoita esimerkiksi yleisen turvallisuuden perusteella annettuja, suhteellisuusperiaatteen mukaisia kansallisia sijaintivaatimuksia. Kansallisesti ei tule asettaa asetuksen vastaisia sijaintivaatimuksia tiedolle. Myös tietosuoja-asetuksen 1 (3) artikla edellyttää,

että henkilötietojen vapaata liikkuvuutta unionin sisällä ei saa rajoittaa eikä kieltää syistä, jotka liittyvät luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä.

Vaikka myös EU/ETA-alueelta tuotettaviin pilvipalveluihin voi liittyä lainsäädäntöjohdannaisia riskejä, on näihin riskeihin kiinnitettävä huomiota erityisesti silloin, kun hyödynnetään EU/ETA-alueen ulkopuolelta tuotettavia pilvipalveluja. Palvelun tuottamiseen liittyvät riskit on arvioitava ja huomioitava käytettävissä suojauskeinoissa. Myös erilaiset maiden tai organisaatioiden väliset sopimukset voivat vaikuttaa sijaintiin liittyviin riskeihin. Henkilötietojen osalta on huomioitava jäljempänä 2.7. kohdassa esitetty, salassa pidettävien tietojen osalta kohdassa 2.8. esitetty ja turvallisuusluokitellun tiedon osalta kohdassa 2.9. esitetty.

Julkisten pilvipalvelujen globaaliin tuotantomalliin liittyy toimintatapa, 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 toteutuksesta yhteentoimivuutta edistävällä tavalla.

Tiedonhallintayksikön tulee hankinnan 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 palvelutuottaja Valtorin palvelut, palvelukuvaukset, palveluarkkitehtuurit ja suunnitteilla olevan tietojärjestelmän soveltuvuus käyttöympäristöihin. Yhteisten palvelujen laaja käyttäjäkunta ja palvelukeskuksen yhteisesti sovitut hallintamallit varmistavat palvelujen tasalaatuisuuden, tietoturvallisuuden vähimmäisvaatimusten toteutumisen, 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.

Valtion tieto- ja viestintätekniikkakeskus Valtori on yhdessä sen asiakkaiden kanssa suunnittelut ja toteuttanut valtion yhteisiä pilvipalveluja. Valtorin asiakkaiden pilvipalvelujen ja kokonaisturvallisuuden yhteistyöryhmät ovat laajasti käsitelleet yhteisten pilvipalvelujen tuottamiseen liittyviä kysymyksiä ja antaneet asiakasohjausta palvelutuottajalle pilvipalvelujen sisällöstä, sekä niihin liittyvistä vaatimuksista. Valtionhallinnon viranomaiset voivat myös hyödyntää näitä määrityksiä omien pilvipalvelujensa toteuttamisessa. Tietoja määrityksistä ja valtion yhteisten pilvipalvelujen teknisistä ratkaisuista antaa Valtori asiakkailleen.

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) säännökset 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 itse tarvittavia hankintoja valtion yhteisten 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.

Osana pääministeri Orpon hallitusohjelman säästötavoitteita, on talouspoliittisen ministeriövaliokunnan päätöksellä 7.2.2024 asetettu tavoitteeksi tehostaa ohjelmistojen hankintaa osana valtionhallinnon tuottavuutta. Tavoitteena on yhteishankintoja tehostamalla saavuttaa säästöjä ohjelmistojen hankinnassa. Säästötavoitteet kohdistuvat myös pilvipalveluihin. Säästötavoitteiden toteuttamiseksi on lähdetty selvittämään keinoja yhteishankintojen tehostamiseksi ja julkisen hallinnon hankintavolyymien yhtenäistämiseksi.

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. Valtiovarainministeriö on käynnistänyt julkisen hallinnon IT-sopimusehtojen (JIT) uudistamisen vuonna 2024 ja tavoitteena on huomioida pilvipalvelut uusissa sopimusehdoissa erityisesti tietosuojan ja -turvallisuuden osalta. Valtiovarainministeriön Cirrus-hankkeessa on valmisteltu julkisen hallinnon käyttöön tietosuojaan liittyviä vakioehtoja, joita tullaan hyödyntämään osana JIT-ehtojen uudistamista.

2.5 Pilvipalvelujen hankinta, käyttöönotto ja hyödyntäminen

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

Tiedonhallintayksikön tulee varmistaa huolellisella suunnittelulla pilvipalvelujen käyttöönotto vastaavalla tavalla, kuin perinteiset tietojärjestelmien hankinnat ja käyttöönotot on suunniteltu. Tässä linjauksessa on tarkoitus tuoda esille 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), jäljempänä tiedonhallintalaki, 5 §:n mukaiseen tiedonhallintamalliin ja tarvittaessa tehtävä pykälän 4 momentin mukainen muutosvaikutuksen arviointi. Pilvipalvelujen hyödyntäminen 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 hankintatoimen, tietosuojan, tietoturvallisuuden ja riskienhallinnan osaamista. Pilvipalvelujen käyttöönotto edellyttää organisaatiolta riittäviä kyvykkyyksiä.

Tiedonhallintayksiköt ovat jo aiemmin hankkineet tietojenkäsittelypalveluita yhteiskäyttöisistä palvelutuotantoympäristöistä, jossa tietojenkäsittelylaitteet, tietojärjestelmien hallinta- ja ylläpitopalvelut sekä fyysiset laitetilat on ostettu palveluna palvelutuottajilta. Jaettuja palvelutuontantoympäristöjä hankittaessa on jo ratkaistu vastaavat eriyttämiseen liittyvät haasteet, joita nyt ratkaistaan pilvipalveluissa. Jaettujen palvelujen hyödyntämiseen liittyvät riskit on aiemmin arvioitu ja niitä on hallittu riittävän kattavilla hallinnollisilla ja teknisillä kontrolleilla huomioiden voimassaolevat säädökset. Julkisten pilvipalvelujen vaatimuksenmukaisuutta voidaan arvioida hyödyntämällä jo nykyisin käytössä olevia hallinnollisilla ja teknisiä kontrolleja. Tiedonhallintayksikön tulee toimitussopimuksia tehdessään huolellisesti arvioida ja varmistaa vaatimuksenmukaisuuden ehtojen täyttyminen. Pilvipalveluissa on laajasti käytössä erilaisia teknisiä kontrolleja, joita voidaan hyödyntää riskien hallitsemiseksi.

Pilvipalvelut tuottavat viranomaisten varautumiseen uudenlaisia mahdollisuuksia ja haasteita palvelutuotantomallin sekä tiedon fyysisen sijoittumisen moninaisuuden takia. Varautumisesta tulee pilvipalveluiden kohdalla huolehtia vastaavasti kuin muissakin tietojärjestelmäpalveluissa. Viranomaisella on valmiuslain (1552/2011) 12 § perusteella velvollisuus huolehtia toimintansa ennakollisesta varautumissuunnittelusta, sisältäen myös varautumisjärjestelyjen toteuttamisen ja testaamisen. Pilvipalvelujen osalta varautumisessa tulee erityisesti ottaa huomioon lainsäädäntöjohdannaiset riskit. Lisäksi on huomioitava viranomaisen toiminnan jatkuvuus kaikissa olosuhteissa. Valtion yhteisten tieto- ja viestintäteknisten palvelujen osalta Valtori tarjoaa asiakkailleen toimintamalleja ja teknologioita varautumisen toteuttamiseksi.

2.6 Julkinen tieto julkisessa pilvipalvelussa

Julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturvallisuus, 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. Mikäli julkisiin tietoihin sisältyy myös henkilötietoja, on huomioitava linjaus 8. Tiedonhallintalain 4 luvussa asetetut tietoturvallisuus- ja tiedonhallintavaatimukset koskevat myös julkisen tiedon käsittelyä. Vaatimusten noudattaminen 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 huolehtia tiedon saatavuudesta. Tiedonhallintayksikön tulee tiedonhallintalain 4 luvun mukaisten tietoturvallisuusvaatimusten 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 tarvittavilla varayhteyksillä.

Tiedonhallintalain 13 §:n vaatimus tietoaineistojen saatavuuden varmistamisesta koko elinkaaren ajan ja 13 a §:n vaatimus häiriötilainteisiin varautumisesta edellyttävät tiedon saatavuuden arviointia. Lähtökohtana varautumisessa on perinteisesti ollut tiedon sijoittaminen Suomen rajojen sisäpuolelle tai huolehtiminen tiedon siirtämisestä tarvittaessa Suomeen. Viranomaisten varautumissuunnittelussa on kuitenkin hyvä arvioida myös mahdollista tarvetta sijoittaa tiedot Suomen rajojen ulkopuolelle tietojen saatavuuden varmistamiseksi.

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 eri tietoaineistojen käsittelyyn arvioitaessa organisaation on selvitettävä pilvipalvelun turvallisuuteen liittyvät riskit.

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 tiedonhallintayksiköille 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 tai useiden valtioiden 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 esimerkiksi tiedon sijoittamisella sellaiseen pilvipalveluun, johon sovelletaan Suomen lainsäädäntöä, sekä huolehtimalla riittävästä tiedon salaamisesta luotettavalla tavalla. Salaaminen tulee toteuttaa tarkoituksenmukaisella tavalla ja valita riskien arvioinnin jälkeen riittävän turvallinen salausmenetelmä. Erilaiset salausmenetelmät soveltuvat erilaisia riskejä vastaan. Valinnan jälkeen tulee arvioida koko tietojenkäsittely-ympäristöön kohdistuvat riskit ja hyväksyä jäännösriskit kokonaisuutena.

Suunniteltaessa ja arvioitaessa salassa pidettävän turvallisuusluokittelematto-man tiedon käsittelyä pilvipalveluissa voidaan hyödyntää muun muassa seuraavia suosituksia:

- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö Julkri (VM 2023:46)
- Tiedonhallintalautakunnan suositus salassa pidettävien asiakirjojen käsittelystä pilvipalveluissa (VM 2022:4)

Salassa pidettävän tiedon osalta on myös huomioitava mahdollinen kasaumavaiku-tus. Käytännössä salassa pidettävää tietoa sisältävä tietovaranto voi kokonaisuutena synnyttää turvallisuusluokiteltavana tietona pidettävän kasauman. Tällainen tilanne voi edellyttää tiedon sijainnin ja suojauksen uudelleenarviointia. On kuitenkin huo-mioitava, että suurikaan määrä salassa pidettävää tietoa ei ole automaattisesti peruste kasaumavaikutukselle ja turvallisuusluokittelun perusteiden täyttymiselle.

2.8 Henkilötieto julkisessa pilvipalvelussa

Henkilötietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturval-lisuus, 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, jota täydentää Suomessa kansallinen tietosuojalaki (1050/2018). Lisäksi on olemassa asetuksen kansallisen liikkumavaran perusteella annettua erityislainsäädäntöä. Henkilötietojen käsittelyyn rikosasioissa ja kansalli-sen turvallisuuden ylläpitämisen yhteydessä sovelletaan henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia (1054/2018). Tietosuojasääntely ei ota suoraan kantaa pilvipalveluihin, mutta aset-taa vaatimuksia henkilötiedon käsittelylle toteutustavasta riippumatta.

Yleinen tietosuoja-asetus rajoittaa henkilötietojen siirtoa EU:n ja ETA-alueen ulko-puolelle kolmansiin maihin. Henkilötietojen siirrolle on tällöin oltava tietosuo-ja-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 silloin, kun 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. 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 tullut 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 välein. 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.

Yleisen tietosuoja-asetuksen nojalla tehdyt vastaavuuspäätökset eivät sovellu tietojen siirtoihin rikosasioiden tietosuojalain soveltamisalalla, eikä vastaavuuspäätöksiä rikosasioiden tietosuojadirektiivin (EU) 2016/680 nojalla ole vielä Iso-Britanniaa lukuunottamatta annettu. Tällaisissa kolmansiin maihin tehtävissä siirroissa on noudatettava henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018) 7 luvun säännöksiä.

2.9 Turvallisuusluokan IV tieto julkisessa pilvipalvelussa

Turvallisuusluokan IV tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturvallisuus, 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 lainsäädännön asettamien vaatimusten mukaisesti koko tiedon elinkaaren ajan ja huomioiden muun muassa edellä kuvatut lainsäädäntöjohdannaiset ja toisen valtion määräysvaltaan liittyvät riskit.

Turvallisuusluokitteluvelvoitteesta säädetään tiedonhallintalain 18 §:ssä. Turvallisuusluokittelusta, turvallisuusluokitellun tiedon merkitsemisestä ja sen tietoturvallisesta käsittelystä säädetään valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jäljempänä turvallisuusluokitteluasetus. Asetuksessa on korostettu turvallisuusluokiteltujen asiakirjojen monitasoista suojausta (asetuksen 7 §), tiedonsaantitarvetta ja 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.

Turvallisuusluokitteluasetus sääntelee turvallisuusluokiteltujen tietojen käsittelyä. Asetuksen 9 §:n mukaan tiedonhallintayksikön on määritettävä seuraavat fyysisesti suojatut *turvallisuusalueet* turvallisuusluokiteltujen asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi asetuksen 10 §:ssä tarkoitetulla tavalla:

> 1) *hallinnolliset alueet,* joilla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa;
>
> 2) *turva-alueet,* joilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle.

Turvallisuusluokitteluasetuksen 10 §:n 1 momentin mukaan turvallisuusluokiteltuja asiakirjoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta. Turvallisuusluokitteluasetuksen 10 §:n 3 momentin 3 ja 4 kohtien perusteella turvallisuusluokan IV paperiasiakirjat on säilytettävä turvallisuusalueella ja turvallisuusluokan IV asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turvallisuusalueelle. Myös hallinnollinen alue on turvallisuusalue, joten esimerkiksi turvallisuusluokan IV asiakirjojen käsittelyyn tarkoitetun pilvipalvelun osalta on vaatimuksena sen sijoittaminen vähintään hallinnolliselle alueelle.

Tiedonhallintalautakunnan suosituksen turvallisuusluokiteltavien asiakirjojen käsittelystä mukaan hallinnollisella alueella tarkoitetaan viranomaisen normaaliin työskentelyyn tarkoitettuja alueita ja tiloja, kuten toimistotilaa tai useista eri toimistotiloista muodostuvaa kokonaisuutta. Niitä voivat olla esimerkiksi palvelintilat, konesalit tai esimerkiksi yritysten tilat. Tilaa hallitseva toimija varmistaa, että tiloihin on itsenäinen pääsy ainoastaan viranomaisen ennalta valtuuttamilla henkilöillä. Hallinnollista aluetta rajaavalle rakenteelle ei aseteta erityisiä vaatimuksia (Tiedonhallintalautakunta 2021, s.36). Tiedonhallintayksikön riskien arvioinnin tulos voi vaikuttaa siihen, millaisia fyysisiä tai muita turvatoimia on kulloinkin syytä asettaa.

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö Julkrissa on esitetty esimerkkejä siitä, kuinka alueeseen liittyvän vaatimuksen voi viranomaisen toimeksiannosta toteuttaa ja hallinnoida myös pilvipalvelun tarjoaja, tiedonhallintayksikön edelleen vastatessa palvelusta. Tämän lisäksi esimerkiksi salausta voidaan käyttää

keinona, jolla tietoja suojataan sivullisilta turvallisuusluokitteluasetuksen 10 §:n 1 momentin mukaisesti. Turvallisuusluokitteluasetus ei sisällä vaatimusta, jonka mukaan hallinnollisen alueen tulisi sijaita Suomessa.

Valtion tieto- ja viestintätekniikkakeskus Valtori on yhdessä asiakkaidensa tietoturvallisuus- ja riskienhallinta-asiantuntijoiden kanssa laatinut käytännön ohjeita TL IV tiedon käsittelyn mahdollistamiseksi julkisissa pilvipalveluissa. Ohjeissa käsitellään myös vaihtoehtoisia suojaamiskeinoja sekä näiden pohjalta tehtävää jäänösriskiarviota. Ohjeiden tarkoituksena on antaa tukea tiedonhallintalain 13 §:n mukaisen riskiarvion tekemiseen ja riskipohjaiseen päätöksentekoon. Näidenkin ohjeiden osalta tulee kuitenkin huomioida, että tiedonhallintayksikkö vastaa tietojensa asianmukaisesta suojaamisesta riskiarviointinsa perusteella, ja että tiedonhallintayksikön tulee pystyä tietoisesti hyväksymään tietojenkäsittelynsä valintoihin liittyvät jäännösriskit.

Tiedonhallintalain 14 §:ssä ja vastaavasti turvallisuusluokitteluasetuksen 12 §:n 2 momentissa edellytetään tiedon salaamista sen siirtämiseksi yleisessä tietoverkoissa ja turvallisuusalueen ulkopuolella. Tietoa voidaan kuitenkin siirtää salaamattomana turvallisuusalueen sisällä muussa kuin yleisessä tietoverkossa. 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 mm. Julkri-kriteeristöä soveltaen riskilähtöisesti organisaation omiin tarpeisiin.

Turvallisuusluokitteluasetuksen mukaisesti valtionhallinnon viranomaisen on myös ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle (6 §). Viranomaisen tiedonhallintayksikön tulee valita soveltamansa menettely ennakolta varmistamisen toteuttamiseen. Joissain tilanteissa saattaa olla perusteltua hyödyntää esimerkiksi sopimuksia, pilvipalveluntarjoajan itsearviointeja tai riippumattomien ulkoisten toimijoiden arviointeja. Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa (1406/2011), jäljempänä arviointilaki, säädetään mahdollisuudesta hankkia todistus tietojärjestelmien vaatimuksenmukaisuudesta, mitä

voidaan tyypillisesti soveltaa Suomen lainsäädännön piirissä toimiviin pilvipalvelun-tarjoajiin. Pilvipalvelujen käytön osalta kannattaa lisäksi huomioida, että velvoitetta arviointilain 8 §:ssä tarkoitetun todistuksen hankkimiseen kansallisen turvalli-suusluokan IV tiedon käsittelyä varten ei ole säädetty. Kuten muussakin tietojen käsittelyssä, tiedonhallintayksikkö tai virasto itse vastaa lopulta pilvipalvelun hyö-dyntämiseen liittyvien riskien hallinnasta.

Seuraavia turvallisuusluokan IV-tiedon käsittelyyn liittyviä ohjeita voidaan soveltu-vin osin hyödyntää palvelujen suunnittelussa:

- Julkisen hallinnon tiedonhallintalautakunnan suositukset: Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5)
- Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa (VM 2022:4)
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö (VM 2023:46)
- Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille (VM 2020:73).
- Ohje turvallisuuskriittisiin hankintoihin: Määräysvaltamuutoksiin varautuminen turvallisuuskriittisissä tieto- ja viestintäjärjestelmien sekä -ratkaisujen hankinnoissa (VM 2019:7)

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. Vierailtu 5.9.2024.

Tiedonhallintalautakunta 2023. Suositus tietoturvallisuudesta hankinnoissa. Valtiovarainministeriön julkaisuja 2023:57. Valtioneuvoston hallintoyksikkö, Helsinki. Osoitteessa: http://urn.fi/URN:ISBN:978-952-367-645-9. Viitattu 5.9.2024.

Tiedonhallintalautakunta 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 5.9.2024.

Tiedonhallintalautakunta 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 5.9.2024.

Tiedonhallintalautakunta 2022. Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa. Valtiovarainministeriön julkaisuja 2022:4. Valtioneuvoston hallintoyksikkö, Helsinki. Osoitteessa: http://urn.fi/URN:ISBN:978-952-367-906-1. Viitattu 5.9.2024.

Tiedonhallintalautakunta 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Valtiovarainministeriön julkaisuja 2021:5. Valtioneuvoston hallintoyksikkö, Helsinki. Osoitteessa: http://urn.fi/URN:ISBN:978-952-367-500-1. Viitattu 5.9.2024.

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 5.9.2024.

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 5.9.2024.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

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

ISSN 1797-9714 (pdf)
ISBN 978-952-367-844-6 (pdf)

Syyskuu 2024