DIGI- JA VÄESTÖTIETO-VIRASTO

Tietosuoja pilvipalve-luissa

VAHTI hyvät käytännöt tukimate-riaali

9.11.2022

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Sisällysluettelo

Tietosuoja pilvipalveluissa

1 Yleistä

Tämä asiakirja on tarkoitettu vapaasti hyödynnettäväksi ja sovellettavaksi tukimateriaalina. Oppaan tarkoituksena on kuvata yleisesti tietosuojan kannalta huomioitavia asioita pilvipalveluita käytettäessä.

Toivomme, että annat palautetta tästä tukimateriaalista:

https://response.questback.com/dvv/digiturvahyvatkaytannotpalaute

Muut yhteydenotot koskien tätä tukimateriaalia:
digiturva@dvv.fi

Tämän tukimateriaalin tuottamisesta on vastannut VAHTI ICT-palveluiden tietoturvallisuuden kehittämisen sekä tietosuojan kehittämisen työryhmien asiantuntijat.

2 Pilvipalveluiden määritelmät

Pilvipalveluilla tarkoitetaan palveluita, jossa palveluntarjoaja tarjoaa tietoteknisiä resursseja, kuten esimerkiksi sovelluksia, laskentakapasiteettia, palvelimia tai tallennustilaa tilaajan käytettäväksi verkon välityksellä palveluntarjoajan hallinnoimasta kapasiteetistä.

2.1 Pilvipalveluiden tuotantomallit

2.1.1 Toiminnallinen malli

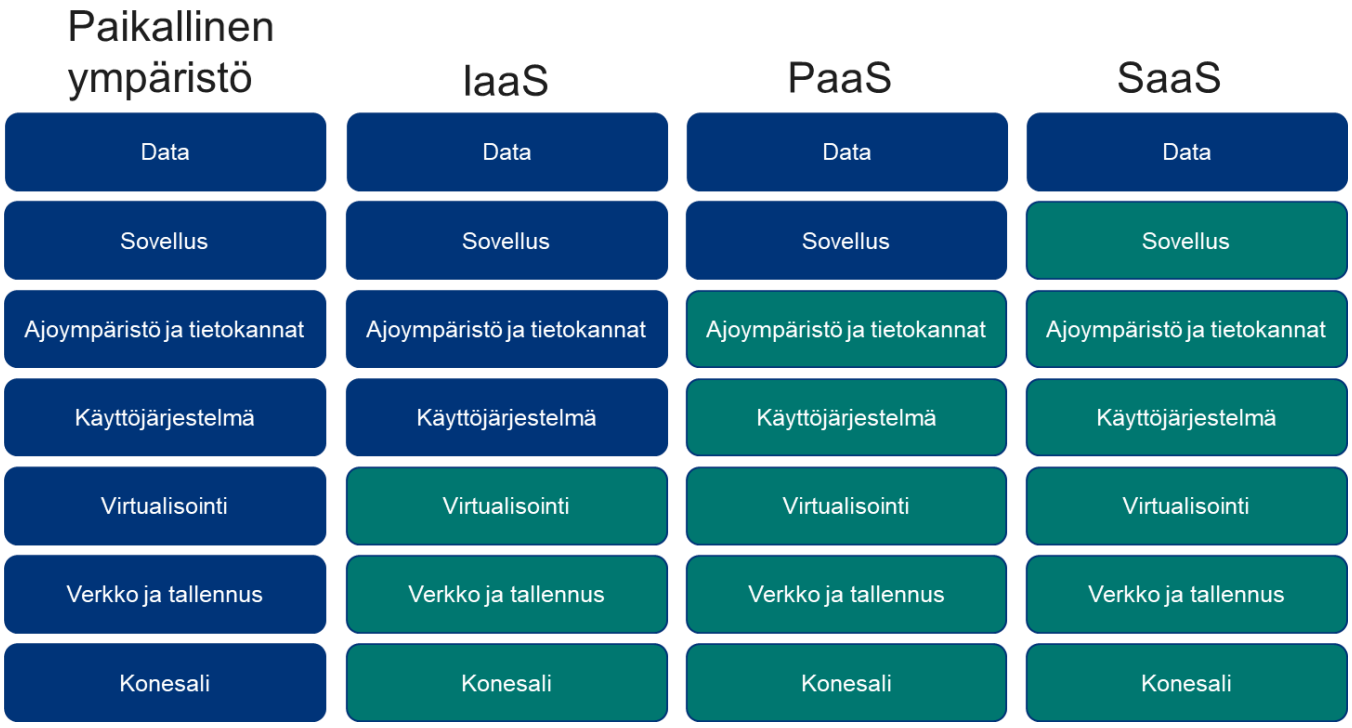
Pilvipalveluna toteutetun järjestelmän tai ympäristön toiminnallinen malli vaikuttaa myös pilvipalveluiden tietosuojaan liittyviin kysymyksiin. Alla on avattu erilaisia toiminnallisia malleja ja niihin liittyviä huomioitavia seikkoja palvelun näkökulmasta

Termi	Määritelmä
Yksityinen pilvi	Yksityisellä pilvellä tarkoitetaan palvelua, joka tuotetaan vain palvelua käyttävälle asiakkaalle. Palvelua voidaan tuottaa joko palveluntarjoajan tai/ja tilaajan konesalista. Yksityisen pilven tyypillisenä vahvuutena on pilvipalveluinfrastruktuurin sekä siinä käsiteltävien tietojen fyysisen ja loogisen tason luotettava erottelu muista tietojenkäsittely-ympäristöistä ja ulkoisista toimijoista.
Julkinen pilvi	Julkisella pilvellä tarkoitetaan yleisesti palvelua, joka on julkisesti tarjolla ja kaikkien toimijoiden hankittavissa. Palvelua tuotetaan lähes poikkeuksetta palveluntarjoajan konesaleista ja usein pääsy julkisen pilven palveluun tapahtuu internetin välityksellä.
Yhdistelmäpilvi	Järjestelmä tai ympäristö on toteutettu käyttäen useampaa eri pilvipalvelua tai paikallista infrastruktuuria. Usein järjestelmien laajennus saattaa johtaa siihen, että osa järjestelmästä sijaitsee organisaation paikallisessa infrastruktuurissa ja osa pilvipalvelussa.
Dedikoitu pilvipalvelu	Dedikoidussa pilvipalvelussa organisaatiolle varataan pilvipalvelun kapasiteettia yksityiseen käyttöön. Dedikoidun pilvipalvelun osalta käsitteistö on vaihtelevaa, ja se voikin tapauskohtaisesti tarkoittaa esimerkiksi dedikoituja virtuaalipalvelimia tai dedikoituja fyysisiä palvelimia ja tallennuskapasiteettia. Palvelun hankintavaiheessa tulisikin selvittää kattavasti mitä dedikoitu kapasiteetti kunkin palvelun osalta tarkoittaa.
Jaettu pilvi	Jaetussa pilvipalvelussa palvelun taustalla toimiva kapasiteetti tuotetaan usealle palvelun käyttäjälle jaetusta infrastruktuurista. Jaetun pilvipalvelun taustalla toimiva käyttöliittymä ja varsinainen kapasiteetin jakamisesta vastaava teknologia saattaa sisältää palveluntarjoajan omia ratkaisuja.

2.2 Palvelumallit

Pilvipalveluissa voidaan hyödyntää myös erilaisia palvelumalleja. Palvelumallit eroavat toisistaan enimmäkseen teknisten kerrosten, kuten esimerkiksi tietoliikenneverkkojen tai käyttöjärjestelmän ylläpidon ja hallinnan osalta. Alla oleva kuva osoittaa, miten vastuut tyypillisesti jakautuvat eri palvelumalleissa.

Termi	Määritelmä
IaaS (Infrastructure as a Service)	IaaS-mallissa eli infrastruktuuri palveluna-mallissa kaikki palveluiden tuottamiseen liittyvä infrastruktuuri hankitaan pilvipalvelun tarjoajalta.
PaaS (Platform as a Service)	PaaS-mallissa eli alusta palveluna –mallissa palvelut tuotetaan valmiin ohjelmistoalustan avulla.
SaaS (Software as a Service)	SaaS-mallissa eli ohjelmistopalvelu –mallissa pilvipalvelun tarjoaja tuottaa tietyn ohjelmiston käyttöön liittyvät palvelut kokonaisuudessaan.



Kuva 1. Vastuunjako eri palvelumalleissa

3 Pilvipalveluiden erityispiirteet tietosuojan kannalta

Pilvipalveluihin liittyy useita erityispiirteitä, joita tulee ottaa huomioon suunniteltaessa henkilötietojen käsittelyä. Näistä olennaisimpia ovat palveluiden sijainti sekä vastuunjako tarjotun kapasiteetin, että palveluiden ylläpidon osalta.

Läpinäkyvyys

Tilaajan näkyvyys pilvipalveluiden tuotannossa käytettyyn infrastruktuuriin ja ylläpitoon liittyviin ratkaisuihin on useimmiten melko vähäistä. Tietosuojan kannalta tämä hankaloittaa erityisesti henkilötietojen käsittelyn suunnittelua sillä pilvipalvelun käyttäjä ei useinkaan tiedä millaisia prosesseja palvelun taustalla pyörii. Useimmissa pilvipalveluissa on kuitenkin mahdollista rajata esimerkiksi tiedon fyysinen sijainti tietyn alueen, kuten esimerkiksi Euroopan Unionin sisälle.

Hallinnan ja vastuiden jakautuminen

Vastuu turvallisuustoimenpiteistä pilvipalveluissa jakautuu tilaajan sekä toimittajan välillä. Toimittajat vastaavat usein pilvipalveluiden fyysisestä turvallisuudesta sekä infrastruktuurin, kuten verkkojen ja palvelinlaitteistojen turvallisuudesta. Tilaaja kuitenkin vastaa tapauksesta ja palvelumallista riippuen esimerkiksi järjestelmän konfiguroinnista ja käyttöoikeuksista. Kohdassa *2.2 Palvelumallit* on esitelty tarkemmin yleisimpiä palvelumalleja ja näiden vastuunjakoa, joka noudattelee myös tietoturvatoimenpiteiden osalta samaa kaavaa.

Palveluiden sijainti

Palvelujen sijainti on tietosuojan kannalta merkittävä erityispiirre erityisesti kansainvälisissä pilvipalveluissa. Kansainvälisissä pilvipalveluissa palvelun taustalla oleva infrastruktuuri voi sijaita lähes missä päin maailmaa tahansa ja sijainti onkin usein tilaajan itse valittavissa. Palvelutuotantoon liittyy kuitenkin paljon muitakin tekijöitä kuin pelkkä infrastruktuuri. Kansainvälisissä pilvipalveluissa tulee huomioida myös se, mistä palvelua tuottava henkilöstö toimii ja onko heillä teknisesti mahdollista käsitellä asiakkaan pilvipalveluihin tallentamia henkilötietoja.

Alihankkijat

Palveluntarjoajat saattavat myös hyödyntää alihankkijoita pilvipalvelun tuottamisessa, joten on tärkeätä kyetä selvittämään kaikki henkilötietojen käsittelyyn liittyvät alihankkijat. Palveluntarjoaja voi hyödyntää alihankkijoita hyvinkin erilaisiin tehtäviin palvelutuotannossa aina konesalien ylläpidosta asiakasyhteydenottojen käsittelyyn.

Lisäksi erityisesti SaaS-palvelumallin mukaiset pilvipalvelut saattavat olla järjestetty niin, että varsinainen palvelun toimittaja toimittaa vain sovelluskerroksen ja varsinainen kapasiteetti toimitetaan alihankkijan kautta esimerkiksi kansainväliseltä pilvipalvelualustalta.

Tiedon omistajuus

Useimmiten myös pilvipalveluissa tiedon omistajuus säilyy asiakkaalla tai rekisterinpitäjällä, vaikka tietoa siirretäänkin palveluntarjoajan hallitsemiin ympäristöihin. Tämä on kuitenkin oleellista varmistaa sopimusehtoja laadittaessa.

Palveluiden dokumentaatio

Palveluiden kattava dokumentaatio on olennaista tietosuoja-asetuksen vaatimusten osalta. Rekisterinpitäjän on tiedettävä, missä henkilötietoja käsitellään ja kenen toimesta, sekä millaisia tietoturvallisuustoimenpiteitä palvelussa on toteutettu. Pilvipalveluita käytettäessä tuleekin tutustua toimittajan tarjoamaan dokumentaation kattavasti sekä tarvittaessa myös vaatia tarkempaa dokumentaatiota pilvipalvelun rakenteesta läpinäkyvyyden lisäämiseksi.

Myös palveluntarjoajan ajantasaiset sertifioinnit ovat olennainen osa näiden toimenpiteiden ja mallien todentamisessa.

4 Tietosuojariskien hallinta pilvipalveluissa

Henkilötietojen käsittely edellyttää tietojen luonteen perusteella tehtävää riskiarviointia, mistä voi seurata rajoitteita myös tietojen fyysisen sijainnin, tietojen hallinnoinnin ja palveluntarjoajan valintaan.

Tässä luvussa on kuvattu yleisimpiä tietosuojaan liittyviä riskejä pilvipalveluja käytettäessä. Osa riskeistä on sellaisia, jotka on huomioitava myös muussa kuin pilvipalveluna toteutettavassa henkilötietojen käsittelyssä.

4.1 Muutoshallintaan liittyvät riskit

Pilvipalveluiden tarjoamat toiminnallisuudet kehittyvät ja laajenevat ajoittain erittäin nopeasti. Tämä edellyttää seurantaa ja kehittämisen ketteryyttä, mikäli tarvittu palvelun osa tai toiminnallisuus muuttuu. Lisäksi on mahdollista, että jokin tarvittu toiminnallisuus poistuu tai muuttuu käyttökelvottamaksi kyseisessä käyttötapauksessa.

Pilvipalveluiden muutoshallintaan liittyvät riskit voivat olla esimerkiksi:

- Yksipuoliset ja osin ennakoimattomat muutokset pilvipalvelussa. Tällainen tapaus voi olla esimerkiksi, jos jokin tiedon käsittelyn kannalta olennainen toiminto päivittyy tai poistuu palvelusta.
- Ominaisuuksien hallitsematon käyttö ja käyttöönotto
- Hallintatunnusten myöntäminen, ylläpito ja käyttö
- Pilvipalveluiden konfiguroinnissa tapahtuvat virheet

Usean erilaisen ympäristön kokonaisuuden hallinta ja toimivan pilvipalveluiden hallintamallin järjestäminen vaatii organisaatiolta suunnittelua ja aktiivista ylläpitoa. Hyvään hallintamalliin kuuluu riittävän tarkka roolien ja vastuiden sekä palveluiden hallintaan liittyvien prosessien kuvaaminen.

4.2 Sijantiin liittyvät riskit

Pilvipalvelut voivat olla ulkomaisen lainsäädännön piirissä, jolloin tallennettavat henkilötiedot altistuvat suoralle ulkomaiselle lainkäytölle (esim. turvallisuus- ja paikallinen lainsäädäntö). Paikallinen lainsäädäntö voi sisältää pykäliä esimerkiksi paikallisen turvallisuustoimijan pääsystä pilvipalvelussa sijaitsevaan dataan.

Tästä johtuen hyödynnettäessä pilvipalveluita henkilötietojen käsittelyssä tulisi selvittää millaisen lainsäädännön piirissä kyseinen pilvipalvelu on ja tarvittaessa hallita lainsäädännöstä johtuvia riskejä erilaisin kontrollein. Näitä kontrolleja voi olla muun muassa tiedon salaus tai anonymisointi ennen sen siirtämistä pilvipalveluun ja suunnitelmat pilvipalvelun käytön lopettamisesta ja tietojen siirtämisestä muualle.

Mikäli pilvipalvelussa on tarkoitus käsitellä henkilötietoja, on hyvä myös tutustua pilvipalvelun mahdollisuuksiin toteuttaa salaus ja salausavainten hallinta rekisterinpitäjän omien määritysten mukaisesti.

4.3 Omistajuuteen ja jatkuvuuteen liittyvät riskit

Pilvipalveluiden omistajuuteen ja jatkuvuuteen liittyy vastaavanlaisia riskejä kuin minkä tahansa ulkoistetun palvelun omistajuuteen ja jatkuvuuteen. Lähtökohtaisesti pilvipalveluntarjoaja omistaa palvelun tuotantoon liittyvän kapasiteetin ja resurssit, jolloin tulee huomioida myös palveluntarjoajan pitkän tähtäimen mahdollisuudet tarjota kyseistä palvelua sovituin ehdoin.

Esimerkiksi muutokset palvelua tarjoavan yrityksen omistajuudessa saattavat aiheuttaa myös tietosuojan kannalta huomioitavia muutoksia joko sijainnin tai palveluiden järjestämisen suhteen.

Pilvipalveluita käyttöönotettaessa onkin tärkeätä pyrkiä selvittämään pilvipalvelun tarjoajan omistajuuteen ja taloudelliseen tilanteeseen liittyvät asiat tarkasti.

4.4 Julkisuusarvoon liittyvät riskit

Pilvipalveluihin kohdistuvat viranomaispäätökset tai uutisointi saattaa vaikuttaa kyseisen pilvipalvelun luotettavuuteen ja sitä kautta myös pilvipalvelua hyödyntävien organisaation luotettavuuteen. Julkisuusarvoon liittyviä riskejä arvioitaessa tulisikin ottaa huomioon kuinka luotettavana palvelua ja sen tarjoajaa yleisesti pidetään tietosuojan osalta.

4.5 Taloudelliset vaikutukset

Pilvipalveluita käyttöönotettaessa on huomioitava myös se riski, että palvelun käyttö saattaa olla joko nyt tai tulevaisuudessa tietosuoja-asetuksen vastaista. Mikäli käyttöön otetun pilvipalvelun käyttöä joudutaan rajoittamaan tai se joudutaan lopettamaan kokonaan tietosuojaviranomaisen päätöksellä, saattaa siitä koitua huomattavia kustannuksia käyttäjälle prosessien tai järjestelmien muutosten myötä.

Pilvipalveluita käytettäessä tuleekin kiinnittää erityistä huomiota viranomaisten päätöksiin sekä siihen, että myös omassa käytössä oleva palvelu on tarvittaessa riskiperusteisesti arvioitu ja että palvelun siirtämiseen tai muuttamiseen on laadittu suunnitelmat jo etukäteen.

4.6 Vakiosisältöisiin käyttöehtoihin liittyvät riskit

Erityisesti tietyillä palvelumalleilla, kuten esimerkiksi Software as a Service -palvelumalliin, tuotetuissa pilvipalveluissa on usein vakiosisältöisen käyttöehdot, jotka tulee hyväksyä palvelun käyttöönoton yhteydessä. Tällaisia palveluita käytettäessä henkilötietojen käsittelyyn tulee arvioida käyttöehdot ja tietosuojaehdot tarkoin, jotta

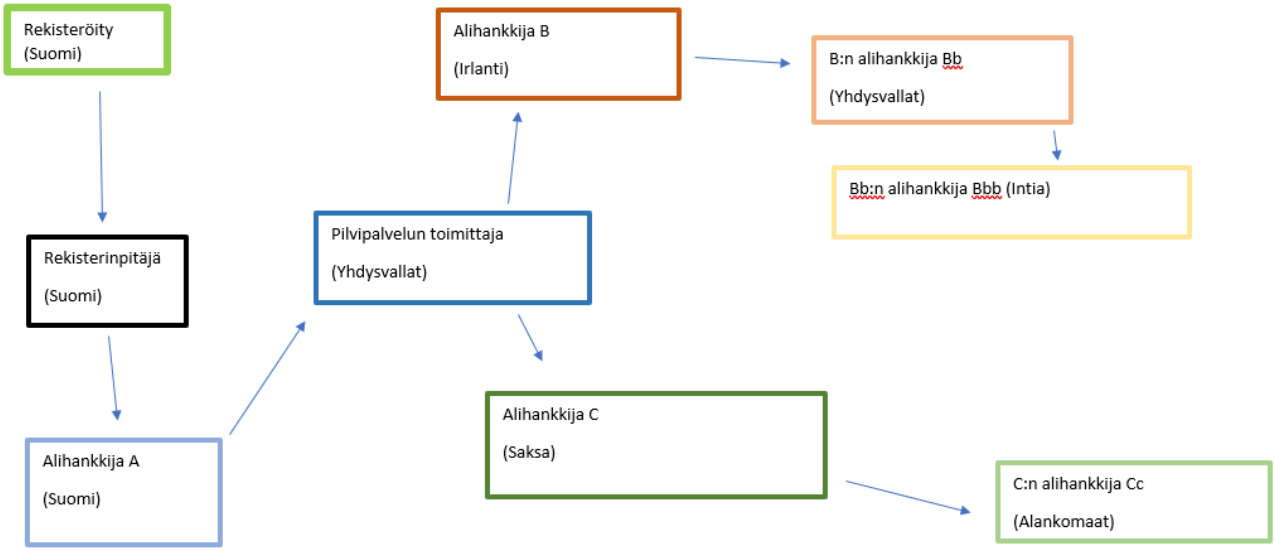
ehdoissa ei ole mitään sellaista, mitä organisaatio ei voi hyväksyä. Vakiosisältöisiin käyttöehtoihin saattaa tilanteesta riippuen olla erittäin hankalaa saada neuvoteltua tarvittavia muutoksia.

5 Tiedot

5.1 Tietovirtojen kuvaaminen toimitusketjuissa

Pilvipalveluissa alihankkijaketjut voivat olla monimutkaisia, ja niiden hahmottaminen vaikeaa. Hyvä keino tätä helpottamaan on tietovirtakartta. Tietovirtakarttaan kuvataan esimerkiksi tiedot siitä, kenen tietoja käsitellään (rekisteröity), kuka tietoja käsittelee (rekisterinpitäjä ja tiedonkäsittelijät) ja missä tietoa käsitellään (maantieteellinen sijainti).

Alla on esimerkki tietovirtakartasta, jossa pilvipalvelun toimittajalla on useita palvelutuotantoon liittyviä alihankkijoita eri maissa.



Kuva 2. Esimerkki tietovirtakartasta

5.2 Tiedon elinkaaren hallinta pilvipalveluissa

5.2.1 Tietojen säilytys

Mikäli pilvipalvelussa käsiteltävät tiedot sisältävät myös henkilötietoja, tulee huomioida tietosuoja-asetuksen mukainen vaatimus säilytysaikojen minimoisesta ja sen mukainen säilytysaikojen toteutuminen. Käytännössä tulee varmistua siitä, että palvelussa on tarvittavat ominaisuudet tai mekanismit säilytysaikojen toteutumiselle. Jos tieto on määräajan säilytettävää, tulee varmistua siitä, että tieto on mahdollista poistaa kokonaan, kts. kohta *5.2.3 Tietojen poistaminen*.

5.2.2 Tietojen siirtäminen

Henkilötietojen siirtämisessä tulee huolehtia riittävästä suojauksesta siirron aikana esimerkiksi salaamalla tieto. Lisäksi laajamittaisessa tietojen siirtämisessä vaikutukset tulee arvioida tapauskohtaisesti.

Tietojen siirtämisen yhteydessä on hyvä huomioida myös mahdolliset muutokset henkilötietojen käsittelyyn liittyviin prosesseihin ja kuvauksiin, kuten esimerkiksi tietovirtakarttoihin.

5.2.3 Tietojen poistaminen

Pilvipalveluista ja muista virtualisoiduista ympäristöistä suoritettava tietojen tuhoaminen ei ole itsestäänselvyys perinteisten tietosuojavaatimusten mukaisesti. Palvelut ovat virtualisoituja ja resurssit jaettuja. Jaetuilla resursseilla tarkoitetaan esimerkiksi tallennusratkaisuja, tietokantaratkaisuja ja resursseja, joita käytetään hetkellisesti.

Perinteistä kiintolevyjen ylikirjoitusta ja muistien tyhjentämistä ei välttämättä tapahdu, kun asiakas poistuu pilvipalvelutarjoajan palvelusta koska tiedot ovat usein pirstaloituneina pilvipalvelutarjoajan eri konesaleissa useilla palvelimilla ja tallennusvälineillä.

Tiedon poistaminen näissä tilanteissa perustuu pilvipalvelutoimittajan ja asiakkaan välisiin sopimuksiin, ja tieto ei poistu aina välittömästi pilvipalvelutarjoajan ympäristöstä, eikä asiakas saa siitä välttämättä automaattisesti vahvistusta.

Hyvä tapa voi olla kuitenkin käyttää tietojen salauksessa omia salausavaimia, jolloin tiedot voidaan mitätöidä poistamalla salausavain. Tässä tapauksessa tiedot poistetaan pyydettäessä sopimusten mukaisesti, mutta ne ovat teoriassa muutettu hyödyttömään muotoon jo aikaisemmin.

Pilvipalveluissa erityisesti huomioitavia poistokohteita palveluntarjoajalta voivat olla muun muassa:

- Virtuaalikoneet
- Tiedontallennusratkaisut
- Varmuuskopiot
- Tietokannat ja muut tietovarannot
- Käyttö-, diagnostiikka- ja ylläpitolokitiedot

5.3 Pilvipalveluiden keräämät tiedot palveluiden käytöstä

Pilvipalvelutoimijat keräävät palveluiden käytöstä erilaista tietoa, josta osa on myös henkilötietoa. Kerättävä henkilötieto on suurimmaksi osaksi laitteeseen ja käytettyyn ohjelmistoon liittyvää tietoa. Usein tiedot sisältävät esimerkiksi laitteen IP-osoitteen tai muita tunnistetietoa käyttäjästä tai laitteesta, joten ne luokitellaan henkilötiedoksi. Niiden ei tule sisältää varsinaista asiakkaan tallentamaa tai käsittelemää tietoa eli asiakkaan omaa dataa.

Käytöstä kerättävää tietoa käsitellään usein massoina, jolloin henkilötiedot ovat pseudonymisoituja, varsinkin jos tämä massoina tapahtuva tietojen käsittely tapahtuu EU/ETA-alueen ulkopuolella, kuten esimerkiksi tietoturvapoikkeaminen etsiminen. Mikäli tällaisessa analyysissa löydetään jokin poikkeama, kuten esimerkiksi mahdollinen

salasanan murto, palautuu tieto pilvipalvelutoimittajan EU/ETA-alueen henkilölle, joka tarvittaessa pystyy selvittämään pseudonymisoidusta tiedosta alkuperäisen käyttäjän tai laitteen ja olemaan loppuasiakkaaseen yhteydessä.

Pilvipalvelutoimittajan keräämät tiedot voidaan useimmiten jaotella seuraaviin ryhmiin:

5.3.1 Diagnostiikka ja lokitiedot

Diagnostiikkaan liittyviä tietoja sekä pilvipalvelun keräämiä lokitietoja voidaan käyttää seuraaviin tarkoituksiin:

- Vianetsintä eli ongelmien ehkäiseminen, havaitseminen ja korjaaminen
- Mahdollisten haittaohjelmien torjuminen, salasanojen kalastelun havainnointi ja estäminen
- Erilaisten muiden kyberhyökkäysten ja tietoverkkorikollisuuden tunnistaminen ja niiltä suojautuminen, reagointi ja häiriöistä palautuminen.
- Palveluiden kehittäminen sekä tuottavuuden, luotettavuuden, tehokkuuden, laadun ja tietoturvan parantaminen.

5.3.2 Liiketoimintoja varten kerätyt tiedot

Liiketoimintoja varten henkilötietojen kerääminen voi liittyä seuraaviin vaihtoehtoihin riippuen käytetyistä palvelumalleista:

- Palveluiden laskutus ja tilin hallinta, kun käytön laskutus perustuu käyttäjäkohtaiseen palvelumalliin
- Liiketoiminnan simulointi; esimerkiksi ennusteet, kapasiteetin suunnittelu ja tuotestrategia
- Laajavaikutteisten petosten, kyberrikollisuuden tai kyberiskujen torjuminen
- Saavutettavuuden, yksityisyyden suojan ja energiatehokkuuden ydintoiminnan parantaminen
- Sisäinen raportointi, tilinpäätösraportointi ja muu lainsäännöllinen raportointi

5.3.3 Tukitiketteihin liittyvä henkilötieto

Tukitiketit sisältävät aina tukitiketin tekijän henkilö- ja yhteystiedot ongelmanselvityksen helpottamiseksi ja yhteydenpidon varmistamiseksi.

Tukitiketit voivat sisältää myös mahdollisia muita henkilötiedoiksi luokiteltuja tietoja ongelmatilanteeseen liittyen, kuten esimerkiksi henkilötietoa siitä käyttäjästä, jolla ongelma on, jos tukitiketin tekijä on eri henkilö.

Lähtökohtaisesti tukitikettien käsittelyssä ei kuitenkaan tulisi tarvita mitään palveluissa käsiteltyä asiakkaan dataa. Myös tukitikettejä avattaessa on huomioitava, että tiketille ei päädy tarpeetonta tietoa.

6 Kontrollit

Pilvipalveluiden toimittaja vastaa usein tietoturvallisuuskontrollien toteutuksesta palvelussaan. Palvelua käytettäessä on huomioitava, että kaikki kontrollit eivät useinkaan ole oletusarvoisesti käytössä ja kontrollien käyttöönotto ja konfigurointi on asiakkaan vastuulla.

Tietosuojan kannalta olennaisia kontrolleja pilvipalveluissa ovat muun muassa identiteetinhallinta sisältäen tunnistautumiseen liittyvät teknologiat, tiedon salaaminen ja anonymisointi, salauksen avaintenhallinta sekä riittävä valvonta ja lokitus.

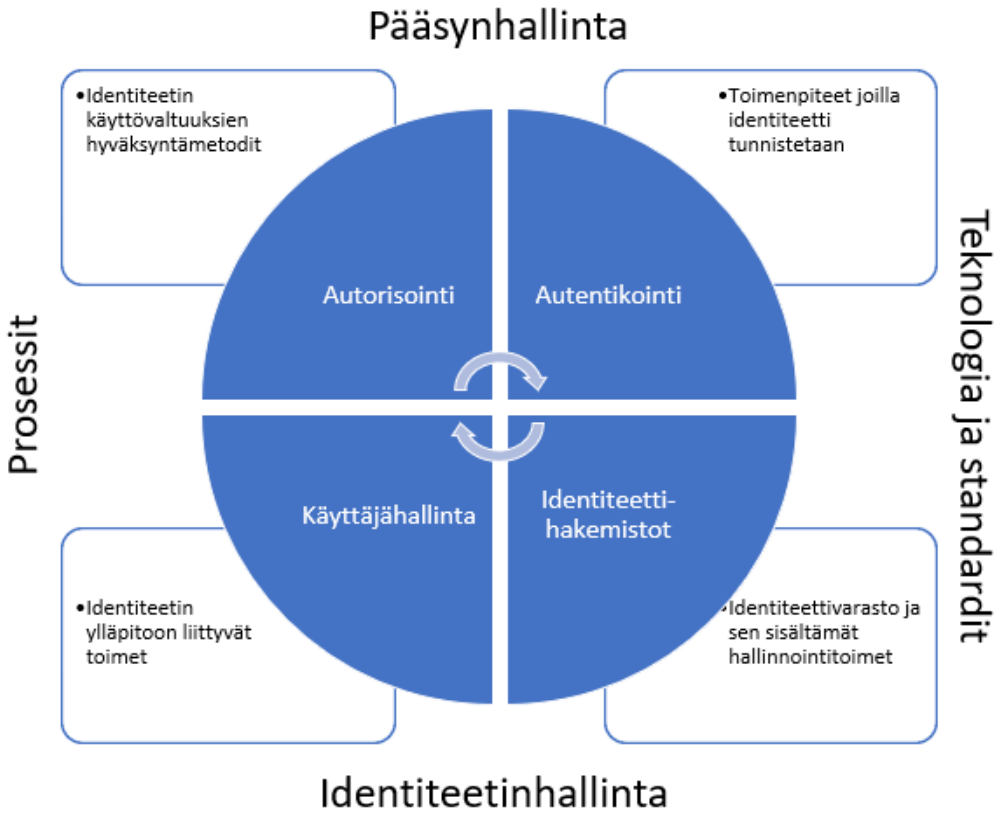
Lisätietoja ja tarkempia kriteerejä pilvipalveluissa hyödynnettävistä kontrolleista löytyy Kyberturvallisuuskeskuksen julkaisusta Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKri [1].

6.1 Identiteetinhallinta pilvipalveluissa

Identiteetinhallinnan avulla voidaan varmistua siitä, että pääsy pilvipalveluissa käsiteltäviin henkilötietoihin on rajattu vain niille henkilöille tai tahoille, joiden tehtävät vaativat kyseiseen tietoon pääsemistä.

Identiteetin ja pääsynhallinnan ytimessä on teknologian, käyttäjätiedon ja prosessien yhdistäminen siten, että käyttäjä pääsee tarvitsemaansa resurssiin yksiselitteisesti, tietoturvallisesti ja luotettavasti. Modernissa pilviympäristössä IAM (*Identity & Access Management*) on palvelu, jota pilvialustat käyttävät. Identiteettikeskeisessä palvelussa käytettävyys ja käyttömukavuus on keskeisessä osassa.

[1] Kyberturvallisuuskeskus. 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKri. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf



Identiteetin ja pääsynhallinta voidaan pilkkoa neljään alueeseen; autentikointiin, autorisointiin, käyttäjähallintaan ja identiteettihakemistoihin.

- Käyttäjähallinta ja käyttäjähakemistojen operointi on enemmän perinteistä identiteetinhallintaa.
- Identiteettihakemistoja ja autentikointia sävyttävät teknologian ja standardien oikeanlainen käyttö.
- Auktorisointi ja autentikointi ovat pääsynhallinnan peruspilarit.

Auktorisointi ja käyttäjähallinta ovat riippuvaisia organisaation prosesseista ja Master data -lähteistä – tämä alue on kaikkein organisaatiokohtaisin. Jokainen osa-alue on sidoksissa toisiinsa ja kaikkiin kuuluu erityyppiset auditointi- ja seurantatoimet.

6.1.1 Identiteettihakemistot

Identiteettihakemistoiksi luokitellaan ne kaikki tietojärjestelmät, joissa on identtiteettitietoa. Identiteettihakemistoiksi voi olla esimerkiksi;

- Aidot käyttäjähakemistot, kuten Active Directory
- Henkilödataa sisältävät (tausta)järjestelmät
- HR-järjestelmät ja palkkajärjestelmät

- Järjestelmädedikoidut käyttäjähakemistot
- Yksittäisten sovellusten omat tunnus/salasana –tyyppiset käyttäjävarastot
    - Koskee myös käyttäjähakemistoreplikointeja järjestelmän tarpeisiin
- Integraatiot, ITSM-järjestelmät ja muut alustat
    - Identiteettitietoa voi olla esimerkiksi integraatioalustan väliaikaishakemistoissa, konversiotauluissa tai tietokannoissa.

Identiteettihakemistojen, replikointien ja synkronointien välinen arkkitehtuuri- tai tietovirtakaavio on olennainen osa henkilödatan liikkuvuuden hahmottamisessa. Identiteettien leviäminen organisaation infrastruktuurissa voi olla laajaa, mutta sen kartoittaminen on tärkeää jo tietosuoja-asetuksen vaatimusten vuoksi. Jokainen identiteettihakemisto itsessään vaatii ymmärryksen teknisestä pääsystä, hallintatavoista, rajapinnoista sekä auditointimetodeista.

6.1.2 Käyttäjähallinta

Käyttäjähallintaan liittyvät kaikki ne automaattiset ja manuaaliset toimet, joilla ylläpidetään käyttäjäidentiteettiä. Identiteetinhallinnan elinkaaren kolme keskeistä asiaa on *Joiner* (tunnuksen syntyminen), *Mover* (muutos) sekä *Leaver* (poistuminen). Yksinkertaistettuna identiteetinhallinta perustuu näiden kolmen aiheuttamiin prosesseihin. Käyttäjähallinnan prosessien automatisointi on yleensä ensimmäinen vaihe, jonka jälkeen voidaan siirtyä käyttövaltuutushallinnan tehostamiseen. Tunnuksen rakentamisella, muutoksella ja poistumisella on lähes aina vaikutuksia myös käyttövaltuuksiin.

Työntekijän tunnus läpikäy elinkaarensa aikana monia muutoksia – ne ovat tyypillisesti organisaatioaseman ja tittelin vaihtumista, määräaikaisuuden jatkumista, lokaation muutoksia ja vastaavia. Tunnuksen muutokset voidaan jakaa organisatorisiin, henkilökohtaisiin ja teknisiin muutoksiin. Osa näistä on vain metadatan muutosta, osalla on laajempia vaikutuksia. Karkeasti muutokset voidaan hahmottaa kahteen ryhmään;

- Muutoksia, joihin liittyy käyttövaltuutusmuutoksia (esimerkiksi roolin tai yksikön vaihtuminen)
- Muutoksia, jotka eivät vaikuta käyttövaltuutuksiin (esimerkiksi sukunimen tai kuvan vaihtuminen)

6.1.3 Auktorisointi ja käyttövaltuudet

Autorisoinnin keskiössä on käyttövaltuudet ja niiden myöntämiskäytännöt

Käyttövaltuuksien myöntämistavat ja erityisesti käyttöoikeuksien väliaikaisuus, toimivat prosessit sekä automatiikka ovat keskeisiä kysymyksiä, koska niiden kautta avautuu pääsy tietorekistereihin.

Autorisioinnin keskeisin ongelma on käyttöoikeuksien kertyminen tunnuksille, joka juontaa juurensa usein raskaasta hallintoprosessista. Käyttöoikeuksilla itsessään pitäisi olla elinkaari ja väliaikaisten käyttöoikeuksien käyttöönottotoimissa tulisi

keskittyä myös oikeuksien nopeaan ja helppoon hyväksyntäprosessiin. Automatisointi tuo lisää turvaa, manuaalisessa hallinnassa virheiden määrä kasvaa.

6.1.4 Autentikointi / kirjautuminen

Autentikoinnissa SSO (Single-Sign-On) on keskeinen periaate. Yhdellä autentikoinnilla ja yhdellä tunnuksella hoidetaan identiteetin todennus. Autentikointi on se piste missä tunnistetaan luotettavasti käyttäjä erilaisin todennusmenetelmin.

SSO perinteisessä teknologiassa tarkoitti yhtä kirjautumistapaa organisaation sisäisessä IT-infrastruktuurissa. Pilvipalveluissa SSO mielletään organisaation tunnuksen käyttämistä kaikkiin pilven palveluihin, olivat ne kumppanien järjestelmiä tai SaaS-tyyppisiä sovelluksia. Eri osapuolten välinen luottosuhde rakennetaan federaatiolla.

Perinteinen todennusmenetelmä on tunnuksen ja salasanan yhteiskäyttö, pilvipalveluissa lähtökohta on monivaiheinen tunnistautuminen, jossa tunnusta ja salasanaa vasten todennetaan käyttäjä tekstiviestillä tai muulla vastaavalla toisella tunnistamismenetelmällä pankkikirjautumisen kaltaisesti.

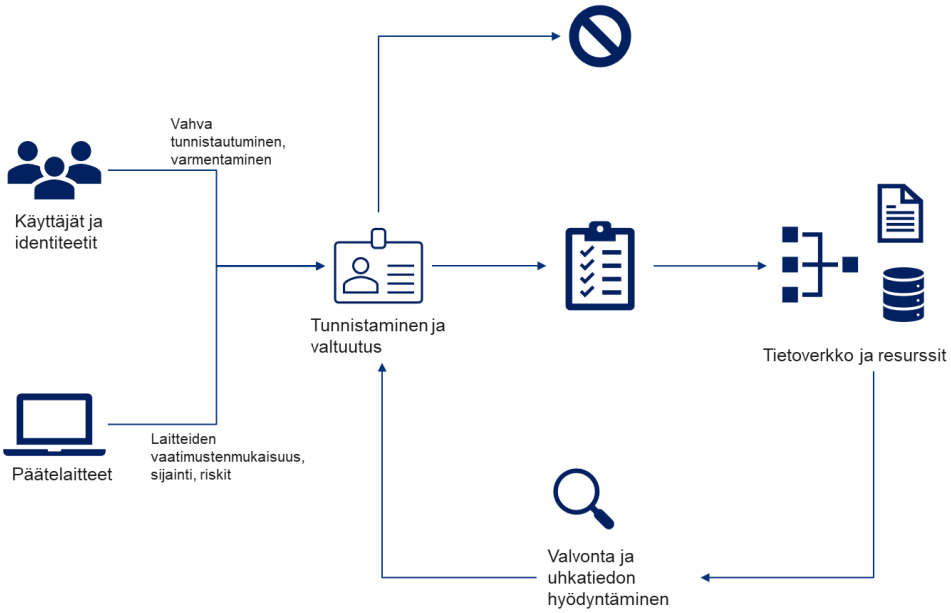
Tulevaisuuden autentikoinnin ytimenä on poistaa salasanat pois autentikointiprosessista. Niin kutsuttu *passwordless* autentikointi rakentuu biometristen sirujen tai vastaavien teknologioiden varaan ja on suoraan yhteensopiva nykyisille kaksivaiheisille todennuksille.

6.1.5 Monivaiheinen tunnistautuminen

Koska erityisesti julkiset pilvipalvelut ovat saavutettavissa julkisen verkon välityksellä lähes mistä vain, tulee käyttäjän tunnistamiseen kiinnittää erityistä huomiota. Eri pilvipalvelut tarjoavat lukuisia mahdollisuuksia käyttäjän tunnistamiseen aina päätelaitteiden vaatimustenmukaisuuden tunnistamisesta käyttäjän monivaiheiseen tunnistamiseen.

Monivaiheisen tunnistamisen käyttöönotto on suositeltava hallintakeino, sillä silloin käyttäjän tunnistaminen vahvistetaan useita eri menetelmiä käyttäen.

Esimerkki pilvipalveluissa hyödynnettävistä tunnistamismenetelmistä on kuvattu alla.



Kuva 3. Esimerkki käyttäjän tai muun identiteetin tunnistamisesta pilvipalvelussa

6.2 Salaaminen

Koska pilvipalveluita hyödynnettäessä liikennöinti tapahtuu usein julkisen verkon välityksellä, tietojen salaaminen sekä siirrettäessä, että tallennettaessa on äärimmäisen tärkeätä. Salausratkaisut ovat usein ainoita suojauksia henkilötiedon luottamuksellisuuden suojaamisessa silloin, kun palvelun käyttö tapahtuu julkisen verkon välityksellä – tavanomaisemmin suoraan internet-selaimella käytettynä.

Pilvipalvelut tarjoavat usein oletusarvoisesti mahdollisuutta salata tiedot, joita pilvipalvelussa käsitellään. Tämän osalta tulee kuitenkin kiinnittää huomiota siihen, kenellä on mahdollisuus purkaa tietojen salaus ja mikä taho hallitsee salauksessa käytettyjä avaimia.

Pilvipalvelusta riippuen päätelaitteen ja järjestelmän – tai esimerkiksi kahden eri järjestelmän - välillä siirrettävää tietoa on mahdollista suojata myös erilaisin verkkoliikenneratkaisuin, esimerkiksi hyödyntämällä päästä päähän salattua VPN-yhteyttä.

Erityisesti pilvipalveluissa salauksen roolina on usein myös eri asiakkaiden tietojen erottelu yhteiskäyttöisessä infrastruktuurissa sekä esimerkiksi tiedon tuhoamisen luotettavuuden tukeminen.

Salauksen suojausvaikutus voidaan menettää osin tai täysin tilanteissa, joissa avaintenhallinnan heikkouksia pystytään valtuuttamattomasti hyödyntämään.

Salausratkaisun salausavainten hallinnointiprosessien tuleekin olla suunniteltuja, toteutettuja ja kuvattuja/ohjeistettuja.[2]

6.3 Avaintenhallinta pilvipalveluissa

Kun tiedot salataan, salaukseen ja sen purkamiseen tarvitaan salausavain, joka on tyypillisesti merkkijono koostuen kirjaimista ja numeroista. Pilvipalveluissa salausavainten hallintaan on useita vaihtoehtoja palvelusta ja palvelumallista riippuen.

Varsinkin SaaS-palvelumallissa palveluntarjoaja vastaa usein muun ylläpidon ja tietoturvan ohella salausavainten luomisesta sekä hallinnasta ja päivittämisestä, eikä tilaajalla välttämättä ole suoraa näkyvyyttä salausavainten hallintaan. Tällaisessa tapauksessa onkin syytä tarkastella palveluntarjoajan dokumentaatiota sekä prosessia salausavainten hallinnan osalta ja arvioida sitä, mahdollistaako tarjottu avaintenhallinnan ratkaisu palveluntarjoajalle tai muulle osapuolelle pääsyn salattuun tietoon.

Osa erityisesti infrastruktuuria palveluna tarjoavista pilvipalveluista mahdollistaa myös tilaajan omien salausavaimien käytön tai jopa dedikoidun laitteen (HSM) salausavainten hallintaan. Tällöin salausavainten hallinta on helpompi varmentaa ja suunnitella tilaajan omien käytäntöjen ja vaatimusten mukaisesti sekä varmistua siitä, että salausavaimet ovat riittävän turvallisia.

6.4 Anonymisointi tai pseudonymisointi

Henkilötiedot voidaan pseudonymisoida tai anonymisoida myös pilvipalveluita käytettäessä samaan tapaan kuin muunkin tyyppisissä ratkaisuissa. Niin pitkään, kun tietojen perusteella voi tunnistaa henkilön suoraan tai tiedot voidaan palauttaa takaisin tunnistettavaan muotoon, ne ovat yhä henkilötietoja ja niihin sovelletaan tietosuoja-asetusta.

Lisätietoja pseudonymisoinnista ja anonymisoinnista tietosuojavaltuutetun toimiston verkkosivustolla[3].

6.5 Valvonta ja lokitus

Useat pilvipalvelut tarjoavat oletuksena mahdollisuuden valvoa ja lokittaa eri toimintojen käyttöä. Näitä toiminnallisuuksia onkin syytä hyödyntää, jotta tarvittaessa voidaan varmistua siitä, että vain ne henkilöt tai prosessit käsittelevät henkilötietoa, joiden tehtäviin se kuuluu ja erilaisia väärinkäytöksiä on mahdollista havaita ja selvittää myös jälkikäteen.

Riippuen pilvipalvelun toteutuksesta, valvottavia kohteita voivat olla esimerkiksi järjestelmäloki, verkkoliikenteen lokit, käyttäjälokit, muutoslokit tai tietokantojen käyttölokit. Myös pilvipalveluiden tuottamat lokitiedot on mahdollista ohjata organisaation keskitettyyn lokienhallintajärjestelmään.

[2] Kyberturvallisuuskeskus. 2020. Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKri. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf
[3] Tietosuojavaltuutetun toimisto. Pseudonymisointi ja anonymisointi. URL: https://tietosuoja.fi/pseudonymisointi-anonymisointi

On kuitenkin syytä huomioida, että myös palvelun tuottama loki voi sisältää henkilötietoja, jolloin niiden käsittelyssä huomioitava tietosuojalainsäädäntö. Kohdassa *5.3 Pilvipalveluiden keräämät tiedot palvelun käytöstä* on kuvattu tarkemmin, millaista tietoa pilvipalvelut keräävät niiden käytöstä.

Lokienhallinnasta ja erilaisista lokilähteistä lisätietoa Kyberturvallisuuskeskuksen verkkosivuilla[4].

7 Arvioinnit

7.1 Tietosuojan vaikutustenarviointi (DPIA)

Ennen pilvipalveluiden käyttöönottoa, riittävän varhaisessa vaiheessa henkilötietojen käsittelyn suunnittelussa tulee arvioida, millaisen riskin henkilötietojen käsittely muodostaa rekisteröidylle.

Tietosuojan vaikutustenarviointi tulee tehdä tietyissä tietosuojalainsäädännön määrittämissä tilanteissa[5]. Pilvipalveluiden hyödyntäminen henkilötietojen käsittelyssä täyttää usein edellytykset tietosuojan vaikutusarvioinnin tekemisestä. Pilvipalveluiden toimintalogiikat, teknologia, toimitusketjut ja muut ominaisuudet tekevät pilvipalveluista niin monimutkaisia kokonaisuuksia, ettei voi olettaa rekisteröidyn helposti hahmottavan, miten hänen henkilötietojansa käsitellään.

Vaikutustenarvioinnin tarkoituksena on auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä. Se on tarkoitettu jatkuvaksi riskien tunnistamisen ja hallitsemisen prosessiksi.

Vaikutustenarviointi on tehtävä ennen käsittelyn aloittamista ja sitä on päivitettävä tarvittaessa.

Tietosuojan vaikutustenarvioinnissa kannattaa huomioida myös ne tilanteet, joissa pilvipalveluiden hyödyntäminen poistaa tai pienentää riskejä, joita on mahdollisesti havaittu vaikutustenarvioinnissa.

Tällaisia tilanteita voivat olla esim.

- Pilvipalveluiden nopea skaalautuvuuskyky, jolloin kapasiteetin ruuhkahuippujen vaikutukset palveluntuotantoon eivät vaikuta asiakkaisiin esim. siten että palvelu hidastuu tai pysähtyy.
- Jossain tilanteissa pilvipalvelu saattaa myös sisältää tiedon suojaamiseen tai havainnointiin tarkoitettuja edistyneitä, automaatioon ja koneoppimiseen perustuvia tietoturvaratkaisuja.

[4] Kyberturvallisuuskeskus. Näin kerää ja käytät lokitietoja. URL: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja
[5] Tietosuojavaltuutetun toimisto. Tietosuojan vaikutustenarvioinnit. URL: https://tietosuoja.fi/vaikutustenarviointi

- Nopea päivitysmahdollisuus ja ketterä toiminnan kehittäminen, jolloin pilvipalvelualusta on aina ajan tasalla ja ongelmakohtiin voidaan reagoida nopeasti.

7.2 Tietojensiirron vaikutustenarviointi (TIA)

Kun henkilötietojen käsittelyyn tai sen järjestämiseen sisällytetään toimittajia ja palveluntuottajia, on aina hyvä kuvata suunnitellut tietovirrat sekä tunnistaa maantieteellisesti missä organisaation tietoja käsitellään. Tietovirtojen kuvaamista käsitellään tarkemmin kappaleessa *5.1Tietovirtojen kuvaaminen toimitusketjuissa.*

Mikäli tietovirtoja kuvatessa todetaan, että toimittajan tai alihankintaketjun kautta henkilötietoja voi siirtyä myös kolmansiin maihin, eikä EU-komissio ole tehnyt kohdemaasta henkilötietojen suojan riittävyyttä koskevaa niin kutsuttua vastaavuuspäätöstä, tulee tehdä tietojensiirron vaikutustenarviointi (*Transfer Impact Assessment, TIA*).

Tietojensiirron vaikutustenarvioinnilla tarkastellaan sitä, että tietosuojan taso seuraa henkilötietoja myös EU/ETA alueen ulkopuolella, jotta Euroopan tietosuojasääntely pätee myös pilvipalveluita hyödynnettäessä.

Tietojensiirron vaikutustenarvioinnissa arvioidaan mm.

- Kohdemaiden lainsäädäntöä ja tietosuojan riittävyyttä tapauskohtaisesti silloin kun, tietojen käsittelysopimuksessa hyödynnetään mallisopimuslausekkeita.
- Teknisten ja hallinnollisten suojatoimien riittävyyttä.
- Tietosisällön soveltuvuutta aiottuun siirtotoimeen.
- Siirtoon liittyviä ominaisuuksia, kuten esimerkiksi tietojensiirron kesto.
- Riskejä, joita kohdistuu siirrettävään tietoon ja näiden tunnistettujen riskien hallintakeinoja.

Arvioinnissa tulee huomioida koko palveluntuotantoketju mahdollisimman kattavasti. Lisäksi tietojensiirron vaikutustenarvioinnissa kannattaa myös nostaa esiin riskejä, joiden mahdollinen hallintakeino itse tietojensiirto voi olla, jos sellaisia tunnistetaan.

Tietojensiirron vaikutustenarviointi on suositeltavaa hyväksyttää organisaation johdolla ennen kuin tietojensiirtoa aloitetaan. Arviointi tulee myös käydä läpi aiotun siirtokumppanin kanssa, joka voi olla esimerkiksi pilvipalvelun toimittaja tai muu palveluntuotantoon liittyvä toimija. Palveluntuottajien tulee pystyä sitoutumaan arvioinnin sisältöön.

Huomioitavaa on, että tietojen siirtoa on myös se, mikäli henkilötietojen käsittelijällä on EU/ETA-alueen ulkopuolelta pääsy tietoihin etäyhteydellä.

Toisin sanoen, vaikka tietoa säilytettäisiin kaikissa käsittelyn vaiheissa EU/ETA-alueella, mutta toimittajalla on mahdollisuus päästä tietoon kolmansista maista, tulee tehdä tietojensiirron vaikutustenarviointi. Myös sellaisissa tapauksissa, joissa tieto on

salattu, mutta toimittajalla on mahdollisuus päästä salausavaimiin käsiksi EU/ETA-alueen ulkopuolelta, on tulkittavissa tietojen siirroksi kolmansiin maihin.

8 Sopimukset

Pilvisiirtymä vaatii uudenlaista osaamista organisaatiolta. Yksi keskeinen asia pilviympäristöjen käytössä on sopimusten hallinta. Pilviympäristö on käytännössä konesali, joka on jonkun toisen hallussa. Toinen tai toiset osapuolet tulee sitouttaa sopimuksin noudattamaan organisaation strategioita, politiikoita ja vaatimuksia.

Sopimuksissa tulee huomioida mm. riskienhallinta, vaatimustenmukaisuus, jatkuvuudenhallinta – esimerkiksi se, miten pilvipalvelusta voidaan luopua nopeasti hallitusti, mikäli siihen tulee tarve.

Tärkeä osa-alue pilvipalveluiden sopimuksissa on tietosuoja. Jo vaatimusmäärittelyvaiheessa kannattaa aloittaa tässä dokumentissa aiemmin mainittujen tietosuojan vaikutustenarvioinnin ja tietojensiirron vaikutustenarvioinnin laatiminen. Molempia dokumentteja kannattaa päivittää yhdessä pilvipalveluiden tuottajan kanssa ennen lopullisen sopimuksen tekemistä.

Pilvipalveluiden osalta sopimusneuvottelut voivat olla haastavat. Julkisen pilven käytön osalta, varsinkin jos sopimuskumppanina on kansainväliset teknologiajätit, voi organisaation vaikutusmahdollisuus sopimusten sisältöön olla rajallinen. Tästä syystä vaatimusmäärittelyllä, käsittelytoimien kuvauksilla ja vaikutustenarvioinneilla on suuri rooli, kun pilvipalveluita halutaan ottaa käyttöön.

Yksityisen pilven osalta organisaatiolla saattaa olla enemmän mahdollisuuksia neuvotella sopimusten sisällöistä pilvipalveluiden tuottajan kanssa.

Vaikutustenarvioinnin ja sen sisältämän riskiarvioinnin pohjalta tulee pystyä hahmottamaan, minkälaisia henkilötietoja pilvessä aiotaan käsitellä. Henkilötietotyypit vaikuttavat sopimusehtojen sisältöön.

Kansainvälisten teknologiajättien tuottamissa julkisissa ja jaetuissa pilvipalveluissa voi tulla tilanteita, joissa pilviympäristön toimittaja muuttaa yksipuolisesti joko ympäristöä, sopimusehtoja tai molempia. Pilvipalveluita hankkivan organisaation tulee aktiivisesti seurata pilviympäristön muutoksia sekä toimittajalta tulevia ilmoituksia.

8.1 Sopimuksissa huomioitavat asiat

Mikäli mahdollista, sopimuksissa pilvitoimittaja on sitoutettava tuottamaan palvelut EU/ETA-alueen sisältä tai alueelta, joissa on EU komission hyväksymä riittävä tietosuojan taso. Tuotettujen pilvipalveluiden osalta EU/ETA alueella tulee tuottaa mm. konesalipalvelut, tukipalvelut ja muut tietojen käsittelyyn liittyvät palvelut, jotka kattavat asiakkaan tiedot, tiedon metatiedot, tukitiedot ja lokitiedot.

Tiedon siirrot kolmansiin maihin tulee minimoida. Mikäli mahdollista, henkilötiedot tulee pseudonymisoida tai anonymisoida. Pseudonymisointiavaimet on syytä säilyttää pilviympäristön ulkopuolella, mikäli mahdollista.

Mahdolliset tietojen siirrot kolmansiin maihin tulee suorittaa sopimuksissa määritettyjä ehtoja noudattaen.

Sopimuksissa huomioitavia asioita voivat olla esim.:

- Sopimusehdoissa tulee hyödyntää EU komission vakiosopimuslausekkeita (standard contractual clauses, SCC)
    - Lisäsuojaustoimenpiteistä sovittava
- Sopimuksissa palveluntuottaja on velvoitettava kysymään rekisterinpitäjän suostumus ennen kuin tietojen siirtoa kolmansiin maihin tehdään. Näitä tapauksia voivat olla muun muassa:
    - Tekninen tuki, sellaisessa tapauksessa, jossa tuki täytyy toteuttaa kolmansista maista perustellusta syystä.
    - Kolmansien maiden lainsäädännöstä johtuva tietoihin meno kohdemaan asianmukaisen oikeusasteen päätöksen perusteella.
    - Digitaaliseen turvallisuuteen liittyvän tilanteen, kuten haittaohjelman aiheuttaman riskin torjumiseksi, selvittämiseksi, kyberrikollisen toimien selvittämiseksi ja korjaamiseksi, kriittisen päivityksen toteuttamiseksi, jolla suojataan rekisterinpitäjän tai muun tahon turvallisuutta.
- Sopimuksessa tulee kuvata tilanteet, joissa ennakkosuostumuksesta voidaan poiketa. Näiden tapausten osalta sopimuksessa tulee palveluntuottaja velvoittaa toimittamaan rekisterinpitäjälle selvitys henkilötietojen käsittelystä ja perusteet, miksi ennakkosuostumusta ei voitu kysyä ilman aiheetonta viivytystä.
- Mikäli tiedot ovat pseudonymisoitu tai salattu ja palveluntuottajalla on mahdollisuus päästä käsiksi pseudonymisointiin tai salaukseen käytettyihin avaimiin ja siten palveluntuottajalla on mahdollisuus käsitellä henkilötietoja kolmansista maista, tulee sopimuksessa huomioida, että palveluntuottajan tulee ennakolta pyytää rekisterinpitäjän suostumus pseudonymisointi- tai salausavainten käsittelyyn.
- Sopimuksessa palveluntuottaja on velvoitettava hyödyntämään etätyöpöytä- tai vastaavia tekniikoita aina kuin se on mahdollista, siten että voidaan minimoida riski, että itse tietosisältö päätyy kolmansissa maissa oleville palvelimille.
    - Mikäli etäkatselu ei ole mahdollista, tulee tiedon siirrolle kolmansiin maihin Data at rest -tilanteisiin pyytää rekisterinpitäjän suostumus, mikäli se on mahdollista.
    - Mikäli suostumuksen pyytäminen etukäteen ei ole mahdollista, palveluntuottaja tulee velvoittaa antamaan jälkikäteen ilman aiheetonta viivytystä selvitys, miksi tieto siirrettiin kolmansiin maihin edellä kuvatulla tavalla ja miksi etäyhteys ei ollut sovellettavissa.

Kansainvälisten pilvitoimittajien osalta voi tulla tilanteita, joissa toimittaja ei noudata tai ei voi noudattaa sopimuksissa sovittuja ehtoja. Tällaisia tilanteita varten on hyvä suunnitella toimenpiteitä, esim. sanktiointi tai sopimuksen purkaminen.

Edellä mainitussa tietojensiirron vaikutustenarvioinnissa tulee arvioida, missä määrin toimittaja ei noudata tai ei voi noudattaa tietojen siirrolle asetettuja ehtoja.

9 Lisätietoja

Euroopan tietosuojaneuvoston ohjeet:
https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en

VAHTI tietosuojan työkalut ja mallipohjat:
https://dvv.fi/digiturvajulkaisut

IAPP tietojensiirron vaikutustenarviointi -työkalu:
https://iapp.org/resources/article/transfer-impact-assessment-templates/