VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa

Lautakunnat

Valtiovarainministeriön julkaisuja – 2022:4

Valtiovarainministeriön julkaisuja 2022:4

Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa

Valtiovarainministeriö Helsinki 2022

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

ISBN pdf: 978-952-367-906-1
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2022

Kuvailulehti

10.1.2022

Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa

Valtiovarainministeriön julkaisuja 2022:4		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	suomi	**Sivumäärä**	30

Tiivistelmä

Tämä tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa täydentää aiemmin annettua suositusta turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5). Nämä kaksi suositusta opastavat täyttämään julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 18 §:n ja asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun valtioneuvoston asetuksen (1101/2019) vaatimuksia. Tiedonhallintayksiköitä suositellaan valitsemaan pilvipalvelu siinä käsiteltävien turvallisuusluokiteltujen tietoaineistojen tiedonhallinta- ja tietoturvallisuusvaatimusten sekä käsittelyn käyttötapausten perusteella. Pilvipalveluihin liittyvien riskien hallitsemiseksi tiedonhallintayksiköitä suositellaan käyttämään sellaisia pilvipalveluita, joiden turvallisuus ja joiden tarjoajan turvallisuus on arvioitu turvallisuusselvityslain mukaan tehdyissä yritysturvallisuusselvityksissä, tai joille on myönnetty tietoturvallisuuden arviointitoimintaa koskevien säännösten mukainen turvallisuusvaatimustenmukaisuutta osoittava todistus.

Tiedonhallintalautakunta hyväksyi suosituksen 13.12.2021.

Asiasanat	tiedonhallintalautakunta, tiedonhallintalaki, suositus, Julkisen hallinnon ICT, lautakunnat, tietoturva, julkinen hallinto, luokitukset, asiakirjat, tieto

ISBN PDF	978-952-367-906-1	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-906-1		

Presentationsblad

10.1.2022

Hantering av säkerhetsklassificerade handlingar i molntjänster

Finansministeriets publikationer 2022:4		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	finska	**Sidantal**	30

Referat

Denna rekommendation från informationshanteringsnämnden om hantering av säkerhetsklassificerade handlingar i molntjänster kompletterar den tidigare rekommendationen om hantering av säkerhetsklassificerade handlingar (FM 2021:5). Dessa två rekommendationer hjälper att uppfylla kraven i 18 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019) och i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019). Det rekommenderas att informationshanteringsenheterna väljer en molntjänst på basis av informationshanterings- och informationssäkerhetskraven samt användningsfallen i fråga om sådant säkerhetsklassificerat informationsmaterial som behandlas i tjänsten. För att hantera riskerna i anslutning till molntjänster rekommenderas det att informationshanteringsenheterna använder sådana molntjänster vars säkerhet och erbjudarens säkerhet har bedömts i säkerhetsutredningar av företag enligt säkerhetsutredningslagen, eller som beviljats ett intyg om överensstämmelse med säkerhetskraven enligt bestämmelserna om bedömning av informationssäkerhet.

Informationshanteringsnämnden godkände rekommendationen den 13 december 2021.

Nyckelord	informationshanteringsnämnden, informationshanteringslagen, rekommendation, den offentliga förvaltningens IKT, nämnderna, informationssäkerheten, den offentliga förvaltningen, klassificeringar, handlingar, information		
ISBN PDF	978-952-367-906-1	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-906-1		

Description sheet

10 January 2022

Handling of classified documents in cloud computing services

Publications of the Ministry of Finance 2022:4		**Subject**	Board
Publisher	Ministry of Finance		
Group author	Information Management Board		
Language	Finnish	**Pages**	30

Abstract

This recommendation of the Information Management Board on the handling of classified documents in cloud computing services supplements the previous recommendation on the handling of documents that are subject to security classification (Ministry of Finance 2021:5). These two recommendations offer guidance on how to meet the requirements of section 18 of the Act on Information Management in Public Administration (906/2019) and the Government Decree on Security Classification of Documents in Central Government (1101/2019). It is recommended that information management units select a cloud computing service based on use cases and on the information management and information security requirements specified for the classified information materials handled in the service. To manage the risks associated with cloud computing services, it is recommended that information management units use services or providers that have undergone facility security clearances under the Security Clearance Act or that have been granted a certificate of conformity with security requirements referred to in the provisions regarding information security assessment.

The Information Management Board approved the recommendation on 13 December 2021.

Keywords Information Management Board, Information Management Act, recommendation, public sector ICT, boards, information security, public administration, classification, documents, information

ISBN PDF	978-952-367-906-1	**ISSN PDF**	1797-9714
URN address	https://urn.fi/URN:ISBN:978-952-367-906-1		

Sisältö

1 Johdanto

Tämä tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa on valmisteltu tiedonhallintalautakunnan kaudelle 1.4.2020–31.12.2021 asettamassa turvallisuusluokiteltavien asiakirjojen jaostossa. Jaoston puheenjohtajana on toiminut tietohallintoneuvos Tuija Kuusisto valtiovarainministeriöstä. Tiedonhallintalautakunta on nimennyt jaoston jäseniksi asiantuntijoita eri tiedonhallintayksiköistä. Suositusluonnos oli avoimesti kommentoivana julkisen lausuntopalvelun kautta 15.10.-15.11.2021 välisenä aikana.

Tämä suositus täydentää aiemmin annettua suositusta turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5). Nämä kaksi suositusta opastavat täyttämään julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, jatkossa TihL tai tiedonhallintalaki) 18 §:n ja asiakirjojen turvallisuusluokittelusta valtionhallinnossa annetun valtioneuvoston asetuksen (1101/2019, turvallisuusluokitteluasetus tai TLa) vaatimuksia. Tässä suosituksessa ei käsitellä muita pilvipalvelujen käyttöä rajoittavia säännöksiä, kuten tietosuojaa tai kansainvälisen tietoturvallisuusvelvoitteen mukaisesti turvallisuusluokiteltuihin aineistoihin liittyviä säännöksiä.

Tiedonhallintalain mukaan valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Suosituksessa turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5) on linjattu seuraavasti turvallisuusluokiteltavien asiakirjojenkäsittelyä pilvipalveluissa: ”Turvallisuusluokan IV asiakirjojen käsittely ja säilytys on mahdollista sellaisissa pilvipalveluissa, joihin ei arvioida kohdistuvan lainsäädäntöjohdannaisia riskejä edellyttäen, että viranomainen on huomioinut myös kaikki muutkin turvallisuusluokitellun tiedon käsittelyyn liittyvät suojaustarpeet ja -velvoitteet. Turvallisuusluokan IV asiakirjojen säilyttäminen muissa pilvipalveluissa on mahdollista vain luotettavasti salatussa muodossa siten, että salausta ei voida purkaa tiedon elinkaaren aikana kyseisessä palvelussa. Siten osa viranomaisen turvallisuusluokitellun tiedon käsittely-ympäristöstä voi olla toteutettu pilviteknologiaa hyödyntäen.” Näitä linjauksia on tässä suosituksessa ajantasaistettu ja täsmennetty.

Tässä suosituksessa kuvataan turvallisuusluokiteltavien asiakirjojen käsittelyyn pilvipalveluissa liittyvät keskeiset säännökset sekä turvallisuusluokiteltavien asiakirjojen suojaamisen riskienhallintamenettelyä ja riskienhallinnan vaikutusten arviointia. Suosituksessa kuvataan myös turvallisuusluokiteltavien asiakirjojen käsittelyssä käytettävien pilvipalveluiden ja niiden tarjoajien luotettavuuden arviointia sekä pilvipalveluja koskevissa palvelusopimuksissa huomioitavia näkökulmia.

2 Säädökset ja muu ohjeistus

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa on erityisesti suunnattu tiedonhallinnan ja -käsittelyn asiantuntijoille, pilvipalveluiden ja teknologian hankinnasta vastaaville ja kehittäjille sekä tiedon suojaamisesta vastaaville tahoille. Pilviteknologialla tarkoitetaan teknologisia ratkaisuja, joihin pilvipalvelujen tarjoaminen perustuu. Suositus koskee tiedonhallintalakia ja turvallisuusluokitteluasetusta:

- **Laki julkisen hallinnon tiedonhallinnasta (906/2019, TihL tai tiedonhallintalaki).** Tiedonhallintalaissa säädetään muun muassa viranomaisten tietoaineistojen tietoturvallisesta käsittelystä ja tietoturvallisuustoimenpiteiden toteuttamisesta. Laki velvoittaa julkisen hallinnon tiedonhallintayksiköitä ja viranomaisia sekä julkisia hallintotehtäviä hoitavia yksityishenkilöitä, yhteisöjä ja muita kuin viranomaisina toimivia julkisoikeudellisia yhteisöjä. Tiedonhallintalaissa säädetään muun muassa tietoturvallisuustoimenpiteiden vähimmäistasosta, mutta jätetään tiedonhallintayksiköille riskiperusteista harkintavaltaa toimenpiteiden toteuttamiseksi. Tiedonhallintalain 18 §:ssä säädetään valtion virastoissa, laitoksissa ja valtion liikelaitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien velvollisuudesta turvallisuusluokitella tietyt asiakirjat.

- **Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019,** turvallisuusluokitteluasetus tai **TLa).** Asetuksessa säädetään tarkemmin tiedonhallintalain mukaisten turvallisuusluokiteltavien asiakirjojen turvallisuusluokittelusta ja turvallisuusluokittelumerkinnöistä sekä tietoturvallisesta käsittelystä.

Suositus ei koske muita pilvipalvelujen käyttöä rajoittavia säännöksiä. Turvallisuusluokiteltujen asiakirjojen käsittelyyn pilvipalveluissa liittyviä muita keskeisiä säännöksiä ovat:

- **Euroopan parlamentin ja neuvoston asetus (EU) 2018/1807, muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa.** Asetuksen keskeinen vaikutus on, että jäsenvaltiot eivät voi vaatia sähköisessä muodossa olevaa muuta kuin henkilötietoa säilytettäväksi tai käsiteltäväksi tietyllä alueella, ellei vaatimusta voi perustella yleisellä turvallisuudella.

- **Laki viranomaisten toiminnan julkisuudesta (621/1999, julkisuuslaki).** Julkisuuslaissa säädetään mm. julkisuusperiaatteesta, viranomaisen tiedon luovuttamisesta sekä salassapidosta. Tiedonhallintalain 18 §:n mukaan turvallisuusluokittelu tulee tehdä julkisuuslain 24 §:n 1 momentin 2, 5 ja 7-11 kohdissa määritellyille asiakirjoille, joiden sisältämän tiedon oikeudeton käyttö tai paljastuminen voi aiheuttaa vahinkoa muun muassa kansalliselle turvallisuudelle.

- **Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011, arviointilaki).** *"Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden arvioinnissa vain tässä laissa tarkoitettua menettelyä tai sellaista arviointilaitosta, joka on saanut Viestintäviraston"* (nykyisin Liikenne- ja viestintävirasto, jäljempänä Traficom) *"hyväksynnän **tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011, arviointilaitoslaki**) mukaan."*

- **Turvallisuusselvityslain (726/2014)** *"tarkoituksena on parantaa mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita, yleistä turvallisuutta tai muuta niihin verrattavaa yleistä etua taikka erittäin merkittävää yksityistä taloudellista etua taikka edellä tarkoitettujen etujen suojaamiseksi toteutettavia turvallisuusjärjestelyjä".* Turvallisuusselvityslain 9 §:n 3 momentin mukaisesti Traficom *"laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen".*

Lukijaa kehotetaan tämän suosituksen lisäksi tutustumaan tiedonhallintalautakunnan muihin suosituksiin sekä valtiovarainministeriön pilvipalveluita koskeviin linjauksiin ja ohjeisiin (Valtiovarainministeriö 2018:35, 2020:66, 2020:73). Lisäksi Traficomin Kyberturvallisuuskeskus on julkaissut Pilvipalveluiden turvallisuuden arviointikriteeristön (Pitukri, Traficomin julkaisuja 13/2020).

3 Riskienhallinta ja vaikutusten arviointi

Tiedonhallintayksikön on tiedonhallintalain 13 §:n mukaan selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Tiedonhallintayksikön riskienhallintaa on yleisesti käsitelty tiedonhallintalautakunnan suosituskokoelmassa tiettyjen tietoturvallisuussäännösten soveltamisesta (VM 2021:65).

Kun pilviteknologiaa harkitaan käytettäväksi turvallisuusluokiteltavien asiakirjojen käsittelyssä, tiedonhallintayksikön tulee riskiarvioinnin mahdollistamiseksi tunnistaa

- mitä turvallisuusluokiteltavia tietoaineistoja pilviteknologialla on tarkoitus käsitellä, ja
- mitkä ovat näiden tietoaineistojen käsittelyn tiedonhallinta- ja tietoturvallisuusvaatimukset ja käsittelyn käyttötapaukset, sekä niihin liittyvät viranomaisprosessit.

Lisäksi tiedonhallintayksikön tulee arvioida tarpeet pilviteknologian käytölle. Pilviteknologian käytöllä turvallisuusluokiteltavien asiakirjojen käsittelyssä voidaan tavoitella esimerkiksi kustannustehokkuutta, tiedon säilyttämistarpeita tai tietyn pilviteknologian mahdollistaman teknologian, kuten laajan analytiikan tai tekoälyn hyödyntämistä.

Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn liittyvät riskit luvuissa 3.1 ja 3.2 kuvatulla tavalla huomioiden pilviteknologialla käsiteltäviksi suunnitellut turvallisuusluokitellut tietoaineistot, ja niiden tiedonhallinta- ja tietoturvallisuusvaatimukset, sekä käyttötapaukset ja viranomaisprosessit, sekä mitoitettava tietoturvallisuustoimenpiteet tämän mukaisesti. Lisäksi tiedonhallintayksikön tulee myös tehdä tiedonhallintalain 5 §:ssä tarkoitettu tietojenkäsittelyyn liittyvä muutosvaikutusten arviointi, jos kyseessä on muutos olemassa olevaan tietojen käsittelyprosessiin. Muutosvaikutusten arvioinnissa tulee ottaa huomioon myös käsittelyn kannalta olennaiset poikkeustilanteiden jatkuvuudenhallintaan liittyvät toimenpiteet sekä menettelyt. Jos turvallisuusluokiteltaviin asiakirjoihin sisältyy henkilötietoja, tiedonhallintayksikön tulee arvioida erillisen tietosuojavaikutusten arvioinnin tarve.

3.1 Turvallisuusluokiteltavien asiakirjojen käsittelyyn pilvipalveluissa liittyvästä riskienhallinnasta

Turvallisuusluokiteltavien asiakirjojen käsittelyä pilviteknologioilla toteutetuissa palveluissa koskevat merkittävimmät riskit ja niiden hallitsemiseksi tarvittavat toimenpiteet liittyvät turvallisuusluokiteltujen tietojen tai tiedonkäsittelijöiden fyysiseen sijaintiin eli pilvipalveluiden tuotantomalliin sekä pilvipalveluiden toteutus- ja palvelumalleihin ja tarjoajaan.

Turvallisuusluokiteltavien asiakirjojen käsittelyyn erityisesti muissa kuin Suomesta tuotetuissa pilvipalveluissa liittyy useita globaaleihin tuotantoketjuihin ja toimijoihin liittyviä riskejä. Turvallisuusluokiteltaviin asiakirjoihin kohdistuvien riskien näkökulmasta pilvipalvelujen tuotantomallit voidaankin ryhmitellä kahteen päämalliin: Suomesta tuotettu pilvipalvelu ja kansainvälinen pilvipalvelu. Asiantuntija-arvioinnin perusteella ei tällä hetkellä ole mahdollista jakaa tuotantomalleja tarkemmin ja tunnistaa muita, esimerkiksi maantieteeseen perustuvia kansainvälisiä pilvipalvelujen tuotantomalleja.

Yleisimpiä pilvipalvelujen toteutusmalleja ovat yksityinen pilvi, yhdistelmäpilvi ja julkinen pilvi. Yleisimpiä palvelumalleja ovat SaaS, PaaS, IaaS ja CaaS. Palvelumalleihin liittyviä riskejä on käsitelty seuraavissa ohjeissa: VM 2018:35, 2020:66 ja Pitukri. Tuotanto-, toteutus- ja palvelumalleja on kuvattu tarkemmin liitteenä 1 olevassa termistössä.

Pilvipalvelun käyttöönottoa suunniteltaessa on kiinnitettävä huomiota yksittäisen asiakirjan turvallisuusluokan lisäksi siihen, mihin kokonaisuuteen asiakirja kuuluu sekä siihen, mikä on kokonaisuuden turvallisuusluokka. Tämän niin sanotun kasaumavaikutuksen arvioinnista on kirjoitettu Suosituksessa turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5), luvussa 5.3. Lisäksi on arvioitava pilvipalvelun ja sen sisältämän turvallisuusluokitellun tiedon kriittisyys myös jatkuvuudenhallinnan ja poikkeusoloihin varautumisen näkökulmasta. Turvallisuusluokiteltujen tietojen tulee useissa käyttötapauksissa ja viranomaisprosesseissa olla käytettävissä kaikissa turvallisuustilanteissa, myös normaaliolojen häiriötilanteissa ja poikkeusoloissa, jolloin tiedon maantieteellinen sijainti ei voi olla – ainakaan yksinomaan - Suomen ulkopuolella.

Joissakin erityistilanteissa kansainvälisten pilvipalvelujen käyttö voi olla viranomaisen operatiivisten tarpeiden vuoksi välttämätöntä turvallisuusluokitellun tiedon käsittelyssä. Esimerkiksi viranomaisen operatiiviseen toimintaan voi sisältyä ihmishenkien pelastaminen ulkomailla yllättäen tapahtuneessa luonnonkatastrofitilanteessa, jolloin tavanomaisia turvallisia viestintäyhteyksiä ei aina ole mahdollista ottaa käyttöön riittävän nopeasti. Tällaisessa tilanteessa turvallisuusluokiteltujen tietojen salassapito- ja turvallisuusluokitteluaika on hyvin lyhyt ja turvallisuusluokiteltuja tietoja tarvitaan ja ne voidaan luovuttaa esimerkiksi usean maan viranomaisten yhteistyökokouksissa käsiteltäviksi.

Kun käsiteltävät turvallisuusluokitellut tietoaineistot, niiden tiedonhallinta- ja tietoturvallisuusvaatimukset ja käyttötapaukset sekä viranomaisprosessit ja tarpeet pilviteknologian käytölle on kuvattu, tiedonhallintayksikön tulee riskiperustaisesti käyttötapauksittain päättää siitä, mitä pilvipalvelun tuotanto-, toteutus- ja palvelumallia voidaan käyttää minkäkin turvallisuusluokitellun tietoaineiston käsittelyssä. Riskiperustainen päätöksenteko tarkoittaa sitä, että tiedonhallintayksikkö arvioi pilvipalvelujen tuotanto-, toteutus- ja palvelumalleihin sekä palveluntarjoajaan liittyvät riskit ja toteuttaa niiden hallitsemiseksi tarvittavat toimenpiteet ennen kuin turvallisuusluokiteltuja tietoja käsitellään pilvipalveluissa. Suositeltavaa on, että riskienhallinnassa tiedonhallintayksikkö tekee tai hyödyntää jo tehtyjä selvityksiä ja arvioita tiedonhallinnan ja tietoturvallisuuden vaatimustenmukaisuuden toteutumisesta.

Pilvipalveluiden käyttöön liittyvien tietoturvallisuustoimenpiteiden suunnittelussa ja valinnassa voidaan hyödyntää tiedonhallintalautakunnan suositusten lisäksi yleisimpiä turvallisuusluokiteltuun tietoon kohdistuvien riskien vaikutuksia pienentämään suunnattuja ohjeita, kuten kansallisen turvallisuusviranomaisen julkaisemaa Katakri 2020 -arviointityökalua ja Kyberturvallisuuskeskuksen julkaisemaa PiTuKri-ohjetta. Yleisten turvallisuusluokiteltuun tietoon kohdistuvien riskien lisäksi tiedonhallintayksikön tulee huomioida erityiset riskit, jotka liittyvät arvioitavassa pilvipalvelussa käsiteltäviksi suunniteltuihin turvallisuusluokiteltuihin tietoaineistoihin ja niiden käsittelyyn eri käyttötapauksissa ja viranomaisprosesseissa. Erityisten riskien hallitsemiseksi on suunniteltava ja toteutettava hallintamenettelyt. Nämä menettelyt tulee valita huomioiden sekä tietoturvallisuustoimenpiteiden toteutusvaatimukset, että kokonaistaloudellinen edullisuus.

Turvallisuusluokiteltuun tietoaineistoon kohdistuvien riskien tunnistamisen ja arvioinnin sekä tietoturvallisuustoimenpiteiden riskiarvioon perustuvan toteuttamisen tarkoituksena on täydentää ja täsmentää säädöksissä asetettuja turvallisuusluokitellun tiedon suojaamiseen kohdistuvia vähimmäisvaatimuksia. Jokainen tunnistettu riski tulee arvioida. Jos arvioinnin tuloksena todetaan, että riskin jäännösriski voidaan hyväksyä tai että riskin todennäköisyys tai vaikutus on hyvin alhainen kyseeseen tulevissa turvallisuusluokiteltujen tietoaineistojen käsittelyn käyttötapauksissa tai viranomaisprosesseissa, tiedonhallintayksikkö voi jättää riskiin liittyvän hallintatoimenpiteen tai suojauksen toteuttamatta.

Tiedonhallintayksikkö voi jättää riskiin liittyvän hallintatoimenpiteen tai suojauksen toteuttamatta myös, jos jokin toinen riskien hallintatoimenpide tai suojaus ehkäisee tunnistetun riskin vaikutukset luotettavasti. Esimerkiksi tehokkaalla poikkeamien havainnointi- ja reagointikyvyllä voi tietyissä tapauksissa olla mahdollista pyrkiä täydentämään muissa suojaustavoissa tunnistettuja puutteita. Lisäksi esimerkiksi yksityisen pilvipalvelun koko tietojenkäsittely-ympäristön eriyttäminen, mukaan lukien päätelaitteiden fyysinen eriyttäminen, voi ehkäistä useiden tietoverkkoihin liittyvien riskien vaikutuksia tehokkaasti ja siten toimia riittävänä suojauksena. Pilvipalveluun sijoitetun sovelluksen syötteiden

käsittelyn puutteisiin liittyviä riskejä voi esimerkiksi olla mahdollista pienentää käyttämällä sovellusrajapinnan edessä sovelluspalomuuria (WAF, Web Application Firewall). Esimerkiksi haittaohjelmiin liittyviä riskejä voi olla mahdollista hallita validoimalla sisään tuotavia tietoja pilvipalvelun rajapinnoissa. Tiedonhallintayksikön riskiarvioinnin perusteella päätettyjen hallintatoimenpiteiden/suojausten toteuttamatta jättämisen ei tule kuitenkaan johtaa tilanteeseen, jossa jäljempänä kuvattavat keskeiset riskit jätetään huomioimatta tai niiden vaikutuksia pienentävät säädetyt vähimmäisvaatimukset ja tarvittavat suojaavat hallintatoimenpiteet jätetään toteuttamatta.

3.2 Keskeisiä turvallisuusluokiteltaviin asiakirjoihin pilvipalveluissa kohdistuvia riskejä

Turvallisuusluokiteltuihin tietoihin kohdistuvat erityisriskit voidaan jakaa:

- lainsäädäntöjohdannaisiin riskeihin,
- ulkomaiseen omistukseen ja vaikutusvaltaan (FOCI, Foreign Ownership, Control or Influence) liittyviin riskeihin,
- turvallisuusluokiteltuihin tietoihin määräysvallassa olevien viranomaisten varaamaan tarkastusoikeuteen liittyviin riskeihin, ja
- yksittäisten teknisten suojausten toteutusvarmuuteen liittyviin riskeihin.

Nämä riskit ovat tyypillisesti merkittävämpiä kansainvälisissä pilvipalveluissa kuin Suomesta tuotetuissa pilvipalveluissa. Lainsäädäntöjohdannaisia riskejä on käsitelty turvallisuusluokiteltavien asiakirjojen käsittelystä annetun suosituksen (VM 2021:5) luvussa 7. Ulkomaiseen omistukseen ja vaikutusvaltaan liittyviä riskejä on sivuttu valtiovarainministeriön ohjeessa määräysvallan muutosriskeistä (VM 2019:7).

Turvallisuusluokiteltuihin tietoihin määräysvallassa olevat viranomaiset varaavat usein itselleen tarkastusoikeuden kaikkiin tietojenkäsittely-ympäristöihin, joissa heidän määräysvallassaan olevia turvallisuusluokiteltuja tietoja käsitellään. Erityisesti kansainvälisten turvallisuusluokiteltujen tietojen osalta määräysvallassa olevista viranomaisista käytetään usein myös termiä ”tiedon omistaja” ja samansuuntaisessa merkityksessä joskus myös termiä ”tiedon originaattori”. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltäviin tietoihin. Pilvipalveluissa, joissa käsitellään usean eri viranomaisen tietoja, tulee tietojenkäsittely-ympäristön rakenteen mahdollistaa tarkastusten toteuttaminen niin, että tietoihin määräysvallassa olevat eri viranomaiset eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä.

Tarkastusoikeuteen liittyvien riskien pienentämiseen voidaan käyttää sekä teknisiä että hallinnollisia menettelyjä. Teknisiä menettelyjä on käsitelty yksityiskohtaisemmin Katakri 2020 -arviointityökalussa (kohta I-06), PiTuKri-ohjeessa (kohta JT-03) sekä myös esimerkiksi Saksan tietoturvaviranomaisen BSI:n julkaisemassa C5-pilviturvallisuuskehyksessä (kohdat OPS-24 ja COS-06). Yleisin hallinnollinen menettely on vaatia usean eri viranomaisen tietoja sisältävää pilvipalvelua käyttäviltä viranomaisilta sitoutumista siihen, että ne eivät käytä teknistä tarkastusoikeutta pilvipalveluun ja luottavat esimerkiksi turvallisuusselvityslain (726/2014) mukaisen yritysturvallisuusselvityksen tuottamaan tietoon. Pilvipalvelun tarjoajan ja pilvipalvelun luotettavuuden arviointia käsitellään tarkemmin luvussa 4.

Teknisten suojausten toteutusvarmuuden näkökulmat liittyvät pilvipalveluiden tuottamiseen, ylläpitoon ja hallintaan sekä tiedon liikkumiseen. Tiedonhallintayksikön tulee tunnistaa ja arvioida pilvipalvelun tuotanto-, toteutus- ja palvelumalleihin liittyviä alihankkijaketjujen ja alihankkijoiden riskejä sekä eri teknologioiden käyttöön ja palvelun ja sen tuottamiseksi tarvittavien palveluiden aiheuttamaan turvallisuusluokiteltujen tietojen käsittelyyn liittyviä riskejä. Esimerkiksi salausratkaisuissa on lisäksi huomioitava sekä tiedon säilyttämiseen (data at rest) että tiedon liikkumiseen (data in transit, data in motion) liittyviä riskejä. Turvallisuusluokiteltujen tietojen suojaamisessa käytettyjen salausratkaisujen tulee myös pystyä tarjoamaan turvallisuusluokitellulle tiedolle sen salassapitoajan kestävä suojaus huomioiden edistyneemmillä hyökkääjillä käytössään olevat menetelmät.

Salausratkaisujen lisäksi on huomioitava tietojen prosessoinnin turvallisuus ja siihen liittyvät riskit esimerkiksi tilanteessa, jolloin tietojen salaus on purettava matemaattisia operaatioita ja muuta tietojen analysointia varten. Myös pilvipalvelujen käyttötapoihin voi liittyä toisinaan hankalastikin ennakoitavia riskejä. Esimerkiksi päätelaitteelle asennettu haittaohjelmien torjuntaohjelmisto saattaa olla oletusarvoisesti konfiguroitu siten, että se pyrkii lähettämään epäilyttäväksi tunnistamansa tiedoston tiivisteen tai tiedostoon liittyviä metatietoja, kuten tiedoston nimen ja aikaleiman, tai jopa koko tiedoston torjuntaohjelmiston valmistajan pilvipalveluun analysointia varten.

Turvallisuusluokitteluasetuksessa asetetuista teknisistä suojausvaatimuksista on huomioitava pilvipalveluita käytettäessä erityisesti tiedonsaantitarpeen ja turvallisuusluokitellun tiedon suojaamista koskevien velvoitteiden jalkautusvelvoitteet (8 §), tiedon ja tietojärjestelmän suojaaminen turvallisuusalueiden avulla (10 §), erotteluvelvoite alemman turvallisuustason ympäristöistä (11 § 1 mom 1 k), yleisiä verkkohyökkäyksiä vastaan suojautuminen sekä suojauksista huolehtiminen koko tietojärjestelmän elinkaaren ajan (11 § 1 mom 2 k), vähimpien oikeuksien periaatteen toteuttaminen (11 § 1 mom 3 k), tietojärjestelmän eheyden suojaaminen (11 § 1 mom 4 k), käyttäjien, laitteiden ja tietojärjestelmien tunnistaminen (11 § 1 mom 5 k), kovennuskäytännöt (11 § k 6) ja salausratkaisujen riittävä turvallisuus (11 § 1 mom 7 k).

Riittävän turvallisia salausratkaisuja edellytetään erityisesti siirrettäessä turvallisuusluokiteltuja tietoja fyysisten turvallisuusalueiden ulkopuolella tai matalamman turvallisuustason verkon kautta (12 §, myös tiedonhallintalain 14 §). Tarpeettomaksi käynyt turvallisuusluokiteltu asiakirja on tuhottava kyseessä olevalle turvallisuusluokalle riittävällä tavalla, jolla estetään luotettavasti tietojen palauttaminen tai kokoaminen uudelleen joko kokonaan tai osittain (15 §). Lisäksi turvallisuusluokasta III lähtien tulee huomioida hajasäteily ja riittävä suojautuminen elektroniselta tiedustelulta (11 § 2 mom) . Näiden vaatimusten toteuttamista on käsitelty yksityiskohtaisemmin tiedonhallintalautakunnan suosituksessa turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5).

3.3 Riskiarvioinnin perusteella annetut suositukset koskien pilvipalveluiden käyttöä

Tiedonhallintayksiköitä suositellaan valitsemaan pilvipalvelu siinä käsiteltävien turvallisuusluokiteltujen tietoaineistojen tiedonhallinta- ja tietoturvallisuusvaatimusten, sekä käsittelyn käyttötapausten ja niihin liittyvien viranomaisprosessien perusteella. Suositeltavaa on, että pilvipalveluiden käytön riskiarviointia suoritetaan jatkuvasti koko palvelun elinkaaren ajan huomioiden erityisesti pilvipalveluihin liittyvät riskit, joita on käsitelty luvuissa 3.1 ja 3.2, sekä teknologioiden nopeasta muuttumisesta aiheutuvat riskit. Suositeltavaa on, että tiedonhallintayksikkö hyväksyy jäännösriskit kirjallisella päätöksellä.

Suositeltavaa on, että pilvipalveluihin liittyvien riskien hallitsemiseksi käytetään ainoastaan viranomaisten luotettaviksi arvioimia pilvipalveluita ja tarjoajia. Pilvipalvelun tarjoajan ja pilvipalvelun luotettavuuden arviointia käsitellään tarkemmin luvussa 4. Jos turvallisuusluokiteltavia tietoaineistoja käsitellään kansainvälisissä pilvipalveluissa, suosituksena on lisäksi, että käsiteltävät turvallisuusluokitellut tietoaineistot rajataan ja valitaan käyttötapausten ja niihin liittyvien viranomaisprosessien perusteella tarkasti ja siten, että ne ovat luovutettavissa valtioihin, joiden lainkäyttövaltaan pilvipalvelujen tarjoaja ja sen alihankkijat kuuluvat.

Turvallisuusluokitellut asiakirjat ovat yleensä tulkittavissa Suomen kansallisen turvallisuuden piiriin kuuluviksi. Kansainvälisissä pilvipalveluissa ei suositella käsiteltäväksi sellaisia turvallisuusluokiteltavia asiakirjoja, jotka on rajattu *Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1807, muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa* soveltamisalan ulkopuolelle. Asetuksen soveltamisalan tulkintaa on käsitelty liikenne- ja viestintäministeriön julkaisussa 2019:11. Kansallisen turvallisuuden ja varautumisen perusteella asetetut sijaintia koskevat vaatimukset eivät kuulu asetuksen soveltamisalaan, eivätkä asetuksen velvoitteet koske niitä.

Esimerkiksi valtioiden välinen kansainvälinen yhteistoiminta tai kansainvälisiin hankintoihin liittyvä tiedonvaihto voivat olla perusteita käyttää viranomaisten luotettaviksi arvioimia kansainvälisiä pilvipalveluita turvallisuusluokiteltujen tietoaineistojen käsittelyssä. Tietoaineistojen tulee tällöin olla tarkkaan rajattuja ja valittuja ja perustua tiedonhallintayksikön jäännösriskeiltään hyväksymään riskiarvioon. Jos esimerkiksi suomalainen viranomainen tekee yhteistyötä ruotsalaisen viranomaisen kanssa, osa tähän yhteistyöhön liittyvistä kansallisista turvallisuusluokiteltavista asiakirjoista saattaa olla luovutettavissa ruotsalaisessa pilvipalvelussa käsiteltäväksi.

4 Turvallisuusluokiteltavien asiakirjojen käsittelyssä käytettävien pilvipalveluiden ja niiden tarjoajien luotettavuuden arvioinnista

Luotettavuuden arvioinnin säädösperusteet

Julkisuuslain 26 §:n 3:n momentin mukaisesti *"viranomainen voi antaa salassa pidettävästä asiakirjasta tiedon antamansa virka-aputehtävän suorittamiseksi sekä toimeksiannostaan tai muuten lukuunsa suoritettavaa tehtävää varten, jos se on välttämätöntä tehtävän suorittamiseksi. Salassa pidettäviä tietoja voi kuitenkin luovuttaa mainittuja tehtäviä varten myös silloin, kun salassa pidettävien tietojen poistaminen niiden suuren määrän tai muun niihin verrattavan syyn vuoksi ei ilmeisesti ole tarkoituksenmukaista. Viranomaisen on ennakolta varmistuttava siitä, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti."* Turvallisuusluokitteluasetuksen 6 §:n mukaisesti *"valtionhallinnon viranomaisen on ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle"*. Tämä tarkoittaa, että turvallisuusluokiteltuja tietoja ei saa luovuttaa myöskään pilvipalvelun tarjoajalle ennen kuin tiedonhallintayksikkö on varmistunut pilvipalvelun tarjoajan luotettavuudesta sekä siitä, että tarjoaja käsittelee tietoja tiedonhallintalain ja turvallisuusluokitteluasetuksen mukaisesti.

Lisäksi on huomioitava, että turvallisuusluokitteluasetuksen 8 §:n 1 momentin mukaan *"turvallisuusluokitellun asiakirjan käsittelyoikeus voidaan antaa vain sille, jolla työtehtäviensä tai muiden valtionhallinnon viranomaisen tehtävien hoitamiseen liittyvän tarpeen vuoksi on tarve saada tietoja asiakirjasta tai muutoin käsitellä sitä ja jolle on selvitetty turvallisuusluokiteltujen tietojen suojaamista koskevat ohjeet ja menettelyt ja joka tuntee asiakirjojen k*äsittelyä koskevat velvoitteet". Tämä tarkoittaa, että turvallisuusluokiteltuja tietoja ei saa luovuttaa myöskään pilvipalvelun tarjoajalle ennen kuin tiedonhallintayksikkö on varmistunut pilvipalvelussa käsiteltävien turvallisuusluokiteltujen tietoaineistojen käsittelyoikeuksista sekä siitä, että näitä tietoaineistoja käsittelevät henkilöt tuntevat turvallisuusluokiteltujen tietojen suojaamista koskevat ohjeet ja menettelyt sekä niiden käsittelyä koskevat velvoitteet.

Yritysturvallisuusselvitys Suomesta tuotettujen pilvipalveluiden luotettavuuden arvioinnissa

Yksi säännösten mukainen menettely pilvipalvelun tarjoajan luotettavuuden arviointiin on turvallisuusselvityslain mukainen yritysturvallisuusselvitys, joka kohdistetaan Suomesta tuotettuun tai tulevaisuudessa tuotettavaan pilvipalveluun ja sen tarjoajaan. Yritysturvallisuusselvityksessä arvioidaan yrityksen vastuuhenkilöiden luotettavuutta sekä yrityksen tietoturvallisuuden tasoa ja kykyä hoitaa sitoumuksensa. Turvallisuusselvityslain 9 §:n mukaisesti Traficom *"laatii osana yritysturvallisuusselvitystä tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen".* Yritysturvallisuustodistuksen voimassaoloaika on oletusarvoisesti 5 vuotta, ja siihen liittyvän tietojärjestelmien ja tietoliikennejärjestelyjen osuuden 3 vuotta. Yritysturvallisuusselvitysprosessia on kuvattu yksityiskohtaisemmin Suojelupoliisin verkkosivuilla.

Arviointilain mukainen vaatimustenmukaisuudesta annettava todistus Suomesta tuotettujen pilvipalveluiden luotettavuuden arvioinnissa

Pilvipalvelun ja sen tarjoajan luotettavuutta voidaan arvioida myös arviointilain mukaisilla arvioinneilla. Arvioinnissa käytetään kunkin turvallisuusluokan tietojen käsittelyn vaatimuksia. Arviointilain soveltamisala on rajattu viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiin. Arviointilaitoslakia sovelletaan *"elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat tietoturvallisuustason (tietoturvallisuuden arviointilaitos) ja jotka haluavat toiminnalleen Viestintäviraston* [nyk. Traficom] *hyväksynnän"* sekä arviointilaitosten hyväksymismenettelyyn. Tietoturvallisuudella tarkoitetaan luottamuksellisuuden, saatavuuden ja eheyden varmistamista.

Arviointilain 4§:n mukaisesti viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn vaatimustenmukaisuuden arviointi tehdään toimeksiannosta, jonka voi tehdä viranomaisen lisäksi se, joka tekee hankintoja viranomaisen lukuun, tuottaa viranomaiselle tietojenkäsittely- tai tietoliikennepalveluja tai hoitaa edellä mainittujen palvelujen järjestämiseen liittyviä palvelutehtäviä. Arvioinnin voi tehdä arviointilain mukaan Traficom tai hyväksytty arviointilaitos sille hyväksytyn pätevyysalueen mukaisesti. Arviointilaitoksille ei ole toistaiseksi myönnetty pätevyyttä arvioida korkeimpien turvallisuusluokkien järjestelmiä (TL II ja TL I), joten ainoastaan Traficom voi suorittaa niiden arviointeja. Traficom voi myös tehdä arviointeja turvaluokkien TL IV ja TL III tietojärjestelmistä tai tietoliikennejärjestelyistä. Traficom voi antaa tietojärjestelmälle tai tietoliikennejärjestelylle arviointilain mukaisen vaatimustenmukaisuutta koskevan todistuksen. Se on oletusarvoisesti voimassa 3 vuotta. Arviointilain mukaista arviointimenettelyä on kuvattu yksityiskohtaisemmin Traficomin Kyberturvallisuuskeskuksen verkkosivuilla.

Suomesta tuotettujen pilvipalveluiden luotettavuuden arviointia koskevat suositukset

Tiedonhallintayksiköitä suositellaan käyttämään sellaisia pilvipalveluita, joiden turvallisuus ja myös tarjoajan turvallisuus on arvioitu turvallisuusselvityslain mukaan tehdyissä yritysturvallisuusselvityksissä tai joille on myönnetty arviointilaissa tarkoitettu turvallisuusvaatimustenmukaisuutta osoittava todistus. Suositeltavaa on, että arvioinnin tilaaja sopii arvioinnista Traficomin kanssa siten, että arvioitavan pilvipalvelun tuottaja voisi kertoa, että arviointi on toteutettu. Arvioinnin tulokset voidaan jakaa niitä tarvitseville tiedonhallintayksiköille ainoastaan arvioinnin tilaajan luvalla.

Tiedonhallintayksikkö voi pyrkiä myös itse arvioimaan pilvipalvelujen tarjoajien tai pilvipalvelujen luotettavuutta. Tässä haasteena on se, että tyypillisesti tiedonhallintayksiköillä ei ole riittävästi tietoa riskiarviointia varten eikä siten mahdollisuuksia syvälliseen ja luotettavaan arviointiin. Syvällinen arviointi edellyttää myös erikoisosaamista, jota ei kaikilla tiedonhallintayksiköillä ole - eikä ole tarpeenkaan olla. Myöskään säädökset eivät mahdollista sitä, että kaikki yritysturvallisuusselvityksessä käytettävät tietolähteet olisivat kaikkien tiedonhallintayksiköiden saatavilla. Osa pilvipalvelujen tarjoajista voi myös kieltäytyä luovuttamasta yksityiskohtaisia tietoja palvelustaan kaikille tiedonhallintayksiköille. Tiedonhallintayksikön voikin olla haastavaa pystyä uskottavasti arvioimaan pilvipalvelujen tarjoajien tai pilvipalvelujen luotettavuutta turvallisuusluokiteltujen tietojen käsittelyssä, jos se joutuu arvioimaan lakisääteisten vaatimusten täyttymistä esimerkiksi vain pilvipalvelujen tarjoajien itsearviointiin, kaupallisiin sertifiointeihin ja sopimuksiin perustuen.

Kansainvälisten pilvipalveluiden luotettavuuden arviointi kansainvälisen yritysturvallisuusselvityksen avulla

Suomi on tehnyt tietoturvallisuussopimuksia useiden valtioiden ja kansainvälisten järjestöjen kanssa. Tietoturvallisuussopimuksen *"tarkoituksena on suojata sellaista valtioiden tai kansainvälisten järjestöjen turvallisuusluokiteltua tietoa, jota sopimuspuolet vaihtavat suoraan keskenään tai jota vaihdetaan niiden lainkäyttövaltaan kuuluvien julkis- tai yksityisoikeudellisten oikeushenkilöiden tai luonnollisten henkilöiden kesken"* (Turvallisuusviranomaisten käsikirja yrityksille, 2015).

Kansainvälisillä tietoturvallisuusvelvoitteilla tarkoitetaan Suomen tekemän tietoturvallisuussopimuksen määräyksiä erityissuojattavan tietoaineiston suojaamisesta. Kansainvälisten tietoturvavelvoitteiden vastuista on säädetty kansainvälisistä tietoturvavelvoitteista annetussa laissa (588/2004). Lain 4 §:n mukaan ulkoministeriö toimii kansainvälisten tietoturvavelvoitteiden toteuttamisessa kansallisena turvallisuusviranomaisena (NSA) ja Traficom tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa lain tarkoittamana määrättynä turvallisuusviranomaisena (DSA). Muita määrättyjä turvallisuusviranomaisia ovat puolustusministeriö, pääesikunta ja suojelupoliisi, jotka *"toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja*

toimitilaturvallisuutta koskevissa asioissa". Erityissuojattavalla tietoaineistolla tarkoitetaan *"sellaisia salassa pidettäviä asiakirjoja ja materiaaleja sekä asiakirjoista ja materiaaleista saatavissa olevia tietoja sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu".*

Valtioiden välinen turvallisuussopimus ei aiheuta sitä, että sopimuksessa osallisena olevien valtioiden kaupalliset toimijat toteuttaisivat turvallisuussopimuksen velvoitteita. Turvallisuussopimuksen velvoitteet saatetaan koskemaan kaupallisia toimijoita kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitetun yritysturvallisuusselvitysmenettelyn (FSC) avulla. Se on lähtökohtaisesti käytettävissä turvallisuusluokkaa TL III / CONFIDENTIAL ja tätä korkeampien turvallisuusluokkien asiakirjoja käsiteltäessä.

Kansainvälisten pilvipalveluiden luotettavuuden arviointiin liittyvät suositukset

Kansainvälisten pilvipalvelujen tarjoajan ja kansainvälisten pilvipalvelujen luotettavuuden arvioinnissa on suositeltavaa hyödyntää kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettua yritysturvallisuusselvitysmenettelyä aina, kun se on mahdollista. Tämän vuoksi suosituksena on, että jos turvallisuusluokiteltavia asiakirjoja on tarkoitus käsitellä kansainvälisissä pilvipalveluissa, tiedonhallintayksikkö on etukäteen yhteydessä kansalliseen turvallisuusviranomaiseen (NSA) ja

- selvittää kansainvälisten turvallisuusuussopimusten tilanteen Suomen valtion ja niiden valtioiden välillä, joiden lainkäyttövaltaan pilvipalvelujen tarjoaja ja sen alihankkijat kuuluvat, sekä
- selvittää turvallisuussopimuksiin liittyvien pilvipalveluntarjoajaa koskevien yritysturvallisuusselvitysten (FSC) tilanteen, ja
- yhteistyössä NSA:n kanssa arvioi sitä, että toteutuvatko mahdollisten turvallisuussopimusten mukaiset kansainväliset tietoturvallisuusvelvoitteet kyseistä pilvipalvelua käytettäessä, ja
- keskustelee NSA:n kanssa siitä, onko tietojen luovutukselle pilvipalvelun tarjoajalle edellytyksiä.

5 Turvallisuusluokiteltavien asiakirjojen käsittelyssä käytettäviin pilvipalveluihin liittyvistä palvelusopimuksista

Kun pilvipalveluita käytetään turvallisuusluokiteltavien asiakirjojen käsittelyssä, turvallisen tietojen käsittelyn varmistaminen perustuu luvussa 4 kuvattuun pilvipalvelun tarjoajien ja pilvipalvelujen luotettavuuden arviointiin sekä tiedonhallintayksikön ja pilvipalvelun tarjoajan sekä mahdollisen integraattorin kanssa tehtyihin sopimuksiin. Sopimuksissa on muun muassa huomioitava se, missä valtioissa tietoa käsitellään. Huomiota tulee kiinnittää maakohtaisiin säädöksiin, muun muassa alihankintaketjujen kattavuuteen (katetaanko kaikki alihakkijat ja palvelun mahdollinen tukijärjestely), sekä siihen, miten palveluntarjoaja osoittaa riittävän turvallisuustason, esimerkiksi tarkastusraporttien ja auditointien avulla.

Tiedonhallintayksikön tulee varmistaa se, että palvelusopimus täyttää turvallisuusluokiteltujen tietojen käsittelyyn liittyvät vaatimukset. Tietoturvallisuudesta sopimista on käsitelty kattavammin tiedonhallintalautakunnan suosituskokoelmassa tiettyjen tietoturvallisuussäännösten soveltamisesta (VM 2021:65). Lisäksi on riskiperusteisesti varmistuttava viimeistään sopimuksen voimassaoloaikana siitä, että palveluntarjoaja noudattaa sopimuksen tietoturvallisuusvelvoitteita.

Pilvipalvelun tuottamiseen liittyvän mahdollisen alihankintaketjun arviointi sisältyy tyypillisesti luvussa 4 kuvattuihin tietojärjestelmien ja tietoliikennejärjestelyjen arviointeihin. Mikäli tällaista arviointimenettelyä ei ole kuitenkaan käytetty, tiedonhallintayksikön on tärkeää kartoittaa sopimusketju kokonaisuudessaan sekä selvittää, mitkä ja missä sijaitsevat alihankkijat voivat mahdollisesti osallistua tiedonhallintayksikön tietojen käsittelyyn. Usein tiedonhallintayksiköt eivät ole suorassa sopimussuhteessa pilvipalvelun tarjoajaan, vaan pilvipalveluiden käyttö perustuu pidempään sopimusketjuun, johon osallistuu useampia toimijoita. Tällöin tiedonhallintayksikkö hankkii pilvipalvelun tyypillisesti integraattorin kautta ja sopimusketjun ensimmäisen askeleen muodostaa tiedonhallintayksikön ja integraattorin välinen ICT-palvelusopimus tai muu sopimus. Sopimusketjussa integraattorin ja pilvipalvelun tarjoajan välissä saattaa vielä olla eri pilvipalveluiden ratkaisuja ja palveluita välittävä ja operoiva välittäjä tai jälleenmyyjä, jonka kanssa integraattori on tehnyt hankintasopimuksen. Tällöin sopimusketjun kolmannen askeleen muodostaa välittäjän tai jälleenmyyjän ja pilvipalvelun tarjoajan välinen sopimus. Lisäksi on huomioitava, että pilvipalvelun tarjoajat voivat käyttää lukuisia alihankkijoita, jotka osallistuvat

palveluiden toteuttamiseen ja toimittamiseen loppukäyttäjänä olevalle tiedonhallintayksikölle. Alihankkijat voivat toimia useissa eri maissa, mikä kasvattaa selvitettävien säädösten määrää. Tällöin on erityisesti selvitettävä lainsäädäntöjohdannaiset riskit. Lisäksi on otettava huomioon henkilötietojen käsittelyn ja siirtämisen asettamat vaatimukset.

Pilvipalveluiden käytönaikaisessa hallinnassa korostuvat sopimusmuutosten seuranta ja valvonta sekä pilvipalvelun turvallisuuden valvonta ja käyttöoikeuksien ja ylläpidon hallinta. Suosituksena on, että tiedonhallintayksiköt käyttävät pilvipalvelun tarjoajaa, joka on arvioitu tietoturvallisuusvaatimukset täyttäväksi turvallisuusselvityslain tai arviointilain mukaisesti, ja joka vastaa myös konfiguraatiosta palveluna.

Suositeltavaa on, että pilvipalvelujen tarjoajaa vaaditaan ilmoittamaan palveluun ja sopimuksiin tehtävistä merkittävistä muutoksista hyvissä ajoin etukäteen. Ilmoitusta kaikista tietoturvallisuuspoikkeamista on suositeltavaa vaatia viipymättä ja ilmoitusta muista merkittävistä pilvipalvelun tuotantoympäristön tapahtumista kuukausittain. Ilmoitusta palvelun turvallisuuden kokonaiskuvasta on hyvä vaatia määräajoin, esimerkiksi neljä kertaa vuodessa. Osa pilvipalvelun tarjoajista tarjoaa raporttien tarkasteluun työkaluja, mutta nämä eivät useinkaan sisällä tietoja järjestelmän sisäisestä turvallisuudesta tai kokonaiskuvasta, joka syntyy useamman pilvipalvelukomponentin käytöstä. Suosituksena on, että tiedonhallintayksikkö huolehtii siitä, että turvallisuusluokiteltavien asiakirjojen käsittelyyn käytettävän pilvipalvelun turvallisuuden valvonta (havainnointi, reagointi ja analysointi) on varmistettu esimerkiksi pilvipalvelun tarjoajasta riippumattoman tieto- ja kyberturvallisuuden valvontapalvelun (SOC) avulla.

Tiedonhallintalain 13 §:n mukaan *"tiedonhallintayksikön on varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan"*. Tiedonhallintayksikön tehtävänä on siten varmistaa turvallisuusluokiteltavien asiakirjojen ja niitä käsittelevien tietojärjestelmien, kuten pilvipalveluiden, tietoturvallisuus koko niiden elinkaaren ajan. Pilvipalvelut ovat jatkuvan muutoksen alaisia. Niille ominaista on nopea ja laaja kehittyminen, mikä edellyttää jatkuvaa sopimusten seurantaa ja valvontaa sekä muutostenhallintaa. Muutokset kasvattavat riskiä siitä, että palvelu, sen tarjoaja tai jokin uusi ominaisuus muuttuu sopimuksen- tai vaatimustenvastaiseksi tai määräysvaltamuutosriskejä toteutuu. Lisäksi on huomioitava, että tiedon elinkaaren ajan kestävästä tietoturvallisuudesta voi olla mahdotonta varmistua sellaisten pilvipalvelun tarjoajien kanssa, jotka varaavat sopimuksiinsa yksipuolisen mahdollisuuden muuttaa sopimusehtoja.

Jos tiedonhallintayksiköllä ei ole osaamista seurata pilvipalvelun tarjoajien palveluiden kehitystä ja kehitystoimien myötä tulevia muutoksia, on suositeltavaa käyttää luotetun palveluntoimittajan kautta hankittuja palveluja. Suosituksena on käyttää turvallisuusvaatimusten mukaisiksi todettuja, Suomesta tuotettuja pilvipalveluita aina, kun se on mahdollista, jotta kansainvälisiin pilvipalveluihin liittyvien riskien hallitseminen olisi mahdollista

turvallisuusluokiteltavien asiakirjojen koko elinkaaren ajan. On hyvä harkita Hanselin tai Valtion tieto- ja viestintätekniikkakeskus Valtorin kautta hankittujen, viranomaisten edellyttämien turvallisuusvaatimusten mukaisiksi arvioitujen pilvipalvelujen käyttöä.

Tiedonhallintayksikkö voi lopettaa pilvipalveluiden käytön pilvipalvelun elinkaaren loppuessa, käyttötarpeen päätyttyä tai, jos palvelu palautetaan Suomesta tuotetuksi tai muuten siirretään toiselle tarjoajalle. Tiedonhallintayksikön tuleekin huomioida pilvipalvelun koko elinkaaren ajan, lähtien jo hankinnasta ja suunnittelusta, että palvelun päättäminen tai palvelun tarjoajan vaihtaminen on mahdollista. Pilvipalvelun käytön päättämistä käsitellään erillisessä tiedonhallintalautakunnan suosituksessa.

6 Tiivistelmä suosituksista

Tiedonhallintayksiköitä suositellaan valitsemaan pilvipalvelu siinä käsiteltävien turvallisuusluokiteltujen tietoaineistojen tiedonhallinta- ja tietoturvallisuusvaatimusten sekä käsittelyn käyttötapausten ja niihin liittyvien viranomaisprosessien perusteella. Suosituksena on, että pilvipalveluiden käytön riskiarviointia suoritetaan jatkuvasti koko palvelun elinkaaren ajan huomioiden erityisesti pilvipalveluihin liittyvät riskit, joita on käsitelty luvussa 3, sekä teknologioiden nopeasta muuttumisesta aiheutuvat riskit. Suositeltavaa on, että tiedonhallintayksikkö hyväksyy jäännösriskit kirjallisella päätöksellä.

Pilvipalveluihin liittyvien riskien hallitsemiseksi tiedonhallintayksiköitä suositellaan käyttämään sellaisia pilvipalveluita, joiden turvallisuus ja joiden tarjoajan turvallisuus on arvioitu turvallisuusselvityslain mukaan tehdyissä yritysturvallisuusselvityksissä, tai joille on myönnetty tietoturvallisuuden arviointitoimintaa koskevien säännösten mukainen turvallisuusvaatimustenmukaisuutta osoittava todistus. Suositeltavaa on, että arvioinnin tilaaja sopii arvioinnista Traficomin kanssa siten, että arvioitavan pilvipalvelun tuottaja voisi kertoa, että arviointi on toteutettu.

Jos turvallisuusluokiteltavia tietoaineistoja käsitellään kansainvälisissä pilvipalveluissa, suosituksena on lisäksi, että turvallisuusluokitellut tietoaineistot rajataan ja valitaan käyttötapausten ja niihin liittyvien viranomaisprosessien perusteella tarkasti ja siten, että ne ovat luovutettavissa valtioihin, joiden lainkäyttövaltaan pilvipalvelujen tarjoaja ja sen alihankkijat kuuluvat. Kansainvälisten pilvipalvelujen ja niiden tarjoajan luotettavuuden arvioinnissa on suositeltavaa hyödyntää kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettua yritysturvallisuusselvitysmenettelyä luvussa 4 kuvatulla tavalla.

Suosituksena on, että tiedonhallintayksikkö huomioi ja varautuu pilvipalveluiden koko elinkaaren ajan, lähtien jo suunnittelusta, hankinnasta ja sopimuksista, siihen, että palvelun päättäminen tai palvelun tarjoajan vaihtaminen on mahdollista. Suositeltavaa on, että teknologioiden muuttumista ja sopimusmuutoksia seurataan jatkuvasti.

7 Lähteet

Liikenne- ja viestintäministeriö (2019:11). Muiden kuin henkilötietojen vapaan liikkuvuuden esteet Suomessa. http://urn.fi/URN:ISBN:978-952-243-571-2

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020:13. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri

Tiedonhallintalautakunta (VM 2021:5). Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. http://urn.fi/URN:ISBN:978-952-367-500-1

Tiedonhallintalautakunta (VM 2021:65). Suositus tiettyjen tietoturvallisuussäännösten soveltamisesta. http://urn.fi/URN:ISBN:978-952-367-897-2

Ulkoministeriö, Kansallinen turvallisuusviranomanomainen (NSA) 2020. Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje. https://um.fi/turvallisuusluokitellun-tiedon-kasittelyohje

Ulkoministeriö, Kansallinen turvallisuusviranomanomainen (NSA) 2015. Turvallisuusviranomaisten käsikirja yrityksille. https://um.fi/documents/35732/48132/turvallisuusviranomaisten_k%C3%A4sikirja_yrityksille/b5853259-0795-5fae-ad02-7e9eac6d5841?t=1525647184899

Valtiovarainministeriö 2018:35. Julkisen hallinnon pilvipalvelulinjaukset. http://urn.fi/URN:ISBN:978-952-251-982-5

Valtiovarainministeriö 2020:66. Tuottavuutta pilvipalveluilla. Ohje julkisen hallinnon pilvipalvelujen hyödyntämiseen. http://urn.fi/URN:ISBN:978-952-367-327-4

Valtiovarainministeriö 2020:73. Pilvipalvelujen soveltamisohje – Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon tiedonhallintayksiköille. http://urn.fi/URN:ISBN:978-952-367-503-2

LIITE 1. Termistö

Termi	Määritelmä
Asiakirja	Asiakirjalla tarkoitetaan tässä suosituksessa viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 5.1 §:n mukaista asiakirjaa eli mitä tahansa jollekin alustalle tallennettua kirjallista tai kuvallista esitystä, kuten päätöstä, muistiota, ilmoitusta, luetteloa, valokuvaa, piirrosta tai taulukkoa. Asiakirjalla tarkoitetaan edelleen sellaisia käyttönsä vuoksi yhteenkuuluvia merkkien yhdistelmiä, kuten sähköisiä tallenteita ja muita viestejä, joiden sisältö on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden tai muiden apuvälineiden avulla. Näin ollen asiakirjoja voivat olla myös esimerkiksi pilvipalveluiden tietokantoihin tai muulle tallennusvälineelle tallennetut tiedot.
Tieto	Tiedolla tarkoitetaan tässä suosituksessa samaa kuin asiakirjalla.
Tietoaineisto	Tietoaineistolla tarkoitetaan tässä suosituksessa julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 2 §:n mukaista tietoaineistoa eli asiakirjoista ja muista vastaavista tiedoista muodostuvaa, tiettyyn viranomaisen tehtävään tai palveluun liittyvää tietokokonaisuutta.
Tietojärjestelmä	Tietojärjestelmällä tarkoitetaan tässä suosituksessa julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 2 §:n mukaista tietojärjestelmää eli tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaa kokonaisjärjestelyä. Tietojärjestelmiä ovat esimerkiksi erilaiset pilvipalvelut ja niiden käyttöön käytettävät päätelaitteet.
Pilvipalvelu	Pilvipalvelulle löytyy monenlaisia määritelmiä. Tässä suosituksessa pilvipalvelulla tarkoitetaan NIS-direktiivin[1] mukaisesti ”digitaalista palvelua, joka mahdollistaa pääsyn skaalautuvaan ja mukautuvaan joukkoon jaettavissa olevia tietoteknisiä resursseja”. Pilvipalvelulla tarkoitetaan edelleen ”verkon yli saavutettavaa tietojenkäsittelykapasiteettia tai -palvelua, jonka tuottamisessa hyödynnetään jaettujen, skaalautuvien ja joustavien resurssien mallia, joka on automatisoitu osin itsepalveluperiaatteella tuotettavaksi” (PiTuKri). Pilviteknologialla tarkoitetaan usein samaa kuin yllä viitatuilla pilvipalvelujen määrityksillä. Usein pilvipalvelulla tarkoitetaan ainoastaan kansainvälisten toimittajien pilviteknologiaa hyödyntäen tarjoamia palveluita.
Pilviteknologia	Tässä suosituksessa pilviteknologialla tarkoitetaan teknologisia ratkaisuja, joihin pilvipalvelujen tarjoaminen perustuu.

[1] Direktiivi 2016/1148 toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

Termi	Määritelmä
Pilvipalvelun tarjoaja	Tässä suosituksessa pilvipalvelun tarjoajalla tarkoitetaan toimijaa, joka tarjoaa IaaS-, PaaS- tai SaaS-mallista palvelua tai muuta pilviteknologiaan perustuvaa palvelua.
Pilvialustan toimittaja	Tässä suosituksessa pilvialustan toimittajalla tarkoitetaan toimijaa, joka tuottaa pilvipalvelun, johon kuuluu infrastruktruurin kapasiteetti, suorituskyky, tietoliikenne ja mahdolliset lisäpalvelut. Palvelut ovat tilaajan ja sovellustoimittajan valittavissa ja mahdollisesti konfiguroitavissa.
Palveluntoimittaja	Tässä suosituksessa palveluntoimittajalla tarkoitetaan toimijaa, joka toimittaa pilvialustalle tuotetun palvelun. Palvelu voi sisältää virtuaalipalvelimia, sovelluksia tai järjestelmiä, jotka on rakennettu pilvialustan kapasiteetin ja ratkaisujen päälle. Palveluntoimittajalla on usein hallintaoikeudet itse järjestelmään ja sovellukseen. Palveluntoimittajalla ja sovellustoimittajalla voi olla omat alihankkijat. Palveluntoimittaja voi toimia myös integraattorin roolissa.
Integraattori	Tässä suosituksessa integraattorilla tarkoitetaan toimijaa, joka hankkii palveluita tilaajan puolesta sekä pilvialustan toimittajilta että palveluntoimittajilta ja sopimuksellisesti usein vastaa palveluiden turvallisuudesta ja yhteensopivuudesta.
Tiedonhallintayksikkö	Tiedonhallintayksikkö on tiedonhallintalain 2 §:n mukaan viranomainen, jonka tehtävänä on järjestää tiedonhallinta tiedonhallintalain vaatimusten mukaisesti.
Tilaaja	Tiedonhallintayksikkö tilaa palvelun suoraan pilvipalvelun tarjoajalta tai käyttää apuna palveluntoimittajaa tai integraattoria palvelun hankinnassa ja määrittelyssä. Tilaajana voi olla myös yhteishankintayksikkö, kuten Hansel.
IaaS (Infrastructure as a Service)	*Pilvipalvelun palvelumalli:* IaaS-mallissa eli infrastruktuuri palveluna -mallissa kaikki palveluiden tuottamiseen liittyvä infrastruktuuri hankitaan pilvipalvelun tarjoajalta.
PaaS (Platform as a Service)	*Pilvipalvelun palvelumalli:* PaaS-mallissa eli alusta palveluna –mallissa palvelut tuotetaan valmiin ohjelmistoalustan avulla.
SaaS (Software as a Service)	*Pilvipalvelun palvelumalli:* SaaS-mallissa eli ohjelmisto palveluna –mallissa pilvipalvelun tarjoaja tuottaa palvelut kokonaisuudessaan.
CaaS (Containers as a Service)	*Pilvipalvelun palvelumalli:* CaaS-mallissa eli kontit palveluna –mallissa pilvipalvelun tilaaja voi ladata, organisoida, käynnistää, skaalata ja muualla tavoin hallita ohjelmistokontteja, sovelluksia ja klustereita. Ohjelmistokontit ovat ohjelmistoja, jotka voidaan siirtää paikasta toiseen ilman, että niitä on tarve muokata. Ohjelmistokontti voidaan esimerkiksi siirtää omasta konesalista pilvipalveluun.

Termi	Määritelmä
Yksityinen pilvi (Private cloud)	*Pilvipalvelun toteutusmalli:* Yksityisellä pilvellä tarkoitetaan yleisesti palvelua, joka tuotetaan vain palvelua käyttävälle tiedonhallintayksikölle. Palvelua voidaan tuottaa joko palveluntarjoajan tai/ja tiedonhallintayksikön konesaleista. Yksityisen pilven tyypillisenä vahvuutena on pilvipalveluinfrastruktuurin sekä siinä käsiteltävien tietojen fyysisen ja loogisen tason luotettava erottelu muista tietojenkäsittely-ympäristöistä, tiedonhallintayksiköistä ja ulkoisista toimijoista. Yksityisellä pilvellä pystytään toteuttamaan tyypillisesti korkeamman turvatason palveluja kuin muilla toteutusmalleilla.
Julkinen pilvi (Public cloud)	*Pilvipalvelun toteutusmalli:* Julkisella pilvellä tarkoitetaan yleisesti palvelua, joka on julkisesti tarjolla ja kaikkien toimijoiden hankittavissa. Palvelua tuotetaan lähes poikkeuksetta palveluntarjoajan konesaleista. Julkisessa pilvessä pilvipalveluinfrastruktuuriin sekä siinä käsiteltäviin tietoihin kohdistuu yksityistä pilveä laajempi hyökkäyspinta-ala muun muassa palvelun muiden käyttäjien tai ulkoisten toimijoiden taholta.
Yhdistelmäpilvi (Hybrid cloud)	*Pilvipalvelun toteutusmalli:* Yhdistelmäpilvellä tarkoitetaan yleisesti palvelua, jossa yhdistetään yksityinen pilvi sekä julkinen pilvi yhdeksi palvelukokonaisuudeksi. Esimerkiksi tiedonhallintayksikön omassa konesalissa ajettavaa yksityistä pilveä voidaan täydentää julkisesta pilvestä hankittavilla palveluilla. Toteutuva turvataso riippuu tyypillisesti siitä, minkä tietojen on mahdollista siirtyä julkisen pilven puolelle, ja miten turvallisuus on järjestetty pilvitoteutusten rajapinnoissa.
Suomesta tuotettu pilvipalvelu	*Pilvipalvelun tuotantomalli:* Tässä suosituksessa Suomesta tuotetulla pilvipalvelulla tarkoitetaan palvelua, jossa tieto ja kapasiteetti sijaitsevat Suomen alueella ja palvelun tuotanto sekä ylläpito tapahtuvat Suomessa.
Kansainvälinen pilvipalvelu	*Pilvipalvelun tuotantomalli:* Tässä suosituksessa kansainvälisellä pilvipalvelulla tarkoittaa palvelua, jossa tieto ja kapasiteetti sijaitsevat Suomen ulkopuolella tai palvelun tuotanto tai ylläpito tapahtuvat Suomen ulkopuolella. Esimerkiksi pilvipalvelu, jonka konesali sijaitsee Suomessa, mutta jonka ylläpito tapahtuu toisen maan lainsäädännön piiristä toisesta maasta käsin, on tulkittavissa kansainväliseksi pilvipalveluksi.
Määräysvaltamuutos	Määräysvaltamuutos tarkoittaa muutosta siinä, kenellä on määräysvalta pilvipalvelua tarjoavassa yrityksessä tai sen alihankkijoissa, esimerkiksi oikeus nimittää tai erottaa enemmistö jäsenistä yrityksen hallituksessa tai muuten tosiasiallisesti käyttää määräysvaltaa yrityksessä.

LIITE 2. Esimerkit toimijoiden tehtävistä

Alla on kuvattu esimerkit kunkin toimijan pilvipalvelun käytönaikaisen hallinnan tehtävistä.

Tiedonhallintayksikön tehtävät

- Vastaa turvallisuusluokiteltujen tietojen elinkaaren aikaisesta suojauksesta pilvipalvelussa sekä tietojen viemisestä palveluun ja poistamisesta sieltä.
- Määrittää pilvipalvelun sallitun käytön.
- Vastaa valvonnasta ja riskienhallinnasta.
- Vastaa toimitusketjun turvallisuudesta turvallisuusluokiteltujen tietojen käsittelyvaatimuksia vasten.
- Vastaa kokonaisturvallisuuden hallinnasta ja ohjauksesta.
- Valvoo tiedon kasautumista.

Integraattorin tehtävät

- Toteuttaa, valvoo ja raportoi pilvipalvelun teknisistä kontrolleista.
- Seuraa muutoksia, joita pilvipalveluihin on tulossa.
- Pitää järjestelmät ja suojaukset ajan tasalla.
- Sopimuksellisesti vastaa oman toimitusketjunsa turvallisuudesta turvallisuusluokiteltujen tietojen käsittelyvaatimuksia vasten.
- Sopimuksellisesti vastaa kokonaisturvallisuuden hallinnasta ja ohjauksesta.
- Monitorointi- ja valvontarooli
  - Mahdollisesti ulkoistettu kolmannelle osapuolelle (SOC)
  - Poikkeamahavainnointi ja -hallinta

Palveluntoimittajan/Sovellustoimittajan tehtävät

- Muutoshallinta
- Käyttäjäoikeuksien ylläpito ja tarkastus
- Palvelun käytön valvonta
- Riskiarvion ylläpitäminen
- Seuraa muutoksia, joita pilvipalveluihin on tulossa.
- Pitää järjestelmät ja suojaukset ajan tasalla.
- Sopimuksellisesti vastaa oman toimitusketjunsa turvallisuudesta turvallisuusluokiteltujen tietojen käsittelyvaatimuksia vasten.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

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

ISSN 1797-9714 (pdf)
ISBN978-952-367-906-1 (pdf)

Tammikuu 2022