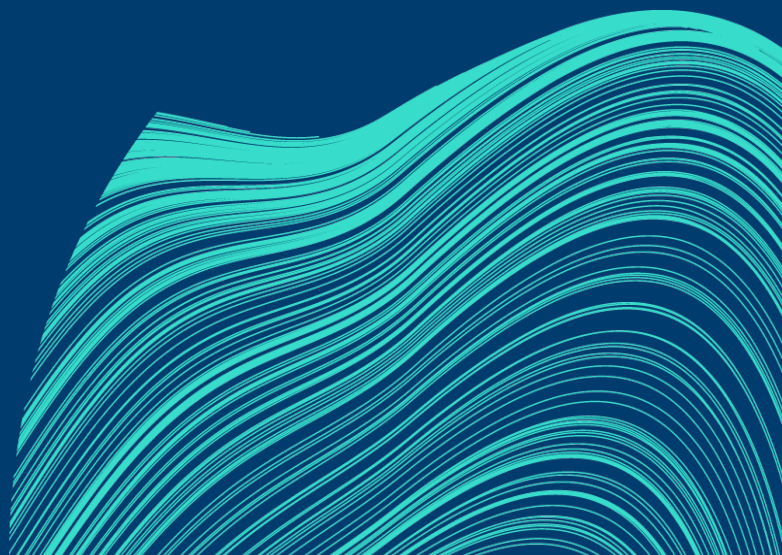
DigiFinland

Cirrus-hanke

Tapausesimerkit

VERSIO 1.0
26.6.2024



Sisällysluettelo

Johdanto

Tämä Cirrus-hankkeessa tuotettu dokumentti esittelee kaksi **kuvitteellista pilvipalveluiden tietosuojaan keskittyvää tapausesimerkkiä**. Hankkeessa aiemmin julkaistuun tekniseen esimerkkikäyttötapaukseen verrattuna näissä keskiössä on organisaation toiminnallinen näkökulma. **Tämä dokumentti ei ole ohje, vaan malli ja pohja tapausesimerkkien laatimista varten.**

Tapausesimerkki 1 kuvaa PaaS (Platform-as-a-Service) eli pilvialusta palveluna tyyppisen tilanteen. Siinä viranomainen siirtää lähtötilanteessa tämän omassa ympäristössä (on-premises) toimivan kansalaisen asiointipalvelun valitsemalleen julkipilvialustalle.

Tapausesimerkki 2 kuvaa IaaS (Infrastructure-as-a-service) eli infrastruktuuri palveluna tyyppisen tilanteen. Siinä viranomainen siirtää käytössään olevasta konesalikapasiteetista (on-premises) tietojärjestelmän palvelimet julkipilvialustalle.

Tapausesimerkeissä pääpaino on tietosuojan vaikutustenarvioinnissa (TVA, eng. Data Protection Impact Assessment, DPIA) eli henkilötietojen käsittelyyn sisältyvien riskien tunnistamisessa, arvioinnissa ja hallitsemisessa. Tässä yhteydessä hyödynnetään toimivaltaisen viranomaisen eli Tietosuojavaltuuten toimiston ohjeita ja työkaluja. Lisäksi pilvipalvelunäkökulmaa tarkastellaan Cirrus-hankkeessa tuotettujen materiaalien avulla:

- Tietosuojan vaikutustenarvioinnin ohje (TVA-ohje), 12/2021, Tietosuojavaltuutetun toimisto
- Tietosuojan vaikustenarvioinnin työkalu (TVA-työkalu), Tietosuojavaltuutetun toimisto
- Tekninen yhteenveto, 15.3.2024, Cirrus-hanke
- Esimerkkikäyttötapaus, Versio 1.0, Cirrus-hanke
- Valtionhallinnon pilvipalvelulinjaukset, Valtiovarainministeriön julkaisuja – 2023:75

Näissä kuvitteellisissa tapausesimerkeissä on pyritty löytämään sellaisia yleisiä ja yhteisiä tekijöitä, jotka ovat tyypillisiä kaikkien viranomaisten järjestelmille. Tavoitteena on kuvata esimerkinomaisesti, kuinka kuvitteellinen organisaatio voisi lähestyä IaaS- ja PaaS-tyyppisten pilvitoteutusten tietosuojaa ja tietoturvaa.

Näitä esimerkkejä ei saa sellaisenaan käyttää suoraan hankinnoissa, vaan aina tulee tehdä käyttötapauskohtainen arvio.

Tapausesimerkki 1 (PaaS)

Tämä tapausesimerkki käsittelee **kuvitteelista kansalaisen asiointipalvelua**. Tapausesimerkissä koko sovelluksen palvelualusta siirretään pilvipalvelualustalle. Toisin sanoen kyseessä on Platform as a Service (PaaS) -tyyppinen ratkaisu. Silloin koko sovelluksen kehitys- ja ajoalusta koostuu pilvipalvelualustalla tarjolla olevista komponenteista.

Kansalaisen asiointipalvelu

Tapausesimerkki käsittelee tyypillistä kansalaisen asiointipalvelua. Sen avulla kansalainen (asiakas) voi asioida sähköisesti viranomaisen kanssa. Asiakas voi palvelussa saattaa asiansa vireille, vastata täydennys- tai lisätietopyyntöihin sekä vastaanottaa asiaansa koskevat valituskelpoiset viranomaispäätökset.

Palvelun toiminnallisuus

Palvelun kansalaiskäyttö tapahtuu menemällä verkkoselaimella julkiseen osoitteeseen *asiakas.esimerkki-1.fi*.

Palvelun keskeiset toiminnot kansalaisen näkökulmasta ovat ovat:

- Rekisteröityminen
- Kirjautuminen
- Hakemuksen tekeminen, täydentäminen sekä liitteiden toimittaminen
- Päätösten tarkastelu
- Asian käsittelyyn liittyvien viestien lähettäminen ja vastaanottaminen
- Omien tietojen tarkastelu, päivittäminen sekä suostumusten hallinta ja tarkastelu

Palvelun viranomaiskäyttö tapahtuu kirjautumalla vahvasti tunnistettuna (esim. virkakortilla) vain viranomaisen sisäverkosta tavoittettavissa olevaan palveluosoitteeseen *viranomainen.esimerkki-1.fi*.

Palvelun keskeiset toiminnot viranomaisen näkökulmasta ovat:

- Vireille pantujen hakemusten työjonon hallinta
- Hakemusten käsittely
- Päätöksenteko
- Päätösasiakirjan sähköinen allekirjoittaminen
- Päätöksen sähköinen tiedoksianto
- Päätösasikirjan sähköinen jäljennos ja arkistointi

Palvelussa käsiteltävät tiedot

Kansalaisen asiointipalvelussa käsiteltävä tieto sisältää eri julkisuusluokkia.

Julkinen tieto
- Ei kirjautumista vaativa tieto
- Palvelun yleiset ohjeet ja kuvaukset

Salassapidettävä tieto
- Palvelun käyttöön liittyvä lokitieto
- Palvelun tekniseen toimintaan sekä tietoturvaan liittyvä valvontatieto

Henkilötietoja
- Asiakkaiden väestötiedot
- Asiakkaiden tahdonilmaisut
- Viranomaisen henkilökunnan henkilötiedot
- Asiakkaiden hakemuksiin liittyvä tieto

Salassa pidettäviä henkilötietoja
- Ei sisälly

Nykytila

Analyysi

Tämän tapausesimerkin lähtötilanteessa asiointipalvelu sijaitsee kokonaan viranomaisen omassa konesaliympäristössä (on-premises).

Nykytilanteen haasteena on se, että käytössä oleva palvelinympäristö (3 palvelinta) on elinkaarensa lopussa ja vaatii investointia uusiin palvelimiin. Myös osa asiointipalvelun varusohjelma-alustoista on joka tapauksessa päivitettävä tuoreempiin tuen loppuessa.

Omassa konelissa sijaitsevan asiointipalvelun suojaaminen nykyään yleisiä palvelunestohyökkäyksiä vastaan on osoittautunut myös vaikeaksi ja teleoperaattorin järeän “pesuripalvelun” kustannukset olisivat liian suuria.

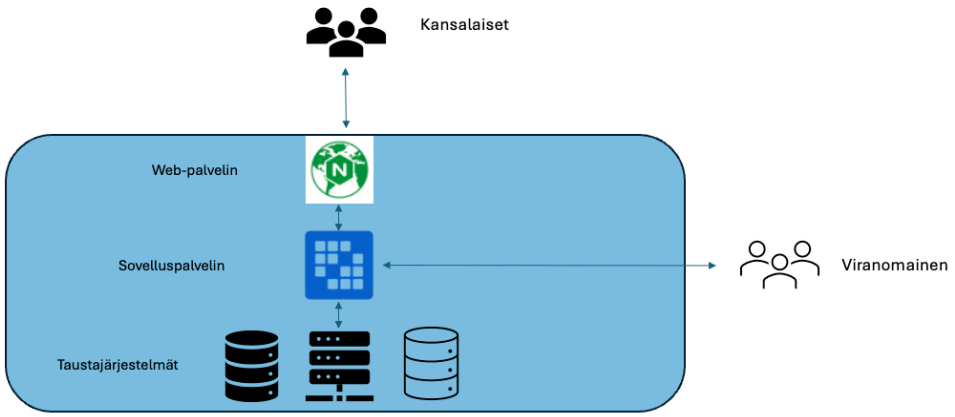
Syksyllä 2024 voimaan tulevan Kyberturvallisuuslain edellyttämä uusi tietoturvallisuuden minimitaso vaatii myös investointeja asiointipalvelun parempiin tietoturvapoikkeamien havainnointi ja reagointikyvykkyyksiin.

Nyky-ympäristössä on ollut myös ruuhkaisimpina hakemusten jättöaikoina suorituskykyhaasteita, joiden ainoaksi ratkaisuksi on tunnistettu palvelinresurssien lisääminen.

Tekninen ratkaisukuvaus

Asiointipalvelun tekninen ratkaisualusta perustuu avoimen lähdekoodin tuotteille.

- Kaikki sovelluksen vaatimat alustat on asennettu yhdelle fyysiselle Linux-palvelimelle.
- Tietokantatuotteena on PostgreSQL.
- Sovelluspalvelimena on Java-pohjainen Liferay-tuote.
- WWW-palvelimena on Nginx ja kaikki kansalaisten asiointiliikenne kulkee sen kautta.



Itse asiointisovelluksen on aikanaan kilpailutuksen perusteella viranomaiselle toteuttanut suomalainen ohjelmistotalo. Viime aikoina asiointisovellusta ei ole enää kehitetty, mutta sen aikanaan toteuttanut ohjelmistotalo tehnyt tarpeen mukaan tuntilaskettavana työnä ylläpitoa ja pienkehitystä. Ohjelmistotalo on kuitenkin ilmoittanut, että se ei enää jatka sopimusta tältä osin nykyisen sopimuskauden päättyessä vuoden 2024 lopussa.

Viranomaisella on kaikki oikeudet asiointisovellukseen ja sen jatkokehitykseen. Myös lähdenkoodi on tämän hallussa.

Tavoitetila

Analyysi

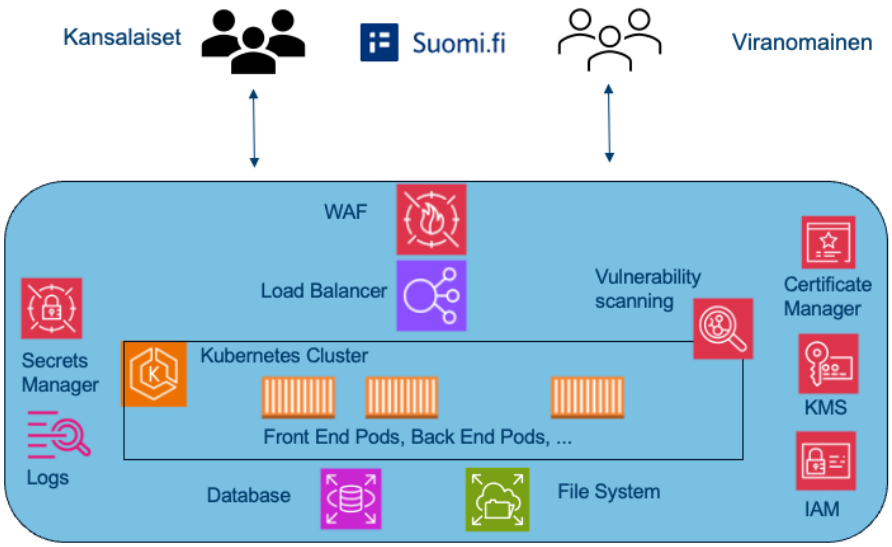
Viranomainen on selvittänyt asiointipalvelun uutta tavoitetilaa. Tässä yhteydessä on päädytty toiminnallisilla, teknisillä sekä kustannussyillä seuraavaan ratkaisuehdotukseen:

- Palvelu siirretään julkipilvialustalle PaaS-tyyppisenä toteuksena.
- Työn tekee kilpailutuksen perusteella valittu uusi integraattori, jolla on laajaa kokemusta vastaavista toteutuksista.
- Ensimmäisessä vaiheessa siirretään nykyinen sovellustoiminnallisuus sellaisenaan ja muutoksia tehdään niiltä osin kuin alustan vaihtaminen sitä edellyttää.
- Tunnistamisratkaisuna otetaan käyttöön Suomi.fi-tunnistus.
- Ensimmäisessä vaiheessa otetaan käyttöön myös suojaukset palvelunestohyökkäyksiä vastaan sekä laaja tietoturvatapahtumien lokitus.
- Palvelua varten perustetaan erilliset kehitys- (DEV), testaus- (TEST) sekä tuotantoympäristöt (PROD).

Etenemisen ehdoksi on kuitenkin astettu tietosuojalainsäädännön mukaisen tietosuojan vaikutustenarvioinnin (TVA, DPIA) tekeminen ratkaisuehdotuksesta.

Tekninen ratkaisukuvaus

Uusi asiointipalvelun arkkitehtuuri on esitetty seuraavassa kuvassa.



Olemassa olevan sovelluksen ajoalusta sekä itse sovellus on siirretään kontteihin, joiden ajamisesta, hallinnasta ja skaalaamisesta huolehtii Kubernetes. Kontit ovat:

- Liferay-ympäristö
- Nginx-ympäristö

Tietokantapalvelimena toimii pilvipalvelutoimittajan tarjoama Postgres SQL-tietokanta. Palveluun liittyvien dokumenttien yhteydessä käytetään julkipilvialustan pilvitallennustilaa. Varmenteet, avaimet ja salaisuudet hallitaan pilvipalvelualustan tarjoamilla palveluilla. Myös lokit ohjataan pilvialustan tarjoamaan palveluun.

Tarkemmin tämä tyyppisen käyttötapauksen teknistä arkkitehtuuria ja teknologioita on kuvattu aiemmin julkaistussa Cirrus-hankkeen teknisessä esimerkkikäyttötapauksessa.

Projektisuunnitelma

Tässä kuvataan lyhyesti edellä kuvattuun perustuen ne projektisuunnitelman päätason tehtävät, joilla eteneminen voisi hankintapäätöksen jälkeen tapahtua.

1. Projektin järjestäytyminen sekä käytäntöjen sopiminen
2. Tavoitetilan mukaisen pilvipalveluympäristön arkkitehtuurin ja sovellettavien teknologioiden tarkempi suunnittelu.
3. **Tietosuojan vaikutustenarvion tekeminen (TVA)**
4. Pilviympäristön perustaminen
5. Toiminnallisten, tietosuoja- ja tietoturvavaatimusten tarkempi määrittäminen
6. Asiointipalvelun “porttaus” ja testiympäristöön vieminen
7. Testaus ja hyväksymisvaihe testiympäristössä
8. Tuotantoympäristön valmistelu
9. Palvelun yliheitto tuotantoympäristöön ja käyttöönotto
10. Palvelun johtaminen, operointi ja kehittäminen

Tietosuojan vaikutustenarviointi (DPIA)

Yleinen kuvaus

Seuraavissa kohdissa käsitellään kuvitteelliseen kansalaisen asiointipalveluun liittyvää tietosuojan vaikutustenarviointia (TVA).

Arviointi tukeutuu seuraaviin lähteisiin:

- Tietosuojan vaikutustenarvioinnin ohje (TVA-ohje), 12/2021, Tietosuojavaltuutetun toimisto
- Tietosuojan vaikustenarvioinnin työkalu (TVA-työkalu), Tietosuojavaltuutetun toimisto
- Tekninen yhteenveto (Cirrus), 15.3.2024, Cirrus-hanke

Lihavoidulla tekstillä korostetaan niitä TVA:n kohtia, joita tulee tarkastella pilvipalveluiden erityispiirteiden näkökulmasta.

Kuvaus henkilötietojen käsittelystä

Tässä tapausesimerkissä oletetaan, että viranomaisella on aina lainmukainen peruste henkilötietojen käsittelyyn kuvitteellisen kansalaisen asiointipalvelun yhteydessä.

Määrittele	Vastaus / analyysi	Ohjeita ja huomautuksia
Käsittelyn tarkoitus ja tavoite	Viranomaisen lakisääteisten tehtävien hoitaminen.	TVA-ohje, s. 9
Käsittelyn kohteena olevat henkilöt (rekisteröidyt)	Asiointipalvelua käyttävät kansalaiset.	TVA-ohje, s. 9
Roolit ja vastuut (rekisterinpitäjä(t), henkilötietojen käsittelijä(t) ja yhteisrekisterinpitäjät)	Rekisterinpitäjä on asiointipalvelun omistava viranomainen. Kyseessä ei ole yhteisrekisteri. Henkilötietojen käsittelijöinä toimivat viranomaisen asiointipalvelualustasta vastaavat tahot.	**Tarkasteltava pilvipalvelun näkökulmasta.** **Henkilötietojen käsittelijöinä toimivat sekä pilvipalvelualustan toimittaja että viranomaisen lukuun tämän asiointipalveluympäristöä operoiva ja kehittävä kotimainen integraattori. Näillä molemmilla voi olla myös alikäsittelijöitä.** TVA-ohje s.9 Cirrus, luku 3 sekä kohdat 5.5 ja 5.6.
Käsiteltävät henkilötiedot	Palveluun tallennettavat kansalaisten henkilötiedot ovat: • Nimi • Osoite • Puhelinnumero, sähköpostiosoite • Henkilötunnus Palvelussa ei käsitellä erityisiä henkilötietoryhmiä.	TVA-ohje, s. 9
Mikä on käsiteltävien henkilötietojen määrä ja maantieteellinen laajuus?	Asiointipalvelussa on n. 100 000 kansalaisen tiedot. Pilvipalvelun lokaationa on EU/ETA-alueella sijaitsevat konesalit.	**Tarkasteltava pilvipalvelun näkökulmasta.** TVA-ohje, s. 9 Cirrus, kohta 2.4 (palvelukuvaukset)
Henkilötietojen elinkaari	Henkilötietojen elinkaaren perusteet määritellään kuvitteellisen tapausesimerkin viranomaista koskevassa lainsäädännössä.	TVA-ohje s.9 **TVA:n perusteella määritelty henkilötietojen elikaaren hallinta tulee huomioida yhtenä vaatimuksena palvelun tekniselle toteutukselle.**
Kuinka käsittely toteutetaan teknisesti?	Palvelu ja sinne tallennetut tiedot sijaitsevat julkipilvialustalle perustetussa viranomaisen omassa ympäristössä. Palvelua käytetään vahvasti tunnistautuneena internetin yli verkkoselaimella.	**Tarkasteltava pilvipalvelun näkökulmasta.** **Huomioi mm. seuraavat asiat ja käsitteet:** • **Cloud Adoption Framework**

		• **Arkkitehtuurisuositukset (Well-Architected Framework)** • **Landing Zone** • **CIS Benchmarks** Cirrus, kohta 2.5

Käsittelyn tarpeellisuus ja oikeasuhteisuus

Tässä tapausesimerkissä oletetaan, että henkilötietojen käsittelyn tarpeellisuus ja oikeasuhtaisuus perustuvat lakiin viranomaisen toiminnasta.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Arvio suunnitellun käsittelyn tarpeellisuudesta	Viranomaisen lakisääteisten tehtävien hoitaminen.	TVA-ohje, s. 10
Onko olemassa vähemmän henkilötietojen suojaan puuttuvia keinoja, joilla päästään samaan tavoitteeseen.	Ei ole. Henkilötietojen käsittely on tarpeen viranomaisen lakisääteisten tehtävien hoitamiseksi.	TVA-ohje, s. 10

Tietosuojaperiaatteet

Tietosuojaperiaatteet ilmenevät tietosuoja-asetuksen 5 artiklasta.

Lainmukaisuus ja kohtuullisuus

Jotta henkilötietoja voidaan käsitellä, on käsittelylle oltava lainmukainen peruste. Käsittelyperusteista säädetään TSA:n 6 artiklassa ja sitä täydentävässä tietosuojalain 4 §:ssä, sekä erityisiin henkilötietoryhmiin kuuluvien tietojen osalta TSA:n 9 artiklassa ja tietosuojalain 6 §:ssä.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Henkilötietojen käsittelyperuste	Viranomaisen lakisääteisten tehtävien hoitaminen.	TVA-ohje, s. 11
Kuinka käsittelyperusteen velvoitteet täytetään? (esim. suostumus tai oikeutettu etu)	Henkilötietojen käsittely perustuu laissa säädetyn tehtävän hoitamiseen. Rekisteröidulle annetaan palveluun kirjautuessa tieto käsittelyperusteesta sekä muut tietosuoja-asetuksen tarkoittamat tiedot.	TVA-ohje, s. 12 **TVA:n perusteella määritellyt käsittelyperusteeseen liittyvät seikat tulee huomioida yhtenä vaatimuksena palvelun tekniselle toteutukselle.**
Onko erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelylle olemassa poikkeusperustetta?	Tapausesimerkissä ei käsitellä erityisiä henkilötietoryhmiä.	TVA-ohje, s. 12
Jos käsittelet henkilötunnuksia, mitkä ovat perusteet näiden tietojen käsittelylle?	Asiointipalvelussa käsitellään henkilötunnuksia rekisteröityjen yksiselitteiseen yksilöimiseen. Tietosuojalain 29 §:n mukaisena perusteena on laissa säädetyn (viranomaisen) tehtävän suorittaminen.	TVA-ohje, s. 12
Jos käsittelet rikostuomioihin ja rikkomuksiin liittyviä tietoja, mitkä ovat perusteet näiden tietojen käsittelylle?	Tapausesimerkissä ei käsitellä rikostuomioihin ja rikkomuksiin liittyviä tietoja.	TVA-ohje, s. 12
Kuinka henkilötietojen käsittelyn ennakoitavuus ja kohtuullisuus ihmisille on huomioitu?	Henkilötietoja käsitellään vain siinä laajuudessa ja tarkoituksessa kuin on viranomaisen tehtävien hoitamiseksi välttämätöntä. Pääsy henkilötietoihin rajoitetaan viranomaisen todellisen tarpeen mukaan, ja henkilöstö perehdytetään huolella, sis. henkilötietojen käsittelyä koskeva ohjeistus. Ennakoitavuus pyritään varmistamaan antamalla rekisteröidylle ennakkoon tarvittavat tiedot heidän henkilötietojensa käsittelystä. Kohtuullisuus pyritään varmistamaan riittävällä informoinnilla, minimointiperiaatteen noudattamisella	TVA-ohje, s. 12 **TVA:n perusteella määritellyt ennakoitavuuteen ja kohtuullisuuteen liittyvät seikat tulee huomioida yhtenä vaatimuksena palvelun tekniselle toteutukselle.**

	sekä varmistamalla rekisteröidyille tietosuoja-asetuksen mukaisten oikeuksien toteutuminen.	

Läpinäkyvyys

Rekisterinpitäjän on kerrottava rekisteröidyille henkilötietojen käsittelystä selkeästi ja ymmärrettävästi. Tästä yleisestä informoinnista on joitakin poikkeuksia (ks. TSA art. 13.4 ja tietosuojalaki 33 §).

Määrittele	Vastaus	Ohjeita ja huomautuksia
Informointi rekisteröidylle: miten henkilötietojen käsittelystä kerrotaan ja missä yhteydessä?	Asiakkaat hyväksyvät sähköisen asiointipalvelun käyttöehdot ja tietosuojaselosteen kirjautuessaan järjestelmään ensimmäistä kertaa. Mikäli niihin tulee muutoksia, esitetään tieto muutoksista seuraavan kirjautumisen yhteydessä.	TVA-ohje, s. 12 **TVA:n perusteella määriteltyyn informointiin liittyvät seikat tulee huomioida yhtenä vaatimuksena palvelun tekniselle toteutukselle.**
Informoinnin yhteydessä annettavat tiedot	Informointi tapahtuu tietosuojaselosteen avulla.	TVA-ohje, s. 12 **TVA:n perusteella määriteltyyn informointiin liittyvät tulee varmistaa, että tietosuojaseloste sekä asianointipalvelun tekninen toteutus vastaavat toisiaan.**
Kuinka tiedon ymmärrettävyys eri kohderyhmille on huomioitu (esim.lapset)?	Asiointipalvelua voivat käyttää ainoastaan täysi-ikäiset kansalaiset.	TVA-ohje, s. 12 **TVA:n perusteella määriteltyyn tiedon ymmärrettävyyteen tulee varmistaa, että asianointipalvelun tekninen toteutus sallii käytön vain täysi-ikäisiltä kansalaisilta.**
Perustelut, jos informointia lykätään tai informointi jätetään tekemättä	Informointia voi lykätä tekninen häiriö tai vikatilanne, joka estää käyttäjän pääsyn verkkosivulle, joissa käyttöehdot ja tietosuojaseloste ovat luettavissa.	TVA-ohje, s. 12

Käyttötarkoitussidonnaisuus

Henkilötietojen käsittelyn tarkoitus tai tarkoitukset on suunniteltava ja määritettävä selkeästi ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tietyssä, nimenomaisessa ja laillisessa tarkoituksessa. Tämä edellyttää käyttötarkoitusten yksilöintiä ja perustelemista.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Tarkoitukset, joita varten henkilötietoja käsitellään	Tarkoituksena on viranomaisen lakisääteisten tehtävien hoitaminen.	TVA-ohje, s. 13
Millaisin teknisin ja organisatorisin keinoin varmistutaan käsittelyn pysymisestä käyttötarkoituksen mukaisena?	Henkilötietoja säilytetään viranomaisen asiointipalveluympäristössä. Se sijaitsee viranomaisen omana ympäristönä julkipilvipalvelualustalla X. Viranomaisen pääsy ympäristöön tapahtuu julkisen verkon yli (Internet) ja vaatii aina vahvaa tunnistautumista. Ympäristön toteutuksessa on huomioitu pilvipalvelutoimittajan hyvät käytännöt ja suositukset. Sen lisäksi asiointipalvelulle on tehty uhka- ja riskimallinnukset ja sovellettavat tietoturvakontrollit on valittu niiden perusteella.	TVA-ohje, s. 13 **Pilvipalvelualustalla sovellettavat tekniset suojauskeinot (tunnistaminen, suojautuminen, havainnointi, reagointi sekä palautuminen) tulee toteuttaa alustan toimittajan suositusten sekä siellä käytettävissä olevien teknisten kontrollien avulla.** Cirrus, Luku 5.
Onko mahdollinen jatkokäsittely yhteensopiva alkuperäisen käsittelytarkoituksen kanssa?	Asiointipalvelun yhteydessä ei tehdä jatkokäsittelyä. Palveluun sisältyvän ulkopuolisen tilastoinnin ja raportoinnin yhteydessä tehdään anonymisointi ja pseudonymisointi.	TVA-ohje, s. 13 **TVA:n perusteella määritellyt jatkokäsittelyn anonymisointiin ja pseudonymisointiin liittyvät periaatteet tulee yhtenä vaatimuksena palvelun tekniselle toteutukselle.**

Tietojen minimointi

Tiedon minimoinnilla tarkoitetaan rekisteröidyistä kerättävien ja käsiteltävien tietojen määrän minimointia. Henkilötietoja saa käsitellä vain silloin, kun se on tarpeellista käsittelyn tarkoituksen kannalta.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kerättävien ja säilytettävien tietojen tarpeellisuus	Kerättävät ja säilytettävät tiedot ovat tarpeen viranomaisen lakisääteisten tehtävien hoitamiseksi.	TVA-ohje, s. 14
Kuinka minimoidaan järjestelmien ja lomakkeiden keräämät tiedot?	Asiointipalvelun yhteydessä kerätään ainostaan ne tiedot, jotka ovat välttämättömiä viranomaisen lakisääteisten tehtävien hoitamiseksi.	TVA-ohje, s. 14
Kuinka tietojen pääsyoikeuksia rajataan?	Pääsyoikeuksia tietoihin rajataan palvelun käyttäjätilien ja tehtäväkohtaisten roolien perusteella. Kansalainen pääsee ainoastaan omiin tietoihinsa. Viranomainen pääsee näkemään ja käsittelemään kaikkia niitä tietoja, jotka ovat välttämättömiä asian ratkaisemikseksi. Tietojen katselusta ja muokkaamisesta jää merkintä palvelun lokitietoihin.	TVA-ohje, s. 14 **TVA:n perusteella määritellyt tietojen pääsyoikeuksiin liittyvät periaatteet tulee huomioda palvelun toteutuksessa.** **Tietojen käsittelyyn liittyvät lokitusvaatimukset tulee huomioida palvelun toteutuksessa.** **Pääsyoikeuksien hallinnan sekä lokituksen toteutuksessa tulisi hyödyntää valitun pilvipalvelualustan valmiita komponentteja.**
Onko tietoja mahdollista anonymisoida tai pseudonymisoida?	Itse asiointitapahtumaan liittyviä tietoja ei ole mahdollista anonymoisida tai pseudonymisoida. Koostesraportoinnin yhteydessä tämä on mahdollista.	TVA-ohje, s. 14 **TVA:n perusteella määritellyt jatkokäsittelyn anonymisointiin ja pseudonymisointiin liittyvät periaatteet tulee yhtenä vaatimuksena palvelun tekniselle toteutukselle.**

Säilytyksen rajoittaminen

Henkilötietoja saa säilyttää vain niin kauan kuin ne ovat tarpeen henkilötietojen käyttötarkoitusta varten. Säilytyksen rajoittaminen on yhteydessä tietojen minimoinnin periaatteeseen: henkilötietojen käsittely tulee minimoida myös ajallisesti.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Mitkä ovat eri tietojen säilytysajat (ml. varmuuskopiot ja lokitiedot)?	Tämän kuvitteellisen tapausesimerkin asiointitapahtumiin liittyvien henkilötietojen säilytysaika on määritelty laissa viideksi (5) vuodeksi asian ratkaisusta. Viranomaisen tulkinnan mukaan tämä koskee myös niiden käsittelyyn liittyviä lokitietoja. Viranomainen ottaa palvelusta säännöllisesti varmuuskopioita kuitenkin niin, että tietojen pitkäaikaissäilytyksessä toteutuu maksimissaan viiden (5) vuoden säilytysaika. Tietoturvan valvontaan liittyvien lokien osalta noudatetaan viranomaisten voimassa olevia suosituksia (tällä hetkellä 24 kk). Palvelusta tuotettavia anonymisoituja henkilötietoja sisältäviä koosteraportteja voidaan säilyttää kymmenen (10) vuotta.	TVA-ohje, s. 15 **TVA:n perusteella määriteltyjen tietojen säilytysaikojen toteutuminen tulee varmistaa toteutuksessa yhteydessä valitulla pilvipalvelualustalla.** **Osa säilysajoista tulee huomioida sovelluksen toteutuksessa. Osa voi taas perustua pilvipalvelualustaan kuuluviin säilytysaikoja kontrolloiviin toimintoihin.**
Onko tiedoille mahdollisia lakisääteisiä säilytysaikoja?	Kts. edellinen kohta	Kts. edellinen kohta

Mikä on prosessi tietojen hävittämiselle (tai anonymisoinnille)?	Palveluun liittyvät yli viisi (5) vuotta vanhat henkilötiedot hävitetään automaattisesti kerran kuukaudessa suoritettavan huoltoajon toimesta. Palvelun tekniset lokit säilytetään pilvipalvelualustan konfiguraatioissa määritellyn ajan (24 kk), jonka jälkeen alusta poistaa ne automaattisesti.	TVA-ohje, s. 15 **Yli viisi (5) vanhojen henkilötietojen automaattinen hävitys tulee huomioida palvelun teknisessä toteutuksessa.** **Pilvipalvelualustan teknisten lokien säilytysajat tulee määritellä alustan konfiguraatioissa TVA-periaatteiden mukaisiksi.**
Kuinka tietojen säilytysaikojen toteutumista seurataan?	Henkilötietojen säilytysajat on dokumentointu palvelun tietosuojaselosteeseen. Viranomainen järjestää kerran vuodessa tai suurten järjestelmämuutosten yhteydessä TVA-periaatteiden katselmoinnin. Sen yhteydessä varmistetaan myös, että palvelussa noudatetaan tietojen säilytysajoille määriteltyjä periaatteita.	TVA-ohje, s. 15 **Säilytysaikojen käytännön toteutuminen tulee varmistaa tarkastusten yhteydessä myös teknisellä tarkastuksella pilvipalvelualustalla mahdollisten toimittajan tekemien muutosten varalta.**

Täsmällisyys

Käsiteltävien henkilötietojen pitää olla käyttötarkoituksen kannalta täsmällisiä. Tiedot on päivitettävä tarvittaessa. Epätarkat ja virheelliset henkilötiedot on oikaistava tai poistettava viipymättä.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka huolehditaan käsiteltävien henkilötietojen täsmällisyydestä, päivittämisestä ja paikkansapitävyydestä?	Vahvasti tunnistautuneen kansalaisen henkilötiedot tuodaan suomi.fi-integraation kautta väestötietojärjestelmästä.	TVA-ohje, s. 15
Kuinka seurataan tietojen ajantasaisuutta?	Suomi.fi-integraation toimintaa ja virheitä seurataan palvelun valvonnan kautta. Kansalaisen on mahdollista pyytää palvelussa virheellisten tietojen (pois lukien väestötietojärjestelmästä automaattisesti tulevat tiedot) oikaisemista.	TVA-ohje, s. 15 **Toiminnallinen vaatimus: Suomi.fi-integraation toimintakunnon valvonta** **Toiminnallinen vaatimus: tietojen oikaisupyytötoiminnallisuus**

Luottamuksellisuus, eheys ja käytettävyys

Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseksi.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Millaisilla toimenpiteillä edistetään tietojen **luottamuksellisuutta**?	Luottamuksellisuutta edistetään seuraavilla hallinnollisilla ja teknisillä kontrolleilla: • Henkilötietojen käsittelijät saavat riittävän perehdytyksen • Palvelun teknisessä toteutuksessa käytetään pääsynhallintaa, tiedon salaamista sekä vahvaa tunnistamista.	TVA-ohje, s. 16 **Palvelun teknisessä toteutuksessa tulee ottaa käyttöön pilvipalvelualustan luottamuksellisuuden varmistamiseen liittyviä kontrolleja.** Cirrus, kohta 3.2
Millaisilla toimenpiteillä edistetään tietojen **eheyttä**?	Sähköisessä asiointipalvelussa asiakkaiden henkilötietoja ei koskaan syötetä käsin, vaan ne haetaan väestötietojärjestelmästä. Palvelussa asiakkaiden on mahdollista pyytää virheellisten tietojen oikaisua.	TVA-ohje, s. 16 **Palveluun tulee toteuttaa Suomi.fi-integraatio.** **Palveluun tulee toteuttaa virheellisten tietojen oikaisutoiminnallisuus.** Cirrus, kohta 3.3

Millaisilla toimenpiteillä edistetään tietojen **käytettävyyttä/saatavuutta**?	Tietojen käytettävyyttä ja saatavuutta edistetään ottamalla käyttöön sitä tukevia palvelualustan toimintoja.	TVA-ohje, s. 16 **Pilvipalvelualustalla otetaan käyttöön saatavuutta varmentamia toiminnallisuuksia (esim. saatavuusvyöhykkeet, DDoS-suojaus).** Cirrus kohta 3.4, kohta 5.10
Toimintatavat tietoturvaloukkauksiin reagoimiseen	Asiointipalvelun yhteydessä otetaan käyttöön palvelualustan tarjoamia tietoturvankontrolleja havainoinnin, reagoimisen sekä palautumisen osa-alueilta. Tietoturvan valvontaa tekevä henkilöstö omaa riittävät tiedot ja taidot. Yleisimpiin tietoturvapoikkeamiin on laadittu pelikirjat, joiden mukaista toimintaa on myös harjoiteltu. Tietoturvaloukkauksiin liittyviin toimintaprosesseihin sisältyy myös viranomaisille ilmoittaminen lain mukaisten aikarajojen puitteissa.	TVA-ohje, s. 16 **Pilvipalvelualustoilla on tarjolla useita kyvykkäitä ja kustannustehokkaita tapoja toteuttaa tietoturvaloukkausten estämistä, havainnointia sekä niihin reagointia.** Cirrus, kohta 2.7

Käsittelijät ja siirrot

Käsittelijät

Henkilötietojen käsittelijä toimii rekisterinpitäjän ohjeiden mukaisesti sen puolesta tai sen lukuun. Henkilötietojen käsittelijällä ei tarkoiteta rekisterinpitäjän alaisuudessa toimivia työntekijöitä, jotka käsittelevät henkilötietoja osana työtehtäviään.

Määrittele	Analyysi	Ohjeita ja huomautuksia
Tunnistetut henkilötietojen käsittelijät	Käsittelijöitä ovat tapausesimerkissä: • viranomaisorganisaation käyttämän palveluintegraattorin henkilöstö alihankkijoineen • valitun pilvipalvelualustan toimittajan henkilöstö alihankkijoineen.	TVA-ohje, s. 17 **Tapausesimerkin yhteydessä palveluintegraattori operoi viranomaisen pilvipalveluympäristöä myös käsittelijän roolissa.** https://tietosuoja.fi/henkilotietojen-kasittelijat **Pilvipalvelualustan osalta tulee tarkastella sen toimittajan yleistä tietosuojadokumentaatiota sekä sopimusmateriaalia (pilvipalvelun tilaus).** Cirrus, kohdat 5.5 ja 5.6
Täyttävätkö käytetyt henkilötietojen käsittelijät niille asetetut kriteerit?	Henkilötietojen käsittelyn kriteerit täytetään: • Viranomaisen ja palveluintegraattorin välisessä sopimuksessa kuvatulla tavalla. • Tekemällä riittävä analyysi pilvipalvelualustan sopimusten ja palvelun muiden tietosuojakuvausten perusteella.	TVA-ohje, s. 17 **Cirrus-teknisessä yhteenvedossa käsitellään pilvipalvelualustojen oman henkilöstön sekä alihankkijoiden pääsyä asiakkaiden tietoon. Henkilötietojen käsittelyn kriteerien toteutumista tulee arvioida näiden kohtien perusteella.** Cirrus, kohdat 5.5 ja 5.6
Sopimukset ja muu ohjeistus henkilötietojen käsittelijöille	Kts. edellinen kohta	Kts. edellinen kohta

Henkilötietojen siirrot ETA-alueen ulkopuolelle

Henkilötietoja saa TSA:n nojalla siirtää Euroopan talousalueen (ETA:n) ulkopuolelle tai kansainvälisille järjestöille vain TSA:n V luvussa määritellyin edellytyksin.

Määrittele	Vastaus	Ohjeita ja huomautuksia
ETA-alueen ulkopuoliset maat tai kansainväliset organisaatiot, joihin tietoja siirretään	Viranomaisen asiointipalveluun suoranaisesti liittyviä tietoja (sisältötiedot) ei siirretä ETA-alueen ulkopuolelle. Pilvipalvelutoimittajan palvelun käytön yhteydessä saattaa pilvipalvelualustan palveludataa siirtyä ETA-alueen ulkopuolelle niin sanottujen globaalien palveluiden osalta.	TVA-ohje, s. 18 **Asiointipalvelun teknisen toteutuksen yhteydessä tulee pakottaa sisältötiedot sijaitsemaan ainoastaan ETA-alueen konesaleihin.** **Palveludatan osalta eri pilvipalvelualustojen käytännöt vaihtelevat ja jotkin palvelut (esim. pilvi-identiteettien hallinta) saattavat olla ns. globaaleja palveluita, joiden sijaintia ei ole mahdollista pakottaa. Pilvipalvelutoimittajat ovat kuitenkin etsineet myös ratkaisuja tähän liittyvään tietosuojaongelmaan ja ajantasainen tilanne palveludatan siirtojen osalta on syytä tarkastaa heidän viimeisimmistä teknisistä kuvauksistaan.** Cirrus, kohta, 5.7, kohta 5.9
Onko Euroopan komission antanut päätöksen tietosuojan riittävyydestä koskien kyseistä maata tai organisaatiota?	Asiointipalvelun tapauksessa ETA-alueen ulkopuolisia henkilötietojen siirtoja voi tapahtua pilvipalvelutoimittajan palveludatan osalta. Sen johdosta on tehty tarkastelu EU-U.S. Data Privacy Frameworkin perusteella käytössä olevan pilvipalvelualustan osalta.	TVA-ohje, s. 18 **Riittävyyspäätöksen osalta tulee tarkastella EU-U.S. Data Privacy Frameworkin tilanne käytössä olevan pilvipalvelutoimittajan osalta.** https://www.dataprivacyframework.gov/list Cirrus, kohta 3.2
Mitkä ovat henkilötietojen siirrossa käytettävät siirtoperusteet?	Asiointipalvelun sisältötietojen osalta siirtoja ei tehdä. Palveludatan osalta siirtoperusteena on pilvipalvelualustan tekninen toiminta ns. globaalien palveluiden osalta.	TVA-ohje, s. 18 **Palveludatan siirrot ja siirtoperusteet eroavat eri pilvipalvelutoimittajien osalta ja tarkastelu tulee tehdä tapauskohtaisesti.** Cirrus, kohta 3.2
Täydentävät suojatoimet	Tapausesimerkin yhteydessä on arvioitu, että täydentäviä organisatorisia, teknisiä tai sopimuspohjaisua suojatoimia ei tarvita.	TVA-ohje, s. 18

Rekisteröidyn oikeudet

Rekisterinpitäjän on helpotettava rekisteröidyn tietosuojaoikeuksien käyttämistä sekä tarvittaessa toteutettava tietosuojaoikeudet rekisteröidyn pyynnön mukaisesti.

Menettely oikeuksien toteuttamiseksi

TSA 12 artiklassa määritellään, millä tavalla tietosuojaoikeuksia koskevat pyynnöt on käsiteltävä. Rekisterinpitäjän on varmistettava, että nämä vaatimukset pyyntöjen käsittelystä toteutuvat.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka rekisteröity tunnistetaan?	Rekisteröity tunnistetaan palvelun vahvan tunnistautumisen (Suomi.fi) avulla.	TVA-ohje, s. 20 **Palvelun toteutuksessa tulee huomioida rekisteröityjen vahva tunnistaminen (Suomi.fi -integraatio).**
Kuinka pyyntöihin vastataan (vastuuhenkilöt, määräajat, yhteydenottokanava)?	Rekisteröityjen pyynnöt ohjautuvat omaan työjonoonsa palvelussa. Sinne tulevat pyynnöt tulevat käsiteltäväksi tähän tehtävään vastuutetuille viranomaisen tehtävärooleille. Työjonon yhteydessä valvotaan määräaikojen toteutumista ja tarvittaessa pyyntöjen käsittelystä vastuullisille tahoille muodostetaan erilaisia hälytyksiä.	TVA-ohje, s. 20 **Palveluun tulee toteuttaa erillinen työjono tähän asiaan liittyvien palvelupyyntöjen suorittamiseksi.**
Kuinka oikaisusta, poistosta tai rajoituksesta ilmoitetaan tietojen vastaanottajille?	Lähtökohtaisesti informointi tapahtuu palvelun viestintätoimintojen avulla. Toissijaisena viestintäkanavana toimii Suomi.fi-palvelun viestit.	TVA-ohje, s. 20 **Palveluun tulee toteuttaa rekisteröityjen informointiin liittyvät viestitoiminnot. Tähän liittyvät viestit tulee kyetä välittämään myös kansalaisen Suomi.fi -palvelussa valitsemaan asiointitapaan (sähköinen tiedoksianto, kirje).**

Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, käsitteleekö tämä häntä koskevia henkilötietoja sekä oikeus saada jäljennös käsiteltävistä tiedoista.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka tiedot toimitetaan rekisteröidylle?	Jos rekisteröity on vielä palvelun käyttäjä, niin hän voi tilata häntä koskevien tietojen jäljennöksen asiointipalveluun tai vaihtoehtoisesti Suomi.fi-viestinä. Mikäli rekisteröity ei ole enää palvelun käyttäjä, niin hän voi kuitenkin lähestyä palvelun sivuilla olevan yhteydenottolomakkeen kautta. Kun viranomainen on tunnistanut rekisteröidyn käytössään olevilla menetelmillä, voidaan tälle lähettää palvelusta tulostettu häntä koskien tietojen jäljennys turvapostilla.	TVA-ohje, s. 21 **Palveluun tulee toteuttaa mahdollisuus hallita rekisteröityjen pyyntöjä ja tuottaa rekisteröityä koskevien tietojen jäljennös standardina asiakirjamuotona (esim. PDF).**
Mistä lähteistä tiedot kootaan?	Tiedot kootaan ainoastaan asiointipalvelun teknisestä ympäristöstä.	TVA-ohje, s. 21
Onko annettaviin tietoihin lakiin perustuvia rajoituksia?	Tapausesimerkissä ei ole mitään varsinaisia rajoituksia eli kansalainen voi aina saada jäljennöksen häntä koskevista tiedoista. Tietoturvan ja tietosuojan valvontaan liittyvissä toiminnoissa voi olla rajoituksia eikä kaikkea tietoa välttämättä voida antaa.	TVA-ohje, s. 21 **Mikäli tietoturvaan tai tietosuojaan liittyvää valvontatietoa joudutaan toimittamaan rekisteröidylle saattaa tiedon saatavutta rajoittaa pilvipalvelualustalla käytössä olevien tähän liittyvien toiminnallisuuksien ominaisuudet (yhteen henkilöön**

		liittyvät manuaalipoiminnat eivät useinkaan ole suuresta tietomassasta mahdollisia). Cirrus, kohdat 2.6 ja 2.7

Oikeus tietojen oikaisemiseen

Rekisteröidyillä on oikeus tulla arvioiduksi oikeiden ja täsmällisten tietojen perusteella. Jos tiedot ovat virheellisiä tai puutteellisia, on tiedot oikaistava.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka oikaisupyynnöt toteutetaan?	Rekisteröityjen oikaisupyynnöt ohjautuvat omaan työjonoonsa palvelussa. Sinne tulevat pyynnöt tulevat käsiteltäväksi tähän tehtävään vastuutetuille viranomaisen tehtävärooleille.	TVA-ohje, s. 22 **Palveluun tulee toteuttaa työjono tähän asiaan liittyvien palvelupyyntöjen suorittamiseksi.**
Kuinka menetellään oikaisuun liittyvissä erimielisyyksissä?	Rekisteröidyn kanssa pyritään pääsemään yhteisymmärrykseen erimielisyyden syistä ja ratkaisemaan asia siten, että rekisteröidyn oikeuksia voidaan noudattaa – ellei kyseessä ole laista johtuva syy viranomaisen toiminnalle.	TVA-ohje, s. 22 **Palvelun oikaisupyyntöjen toteutuksen yhteyteen tulee kyetä myös dokumentoimaan mahdolliset erimielisyykset sekä asian ratkaisu perusteluineen.**

Oikeus tietojen poistamiseen

Rekisteröidyllä on tietyissä tilanteissa oikeus saada rekisterinpitäjä poistamaan itseään koskevat tiedot ilman aiheetonta viivytystä.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Mikä on prosessi tietojen poistamiseen käytännössä?	Rekisteröityjen poistopyynnöt ohjautuvat omaan työjonoonsa palvelussa. Sinne tulevat pyynnöt tulevat käsiteltäväksi tähän tehtävään vastuutetuille viranomaisen tehtävärooleille.	TVA-ohje, s. 22 **Palvelun teknisessä toteutuksessa tulee huomioida tietojen poistopyynnöt sekä niihin liittyvän päätöksenteon dokumentointi.**
Arvioi tapaukohtaisesti tietojen poisto-oikeuden soveltuvuus (esim. lakisääteiset säilytysajat)	Tapausesimerkissä lakisääteinen poistoaika on viisi (5) vuotta mikäli rekisteröidyn asiassa on tehty lainvoimainen päätös. Mikäli rekisteröity keskeyttää itse keskeneräisen asiointipyyntönsä, on niiden poistaminen mahdollista rekisteröidyn erillisellä pyynnöllä.	TVA-ohje, s. 22 **Palvelun teknisessä toteutuksessa tulee huomioida tietojen poistopyyntöihin liittyvät laista tulevat säännöt.**

Oikeus rajoittaa tietojen käsittelyä

Rekisteröity voi tietyissä tilanteissa pyytää rekisterinpitäjää rajoittamaan väliaikaisesti itseään koskevien henkilötietojen käsittelyä.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka tietojen käsittelyn rajoittaminen toteutetaan käytännössä?	Rekisteröityjen käsittelyn rajoituspyynnöt ohjautuvat omaan työjonoonsa palvelussa. Sinne tulevat pyynnöt tulevat käsiteltäväksi tähän tehtävään vastuutetuille viranomaisen tehtävärooleille. Viranomainen ei tapausesimerkin yhteydessä luovuta henkilötietoja muille, joten rajoittamisesta ei tarvitse ilmoittaa ulkopuolisille tahoille.	TVA-ohje, s. 23 **Palvelun teknisessä toteutuksessa tulee huomioida rekisteröityjen rajoityspyynnöt.**

Millaisin teknisin keinoin käsittelyn rajoittaminen varmistetaan?	Viranomaisen on mahdollista kirjata asiointipalvelussa tieto rajoituksesta rekisteröidyn tietojen yhteyteen.	TVA-ohje, s. 23 **Palvelun teknisessä toteutuksessa mahdollistaa rajoitustiedon liittäminen rekisteröidyn tietojen yhteyteen.**
Kuinka rekisteröityä informoidaan rajoituksen poistamisesta?	Rekisteröity näkee tiedon häntä koskevasta voimassa olevasta rajoituksesta palvelussa.	TVA-ohje, s. 23 **Palvelun teknisessä toteutuksessa tule huomioida rekisteröidyn informoiminen rajoituksesta.**

Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on tietyissä tilanteissa oikeus saada rekisterinpitäjälle toimittamansa henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä halutessaan siirtää kyseiset tiedot toiselle rekisterinpitäjälle.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka siirto-oikeus toteutetaan käytännössä?	Tapausesimerkissä on kyseessä viranomaisen järjestelmä eikä tätä oikeutta ole.	TVA-ohje, s. 23
Kuinka siirto-oikeus soveltuu kyseessä olevaan tietojen käsittelyyn?	Tapausesimerkissä on kyseessä viranomaisen järjestelmä eikä tätä oikeutta ole.	TVA-ohje, s. 23
Mitkä ovat tekniset edellytykset tietojen siirtoon ja vastaanottoon?	Tapausesimerkissä on kyseessä viranomaisen järjestelmä eikä tätä oikeutta ole.	TVA-ohje, s. 23

Oikeus vastustaa tietojen käsittelyä

Rekisteröidyllä on tietyissä tilanteissa oikeus vastustaa henkilötietojensa käsittelyä eli pyytää, että niitä ei käsiteltäisi ollenkaan.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Mikä on prosessi vastustamisoikeuden toteuttamiseen?	Tapausesimerkissä on kyseessä viranomaisen järjestelmä eikä tätä oikeutta lähtökohtaisesti ole.	TVA-ohje, s. 24
Kuinka vastustamisoikeus soveltuu kyseessä olevaan tietojen käsittelyyn?	Tapausesimerkissä on kyseessä viranomaisen järjestelmä eikä tätä oikeutta lähtökohtaisesti ole.	TVA-ohje, s. 24

Automaattinen päätöksenteko (ml. profilointi)

Rekisteröidyllä on pääsääntöisesti oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Sisältyykö henkilötietojen käsittelyyn automaattista päätöksentekoa ja profilointia?	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen profilointia ei tehdä.	TVA-ohje, s. 24
Perusteet automaattiselle päätöksenteolle	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen profilointia ei tehdä.	TVA-ohje, s. 24
Käytössä olevat suojatoimet (ihmisen osallistuminen, päätöksen riitauttaminen)	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen profilointia ei tehdä.	TVA-ohje, s. 24
Kuinka varmistetaan tietosuojaperiaatteiden noudattaminen automaattisen päätöksenteon yhteydessä?	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen profilointia ei tehdä.	TVA-ohje, s. 24
Kuinka rekisteröidylle informoidaan automaattisesta päätöksenteosta?	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen	TVA-ohje, s. 24

	profilointia ei tehdä. Asiasta informoidaan palvelun tietosuojaselosteessa.	

Uhkien tunnistaminen

Seuraavassa kuvassa on tietosuojavaltuuten toimiston TVA-työkalun Uhat-lehdestä muokattu versio. Siihen on pilvisymbolilla merkitty ne näkökulmat, joita tulisi erityisesti tarkastella pilvipalveluiden tapauksessa. Symboli ei tarkoita välttämättä aktiivista uhkaa vaan sen tarkoituksena on korostaa analyysiä kaipaavia näkökulmia. Näitä tulee tarkastella peilaten kulloiseenkin henkilötietojen käsittelyn käyttötapaukseen.

		Tietosuojaperiaatteet							
		A	B	C	D	E	F	G	H
	Tietojen käsittelyn elinkaaren vaihe	Lainmukaisuus ja kohtuullisuus	Läpinäkyvyys	Käyttötarkoitus-sidonnaisuus	Minimointi ja säilytysaikojen rajoittaminen	Täsmällisyys	Eheys	Luottamuk-sellisuus	Käytettävyys
1	Kerääminen		☁						
2	Tallentaminen		☁		☁			☁	☁
3	Yhdistäminen		☁						
4	Käyttö ja muokkaaminen		☁		☁			☁	☁
5	Luovutus ja saataville asettaminen		☁						
6	Siirtäminen 3. maihin ja muut siirtotilanteet		☁						
7	Säilyttäminen		☁		☁			☁	☁
8	Hävittäminen		☁		☁				

Läpinäkyvyys (B1-B8)

Pilvipalveluissa käytössä oleva jaetun vastuun malli johtaa siihen, että asiakkaalla ei ole suoraa näkyvyyttä toimittajan omaan toimintaan. Kun arvioidaan tietosuojan toteutumista tietojen käsittelyn elinkaaren aikana, joudutaan tukeutumaan pilvipalvelutoimittajan dokumentaatioon. Silloin tulee tutustua esimerkiksi seuraaviin toimittajan dokumentteihin:

- Sopimusehdot
- Palvelukuvaukset
- Tekniset kuvaukset
- Ulkopuolisten arviointien (auditoinnit) tulokset
- Mahdolliset luottamukselliset salassapitositoumuksen takana olevat dokumentit
- Toimittajan tiedotteet toteutuneista häiriöistä

Tapausesimerkin tapauksessa on arvioitu, että valitun pilvipalvelualustan osalta on saatu toimittajan dokumentaatioon tutustumalla riittävä läpinäkyvyys tietosuojan toteutumiseen tietojen käsittelyn elinkaaren aikana.

TVA-ohje, s. 24, Cirrus kohta 2.3

Minimointi ja säilytysaikojen rajoittaminen (D2, D4, D7 ja D8)

Pilvipalveluissa tiedot voidaan luokitella asiakkaan omalla vastuulla olevaan sovellustietoon sekä pilvipalvelutoimittajan palvelutietoon. Näistä kummatkin voivat sisältää henkilötietoja. Tyypillisesti asiakkaalla on hyvä kontrolli oman sovellustietonsa säilytysaikoihin, mutta toimittajan palvelutiedon säilyttämisen periaatteet saattavat vaihdella suurestikin. Siksi tulee tarkastella mahdollisuudet tähän liittyvään minimointiin sekä säilytysaikojen rajoittamiseen.

Tapausesimerkissä viiden (5) vuoden säilytysaika tulee laista ja se tullaan huomioimaan sovelluksen toteutuksen yhteydessä (sovellusdata sekä sen käsittelyyn liittyvä lokitieto). Pilvipalvelun palveludatan tapauksessa sen säilytysaika palvelualustalla minimoidaan (90 pv) ja loki ohjataan mahdollisuuksien mukaan palvelun omaan lokitietovarastoon, josta se poistetaan siihen määritellyn säilytysajan puitteissa. Kuitenkin tietoturvan valvontaan liittyvää tietoa säilytetään 24 kk.

TVA-ohje, s. 24, Cirrus kohta “2.6 Lokienhallinta pilvipalveluissa”

Luottamuksellisuus (G2, G4 ja G7)
Pilvipalveluiden käyttöön liittyviä luottamuksellisuusriskejä on tarkasteltu laajasti Cirrus-hankkeen teknisessä yhteenvedossa.

TVA-ohje, s. 16, Cirrus kohta “3.2 Luottamuksellisuus”

Käytettävyys (H2, H4 ja H7)
Pilvipalveluiden käyttöön liittyviä saatavuusriskejä on tarkasteltu laajasti Cirrus-hankkeen teknisessä yhteenvedossa.

TVA-ohje, s. 16, Cirrus kohta “3.4 Saatavuus”

Riskien tunnistaminen ja arviointi

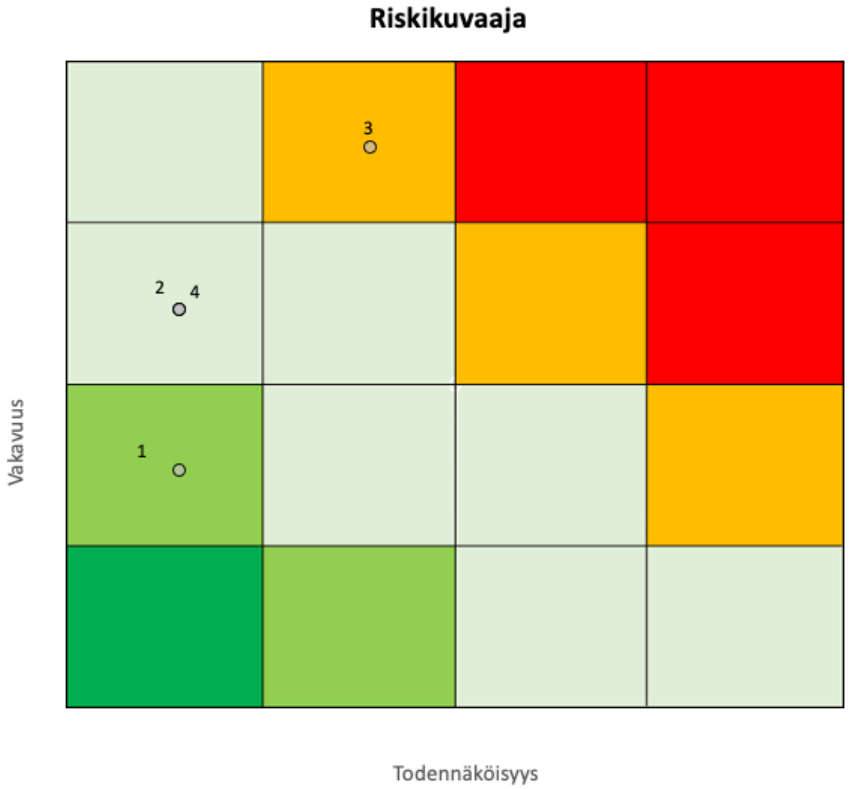
Kuvitteellisessa tapausesimerkissä on tunnistettu 4 keskeistä riskiä. Ne on esitetty seuraavassa taulukossa.

#	Uhan kuvaus	Uhan vaikutukset ja seuraukset rekisteröidylle	Vakavuus	Todennäköisyys	Riskiluku	Suojatoimenpiteet riskin pienentämiseksi	Uusi vakavuus	Uusi todennäköisyys	Uusi riskiluku
1	**Rekisteröityjen oikeudet eivät toteudu pilvipalvelussa riittävän läpinäkyvyyden puuttuessa**	Rekisteröityjen tietoja saattaa siirtyä ETA-alueen ulkopuolelle tai muihin palveluihin.	2	2	4	Riittävä pilvipalvelutoimittajan dokumentaatioon tutustuminen sekä pilven ominaispiirteiden huomioiminen	2	1	2
2	Tietojen minimointia ja säilytysaikoja ei pystytä toteuttamaan pilvipalvelussa	Rekisteröityjen informointi säilytysajoista tietosuojaselosteessa ja käytäntö eivät välttämättä kohtaa.	3	2	6	Säilytysaikavaatimusten huomioiminen toteutuksessa. Pilvipalvelyympäristön oikea konfigurointi.	3	1	3
3	Tietojen luottamuksellisuus vaarantuu tietoturvapuuttees ta johtuvan tietomurron johdosta	Rekisteröityjen tietoja saattaa vuottaa ulkopuolisille vaarantaen heidän yksityisyyttään sekä altiasten esim. identiteettivarkauksille.	4	3	12	Pilvipalvelutoimittajan suositusten noudattaminen, pilvipalvelun edistyneiden tietoturvatoimintojen käyttöönotto	4	2	8
4	Tietojen käytettävyys vaarantuu maan ulkoisten verkkoyhteyksien pitkäkestoisen häiriön johdosta	Rekisteröityjen tiedot eivät ole saavutettavissa tietoliikenteen estyessä pilvipalvelunympäristö ön.	3	2	6	Eri saatavuusalueiden hyödyntäminen.	3	1	3

Kriittisin tunnistettu riski on palveluun kohdistuva tietomurron mahdollisuus. Vaikka sen todennäköisyyttä saadaankin pienennettyä, muodostaa sen mahdollisuus tapausesimerkissä jatkuvaa seurantaa vaativan riskin. On huomattava, että tämä sama riski on yleinen riski kaikille julkisesta verkosta (internet) tavoitettavissa oleville palveluille. Riski oli olemassa siis myös tämän kuvitteellisen tapausesimerkin lähtötilanteessa.

Riskiarvion yhteenveto ja hyväksyminen

Tapausesimerkissä tehtyjen tietosuojariskien suojaustoimenpiteiden jälkeinen riskiarvio on esitetty seuraavassa kuvassa. Suurimpana tunnistettuna riskinä jää tietomurto, joka on yleinen riski kaikille internetistä tavoitettavissa oleville palveluille. Sellaisen vaikutus on aina vakava myös henkilötietojen suojan näkökulmasta.



Riskiarvion lopputuloksena on, että julkisesta verkosta tavoitettavissa olevassa palvelussa on aina tietomurron riski. Toisin sanoen jollakin ulkoisella taholla on **kyky** ja **tahto** siihen. Tietomurron vaikutukset olisivat rekisteröityjen henkilötietojen suojan kannalta tapausesimerkissä aina vakavia.

Tietomurron todennäköisyyttä ei ole mahdollista sulkea kokonaan pois. Erilaisilla hallinnollisilla ja teknisillä kontrolleilla voidaan kuitenkin pienentää sen todennäköisyyttä. Toisin sanoen voidaan vaikuttaa siihen, että ulkoisella taholla on pienempi **tilaisuus** tietomuroon.

Tapausesimerkissä tietomurron riskiä ja vaikutuksia pienennetään seuraavilla hallinnollisilla ja teknisillä kontrolleilla:

- Varmistetaan, että käytettävissä on riittävä pilvipalvelualustaan liittyvä osaaminen.
- Kaikki osapuolet noudattavat toiminnassaan riittävää “kyberhygieniaa” ja hyviä käytäntöjä.
- Pilvipalvelualustalla noudatetaan sen toimittajan hyviä käytäntöjä ja suosituksia.
- Pilvipalvelualustalla otetaan käyttöön soveltuvin osin siellä hyödynnettävissä olevat edistyneet tietoturvatoiminnallisuudet.
- Tietomurron riskiin varaudutaan etukäteen määrittelemällä niihin liittyvät toimintaprosessit ja pelikirjat. Näitä asioita myös harjoitellaan etukäteen.
- Pilvipalveluympäristön tietoturvan tilaa seurataan aktiivisesti ja mahdolliseen muuttuneeseen uhkakuvaan reagoidaan viipymättä.

Edellä mainituilla täydentävillä kontrolleilla voidaan todeta, että tapausesimerkin osalta TVA:ssa tunnistettujen riskien osalta on käytössä riittävät niitä rajoittavat kontrollit. TVA:n osalta voidaan edetä toteutukseen.

Tapausesimerkki 2 (IaaS)

Tämä tapausesimerkki käsittelee **kuvitteellista viranomaisen turvallisuusluokiteltua tietojärjestelmää**. Se liittyy viranomaisen tehtävien hoitamiseen. Järjestelmään voidaan tallentaa henkilötietojen lisäksi julkista, salassapidettävää tai turvallisuusluokan IV (TL IV) tietoa.

Tapausesimerkissä viranomaisen omassa konesalikapasiteetissa sijaitseva tietojärjestelmän palvelinalusta siirretään pilvipalvelukapasiteettiin. Toisin sanoen kyseessä on Infrastructure as a Service (IaaS) -tyyppinen ratkaisu. Silloin koko sovelluksen ajoalusta koostuu pilvipalvelualustalla sijaitsevista virtuaalipalvelimista.

Viranomaisen turvallisuusluokiteltu järjestelmä

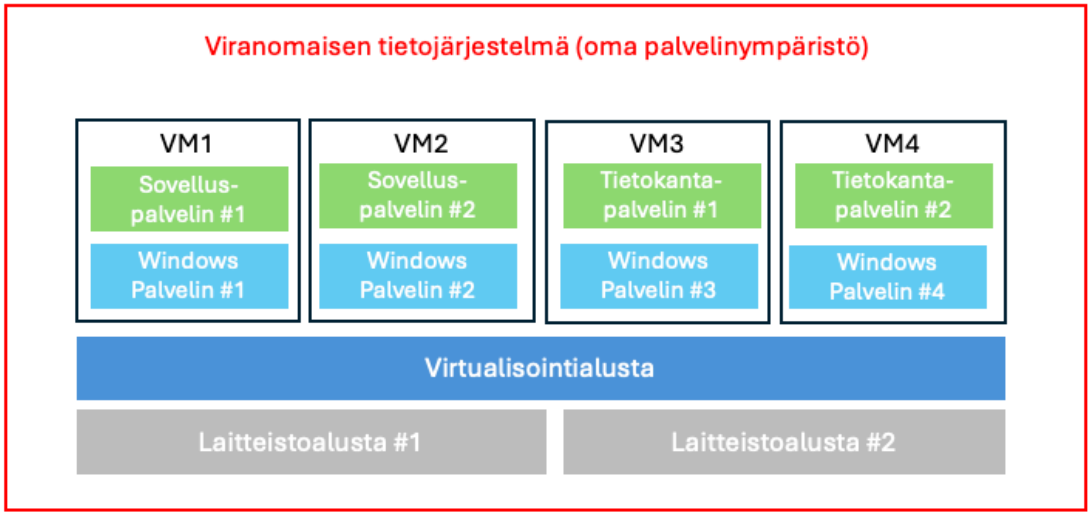
Valtiohallinnon pilvipalvelulinjaukset (Valtiovarainministeriön julkaisuja 2023:75) toteaa seuraavaa (kohdat 2.7-2.9):

- **Salassa pidettävien tietojen käsittelylle julkisissa pilvipalveluissa ei ole lähtökohtaisia lainsäädännöllisiä esteitä**, kunhan on varmistuttu siitä, että salassa pidettävät tiedot eivät päädy tahoille, joilla ei ole oikeutta käsitellä niitä. Pilvipalvelujen soveltuvuutta arvioitaessa organisaation on kuitenkin selvitettävä pilvipalvelun turvallisuuteen liittyvät riskit, erityisesti riskit, jotka liittyvät tietoaineistojen siirtämiseen tietoverkossa, tiedon tallettamiseen ja käsittelyyn pilvipalvelussa.
- **Henkilötietojen käsittelyyn** sovelletaan EU:ssa ja Euroopan talousalueella EU:n yleistä tietosuoja-asetusta (EU) 2016/679, jota täydentää Suomessa kansallinen tietosuojalaki (1050/2018). Lisäksi on olemassa asetuksen kansallisen liikkumavaran perusteella annettua erityislainsäädäntöä. Henkilötietojen käsittelyyn rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä sovelletaan henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia (1054/2018). Tietosuojasääntely ei ota suoraan kantaa pilvipalveluihin, mutta asettaa vaatimuksia henkilötiedon käsittelylle toteutustavasta riippumatta.
- **Turvallisuusluokan IV tietojen käsittelyyn pilvipalvelussa ei ole ehdotonta lainsäädännöllistä estettä**, mikäli asiakirjojen käsittely ja säilytys on toteutettu ennakollisesti vaatimusten mukaisesti ja huomioiden muun muassa edellä kuvatut lainsäädäntöjohdannaiset ja toisen valtion määräysvaltaan liittyvät riskit. Turvallisuusluokiteltavan tiedon käsittelyyn pätee, mitä edellä on todettu salassa pidettävän tiedon käsittelystä. Laissa määritellyn fyysisen turva-alueen rinnalla voidaan katsoa riittävän salauksen olevan riittävä suojauskeino tiedon oikeudettoman käytön estämiseksi pilvipalveluissa. Tiedon salaamisessa ja sen siirtämisessä pilvipalveluun tulee huomioida, että tiedon on oltava salattuna koko sen elinkaaren ajan. Kun vaatimukset tiedon salaamisesta ja eriyttämisestä koko elinkaaren ajan, mukaan lukien tietoliikenteessä, on toteutettu vaatimustenmukaisella tavalla voidaan turvallisuusluokiteltua tietoa käsitellä julkisessa pilvipalvelussa.

Kuvitteellisen tapausesimerkin tietojärjestelmä sisältää päällekkäisiä suojaustarpeita edellyttäviä tietoja. Samassa tietovarannossa on julkista tietoa, salassa pidettävää tietoa, henkilötietoa ja turvallisuusluokiteltua (TL IV) tietoa. Tapausesimerkissä tiedon suojaamisen kontrollit (tietoturvallisuus) tulee mitoittaa korkeimman TL IV -vaatimuksen mukaisesti. Henkilötietojen osalta tulee luonnollisesti arvioida myös tietosuojanäkökulma, mutta TL IV vaatimusten toteuttaminen tukee tätäkin tavoitetta.

Nykytila

Nykytilassa viranomaisen kuvitteellisen tietojärjestelmän palvelimet sijaitsevat kokonaan tämän omassa palvelinympäristössä (on-premises). Ympäristö on kahden salin virtualisoitu ja korkean käytettävyyden ratkaisu.



Konesalit ovat toimivaltaisen viranomaisen auditoimia ja palvelimien voidaan katsoa sijoittuvan laissa tarkoitetulle fyysiselle turva-alueelle. Viranomaisen järjestelmän käyttö on mahdollista ainoastaan turvallisuusluokkaan TL IV hyväksytyiltä viranomaisen työasemilta. Yksittäinen virkamies tunnistautuu vahvasti tietojärjestelmään hyödyntäen virkakorttia (Virtu-käyttäjätunnistusjärjestelmä).

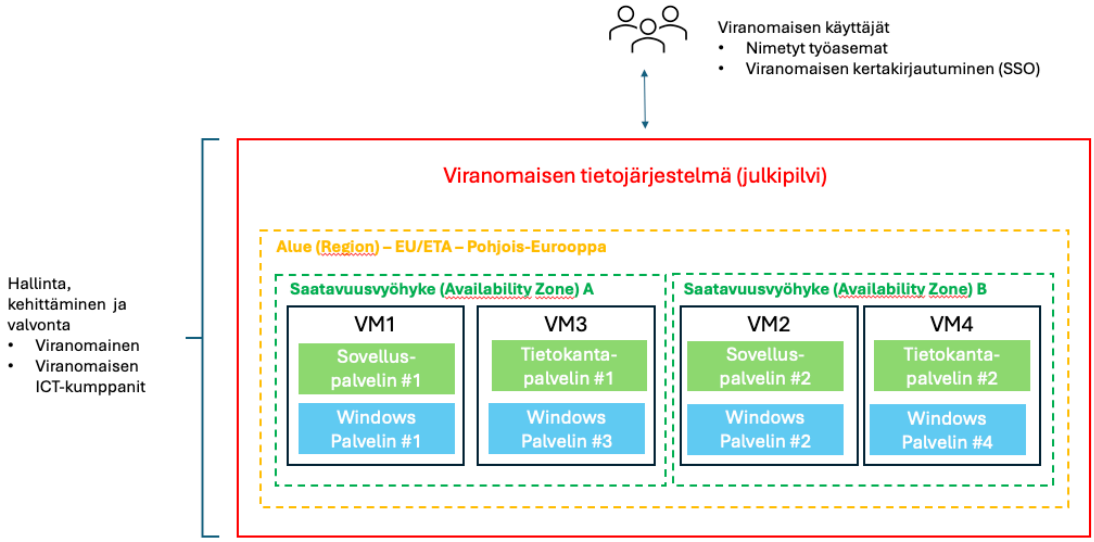
Tavoitetila

Viranomainen on päättänyt siirtää tapausesimerkin kuvitteellisen tietojärjestelmän julkiselle pilvipalvelualustalle. Tässä yhteydessä on tunnistettu seuraavat keskeiset periaatteet:

- Käytettävyyden osalta tähdätään vähintään samaan palvelutasoon kuin nykyisessä viranomaisen omassa palvelinympäristössä.
- Tunnistamisessa ja valtuuttamisessa tukeudutaan edelleen viranomaisen olemassa oleviin ratkaisuihin. Vaikka palvelu sijaitseekin julkipilvialustalla, tulee sen käytön olla edelleen mahdollista ainoastaan viranomaisen omilta TL IV -hyväksytyiltä työasemilta sekä vahvasti virkakortilla tunnistautuneena.
- Turvallisuusluokan TL IV edellyttämä fyysinen turva-alue toteutetaan pilvipalvelussa riittävän vahvalla salauksella tiedon oikeudettoman käytön estämiseksi. Keskiössä on tiedon salaaminen koko elinkaaren ajan viranomaisen itsensä hallitsemilla salausavaimilla.

Seuraavassa kuvassa on esitetty tavoitetilan ylätasoinen arkkitehtuuri. Kuvitteellisen tapausesimerkin tietojärjestelmäympäristö sijoitetaan valitun julkipilviympäristön Pohjois-Euroopassa sijaitsevalle alueelle (Region). Saatavuutta varmistetaan sijoittamalla palvelimet kahdelle eri saatavuusvyöhykkeelle (Availability Zone) alueen sisällä. Alunperin harkinnassa olleesta kahden alueen ratkaisusta päätettiin luopua siihen liittyvien suurempien kustannusten takia. Viranomaisen omassa ympäristössä sijaitsevat taustajärjestelmät (mm. viranomaisen kertakirjautuminen) uuteen pilviympäristöön virtuaaliverkkoratkaisulla (VPC, Virtual Private Cloud).

Viranomaisen itsensä sekä tämän ICT-kumppanien tekemät ylläpitotoiminnot suoritetaan erillisen vahvasti suojatun ja valvotun “hyppy-ympäristön” (Bastion Host) kautta. Pilviympäristössä otetaan käyttöön laaja tietoturvatapahtumien lokitus ja valvonta sekä haavoittuvuusskannaukset. Palvelimille asennetaan viranomaisen käytössä oleva EDR-ratkaisu sekä muut käytössä olevat sensorit. Lokit ja hälytykset ohjataan viranomaisen käytössä olevaan tietoturvavalvomoon (SOC, Security Opeations Center).



Viranomainen on tutustunut Cirrus-hankkeen tekniseen yhteenvetoon (Cirrus-hanke, Tekninen yhteenveto, Versio 1.0, 15.3.2024) ja tunnistanut seuraavat seitsemän keskeistä tähän käyttötapaukseen liittyvää tarkastelunäkökulmaa:

- Pilvipalveluiden yleiset tietoturvakäytänteet (kohta 2.5)
  - Cloud Adoption Framework, Landing Zone, Well-Architected Framework, CIS Benchmarks
- Tietojen salaus (kohdat 3.2 ja 5.1)
  - Data-in-transit, Data-at-rest
- Salausavainten hallinta (kohta 5.2)
  - Palveluntarjoajan hallinnoimat avaimet, asiakkaan hallinnoimat avaimet
- Pääsyoikeuksien hallinta (kohta 5.3)
  - Ihmiset, palvelut
- Pilvipavelun saatavuuden varmistaminen (kohdat 3.4 ja 5.10)
  - Alueet, saatavuusvyöhykkeet
- Pilvipalvelun turvallisuuden seuranta (5.11)
  - Lokitus, monitorointi
- Häiriötilanteiden hallinta (5.12)
  - Tietoturvahäiriöihin varautuminen ja reagoiminen

Projektisuunnitelma

Tässä kuvataan lyhyesti edellä kuvattuun perustuen ne projektisuunnitelman päätason tehtävät, joilla eteneminen voisi hankintapäätöksen jälkeen tapahtua.

1. Projektin järjestäytyminen sekä käytäntöjen sopiminen
2. Tavoitetilan mukaisen pilvipalveluympäristön arkkitehtuurin ja sovellettavien teknologioiden tarkempi suunnittelu
3. Turvallisuusluokan IV edellyttämien tietoturvan, tietosuojan sekä jatkuvuudenhallinnan hallintakeinojen tarkempi suunnittelu.
4. **Tietosuojan vaikutustenarvion tekeminen (TVA).**
5. **Tietoturvallisuuden arviointi viranomaisen itsearviointina, ulkoisena arviointina ja tarvittaessa arviointilaitoksen toimesta.**
6. Pilviympäristön perustaminen
7. Palvelinympäristön migraation suunnittelu
8. Palvelinympäristön siirto pilveen (“lift and shift”)
9. Palvelun johtaminen, operointi ja kehittäminen

Tietosuojan vaikutustenarviointi (DPIA)

Yleinen kuvaus

Seuraavissa kohdissa käsitellään kuvitteelliseen viranomaisen tietojärjestelmään liittyvää tietosuojan vaikutustenarviointia (TVA). Arviointi tukeutuu seuraaviin lähteisiin:

- Tietosuojan vaikutustenarvioinnin ohje (TVA-ohje), 12/2021, Tietosuojavaltuutetun toimisto
- Tietosuojan vaikustenarvioinnin työkalu (TVA-työkalu), Tietosuojavaltuutetun toimisto
- Tekninen yhteenveto (Cirrus), 15.3.2024, Cirrus-hanke
- Esimerkkikäyttötapaus, Versio 1.0, Cirrus-hanke

Lihavoidulla tekstillä korostetaan niitä TVA:n kohtia, joita tulee tarkastella pilvipalveluiden erityispiirteiden näkökulmasta.

Kuvaus henkilötietojen käsittelystä

Tässä tapausesimerkissä oletetaan, että viranomaisella on aina lainmukainen peruste henkilötietojen käsittelyyn asiointipalvelun yhteydessä.

Määrittele	Vastaus / analyysi	Ohjeita ja huomautuksia
Käsittelyn tarkoitus ja tavoite	Viranomaisen lakisääteisten tehtävien hoitaminen.	TVA-ohje, s. 9
Käsittelyn kohteena olevat henkilöt (rekisteröidyt)	Viranomaisen omat henkilöt, jotka ovat tietojärjestelmän käyttäjiä.	TVA-ohje, s. 9
Roolit ja vastuut (rekisterinpitäjä(t), henkilötietojen käsittelijä(t) ja yhteisrekisterinpitäjät)	Rekisterinpitäjä on tietojärjestelmän omistava viranomainen. Kyseessä ei ole yhteisrekisteri. Henkilötietojen käsittelijöinä toimivat viranomaisen tietojärjestelmän ylläpidosta vastaavat tahot.	**Tarkasteltava pilvipalvelun näkökulmasta.** **Henkilötietojen käsittelijöinä toimivat sekä pilvipalvelualustan toimittaja että viranomaisen lukuun tämän tietojärjestelmäympäristöä operoiva ja kehittävä kotimainen integraattori. Näillä molemmilla voi olla myös alikäsittelijöitä.** TVA-ohje s.9 Cirrus, luku 3 sekä kohdat 5.5 ja 5.6.
Käsiteltävät henkilötiedot	Tietojärjestelmää käyttävien viranomaisen henkilöiden käyttäjätiedot. Palvelussa ei käsitellä erityisiä henkilötietoryhmiä.	TVA-ohje, s. 9
Mikä on käsiteltävien henkilötietojen määrä ja maantieteellinen laajuus?	Tietojärjestelmässä on viranomaisen n. 1000 käyttäjän käyttäjätiedot. Kaikki viranomaisen käyttäjät (rekisteröidyt) ovat Suomen kansalaisia.	TVA-ohje, s. 9
Henkilötietojen elinkaari	Viranomaisen käyttäjien henkilötiedot ovat tallennettuna palveluun näiden virkasuhteen keston ajan.	TVA-ohje s.9 **TVA:n perusteella määritelty henkilötietojen elikaaren hallinta tulee huomioida yhtenä vaatimuksena palvelun tekniselle toteutukselle.**
Kuinka käsittely toteutetaan teknisesti?	Tietojärjestelmä ja sinne tallennetut tiedot sijaitsevat julkipilvialustalle perustetussa viranomaisen omassa ympäristössä. Tietojärjestelmää käytetään vahvasti tunnistautuneena internetin yli verkkoselaimella.	**Tarkasteltava pilvipalvelun näkökulmasta.** **Huomioi mm. seuraavat asiat ja käsitteet:** • **Cloud Adoption Framework** • **Arkkitehtuurisuositukset (Well-Architected Framework)** • **Landing Zone** • **CIS Benchmarks** Cirrus, kohta 2.5

Käsittelyn tarpeellisuus ja oikeasuhteisuus

Tässä tapausesimerkissä oletetaan, että henkilötietojen käsittelyn tarpeellisuus ja oikeasuhtaisuus perustuvat lakiin viranomaisen toiminnasta.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Arvio suunnitellun käsittelyn tarpeellisuudesta	Viranomaisen lakisääteisten tehtävien hoitaminen.	TVA-ohje, s. 10
Onko olemassa vähemmän henkilötietojen suojaan puuttuvia keinoja, joilla päästään samaan tavoitteeseen.	Ei ole. Henkilötietojen käsittely on tarpeen viranomaisen lakisääteisten tehtävien hoitamiseksi.	TVA-ohje, s. 10

Tietosuojaperiaatteet

Tietosuojaperiaatteet ilmenevät tietosuoja-asetuksen 5 artiklasta.

Lainmukaisuus ja kohtuullisuus

Jotta henkilötietoja voidaan käsitellä, on käsittelylle oltava lainmukainen peruste. Käsittelyperusteista säädetään TSA:n 6 artiklassa ja sitä täydentävässä tietosuojalain 4 §:ssä, sekä erityisiin henkilötietoryhmiin kuuluvien tietojen osalta TSA:n 9 artiklassa ja tietosuojalain 6 §:ssä.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Henkilötietojen käsittelyperuste	Viranomaisen lakisääteisten tehtävien hoitaminen.	TVA-ohje, s. 11
Kuinka käsittelyperusteen velvoitteet täytetään? (esim. suostumus tai oikeutettu etu)	Henkilötietojen käsittely perustuu laissa säädetyn tehtävän hoitamiseen. Rekisteröidulle esitetään tietojärjestelmään ensimmäistä kertaa kirjautuessa tai muutosten jälkeen tieto käsittelyperusteesta sekä muut tietosuoja-asetuksen tarkoittamat tiedot.	TVA-ohje, s. 12 **TVA:n perusteella määritellyt käsittelyperusteeseen liittyvät seikat tulee huomioida yhtenä vaatimuksena palvelun tekniselle toteutukselle.**
Onko erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelylle olemassa poikkeusperustetta?	Tapausesimerkissä ei käsitellä erityisiä henkilötietoryhmiä.	TVA-ohje, s. 12
Jos käsittelet henkilötunnuksia, mitkä ovat perusteet näiden tietojen käsittelylle?	Viranomaisen tietojärjestelmään ei tallenneta henkilötunnuksia vaan yksittäisen virkamiehen yksilöimiseen käytetään sähköistä asiointitunnusta (SATU).	TVA-ohje, s. 12
Jos käsittelet rikostuomioihin ja rikkomuksiin liittyviä tietoja, mitkä ovat perusteet näiden tietojen käsittelylle?	Tapausesimerkissä ei käsitellä rikostuomioihin ja rikkomuksiin liittyviä tietoja.	TVA-ohje, s. 12
Kuinka henkilötietojen käsittelyn ennakoitavuus ja kohtuullisuus ihmisille on huomioitu?	Henkilötietoja käsitellään vain siinä laajuudessa ja tarkoituksessa kuin on viranomaisen tehtävien hoitamiseksi välttämätöntä. Ennakoitavuus pyritään varmistamaan antamalla rekisteröidylle ennakkoon tarvittavat tiedot heidän henkilötietojensa käsittelystä. Kohtuullisuus pyritään varmistamaan riittävällä informoinnilla, minimointiperiaatteen noudattamisella sekä varmistamalla rekisteröidyille tietosuoja-asetuksen mukaisten oikeuksien toteutuminen.	TVA-ohje, s. 12 **TVA:n perusteella määritellyt ennakoitavuuteen ja kohtuullisuuteen liittyvät seikat tulee huomioida yhtenä vaatimuksena palvelun tekniselle toteutukselle.**

Läpinäkyvyys

Rekisterinpitäjän on kerrottava rekisteröidyille henkilötietojen käsittelystä selkeästi ja ymmärrettävästi. Tästä yleisestä informoinnista on joitakin poikkeuksia (ks. TSA art. 13.4 ja tietosuojalaki 33 §).

Määrittele	Vastaus	Ohjeita ja huomautuksia
Informointi rekisteröidylle: miten henkilötietojen käsittelystä kerrotaan ja missä yhteydessä?	Virkamiehet hyväksyvät tietojärjestelmän käyttöehdot ja tietosuojaselosteen kirjautuessaan järjestelmään ensimmäistä kertaa. Mikäli niihin tulee muutoksia, esitetään tieto muutoksista seuraavan kirjautumisen yhteydessä.	TVA-ohje, s. 12 **TVA:n perusteella määriteltyyn informointiin liittyvät seikat tulee huomioida yhtenä vaatimuksena palvelun tekniselle toteutukselle.**
Informoinnin yhteydessä annettavat tiedot	Informointi tapahtuu tietosuojaselosteen avulla.	TVA-ohje, s. 12 **TVA:n perusteella määriteltyyn informointiin liittyvät tulee varmistaa, että tietosuojaseloste sekä asianointipalvelun tekninen toteutus vastaavat toisiaan.**
Kuinka tiedon ymmärrettävyys eri kohderyhmille on huomioitu (esim.lapset)?	Tietojärjestelmää voivat käyttää ainoastaan viranomaisorganisaation palveluksessa olevat viranhaltijat.	TVA-ohje, s. 12
Perustelut, jos informointia lykätään tai informointi jätetään tekemättä	Informointia voi lykätä tekninen häiriö tai vikatilanne, joka estää käyttäjän pääsyn verkkosivulle, joissa käyttöehdot ja tietosuojaseloste ovat luettavissa.	TVA-ohje, s. 12

Käyttötarkoitussidonnaisuus

Henkilötietojen käsittelyn tarkoitus tai tarkoitukset on suunniteltava ja määritettävä selkeästi ennen käsittelyn aloittamista. Henkilötietoja saa kerätä vain tietyssä, nimenomaisessa ja laillisessa tarkoituksessa. Tämä edellyttää käyttötarkoitusten yksilöintiä ja perustelemista.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Tarkoitukset, joita varten henkilötietoja käsitellään	Tarkoituksena on viranomaisen lakisääteisten tehtävien hoitaminen.	TVA-ohje, s. 13
Millaisin teknisin ja organisatorisin keinoin varmistutaan käsittelyn pysymisestä käyttötarkoituksen mukaisena?	Henkilötietoja säilytetään viranomaisen tietojärjestelmäympäristössä. Se sijaitsee viranomaisen omana ympäristönä julkipilvipalvelualustalla X. Viranomaisen pääsy ympäristöön tapahtuu verkkoselaimella julkisen verkon yli (Internet) ja vaatii aina vahvaa tunnistautumista. Ympäristön toteutuksessa on huomioitu pilvipalvelutoimittajan hyvät käytännöt ja suositukset. Sen lisäksi tietojärjestelmäalustalle on tehty uhka- ja riskimallinnukset ja sovellettavat tietoturvakontrollit on valittu niiden perusteella. Tietojärjestelmäalustalle tehdään vähintään 2 vuoden välein ulkoinen tietoturva-auditointi.	TVA-ohje, s. 13 Cirrus, Luku 5.
Onko mahdollinen jatkokäsittely yhteensopiva alkuperäisen käsittelytarkoituksen kanssa?	Tietojärjestelmän käytön yhteydessä ei tehdä jatkokäsittelyä.	TVA-ohje, s. 13

Tietojen minimointi

Tiedon minimoinnilla tarkoitetaan rekisteröidyistä kerättävien ja käsiteltävien tietojen määrän minimointia. Henkilötietoja saa käsitellä vain silloin, kun se on tarpeellista käsittelyn tarkoituksen kannalta.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kerättävien ja säilytettävien tietojen tarpeellisuus	Kerättävät ja säilytettävät tiedot ovat tarpeen viranomaisen lakisääteisten tehtävien hoitamiseksi.	TVA-ohje, s. 14
Kuinka minimoidaan järjestelmien ja lomakkeiden keräämät tiedot?	Asiointipalvelun yhteydessä kerätään ainostaan ne tiedot, jotka ovat välttämättömiä viranomaisen lakisääteisten tehtävien hoitamiseksi.	TVA-ohje, s. 14
Kuinka tietojen pääsyoikeuksia rajataan?	Pääsyoikeuksia tietoihin rajataan palvelun käyttäjätilien ja tehtäväkohtaisten roolien perusteella. Viranomaisen käyttäjä pääsee ainoastaan omiin käyttäjätietoihinsa. Käyttäjätietojen katselusta ja muokkaamisesta jää merkintä tietojärjestelmän lokitietoihin.	TVA-ohje, s. 14 **TVA:n perusteella määritellyt tietojen pääsyoikeuksiin liittyvät periaatteet tulee huomioda tietojärjestelmän toteutuksessa.** **Tietojen käsittelyyn liittyvät lokitusvaatimukset tulee huomioida tietojärjestelmän toteutuksessa.** **Pääsyoikeuksien hallinnan sekä lokituksen toteutuksessa tulisi hyödyntää valitun pilvipalvelualustan valmiita komponentteja.**
Onko tietoja mahdollista anonymisoida tai pseudonymisoida?	Henkilötietoja (viranomaisen käyttäjätiedot) ei ole mahdollista anonymoisida tai pseudonymisoida.	TVA-ohje, s. 14

Säilytyksen rajoittaminen

Henkilötietoja saa säilyttää vain niin kauan kuin ne ovat tarpeen henkilötietojen käyttötarkoitusta varten. Säilytyksen rajoittaminen on yhteydessä tietojen minimoinnin periaatteeseen: henkilötietojen käsittely tulee minimoida myös ajallisesti.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Mitkä ovat eri tietojen säilytysajat (ml. varmuuskopiot ja lokitiedot)?	Tämän kuvitteellisen tapausesimerkin viranomaisen tietojärjestelmän henkilötietojen (käyttäjätiedot) säilytysaika on sidottu käyttäjän virkasuhteen kestoon. Viranomaisen käyttäjiin liittyviä lokitetoja säilytetään kuitenkin pidempään viranomaisen oman lokipolitiikan mukaisesti. Viranomainen ottaa palvelusta säännöllisesti varmuuskopioita kuitenkin niin, että tietojen pitkäaikaissäilytyksessä toteutuu maksimissaan viiden (5) vuoden säilytysaika. Tietoturvan valvontaan liittyvien lokien osalta noudatetaan viranomaisten voimassa olevia suosituksia (tällä hetkellä 24 kk).	TVA-ohje, s. 15 **TVA:n perusteella määriteltyjen tietojen säilytysaikojen toteutuminen tulee varmistaa toteutuksessa yhteydessä valitulla pilvipalvelualustalla.** **Osa säilysajoista tulee huomioida tietojärjestelmän toteutuksessa. Osa voi taas perustua pilvipalvelualustaan kuuluviin säilytysaikoja kontrolloiviin toimintoihin.**
Onko tiedoille mahdollisia lakisääteisiä säilytysaikoja?	Kts. edellinen kohta	Kts. edellinen kohta
Mikä on prosessi tietojen hävittämiselle (tai anonymisoinnille)?	Virkamiehen henkilötiedot (käyttäjätiedot) poistetaan kuukauden kuluessa tämän virkasuhteen päättymisestä. Palvelun tekniset lokit säilytetään pilvipalvelualustan konfiguraatioissa	TVA-ohje, s. 15 **Käyttäjätietojen poisto tulee huomioida palvelun teknisessä toteutuksessa.**

	määritellyn ajan (24 kk), jonka jälkeen alusta poistaa ne automaattisesti.	**Pilvipalvelualustan teknisten lokien säilytysajat tulee määritellä alustan konfiguraatioissa TVA-periaatteiden mukaisiksi.**
Kuinka tietojen säilytysaikojen toteutumista seurataan?	Henkilötietojen säilytysajat on dokumentointu palvelun tietosuojaselosteeseen. Viranomainen järjestää kerran vuodessa tai suurten järjestelmämuutosten yhteydessä TVA-periaatteiden katselmoinnin. Sen yhteydessä varmistetaan myös, että tietojärjestelmässä noudatetaan tietojen säilytysajoille määriteltyjä periaatteita.	TVA-ohje, s. 15 **Säilytysaikojen käytännön toteutuminen tulee varmistaa tarkastusten yhteydessä myös teknisellä tarkastuksella pilvipalvelualustalla mahdollisten toimittajan tekemien muutosten varalta.**

Täsmällisyys

Käsiteltävien henkilötietojen pitää olla käyttötarkoituksen kannalta täsmällisiä. Tiedot on päivitettävä tarvittaessa. Epätarkat ja virheelliset henkilötiedot on oikaistava tai poistettava viipymättä.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka huolehditaan käsiteltävien henkilötietojen täsmällisyydestä, päivittämisestä ja paikkansapitävyydestä?	Vahvasti tunnistautuneen virkamiehen käyttäjätiedot tuotaan VIRTU-käyttäjätunnistusjärjestelmästä.	TVA-ohje, s. 15 **Tietojärjestelmän teknisessä toteutuksessa tulee toteuttaa VIRTU-integraatio.**
Kuinka seurataan tietojen ajantasaisuutta?	VIRTU-integraation toimintaa ja virheitä seurataan palvelun valvonnan kautta.	TVA-ohje, s. 15 **VIRTU-integraation toiminnalle tulee järjestää riittävä seuranta (lokitus).**

Luottamuksellisuus, eheys ja käytettävyys

Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet henkilötietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaamiseksi.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Millaisilla toimenpiteillä edistetään tietojen **luottamuksellisuutta**?	Luottamuksellisuutta edistetään seuraavilla hallinnollisilla ja teknisillä kontrolleilla: • Tietojärjestelmän teknisessä toteutuksessa käytetään pääsynhallintaa, tiedon salaamista sekä vahvaa tunnistamista. • Valitut luottamuksellisuutta suojaavat kontrollit mitoitetaan suojaustason TL IV mukaiseksi (Julkri).	TVA-ohje, s. 16 **Palvelun teknisessä toteutuksessa tulee ottaa käyttöön pilvipalvelualustan luottamuksellisuuden varmistamiseen liittyviä kontrolleja suojaustason IV vaatimusten mukaisesti.** Cirrus, kohta 3.2
Millaisilla toimenpiteillä edistetään tietojen **eheyttä**?	Tietojärjestelmässä käyttäjien henkilötietoja ei koskaan syötetä käsin, vaan ne haetaan VIRTU-tunnistamisesta.	TVA-ohje, s. 16 **Palveluun tulee toteuttaa VIRTU-integraatio.** Cirrus, kohta 3.3
Millaisilla toimenpiteillä edistetään tietojen **käytettävyyttä/saatavuutta**?	Tietojen käytettävyyttä ja saatavuutta edistetään ottamalla käyttöön sitä tukevia palvelualustan toimintoja.	TVA-ohje, s. 16 **Pilvipalvelualustalla otetaan käyttöön saatavuutta varmentamia toiminnallisuuksia (esim. saatavuusvyöhykkeet, DDoS-suojaus).**

		Cirrus kohta 3.4, kohta 5.10
Toimintatavat tietoturvaloukkauksiin reagoimiseen	Tietojärjestelmän pilvitoteutuksen yhteydessä otetaan käyttöön palvelualustan tarjoamia tietoturvankontrolleja havainoinnin, reagoimisen sekä palautumisen osa-alueilta. Tietoturvan valvontaa tekevä henkilöstö omaa riittävät tiedot ja taidot. Yleisimpiin tietoturvapoikkeamiin on laadittu pelikirjat, joiden mukaista toimintaa on myös harjoiteltu.	TVA-ohje, s. 16 **Pilvipalvelualustoilla on tarjolla useita kyvykkäitä ja kustannustehokkaita tapoja toteuttaa tietoturvaloukkausten estämistä, havainnointia sekä niihin reagointia.** Cirrus, kohta 2.7

Käsittelijät ja siirrot

Käsittelijät

Henkilötietojen käsittelijä toimii rekisterinpitäjän ohjeiden mukaisesti sen puolesta tai sen lukuun. Henkilötietojen käsittelijällä ei tarkoiteta rekisterinpitäjän alaisuudessa toimivia työntekijöitä, jotka käsittelevät henkilötietoja osana työtehtäviään.

Määrittele	Analyysi	Ohjeita ja huomautuksia
Tunnistetut henkilötietojen käsittelijät	Käsittelijöitä ovat tapausesimerkissä: • viranomaisorganisaation käyttämän palveluintegraattorin henkilöstö alihankkijoineen • valitun pilvipalvelualustan toimittajan henkilöstö alihankkijoineen.	TVA-ohje, s. 17 **Tapausesimerkin yhteydessä palveluintegraattori operoi viranomaisen pilvipalveluympäristöä myös käsittelijän roolissa.** https://tietosuoja.fi/henkilotietojen-kasittelijat **Pilvipalvelualustan osalta tulee tarkastella sen toimittajan yleistä tietosuojadokumentaatiota sekä sopimusmateriaalia (pilvipalvelun tilaus).** Cirrus, kohdat 5.5 ja 5.6
Täyttävätkö käytetyt henkilötietojen käsittelijät niille asetetut kriteerit?	Henkilötietojen käsittelyn kriteerit täytetään: • Viranomaisen ja palveluintegraattorin välisessä sopimuksessa kuvatulla tavalla. • Tekemällä riittävä analyysi pilvipalvelualustan sopimusten ja palvelun muiden tietosuojakuvausten perusteella.	TVA-ohje, s. 17 **Cirrus-teknisessä yhteenvedossa käsitellään pilvipalvelualustojen oman henkilöstön sekä alihankkijoiden pääsyä asiakkaiden tietoon. Henkilötietojen käsittelyn kriteerien toteutumista tulee arvioida näiden kohtien perusteella.** Cirrus, kohdat 5.5 ja 5.6
Sopimukset ja muu ohjeistus henkilötietojen käsittelijöille	Kts. edellinen kohta	Kts. edellinen kohta

Henkilötietojen siirrot ETA-alueen ulkopuolelle
Henkilötietoja saa TSA:n nojalla siirtää Euroopan talousalueen (ETA:n) ulkopuolelle tai kansainvälisille järjestöille vain TSA:n V luvussa määritellyin edellytyksin.

Määrittele	Vastaus	Ohjeita ja huomautuksia
ETA-alueen ulkopuoliset maat tai kansainväliset organisaatiot, joihin tietoja siirretään	Viranomaisen tietojärjestelmään liittyviä tietoja (sisältötiedot) ei siirretä ETA-alueen ulkopuolelle. Pilvipalvelutoimittajan palvelun käytön yhteydessä saattaa pilvipalvelualustan palveludataa siirtyä ETA-alueen ulkopuolelle niin sanottujen globaalien palveluiden osalta.	TVA-ohje, s. 18 **Pilvipalvelualustan palveludatan siirrot tulee analysoida sekä hyödyntää vain sellaisia palveluita ja lokaatioita, jossa nämä vältetään tai minimoidaan.** Cirrus, kohta, 5.7, kohta 5.9
Onko Euroopan komission antanut päätöksen tietosuojan riittävyydestä koskien kyseistä maata tai organisaatiota?	Tietojärjestelmän osalta ETA-alueen ulkopuolisia henkilötietojen siirtoja voi tapahtua pilvipalvelutoimittajan palveludatan osalta. Sen johdosta on tehty tarkastelu EU-U.S. Data Privacy Frameworkin perusteella käytössä olevan pilvipalvelualustan osalta. Suojautason TL IV -osalta on huomioitu myös EU:n ulkopuolinen lainsäädäntöjohdannainen riski.	TVA-ohje, s. 18 **Riittävyyspäätöksen osalta tulee tarkastella EU-U.S. Data Privacy Frameworkin tilanne käytössä olevan pilvipalvelutoimittajan osalta.** https://www.dataprivacyframework.gov/list Cirrus, kohta 3.2
Mitkä ovat henkilötietojen siirrossa käytettävät siirtoperusteet?	Tietojärjestelmän sisältötietojen osalta siirtoja ei tehdä. Palveludatan osalta siirtoperusteena on pilvipalvelualustan tekninen toiminta ns. globaalien palveluiden osalta.	TVA-ohje, s. 18 **Palveludatan siirrot ja siirtoperusteet eroavat eri pilvipalvelutoimittajien osalta ja tarkastelu tulee tehdä tapauskohtaisesti.** Cirrus, kohta 3.2
Täydentävät suojatoimet	Tapausesimerkin yhteydessä on arvioitu, että suojaustason TL IV riskien osalta palveluun tannettevat tiedot salataan vahvasti viranomaisen itsensä hallitsemilla salausavaimilla.	TVA-ohje, s. 18

Rekisteröidyn oikeudet

Rekisterinpitäjän on helpotettava rekisteröidyn tietosuojaoikeuksien käyttämistä sekä tarvittaessa toteutettava tietosuojaoikeudet rekisteröidyn pyynnön mukaisesti.

Menettely oikeuksien toteuttamiseksi
TSA 12 artiklassa määritellään, millä tavalla tietosuojaoikeuksia koskevat pyynnöt on käsiteltävä. Rekisterinpitäjän on varmistettava, että nämä vaatimukset pyyntöjen käsittelystä toteutuvat.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka rekisteröity tunnistetaan?	Rekisteröity tunnistetaan viraston sisäisessä käytössä olevan tietosuojan yhteydenottokanavan periaatteiden mukaisesti.	TVA-ohje, s. 20
Kuinka pyyntöihin vastataan (vastuuhenkilöt, määräajat, yhteydenottokanava)?	Rekisterötyjen pyynnöt tehdään viranomaisen käytössä olevalle tietosuojan yhteydenottokanavalle (tiketöintijärjestelmä).	TVA-ohje, s. 20
Kuinka oikaisusta, poistosta tai rajoituksesta ilmoitetaan tietojen vastaanottajille?	Lähtökohtaisesti informointi tapahtuu viranomaisen sisäisessä käytössä olevan yleisen tietosuojan informointikanavan kautta.	TVA-ohje, s. 20

Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, käsitteleekö tämä häntä koskevia henkilötietoja sekä oikeus saada jäljennös käsiteltävistä tiedoista.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka tiedot toimitetaan rekisteröidylle?	Jos rekisteröity on vielä viranomaisen palveluksessa oleva käyttäjä, niin hän voi pyytää tiedot viranomaisen sisäisen tietosuojan yhteydenottokanavan kautta. Mikäli rekisteröity ei ole enää viranomaisen palveluksessa, voi hän tehdä yhteydenoton kirjaamon kautta.	TVA-ohje, s. 21
Mistä lähteistä tiedot kootaan?	Tiedot kootaan ainoastaan tietojärjestelmäpalvelun teknisestä ympäristöstä.	TVA-ohje, s. 21
Onko annettaviin tietoihin lakiin perustuvia rajoituksia?	Tapausesimerkissä ei ole mitään varsinaisia rajoituksia eli rekisteröity voi aina saada jäljennöksen häntä koskevista käyttäjätiedoista (tai niiden poistumisesta). Tietoturvan ja tietosuojan valvontaan liittyvissä toiminnoissa voi olla rajoituksia eikä kaikkea tietoa välttämättä voida antaa.	TVA-ohje, s. 21 **Mikäli tietoturvaan tai tietosuojaan liittyvää valvontatietoa joudutaan toimittamaan rekisteröidylle saattaa tiedon saatavutta rajoittaa pilvipalvelualustalla käytössä olevien tähän liittyvien toiminnallisuuksien ominaisuudet (yhteen henkilöön liittyvät manuaalipoiminnat eivät useinkaan ole suuresta tietomassasta mahdollisia).** Cirrus, kohdat 2.6 ja 2.7

Oikeus tietojen oikaisemiseen

Rekisteröidyillä on oikeus tulla arvioiduksi oikeiden ja täsmällisten tietojen perusteella. Jos tiedot ovat virheellisiä tai puutteellisia, on tiedot oikaistava.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka oikaisupyynnöt toteutetaan?	Rekisteröity voi olla yhteydessä viranomaisen sisäiseen tietosuojan yhteydenottokanavaan.	TVA-ohje, s. 22
Kuinka menetellään oikaisuun liittyvissä erimielisyyksissä?	Rekisteröidyn kanssa pyritään pääsemään yhteisymmärrykseen erimielisyyden syistä ja ratkaisemaan asia siten, että rekisteröidyn oikeuksia voidaan noudattaa – ellei kyseessä ole laista johtuva syy viranomaisen toiminnalle.	TVA-ohje, s. 22

Oikeus tietojen poistamiseen

Rekisteröidyllä on tietyissä tilanteissa oikeus saada rekisterinpitäjä poistamaan itseään koskevat tiedot ilman aiheetonta viivytystä.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Mikä on prosessi tietojen poistamiseen käytännössä?	Rekisteröity voi olla yhteydessä viranomaisen sisäiseen tietosuojan yhteydenottokanavaan. Mikäli poistopyyntö on aiheellinen, poistetaan tiedot tietojärjestelmän ylläpidon toimesta. Sen jälkeen rekisteröityä informoidaan asiasta.	TVA-ohje, s. 22
Arvioi tapaukohtaisesti tietojen poisto-oikeuden soveltuvuus (esim. lakisääteiset säilytysajat)	Henkilötietojen tallentaminen tietojärjestelmään on sidottu rekisteröidyn virkasuhteeseen, jonka jälkeen tiedot poistetaan automaattisesti.	TVA-ohje, s. 22 .

Oikeus rajoittaa tietojen käsittelyä

Rekisteröity voi tietyissä tilanteissa pyytää rekisterinpitäjää rajoittamaan väliaikaisesti itseään koskevien henkilötietojen käsittelyä.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka tietojen käsittelyn rajoittaminen toteutetaan käytännössä?	Viranomainen ei luovuta tietojärjestelmän henkilötietoja muille, joten rajoittamisesta ei tarvitse ilmoittaa ulkopuolisille tahoille.	TVA-ohje, s. 23
Millaisin teknisin keinoin käsittelyn rajoittaminen varmistetaan?	Kts. edellinen kohta	TVA-ohje, s. 23
Kuinka rekisteröityä informoidaan rajoituksen poistamisesta?	Kts. edellinen kohta	TVA-ohje, s. 23

Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on tietyissä tilanteissa oikeus saada rekisterinpitäjälle toimittamansa henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä halutessaan siirtää kyseiset tiedot toiselle rekisterinpitäjälle.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Kuinka siirto-oikeus toteutetaan käytännössä?	Tapausesimerkissä on kyseessä viranomaisen järjestelmän käyttäjätiedot eikä tätä oikeutta siksi ole.	TVA-ohje, s. 23
Kuinka siirto-oikeus soveltuu kyseessä olevaan tietojen käsittelyyn?	Tapausesimerkissä on kyseessä viranomaisen järjestelmän käyttäjätiedot eikä tätä oikeutta siksi ole.	TVA-ohje, s. 23
Mitkä ovat tekniset edellytykset tietojen siirtoon ja vastaanottoon?	Tapausesimerkissä on kyseessä viranomaisen järjestelmän käyttäjätiedot eikä tätä oikeutta siksi ole.	TVA-ohje, s. 23

Oikeus vastustaa tietojen käsittelyä

Rekisteröidyllä on tietyissä tilanteissa oikeus vastustaa henkilötietojensa käsittelyä eli pyytää, että niitä ei käsiteltäisi ollenkaan.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Mikä on prosessi vastustamisoikeuden toteuttamiseen?	Tapausesimerkissä on kyseessä viranomaisen järjestelmän käyttäjätiedot eikä tätä oikeutta siksi ole.	TVA-ohje, s. 24
Kuinka vastustamisoikeus soveltuu kyseessä olevaan tietojen käsittelyyn?	Tapausesimerkissä on kyseessä viranomaisen järjestelmän käyttäjätiedot eikä tätä oikeutta siksi ole.	TVA-ohje, s. 24

Automaattinen päätöksenteko (ml. profilointi)
Rekisteröidyllä on pääsääntöisesti oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi.

Määrittele	Vastaus	Ohjeita ja huomautuksia
Sisältyykö henkilötietojen käsittelyyn automaattista päätöksentekoa ja profilointia?	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen profilointia ei tehdä.	TVA-ohje, s. 24
Perusteet automaattiselle päätöksenteolle	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen profilointia ei tehdä.	TVA-ohje, s. 24
Käytössä olevat suojatoimet (ihmisen osallistuminen, päätöksen riitauttaminen)	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen profilointia ei tehdä.	TVA-ohje, s. 24
Kuinka varmistetaan tietosuojaperiaatteiden noudattaminen automaattisen päätöksenteon yhteydessä?	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen profilointia ei tehdä.	TVA-ohje, s. 24
Kuinka rekisteröidylle informoidaan automaattisesta päätöksenteosta?	Palvelussa ei tapahtu automaattista päätöksentekoa. Rekisteröityjen profilointia ei tehdä. Asiasta informoidaan palvelun tietosuojaselosteessa.	TVA-ohje, s. 24

Uhkien tunnistaminen

Seuraavassa kuvassa on tietosuojavaltuuten toimiston TVA-työkalun Uhat-lehdestä muokattu versio. Siihen on pilvisymbolilla merkitty ne näkökulmat, joita tulisi erityisesti tarkastella tämän käyttätapauksen yhteydessä. Symboli ei tarkoita välttämättä aktiivista uhkaa vaan sen tarkoituksena on korostaa tässä yhteydessä tarkempaa analyysiä kaipaavia näkökulmia.

	Tietojen käsittelyn elinkaaren vaihe	A Lainmukaisuus ja kohtuullisuus	B Läpinäkyvyys	C Käyttötarkoitus-sidonnaisuus	D Minimointi ja säilytysaikojen rajoittaminen	E Täsmällisyys	F Eheys	G Luottamuk-sellisuus	H Käytettävyys
1	Kerääminen		☁						
2	Tallentaminen	☁	☁					☁	
3	Yhdistäminen		☁						
4	Käyttö ja muokkaaminen		☁					☁	☁
5	Luovutus ja saataville asettaminen		☁						
6	Siirtäminen 3. maihin ja muut siirtotilanteet	☁	☁						
7	Säilyttäminen	☁	☁					☁	☁
8	Hävittäminen	☁	☁					☁	

Lainmukaisuus ja kohtuullisuus (A2, A6, A7, A8)

Tässä kuviteellisessa tapausesimerkissä viranomaisen tietojärjestelmään voidaan tallentaa korkeimmillaan turvallisuusluokan TL IV -tietoa. Tässä yhteydessä tulee kuitenkin huomioida lainsäädäntöjohdannaiset ja **toisen valtion määräysvaltaan liittyvät riskit**. Erityisesti jälkimmäisten riskien johdosta tiedon salaamisessa ja sen siirtämisessä pilvipalveluun tulee huomioida, että tiedon on oltava salattuna koko sen elinkaaren ajan. Kun vaatimukset tiedon salaamisesta ja eriyttämisestä koko elinkaaren ajan, mukaan lukien tietoliikenteessä, on toteutettu vaatimustenmukaisella tavalla voidaan turvallisuusluokiteltua tietoa käsitellä julkisessa pilvipalvelussa. Vaatimusten mukaisesti toteutetun turvallisuusluokan IV tiedon suojaamisen voidaan tulkita suojaavan riittävästi myös henkilötietoja toisen valtion määräysvaltaan liittyviltä riskeitä.

Valtionhallinnon pilvipalvelulinjaukset (2023:75) kohta 2.9, s. 24, Cirrus kohdat 5.1 ja 5.2

Läpinäkyvyys (B1-B8)

Pilvipalveluissa käytössä oleva jaetun vastuun malli johtaa siihen, että asiakkaalla ei ole suoraa näkyvyyttä toimittajan omaan toimintaan. Kun arvioidaan tietosuojan toteutumista tietojen käsittelyn elinkaaren aikana, joudutaan tukeutumaan pilvipalvelutoimittajan dokumentaatioon. Silloin tulee tutustua esimerkiksi seuraaviin toimittajan dokumentteihin:

- Sopimusehdot
- Palvelukuvaukset
- Tekniset kuvaukset
- Ulkopuolisten arviointien (auditoinnit) tulokset
- Mahdolliset luottamukselliset salassapitositoumuksen takana olevat dokumentit
- Toimittajan tiedotteet toteutuneista häiriöistä

Tapausesimerkin tapauksessa on arvioitu, että valitun pilvipalvelualustan osalta on saatu toimittajan dokumentaatioon tutustumalla riittävä läpinäkyvyys tietosuojan toteutumiseen tietojen käsittelyn elinkaaren aikana.

TVA-ohje, s. 24, Cirrus kohta 2.3

Luottamuksellisuus (G2, G4 ja G7, G8)
Pilvipalveluiden käyttöön liittyviä luottamuksellisuusriskejä on tarkasteltu laajasti Cirrus-hankkeen teknisessä yhteenvedossa. Tämän kuvitteellisen tapausesimerkin yhteydessä keskiössä on myös turvallisuusluokan IV tiedon koko elinkaaren ajan vaatimustenmukaisesti toteutettu tietoturva, tietosuoja sekä jatkuvuudenhallinta.

TVA-ohje, s. 16, Cirrus kohta “3.2 Luottamuksellisuus”, Valtionhallinnon pilvipalvelulinjaukset (2023:75) kohdat 2.6-2.9.

Käytettävyys (H4 ja H7)
Pilvipalveluiden käyttöön liittyviä saatavuusriskejä on tarkasteltu laajasti Cirrus-hankkeen teknisessä yhteenvedossa. Tämän kuvitteellisen tapausesimerkin yhteydessä on syytä korostaa erityisesti jatkuvuudenhallitaa, koska kyseessä on viranomaisen turvallisuusluokan IV tietojärjestelmä.

TVA-ohje, s. 16, Cirrus kohta “3.4 Saatavuus”, Valtionhallinnon pilvipalvelulinjaukset (2023:75) luku 2.

Riskien tunnistaminen ja arviointi

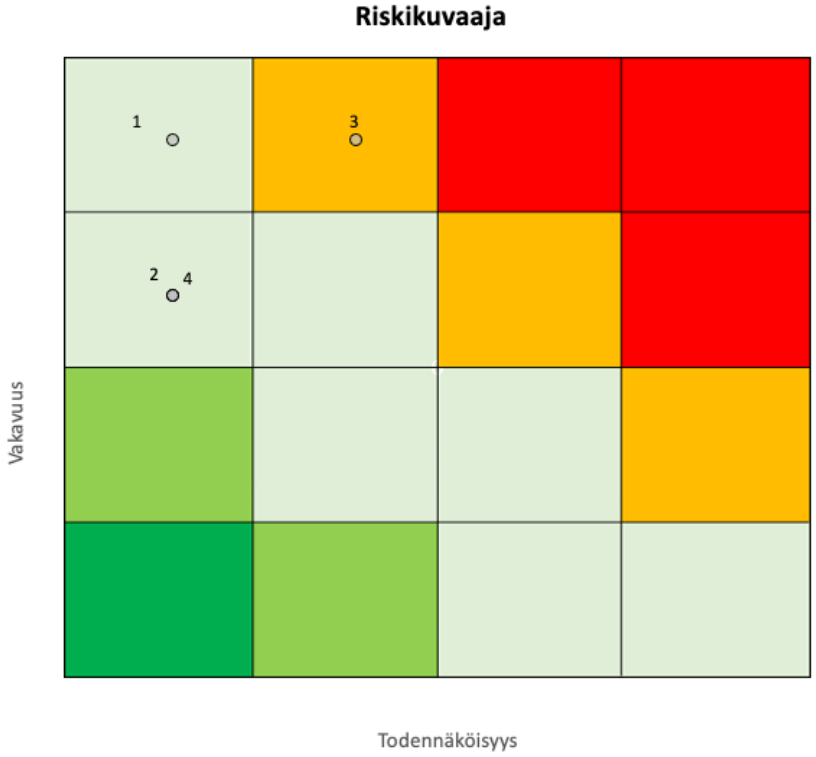
Kuvitteellisessa tapausesimerkissä on tunnistettu 4 keskeistä riskiä. Ne on esitetty seuraavassa taulukossa.

#	Uhan kuvaus	Uhan vaikutukset ja seuraukset rekisteröidylle	Vakavuus	Todennäköisyys	Riskiluku	Suojatoimenpiteet riskin pienentämiseksi	Uusi vakavuus	Uusi todennäköisyys	Uusi riskiluku
1	Valtioneuvoston asetusta asiakirjojen turvallisuus-luokittelusta valtionhallinnossa (1101/2019) tai tiedonhallintalakia ei kyetä noudattamaan pilvipalvelussa.	Turvallisuus-salaisuus paljastuu.	4	2	8	Riittävän vahvan salauksen toteuttaminen pilvipalvelussa. Julkri-kriteeristön vaatimusten toteuttaminen	4	1	4
2	Riittävän läpinäkyvyyden puute pilvipalvelun käsittelijöiden ja alikäsittelijöiden toimintaan.		3	2	6	Pilvipalvelun tietoturva-, tietosuoja- sekä jatkuvuusriskien ymmärtäminen sekä suojaavien kontrollien toteuttaminen	3	1	3
3	**Viranomaisen turvallisuus-luokiteltuun tietojärjestelmään tallennetun tiedon suojaamisessa epäonnistutaan sen elikaaren aikana.**	Viranomaisen käyttäjien henkilötietoja tai salassapidettävää tai turvallisuusluokan IV tietoa saattaa vuotaa.	4	3	12	Riittävä pilvipalvelutoimittajan dokumentaatioon tutustuminen sekä pilven ominaispiirteiden huomioiminen. Riittävän vahva salaus tiedon elinkaaren aikana. Uhkamallinnus sekä ulkoiset auditoinnit.	4	2	8
4	Tietojen käytettävyys vaarantuu maan ulkoisten verkkoyhteyksien pitkäkestoisen häiriön johdosta	Rekisteröityjen tiedot eivät ole saavutettavissa tietoliikenteen estyessä pilvipalvelunympäris töön.	3	2	6	Eri saatavuusalueiden hyödyntäminen.	3	1	3

Kriittisin tunnistettu riski on palveluun kohdistuva tietomurron mahdollisuus. Vaikka sen todennäköisyyttä saadaankin pienennettyä, muodostaa sen mahdollisuus tapausesimerkissä jatkuvaa seurantaa vaativan riskin. On huomattava, että tämä sama riski on yleinen riski kaikille julkisesta verkosta (internet) tavoitettavissa oleville palveluille. Riski oli olemassa siis myös tämän kuvitteellisen tapausesimerkin lähtötilanteessa.

Riskiarvion yhteenveto ja hyväksyminen

Tapausesimerkissä tehtyjen tietosuojariskien suojaustoimenpiteiden jälkeinen riskiarvio on esitetty seuraavassa kuvassa. Suurimpana tunnistettuna riskinä jää tietomurto, joka on yleinen riski kaikille internetistä tavoitettavissa oleville palveluille. Sellaisen vaikutus on aina vakava myös henkilötietojen suojan näkökulmasta.



Riskiarvion lopputuloksena on, että julkisesta verkosta tavoitettavissa olevassa palvelussa on aina tietomurron riski. Toisin sanoen jollakin ulkoisella taholla on **kyky** ja **tahto** siihen. Tietomurron vaikutukset olisivat rekisteröityjen henkilötietojen suojan kannalta tapausesimerkissä aina vakavia.

Tietomurron todennäköisyyttä ei ole mahdollista sulkea kokonaan pois. Erilaisilla hallinnollisilla ja teknisillä kontrolleilla voidaan kuitenkin pienentää sen todennäköisyyttä. Toisin sanoen voidaan vaikuttaa siihen, että ulkoisella taholla on pienempi **tilaisuus** tietomuroon.

Tapausesimerkissä tietomurron riskiä ja vaikutuksia pienennetään seuraavilla hallinnollisilla ja teknisillä kontrolleilla:

- Varmistetaan, että käytettävissä on riittävä pilvipalvelualustaan liittyvä osaaminen.
- Kaikki osapuolet noudattavat toiminnassaan riittävää “kyberhygieniaa” ja hyviä käytäntöjä.
- Pilvipalvelualustalla noudatetaan sen toimittajan hyviä käytäntöjä ja suosituksia.
- Pilvipalvelualustalla otetaan käyttöön soveltuvin osin siellä hyödynnettävissä olevat edistyneet tietoturvatoiminnallisuudet.
- Tietomurron riskiin varaudutaan etukäteen määrittelemällä niihin liittyvät toimintaprosessit ja pelikirjat. Näitä asioita myös harjoitellaan etukäteen.

- Pilvipalveluympäristön tietoturvan tilaa seurataan aktiivisesti ja mahdolliseen muuttuneeseen uhkakuvaan reagoidaan viipymättä.

Edellä mainituilla täydentävillä kontrolleilla voidaan todeta, että tapausesimerkin osalta TVA:ssa tunnistettujen riskien osalta on käytössä riittävät niitä rajoittavat kontrollit. TVA:n osalta voidaan edetä toteutukseen.