Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa

1 Johdanto

Suositus Turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa täydentää Turvallisuusluokiteltavien asiakirjojen käsittelystä annettua suositusta (VM 2021:5). Nämä kaksi suositusta opastavat toteuttamaan julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, jatkossa TihL tai tiedonhallintalaki) 18 §:ssä ja valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019, turvallisuusluokitteluasetus tai TLa) vaatimuksia turvallisuusluokiteltujen asiakirjojen käsittelystä. 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.

Turvallisuusluokiteltavien asiakirjojen käsittelyn suosituksessa (VM 2021:5) on linjattu seuraavasti turvallisuusluokiteltavien asiakirjojen käsittelyä 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.

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

Tiedonhallintayksiköitä suositellaan valitsemaan pilvipalvelu siinä käsiteltävien turvallisuusluokiteltavien asiakirjojen tiedonhallinta- ja tietoturvallisuusvaatimusten, sekä käsittelyn käyttötapausten ja niihin liittyvien viranomaisprosessien perusteella. Tiedonhallintayksiköitä suositellaan käyttämään sellaisia pilvipalveluita, joiden turvallisuus sekä myös joiden tarjoajan turvallisuus on arvioitu turvallisuusselvityslain mukaan tehdyissä yritysturvallisuusselvityksissä, tai joille on myönnetty tietoturvallisuuden arviointitoimintaa koskevien säännösten mukainen vaatimustenmukaisuutta osoittava todistus.

2 Säädökset ja muu ohjeistus

Suositus Turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalveluissa on erityisesti suunnattu tiedonhallinnan ja -käsittelyn asiantuntijoille, pilvipalveluiden ja pilviteknologian hankinnasta vastaaville, pilvipalveluiden ja pilviteknologioiden kehittäjille, sekä tiedon suojaamisesta vastaaville tahoille. Suositukseen liittyvät keskeiset säädökset ovat seuraavat:

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 kohdassa määritellyille asiakirjoille, joiden sisältämän tiedon oikeudeton käyttö tai paljastuminen voi aiheuttaa vahinkoa muun muassa kansalliselle turvallisuudelle.

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 viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien velvollisuudesta turvallisuusluokitella tietyt asiakirjat.

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019, TLa). Asetuksessa säädetään tarkemmin tiedonhallintalain mukaisten turvallisuusluokiteltavien asiakirjojen turvallisuusluokittelusta, turvallisuusluokittelumerkinnöistä ja näiden asiakirjojen tietoturvallisesta käsittelystä.

Laissa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011, arviointilaki) säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. Valtionhallinnon vi-

ranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain mainitussa laissa tarkoitettua menettelyä taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston (nykyisin Liikenne- ja viestintävirasto Traficom) hyväksynnän **tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011, arviointilaitoslaki**) mukaan.

Lukijaa kehotetaan tämän suosituksen lisäksi tutustumaan Tiedonhallintalautakunnan muihin suosituksiin sekä valtiovarainministeriön pilvipalveluita koskeviin linjauksiin ja ohjeisiin (Valtiovarainministeriö 2018:35, 2020:66, 2020:73). Lisäksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus (2020:13) on julkaissut Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri).

3 Riskienhallinta ja vaikutusten arviointi käytettäessä pilvipalveluita turvallisuusluokiteltavien asiakirjojen käsittelyssä

Viranomaisen tiedonhallintayksikön on tiedonhallintalain (906/2019) mukaisesti selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti (13 §). Riskienhallintaa on yleisesti käsitelty tiedonhallintalautakunnan suosituskokoelmassa tiettyjen tietoturvallisuussäännösten soveltamisesta (VM 2020:61).

Kun pilviteknologiaa harkitaan käytettäväksi turvallisuusluokiteltavien asiakirjojen käsittelyssä, niin tiedonhallintayksikön tulee aluksi tunnistaa mitä turvallisuusluokiteltavia asiakirjoja pilviteknologialla on tarkoitus käsitellä, ja mitkä ovat näiden asiakirjojen 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.

Lisäksi joissakin tilanteissa pilvipalvelujen käyttö voi olla viranomaisen operatiivisten tarpeiden vuoksi välttämätöntä turvallisuusluokitellun tiedon käsittelyssä. Esimerkiksi viranomaisen operatiiviseen toimintaan sisältyy 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.

Pilviteknologialla käsiteltävien turvallisuusluokiteltavat asiakirjojen, ja niiden tiedonhallinta- ja tietoturvallisuusvaatimusten, sekä käyttötapausten, ja viranomaisprosessien tunnistamisen lisäksi tiedonhallintayksikön tulee myös tehdä tietojenkäsittelyyn liittyvä muutosvaikutusten arviointi, jos kyseessä on muutos olemassa olevaan tietojen käsittelyprosessiin. Muutosvaikutusten arvioinnin tulee ottaa huomioon myös käsittelyn kannalta olennaiset poikkeustilanteiden jatkuvuudenhallintaan liittyvät toimenpiteet sekä menettelyt. Jos turvallisuusluokiteltaviin asiakirjoihin sisältyy henkilötietoja, niin tiedonhallintayksikön tulee arvioida erillisen tietosuojavaikutusten arvioinnin tarve.

3.1 Turvallisuusluokiteltavien asiakirjojen käsittelyyn pilvipalveluissa liittyvästä riskienhallinnasta

Turvallisuusluokiteltavien asiakirjojen käsittelyä pilvipalveluissa koskevat merkittävimmät riskit ja niiden hallitsemiseksi tarvittavat toimenpiteet liittyvät turvallisuusluokiteltujen tietojen tai tiedonkäsittelijöiden fyysiseen sijaintiin eli pilvipalveluiden tuotantomalliin, sekä pilvipalvelujen toteutusmalliin ja tarjoajaan. Turvallisuusluokiteltaviin asiakirjoihin kohdistuvien riskien näkökulmasta pilvipalvelujen tuotantomallit voidaan ryhmitellä kahteen päämalliin: Suomesta tuotettu pilvipalvelu ja kansainvälinen pilvipalvelu. Toteutusmallien vaihtoehdot ovat yksityinen pilvi, yhdistelmäpilvi ja julkinen pilvi. Tuotanto- ja toteutusmalleja on kuvattu tarkemmin liitteenä 1 olevassa termistössä.

Kun käsiteltävät turvallisuusluokiteltavat asiakirjat, niiden tiedonhallinta- ja tietoturvallisuusvaatimukset ja käyttötapaukset sekä viranomaisprosessit, sekä tarpeet pilvitekniologian käytölle on kuvattu, niin tiedonhallintayksikön tulee riskiperustaisesti käyttötapauksittain päättää siitä, mitä pilvipalvelun tuotanto- ja toteutusmallia voidaan käyttää minkäkin turvallisuusluokiteltavan asiakirjan käsittelyssä. Riskiperustainen päätöksenteko tarkoittaa sitä, että tiedonhallintayksikön arvioi pilvipalvelujen tuotantomalliin, toteutusmalliin ja tarjoajaan liittyvät riskit ja toteuttaa niiden hallitsemiseksi tarvittavat toimenpiteet ennen kuin turvallisuusluokiteltuja tietoja käsitellään pilvipalveluissa. Suositellaan, että riskienhallinnassa tiedonhallintayksikkö hyödyntää selvityksiä ja arvioita tiedonhallinnan ja tietoturvallisuuden vaatimustenmukaisuuden toteutumisesta.

EU-tasolla ja kansainvälisissä järjestöissä on käynnissä useita toimenpiteitä, joiden avulla tavoitellaan turvallisempia teknologioita. Tiedonhallintayksikön tulee kuitenkin huomioida, että turvallisuusluokiteltavien asiakirjojen käsittelyyn erityisesti muissa kuin Suomesta tuotetuissa pilvipalveluissa liittyy useita globaaleihin tuotantoketjuihin ja toimijoihin liittyviä riskejä. Niiden hallitsemiseksi tiedonhallintayksiköllä on usein vain vähän tai ei lainkaan vaikutusmahdollisuuksia.

Pilvipalveluiden käyttöön liittyvien tietoturvallisuustoimenpiteiden suunnittelussa ja valinnassa voidaan hyödyntää tiedonhallintalautakunnan suositusten lisäksi yleisimpiä turvallisuusluokiteltuun tietoon kohdistuvien riskien vaikutuksia pienentämään suunnattuja ohjeita. Näitä ovat esimerkiksi kansallisen turvallisuusviranomaisen julkaisema Katakri 2020 -arviointityökalu sekä Kyberturvallisuuskeskuksen julkaisema PiTuKri-ohje. Yleisten turvallisuusluokiteltuun tietoon kohdistuvien riskien lisäksi tiedonhallin-

tayksikön tulee huomioida erityiset riskit, jotka liittyvät arvioitavassa pilvipalvelussa käsiteltäviksi suunniteltuihin turvallisuusluokiteltaviin asiakirjoihin ja asiakirjojen käsittelyn eri käyttötapauksiin ja käyttötapauksiin liittyviin viranomaisprosesseihin. Erityisten riskien hallitsemiseksi on suunniteltava ja toteutettava hallintamenettelyt. Nämä menettelyt tulee valita huomioiden sekä kokonaisturvallisuuden vaatimukset, että kokonaistaloudellinen edullisuus.

Turvallisuusluokiteltuun tietoon kohdistuvien riskien tunnistamisen ja tietoturvallisuustoimenpiteiden riskiarvioon perustuvan toteuttamisen tarkoituksena on täydentää ja täsmentää säädöksissä asetettuja turvallisuusluokitellun tiedon suojaamiseen kohdistuvia vähimmäisvaatimuksia. Jos tunnistettua riskiä ei arvioida ilmenevän turvallisuusluokiteltavan asiakirjan käsittelyn käyttötapauksissa tai viranomaisprosesseissa, tai riskin jäännösriski voidaan hyväksyä, niin tiedonhallintayksikkö voi jättää riskiin liittyvän hallintatoimenpiteen/suojauksen toteuttamatta. Näin voidaan myös toimia, jos jokin toinen riskien hallintatoimenpide/suojaus ehkäisee tunnistetun riskin vaikutukset luotettavasti. Esimerkiksi tietojenkäsittely-ympäristön fyysinen eriyttäminen voi ehkäistä useiden tietoverkkoihin liittyvien riskien vaikutuksia tehokkaasti ja siten toimia riittävänä suojauksena. Tiedonhallintayksikön riskienarvioinnin 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

Turvallisuusluokiteltuun tietoon kohdistuvat erityisriskit voidaan jakaa seuraavasti:

- lainsäädäntöjohdannaisiin riskeihin,
- ulkomaiseen omistukseen ja vaikutusvaltaan (FOCI, Foreign Ownership, Control or Influence) liittyviin riskeihin,
- turvallisuusluokiteltuun tietoon 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 yksityiskohtaisesti 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).

Turvallisuusluokiteltuun tietoon määräysvallassa olevat viranomaiset varaavat usein itselleen tarkastusoikeuden kaikkiin tietojenkäsittely-ympäristöihin, joissa heidän määräysvallassaan olevaa turvallisuusluokiteltua tietoa käsitellään. Erityisesti kansainvälisen turvallisuusluokiteltavan tiedon osalta määräysvallassa olevista viranomaisista käytetään usein myös termiä "tiedon omistaja" ja samansuuntaisessa merkityksessään joskus myös termiä "tiedon originaattori". Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Pilvipalveluissa, joissa käsitellään usean eri viranomaisen tietoa, tulee tietojenkäsittely-ympäristön rakenteen mahdollistaa tarkastusten toteuttaminen niin, että tietoon 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 tietoa sisältävää pilvipalvelua käyttäviltä viranomaisilta sitoutumista siihen, että he eivät käytä teknistä tarkastusoikeutta pilvipalveluun, ja luottavat esimerkiksi turvallisuusselvityslain (726/2014) mukaisen yritysturvallisuusselvityksen tuottamaan tietoon pilvipalvelun turvallisuudesta varmistumisessa. Pilvipalvelun tarjoajan ja pilvipalvelun luotettavuuden arviointia käsitellään tarkemmin luvussa 4.

Teknisten suojausten toteutusvarmuuden näkökulmat liittyvät pilvipalveluiden tuottamiseen, ylläpitoon ja hallintaan. Esimerkiksi turvallisuusluokiteltujen tietojen suojaamisessa käytettyjen salausratkaisujen tulee pystyä tarjoamaan turvallisuusluokitellulle tiedolle sen salassapitoajan kestävä suojaus myös huomioiden edistyneemmillä hyökkääjillä käytössään olevat menetelmät. Palvelun tuottamiseen, ylläpitoon ja hallintaan liittyviin riskeihin vaikuttavat myös pilvipalvelun palvelumallit, joista yleisimpiä ovat SaaS, PaaS ja IaaS. Nämä termit on kuvattu liitteenä 1 olevassa termistössä. Tiedonhallintayksikön tulee myös tunnistaa alihankkijaketjuihin ja alihankkijoihin liittyviä riskejä, sekä eri teknologioiden käyttöön, ja palvelun- ja sen tuottamiseksi tarvittavien palveluiden aiheuttamaan turvallisuusluokiteltujen tietojen käsittelyyn liittyviä riskejä.

Turvallisuusluokitteluasetuksessa asetetuista teknisistä suojausvaatimuksista pilvipalvelujen osalta on huomioitava erityisesti tiedonsaantitarpeen ja turvallisuusluokitellun tiedon suojaamista koskevien velvoitteiden jalkautusvelvoitteet (8 §), tiedon ja tietojärjestelmän suojaaminen turvallisuusalueiden avulla (10 §), erotteluvelvoite alemman turvallisuustason ympäristöistä (11 § k 1), yleisiä verkkohyökkäyksiä vastaan suojautuminen sekä suojauksista huolehtiminen koko tietojärjestelmän elinkaaren ajan (11 § k 2), vähimpien oikeuksien periaatteen toteuttaminen (11 § k 3), tietojärjestelmän eheyden suojaaminen (11 § k 4), käyttäjien, laitteiden ja tietojärjestelmien tunnistaminen (11 § k 5), kovennuskäytännöt (11 § k 6) ja salausratkaisujen riittävä turvallisuus (11 § k 7). Riittävän turvallisia salausratkaisuja edellytetään erityisesti siirrettäessä turvallisuusluokiteltua tietoa fyysisten turvallisuusalueiden ulkopuolella tai matalamman turvallisuustason verkon kautta (12 §, myös tiedonhallintalain 14 §). Tarpeettomaksi käynyt turvallisuusluokiteltu asiakirja on tuhottava tavalla, jolla kyseiselle turvallisuusluokalle riittävän luotettavasti estetään tietojen palauttaminen sekä kokoaminen uudelleen kokonaan tai osittain (15 §). Lisäksi turvallisuusluokasta III lähtien tulee huomioida hajasäteily ja riittävä suojautuminen elektroniselta tiedustelulta. Näiden toteuttamista on käsitelty yksityiskohtaisemmin tiedonhallintalautakunnan suosituksessa turvallisuusluokiteltujen asiakirjojen käsittelystä (VM 2021:5).

4 Turvallisuusluokiteltavien asiakirjojen käsittelyssä käytettävien pilvipalveluiden ja niiden tarjoajien luotettavuuden arvioinnista

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. Tämä tarkoittaa, että myöskään turvallisuusluokiteltuja tietoja ei saa luovuttaa pilvipalvelun tarjoajalle ennen kuin tiedonhallintayksikkö on varmistunut pilvipalvelun tarjoajan luotettavuudesta sekä siitä, että tarjoaja käsittelee tietoja tiedonhallintalain ja turvallisuusluokitteluasetuksen mukaisesti.

Säännösten mukainen menettely pilvipalvelun tarjoajan luotettavuuden arviointiin on turvallisuusselvityslain (726/2014) mukainen yritysturvallisuusselvitys, joka kohdistetaan Suomesta tuotettuun tai tulevaisuudessa tuotettavaan pilvipalveluun ja sen tarjoajaan. Yritysturvallisuusselvityksessä arvioidaan yrityksen vastuuhenkilöiden luotettavuutta, yrityksen tietoturvallisuuden tasoa ja sen kykyä hoitaa sitoumuksensa. Turvallisuusselvityslain 9 §:n mukaisesti Traficom laatii osana yritysturvallisuusselvitystä tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen. Yritysturvallisuusselvitysprosessia on kuvattu yksityiskohtaisemmin Suojelupoliisin verkkosivuilla.

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 (arviointilaitoslaki 2 §). Tietoturvallisuudella tarkoitetaan luottamuksellisuuden, saatavuuden ja eheyden varmistamista. 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 (arviointilaki 4 §). 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. Arviointilain mukaista arviointimenettelyä on kuvattu yksityiskohtaisemmin Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen verkkosivuilla.

Tiedonhallintayksiköitä suositellaan käyttämään sellaisia pilvipalveluita, joiden turvallisuus sekä myös joiden tarjoajan turvallisuus on arvioitu turvallisuusselvityslain mukaan tehdyissä yritysturvallisuusselvityksissä tai joille on myönnetty tietoturvallisuuden arviointitoimintaa koskevien säännösten mukainen vaatimustenmukaisuutta osoittava todistus.

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). Jos turvallisuusluokiteltavia asiakirjoja käsitellään kansainvälisissä pilvipalveluissa, niin tiedonhallintayksikön on harkittava turvallisuusuussopimuksen tarve Suomen valtion ja niiden valtioiden välillä, joiden lainkäyttövaltaan pilvipalvelujen tarjoaja ja sen alihankkijat kuuluvat, sekä jos turvallisuussopimus on näiden valtioiden kanssa solmittu, niin arvioitava toteutuvatko turvallisuussopimuksen mukaiset kansainväliset tietoturvallisuusvelvoitteet kyseistä pilvipalvelua käytettäessä.

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 ja Traficom tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa lain tarkoittamana määrättynä turvallisuusviranomaisena. 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". Kansainvälisissä tietoturvallisuusvelvoitteissa tarkoitettu yritysturvallisuusselvitys on lähtökohtaisesti käytettävissä turvallisuusluokkaa TL III / CONFIDENTIAL ja tätä korkeampien turvallisuusluokkien asiakirjoja käsiteltäessä. Kansainvälisten pilvipalvelujen tarjoajan luotettavuuden arvioinnissa suositellaan hyödynnettävän kansainvälistä yritysturvallisuusselvitysmenettelyä aina kun se on mahdollista.

Sellaisia turvallisuusluokiteltavia asiakirjoja, jotka on rajattu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1807, muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa soveltamisalan ulkopuolelle, ei suositella käsiteltävän kansainvälisissä pilvipalveluissa. Asetuksen soveltamisalan tulkintaa on käsitelty liikenne- ja viestintäministeriön julkaisussa 2019: 11. Lähtökohtaisesti asetusta ei sovellettaisi esimerkiksi kansallisen turvallisuuden ja varautumisen perusteella asetettaviin tiedon sijaintivaatimuksiin. Jos kansainvälisiä pilvipalveluita käytetään turvallisuusluokiteltavien asiakirjojen käsitellyssä, niin suositellaan, että käsiteltävät turvallisuusluokitellut tietoaineistot rajataan ja valitaan tarkasti, ja käytetään ainoastaan viranomaisten luotettaviksi arvioimia pilvipalveluita, joihin liittyvät jäännösrikit tiedonhallintayksikkö on kirjallisesti päätöksellään hyväksynyt. Esimerkiksi valtioiden välinen kansainvälinen yhteistoiminta tai kansainvälisiin hankintoihin liittyvä tiedonvaihto voivat olla perusteita käyttää jäännösriskeiltään tiedonhallintayksikön hyväksymään riskiarvioon perustuen tarkkaan rajattujen ja valittujen turvallisuusluokiteltujen tietoaineistojen käsittelyssä viranomaisten luotettaviksi arvioimia kansainvälisiä pilvipalveluita.

Tiedonhallintayksikkö voi pyrkiä myös itse arvioimaan pilvipalvelujen tarjoajien tai pilvipalvelujen luotettavuutta. Tässä haasteena on se, että tyypillisesti tiedonhallintayksiköillä ei ole mahdollisuuksia syvälliseen ja luotettavaan pilvipalvelujen tarjoajien tai pilvipalvelujen arviointiin. Syvällinen arviointi edellyttää 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 tarjoajiin tai pilvipalvelujen luotettavuutta turvallisuusluokiteltujen tietojen käsittelyssä, jos se joutuu arvioimaan lakisääteisten vaatimusten täyttymistä esimerkiksi vain pilvipalvelujen tarjoajien itsearviointiin, kaupallisiin sertifiointeihin ja sopimustekniikkaan perustuen.

5 Turvallisuusluokiteltavien asiakirjojen käsittelyssä käytettäviin pilvipalveluihin liittyvistä palvelusopimuksista

Kun pilvipalveluita käytetään turvallisuusluokiteltavien asiakirjojen käsittelyssä, niin turvallisuusluokiteltujen tietojen käsittelyn turvallisuuden varmistaminen perustuu luvussa 4 kuvattuun pilvipalvelun tarjoajien sekä pilvipalvelujen luotettavuuden arviointiin sekä niihin nojautuviin tiedonhallintayksikön ja pilvipalvelun tarjoajan sekä mahdollisen integraattorin kanssa tehtyihin sopimuksiin. Pilvipalvelun tarjoajan sekä pilvipalvelun luotettavuuden arvioinnissa ja palvelujen tarjoamista koskevissa sopimuksissa on muun muassa huomioitava se, missä valtioissa tietoa käsitellään ja siten maakohtaiset säädökset, ja kattavatko nämä koko alihankkijaketjun: kaikki alihankkijat ja palvelun mahdollisen tukijärjestelyn. Lisäksi on huomioitava se, miten palveluntarjoaja osoittaa riittävän turvallisuustason, esimerkiksi tarkastusraporttien ja auditointien avulla.

Tiedonhallintayksikön tulee varmista se, että palvelusopimus täyttää turvallisuusluokiteltavan tiedon käsittelyyn liittyvät vaatimukset. Tietoturvallisuudesta sopimista on käsitelty kattavammin tiedonhallintalautakunnan suosituskokoelmassa tiettyjen tietoturvallisuussäännösten soveltamisesta (VM 2020:61). Riskiperustaisesti on myös arvioitava sopimuksen luotettavuutta ja varmistuttava siitä, että tarjoajan sopimuksessa sopimat asiat on myös toteutettu sovitulla tavalla.

Pilvipalvelun tuottamiseen liittyvän mahdollisen alihankintaketjun arviointi sisältyy tyypillisesti luvussa 4 kuvattuihin yritysturvallisuusselvityksiin sekä tietojärjestelmien ja tietoliikennejärjestelyjen arviointeihin. Mikäli tällaista menettelyä ei ole kuitenkaan käytetty, niin 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. Näin ollen 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 pilvipalveluiden jälleenmyyjä, jonka kanssa integraat-

tori on tehnyt pilvipalveluita koskevan hankintasopimuksen. Tässä tapauksessa sopimusketjun kolmannen askeleen muodostaa välittäjän tai jälleenmyyjän ja pilvipalvelun tarjoajan välinen sopimus. Lisäksi on huomioitava, että pilvipalvelun tarjoajat voivat käyttää lukuisia alihankkijoita, jotka osaltaan osallistuvat palveluiden toteuttamiseen ja toimittamiseen loppukäyttäjänä olevalle tiedonhallintayksikölle. Alihankkijat voivat toimia useissa eri maissa, mikä kasvattaa selvitettävien säädösten määrää, katso tarkemmin kohdasta lainsäädäntöjohdannaisten riskien selvittäminen, ja huomioi henkilötietojen käsittelyn asettamat vaatimukset.

Pilvipalveluiden käytönaikaisessa hallinnassa korostuvat sopimusmuutosten seuranta ja valvonta, sekä pilvipalvelun turvallisuuden valvonta, ja käyttöoikeuksien ja ylläpidon hallinta. Suositellaan, että tiedonhallintayksiköt käyttävät pilvipalvelun tarjoajaa, joka on arvioitu vaatimustenmukaiseksi turvallisselvityslain tai arviointilain mukaisesti, ja joka vastaa myös konfiguraatioista palveluna.

Suositellaan, että pilvipalvelujen tarjoajaa vaaditaan ilmoittamaan merkittävistä muutoksista palveluun ja sopimuksiin hyvissä ajoin etukäteen, sekä kaikista poikkeamista viipymättä, ja muista merkittävistä pilvipalvelun tuotantoympäristön tapahtumista kuukausittain, sekä turvallisuuden kokonaiskuvasta 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. Tiedonhallintayksikköä suositellaan huolehtimaan 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 mukaisesti viranomaisen velvollisuutena on varmistua tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta 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 voimakas kehittyminen, mikä edellyttää jatkuvaa sopimusten seurantaa ja valvontaa sekä muutoshallintaa. Muutokset kasvattavat riskiä siitä, että palvelu, sen tarjoaja tai jokin uusi ominaisuus muuttuu sopimuksen- tai vaatimustenvastaiseksi tai toteutuu määräysvaltamuutosriskejä. Lisäksi on huomioitava, että tiedon elinkaaren ajan kestävästä tietoturvallisuudesta voi olla mahdotonta varmistua sellaisten pilvipalvelun tarjoajien kanssa, jotka varaavat sopimuksiinsa yksipuolisen mahdollisuuden muuttaa sopimusehtojaan.

Tiedonhallintayksiköllä ei tyypillisesti ole eikä ole tarpeenkaan olla osaamista seurata pilvipalvelun tarjoajien palveluiden kehitystä ja kehitystoimien kautta tulevia muutoksia. Tiedonhallintayksiköitä suositellaan käyttämään vaatimustenmukaisiksi todettuja Suomesta tuotettuja pilvipalveluita aina kun se on mahdollista kansainvälisiin pilvipalveluihin liittyvien riskien hallitsemiseksi turvallisuusluokiteltavien asiakirjojen elinkaaren ajan. Valtion virastoja suositellaan harkitsemaan Valtion tieto- ja viestintätekniikkakeskuksen Valtorin kautta hankittujen pilvipalvelujen käyttöä.

Tiedonhallintayksikkö voi lopettaa pilvipalveluiden käytön joko 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 pilvipalveluiden hankinnasta ja suunnittelusta, että pilvipalvelun päättäminen tai palvelun tarjoajan vaihtaminen on mahdollista. Pilvipalvelun käytön päättämistä käsitellään valmisteilla olevassa Tiedonhallintalautakunnan suosituksessa.

6 Keskeiset suositukset

Tiedonhallintayksiköitä suositellaan valitsemaan pilvipalvelu siinä käsiteltävien turvallisuusluokiteltavien asiakirjojen tiedonhallinta- ja tietoturvallisuusvaatimusten, sekä käsittelyn käyttötapausten ja niihin liittyvien viranomaisprosessien perusteella. Tiedonhallintayksiköitä suositellaan käyttämään sellaisia pilvipalveluita, joiden turvallisuus sekä myös joiden tarjoajan turvallisuus on arvioitu turvallisuusselvityslain mukaan tehdyissä yritysturvallisuusselvityksissä, tai joille on myönnetty tietoturvallisuuden arviointitoimintaa koskevien säännösten mukainen vaatimustenmukaisuutta osoittava todistus.

Sellaisia turvallisuusluokiteltavia asiakirjoja, jotka on rajattu Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1807, muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa soveltamisalan ulkopuolelle, ei suositella käsiteltävän kansainvälisissä pilvipalveluissa.

Jos kansainvälisiä pilvipalveluita käytetään turvallisuusluokiteltavien asiakirjojen käsitellyssä, niin suositellaan, että käsiteltävät turvallisuusluokitellut tietoaineistot rajataan ja valitaan tarkasti, ja käytetään ainoastaan viranomaisten luotettaviksi arvioimia pilvipalveluita, joihin liittyvät jäännösrikit tiedonhallintayksikkö on kirjallisesti päätöksellään hyväksynyt. Lisäksi jos turvallisuusluokiteltavia asiakirjoja käsitellään kansainvälisissä pilvipalveluissa, niin tiedonhallintayksikön on harkittava turvallisuusuussopimuksen tarve Suomen valtion ja niiden valtioiden välillä, joiden lainkäyttövaltaan pilvipalvelujen tarjoaja ja sen alihankkijat kuuluvat, sekä jos turvallisuussopimus on näiden valtioiden kanssa solmittu, niin arvioitava toteutuvatko turvallisuussopimuksen mukaiset kansainväliset tietoturvallisuusvelvoitteet kyseistä pilvipalvelua käytettäessä. Kansainvälisten pilvipalvelujen tarjoajan luotettavuuden arvioinnissa suositellaan hyödynnettävän kansainvälistä yritysturvallisuusselvitysmenettelyä aina kun se on mahdollista.

7 Lähdeluettelo

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. https://julkaisut.valtioneuvosto.fi/handle/10024/161294

Valtiovarainministeriö 2020:73. Pilvipalvelujen soveltamisohje – Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon tiedonhallintayksiköille. https://julkaisut.valtioneuvosto.fi/handle/10024/162453

Tiedonhallintalautakunta (VM 2021:5). Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. https://julkaisut.valtioneuvosto.fi/handle/10024/162649

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

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 taikka 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 ohjelmistojen käsittelyyn 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

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

	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.
Pilvipalvelun tarjoaja	Tässä suosituksessa pilvipalvelun tarjoajalla tarkoitetaan toimijaa, joka tarjoaa IaaS-, PaaS- tai SaaS-mallista palvelua tai muuta pilviteknologiaan perustuvaa palvelua.
Pilvialustan toimittaja	Pilvialustan toimittaja tuottaa pilvipalvelun, johon kuuluu infrastruktruurin kapasiteetti, suorituskyky, tietoliikenne ja mahdolliset lisäpalvelut. Palvelut ovat tilaajan ja sovellustoimittajan valittavissa ja mahdollisesti konfiguroitavissa.
Palvelutoimittaja	Palvelutoimittaja toimittaa pilvialustalle tuotetun palvelun. Palvelu voi olla virtuaalipalvelimia, sovelluksia tai järjestelmiä, jotka on rakennettu pilvialustan kapasiteetin ja ratkaisuiden päälle. Palvelutoimittajalla on usein hallintaoikeudet itse järjestelmään ja sovellukseen. Palvelutoimittajalla ja sovellustoimittajalla voi olla omat alihankkijat. Palvelutoimittaja voi toimia myös integraattorin roolissa.
Integraattori	Integraattori hankkii palveluita tilaajan puolesta sekä pilvialustan toimittajilta että palvelutoimittajilta 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 palvelutoimittajaa 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 tarvitsee muokata. Ohjelmistokontti voidaan esimerkiksi siirtää omasta konesalista pilveen.
Yksityinen pilvi (Private cloud)	*Pilvipalvelun toteutusmalli:* Yksityisellä pilvellä tarkoitetaan 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, tiedonhallintayksikköistä ja ulkoisista toimijoista. Yksityisellä pilvellä pystytään toteuttamaan tyypillisesti korkeamman turvatason palveluja, kuin muilla toteutusmalleilla.

Yhdistelmäpilvi (Hybrid cloud)	*Pilvipalvelun toteutusmalli:* Yhdistelmäpilvellä tarkoitetaan 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, mitä tietoja on mahdollista siirtyä julkisen pilven puolelle, ja miten turvallisuus on järjestetty pilvitoteutusten rajapinnoissa.
Julkinen pilvi (Public cloud)	*Pilvipalvelun toteutusmalli:* Julkisella pilvellä tarkoitetaan palvelua, joka on julkisesti tarjolla ja kaikkien toimijoiden hankittavissa. Palvelua tuotetaan lähes poikkeuksetta palvelun tarjoajan konesaleista. Julkisessa pilvessä pilvipalveluinfrastruktuuriin sekä siinä käsiteltäviin tietoihin kohdistuu yksityistä pilveä laajempi hyökkäyspinta-ala muun muassa palvelun muiden käyttäjien tai ulkoisten toimijoiden kautta.
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 Esimerkki toimijoiden tehtävistä

Alla on kuvattu esimerkki kunkin toimijan käytönaikaisen hallinnan tehtävien toteuttamisesta:

Tiedonhallintayksikön tehtävät

- Vastaa turvallisuusluokiteltavan tiedon elinkaaren aikaisesta suojauksesta pilvipalvelussa sekä tiedon viemisestä pilveen ja sen poistamisesta.
- Määrittää sallitun käytön.
- Vastaa valvonnan toteutumisesta ja riskienhallinnasta.
- Vastaa toimitusketjun turvallisuudesta turvallisuusluokiteltavan tiedon käsittelyvaatimuksia vasten.
- Vastaa kokonaisturvallisuuden hallinnasta ja ohjauksesta.
- Valvoo tiedon kasautumista.

Integraattorin tehtävät

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

Palvelutoimittajan/Sovellustoimittajan tehtävät

- Muutoshallinta,
- käyttäjäoikeuksien ylläpito ja tarkastus,
- palvelun käytön valvonta,
- riskiarvion ylläpitäminen,
- seuraa muutoksia, joita pilvipalveluihin on tulossa,
- pitää järjestelmät ja suojaukset ajan tasalla, sekä

- sopimuksellisesti vastaa oman toimitusketjun turvallisuudesta turvallisuusluokiteltavan tiedon käsittelyvaatimuksia vasten.