VALTIOVARAINMINISTERIÖ

Julkisen hallinnon linjaukset tiedon sijainnista ja hallinnasta

LUONNOS
5.7.2018

Valtiovarainministeriö Snellmaninkatu 1 A, Helsinki PL 28, 00023 Valtioneuvosto Puh 0295 16001 (Vaihde) Faksi 09 160 33123 valtiovarainministerio@vm.fi www.vm.fi Y-tunnus 0245439-9

Sisällys

1. Yhteenveto

Linjaukset julkisen hallinnon tiedon sijainnista ja hallinnasta määrittävät, miten julkisen hallinnon organisaation omistamaa tietoa voidaan sijoittaa ja hallita maantieteellisesti.

Linjausten tavoitteena on tukea valtion, maakuntien ja kuntien päätöksentekoa niiden suunnitellessa ja hankkiessa uusia ICT-palveluita. Linjausten keskeisin osa-alue käsittelee jaettuja resursseja tarjoavia ICT-palveluita, erityisesti niin sanottuja pilvipalveluita.

Uudet tietojärjestelmät ja prosessit hyödyntävät enenevässä määrin pilvipalveluteknologiaa ja sille ominaisia etuja ovat kustannustehokkuus, skaalautumiskyky, tietoturva, energiatehokkuus, joustavuus, innovatiivisuus.

Pilvipalveluiden pääpalvelumalleja on viisi: oma konesali, isännöity konesali, infrastruktuuri palveluna (IaaS), ohjelmistoalusta palveluna (PaaS) ja ohjelmisto palveluna (SaaS) ja päätoteutusmalleja neljä: oma konesali, yksityinen pilvi, julkinen pilvi ja hybridipilvi.

Palvelu- ja toteutusmallien sekä tiedon ja sen hallinnan fyysisen sijainnin eri vaihtoehtojen perusteella saadaan rakennettua erilaisia toteutuksia. Näillä toteutuksilla riskit, riskienhallinnan monimutkaisuus, pilviteknologiasta saatavat hyödyt sekä kokonaiskustannukset vaihtelevat selvästi ja kunkin toteutustavan soveltuvuutta tiettyyn tarkoitukseen on lähestyttävä harkiten.

Linjaukset:

1. Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta
2. Tiedon sijaitessa Suomen rajojen ulkopuolella erityistä on kiinnitettävä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen
3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset
4. Mikäli pilvipalvelut tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita
5. Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti vähintään kerran vuodessa ja oleellisten sopimusehtojen muuttuessa.
6. Viranomainen ylläpitää listaa hyväksytyistä palveluntarjoajista
7. Julkisen tiedon käsittelyä ei rajoiteta
8. Henkilötietoa ja suojaustason IV tietoa voi käsitellä julkisessa pilvessä, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu
9. Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

Linjauksia päivitetään uutta tiedonhallintalainsäädäntöä vastaavaksi uuden lain voimaantulon jälkeen.

Jatkotöiksi esitetään arviointipankin, pilviohjeen, yhteisten sopimusehtojen riskianalyysipohjan ja pilviarkkitehtuurin luomista.

2. Taustaa linjauksille

Nämä linjaukset julkisen hallinnon tiedon sijainnista ja hallinnasta on laadittu valtiovarainministeriön (VM) päätöksen VM/276/00.01.00.01/2018 mukaisesti. Linjaukset määrittävä, miten julkisen hallinnon organisaation omistamaa tietoa voidaan sijoittaa ja hallita maantieteellisesti.

Osana linjaustyötä on selvitetty linjausten toteuttamisen mahdollisesti edellyttämiä muutoksia nykyisiin VAHTI- sekä muihin tietoturvallisuutta ja toiminnan jatkuvuutta koskeviin ohjeisiin. Muutokset toteutetaan erikseen osana valtiovarainministeriössä käynnissä olevaa tiedonhallintalaki-uudistusta ja siihen liittyvää VAHTI-ohjeistusuudistusta (”VAHTI 100”).

Linjaukset päivitetään vastaamaan uutta tiedonhallintalakia sen voimaantulon jälkeen.

Tiedon sijainnilla tarkoitetaan tässä sitä, missä maantieteellisessä sijainnissa organisaation omistamaa tai sen käyttöönsä tuottamaa tietoa käsitellään ICT-palvelussa tiedon elinkaaren eri vaiheissa.

Tiedon hallinnalla tarkoitetaan tässä edellä mainitun ICT-palvelun palveluhallintaan liittyviä palveluita, jotka voivat tapahtua maantieteellisesti muualta kuin missä hallinnoitava tieto sijaitsee. Tyypillisesti maantieteelliset alueet jakautuvat Suomi, EU/ETA-alue sekä muu maailma.

Taustamateriaalina on käytetty muun muassa Norjan[1], Skotlannin[2] ja Kanadan[3] vastaavia linjauksia.

[1] https://www.regjeringen.no/en/dokumenter/cloud-computing-strategy-for-norway/id2484403/
[2] http://www.gov.scot/Publications/2017/03/7843
[3] https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/cloud-computing/government-canada-cloud-adoption-strategy.html

3. Linjausten tavoitteet

Linjausten tavoitteena on tukea valtion, maakuntien ja kuntien päätöksentekoa niiden suunnitellessa ja hankkiessa uusia ICT-palveluita. Linjausten keskeisin osa-alue käsittelee jaettuja resursseja (esimerkiksi laskentateho, tallennus-, varmuuskopiointi ja tiedonsiirtokapasiteetti) tarjoavia ICT-palveluita, erityisesti niin sanottuja pilvipalveluita.

Tarkemmin linjausten tavoitteena on:

- Hallita palveluiden tuottamiseen liittyviä riskejä sekä tunnistaa niihin liittyviä mahdollisuuksia; mahdollistaa uusien teknologioiden turvallinen käyttöönotto
- Mahdollistaa ICT-palveluiden kysynnän ja tarjonnan kohtaaminen parantamalla esimerkiksi saatavaa asiakashyötyä ja kustannustehokkuutta
- Tukea pilvipalveluiden käyttöön liittyvää riskienarviointia
- Valmistaa ICT-henkilöstöä pilvipalveluihin
- Antaa julkisen hallinnon organisaatiolle reunaehdot, joita noudattamalla esimerkiksi pilvipalveluja voidaan turvallisesti hyödyntää

Linjausten näkökulmat:

- Ohjausvaikutuksen vaikuttavuus
- Kustannus-hyöty -arviointi
- Hankinta ja sopimukset
- Hallittu riskitaso uuden teknologian hyödyntämisessä

Linjaukset keskittyvät kahteen kokonaisuuteen; pilvipalveluiden hyötyihin ja haasteisiin.

Linjaukset koskevat pääasiassa Suomen ulkopuolelta hankittavia palveluita, mutta niitä tulee soveltaa myös Suomesta hankittaviin palveluihin. Kaikissa hankittavissa palveluissa tarvitsee arvioida toimintaan liittyvät riskit sekä toteuttaa muut palvelulta edellytettävä vaatimustenmukaisuus.

4. Pilvipalvelujen edut sekä toteutus- ja palvelumallit

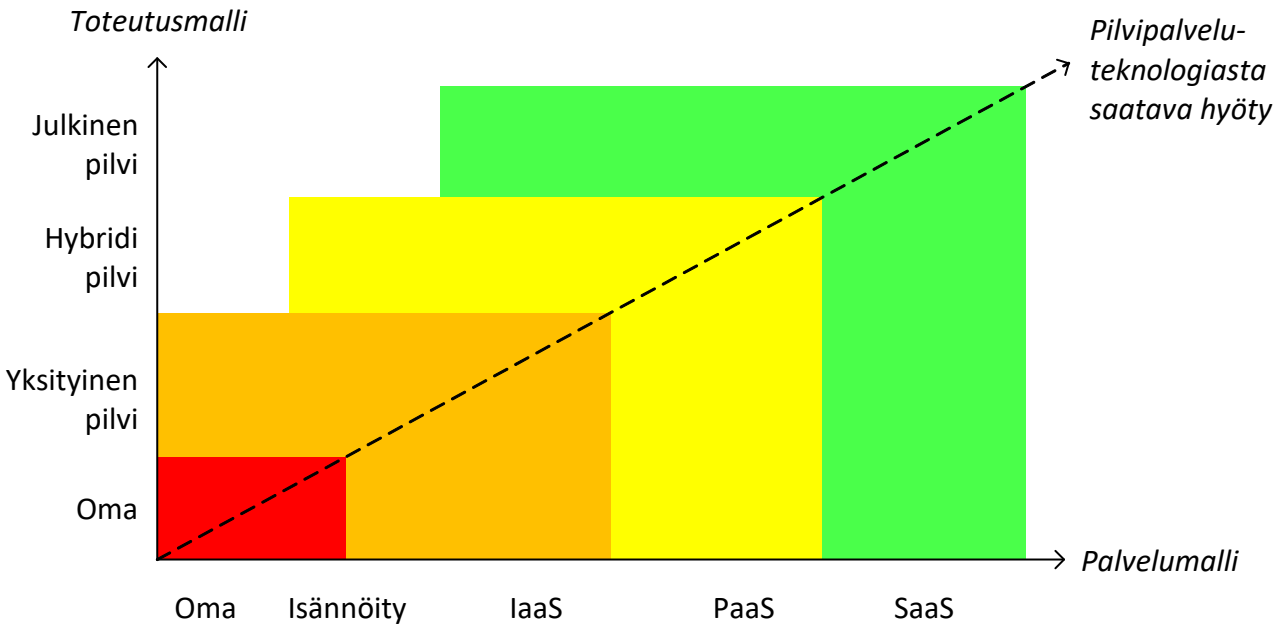
Pilvipalveluilla tarkoitetaan asiayhteydestä riippuen eri asioita; tyypillisesti sillä tarkoitetaan internet-verkkoon kytkettyä ICT-kapasiteettia tai palvelua, jonka tuottamisessa hyödynnetään jaettujen, skaalautuvien ja joustavien resurssien mallia, joka on automatisoitu osin itsepalveluperiaatteella tuotettavaksi. Käsitteenä se kattaa kaikki palveluna hankittavat ICT-palvelut alkaen konesaleista aina ohjelmistoihin saakka.

Tässä kappaleessa tarkastellaan pilvipalveluiden hyötyjä, sekä niiden eri palvelu- ja toteutusmalleja. Yhteenveto pilvipalveluiden toteutus- ja palvelumalleista, sekä niiden suhde saavutettaviin hyötyihin, on nähtävillä kuvassa 1. Maksimaalinen hyöty on saavutettavissa julkisessa pilvessä tuotetusta SaaS tyyppisestä palvelusta.

4.1 Pilvipalveluteknologian edut

Pilvipalveluteknologialle ominaisia etuja ovat:

- Kustannustehokkuus
- Skaalautumiskyky
- Tietoturva
- Energiatehokkuus
- Joustavuus
- Innovatiivisuus



Kuva 1. Toteutus- ja palvelumallien hyödyt

Kustannustehokkuus liittyy ensisijaisesti palvelua tuottavan toimijan mittakaavaetuihin. Palvelun tuottaja pystyy hyödyntämään omaa kapasiteettiaan tehokkaasti, joka mahdollistaa pienemmän yksikkökustannuksen. Palveluiden käyttöönottoon liittyvien toimintojen korkea automatisointiaste parantaa myös kustannustehokkuutta. Palvelun käyttäjältä poistuu palvelun tuottamiseen ja ylläpitämiseen liittyvä osaamistarve.

Nykyaikainen teknologia, kuten virtualisointi ja konttiteknologia, mahdollistavat yhdessä korkean automaatioasteen kanssa palveluiden suuren *skaalautumiskyvyn.* Tällöin palvelun käyttäjä voi esimerkiksi nostaa ja laskea palvelun kapasiteettia ja saatavuutta kulloisenkin tarpeen mukaan.

Pilvipalvelun tuottajilla on tyypillisesti tuottamaansa palveluun liittyen parempi kyvykkyys ja resurssit toteuttaa *tietoturvallisuutta* kuin palvelun käyttäjällä. Palvelun käyttäjän näkökulmasta palvelun tietoturvaan liittyvä osaamistarve pienenee.

Energiatehokkuus liittyy palvelua tuottavan toimijan mittakaavaetuihin. Palvelun tuottaja pystyy esimerkiksi tuottamaan samalla infrastruktuurilla palvelua usealla asiakkaalle.

Pilvipalveluiden *joustavuus* tarkoittaa palveluiden käyttöönoton helppoutta. Palvelut ovat tyypillisesti vakioituja ja käyttöönottoprosessit pitkälle automatisoituja. Palvelun käyttäjällä ei ole käyttöönottoon liittyvää osaamistarvetta.

Palveluiden helppo ja nopea käyttöönotto mahdollistaa *innovatiivisuuden*. Palveluita voidaan testata ja kehittää aiempaa helpommin ja nopeammin.

4.2 Palvelumallit

Pilvipalveluiden pääpalvelumalleja on viisi[4]:

- Oma konesali, On-premises
- Isännöity konesali, Hosted on-premises
- Infrastruktuuri palveluna, Infrastructure as a Service (IaaS)
- Ohjelmistoalusta palveluna, Platform as a Service (PaaS)
- Ohjelmisto palveluna, Software as a Service (SaaS)

Kun ICT-palvelut tuotetaan itse *omasta konesalista*, palvelun käyttäjäorganisaatio tuottaa itse käyttämänsä palvelut. Palveluiden tuottamiseen liittyvä osaamistarve on suurimmillaan.

Isännöity konesali tarkoittaa tilannetta, jossa palvelun käyttäjäorganisaatiolla on oma konesali, mutta sen ylläpidosta vastaa ulkoinen palvelun tuottaja. Käyttäjäorganisaation konesaleihin liittyvä osaamistarve vähenee.

IaaS mallissa kaikki palveluiden tuottamiseen liittyvä infrastruktuuri hankitaan palvelun tuottajalta. Tämä palvelumalli poistaa konesaleihin liittyvän osaamistarpeen.

[4] Järvi, Karttunen, Mäkilä, Ipatti (2011). SaaS-Käsikirja. Turku: Turun Yliopisto.

PaaS mallissa palvelut tuotetaan valmiin ohjelmistoalustan avulla. Käyttäjäorganisaation osaamistarve infrastruktuurin osalta poistuu kokonaan tai vähenee merkittävästi.

SaaS mallissa palvelut tuotetaan kokonaan palvelun tuottajan toimesta. Käyttäjäorganisaatiolta poistuu kaikki palvelun tuottamiseen liittyvä osaamistarve.

4.3 Toteutusmallit

Pilvipalveluiden päätoteutusmalleja on tällä hetkellä neljä:

- Oma konesali
- Yksityinen pilvi (private cloud)
- Julkinen pilvi (public cloud)
- Hybridi pilvi (hybrid cloud)

Oma konesali tarkoittaa palvelua, joka tuotetaan käyttäjäorganisaation omasta konesalista.

Yksityinen pilvi tarkoittaa palvelua, joka tuotetaan vain palvelua käyttävälle organisaatiolle. Palveluiden tuotteistus- ja vakiointiaste voidaan tyypillisesti sovittaa käyttäjäorganisaation mukaisesti. Palveluiden käyttäjän neuvotteluasema tarjoajaan nähden riippuu palveluiden tuottajasta, mutta on parhaimmillaan suuri. Palveluhyöty ja -takuu, sekä käyttösopimukset ovat tyypillisesti neuvoteltavissa.

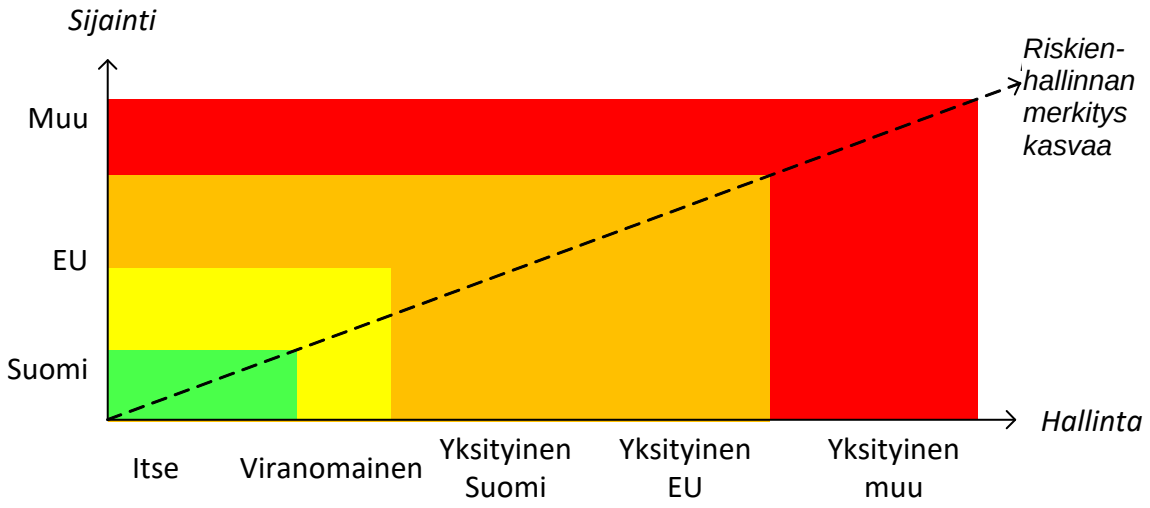
Julkinen pilvi tarkoittaa palvelua, joka on julkisesti tarjolla ja hankittavissa kenen tahansa toimesta. Palvelut ovat tyypillisesti erittäin pitkälle tuotteistettuja ja kustannustehokkaita. Palvelun käyttäjän neuvotteluasema tarjoajaan nähden on pieni, jolloin tarjottavan palvelun palveluhyöty ja -takuu voivat muuttua. Käyttösopimukset ovat myös tyypillisesti standardoituja, jotka täytyy hyväksyä sellaisenaan.

*Hybridi*pilvi tarkoittaa palvelua, jossa yhdistetään oma konesali tai yksityinen pilvi sekä julkinen pilvi yhdeksi palvelukokonaisuudeksi. Tällöin julkista pilveä voidaan käyttää oman konesalin tai yksityisen pilven ”jatkeena” esimerkiksi tilanteessa, jossa tarvitaan nopeasti lisäkapasiteettia. Hybridi pilvi mahdollistaa myös tietojen hajasijoittamisen eri pilvien välillä. Palveluhyöty ja -takuu, sekä käyttösopimukset ovat tyypillisesti neuvoteltavissa.

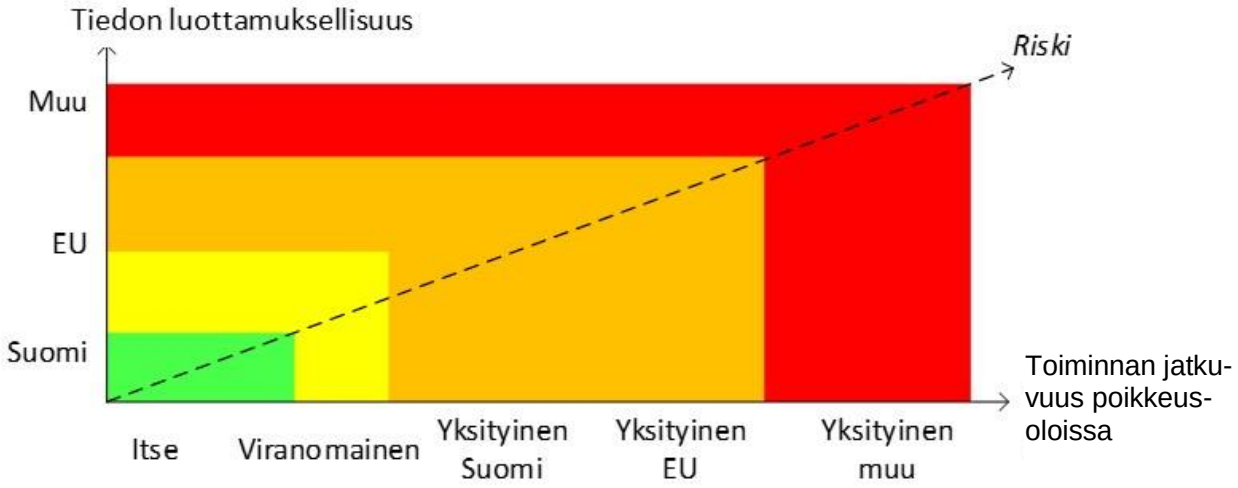
Toteutusmallit kehittyvät koko ajan ja uusia termejä sekä toteutusmalleja tulee markkinoille jatkuvasti, kuten esimerkiksi ”disconnected cloud”, kansallinen pilvi, ”community cloud”. Niissä on otettava huomioon samat reunaehdot kuin muissakin toteutusmalleissa ja tehtävä riittävä riskiarvio palvelutarpeeseen suhteutettuna.

5. Tiedon ja palveluiden sijainti, hallinta ja ohjaus

Tiedon ja palveluiden sijainnin ja hallinnan haasteiden yhteenveto on nähtävillä kuvissa 2 ja 3. Kun sijainti etääntyy Suomesta EU:hun ja sen ulkopuolelle, sekä hallinta omista käsistä muille viranomaisille ja yksityisille toimijoille, palveluhyötyyn ja -takuuseen liittyvät riskit kasvavat.



Kuva 2. Tiedon sijainnin ja hallinnan riskit



Kuva 3. Tiedon luottamuksellisuuden ja toiminnan jatkuvuuteen erityisesti poikkeusoloissa liittyvät riskit suhteessa palvelun tuottamiseen liittyvään malliin.

Julkiseksi luokiteltua tietoa, joka ei sisällä henkilötietoja, voidaan lähtökohtaisesti käsitellä vapaasti sijainnista ja hallinnasta riippumatta. Tällöin, kuten kaikissa muissa tapauksissa, organisaation tulee arvioida myös tiedon ja palvelun kriittisyyteen ja tärkeyteen liittyvät tekijät. Mikäli tällainen julkista tietoa sisältävä palvelu on kriittinen yhteiskunnan, organisaation tai sen asiakkaiden näkökulmasta, organisaation tulee varmistaa palvelun toiminta erilaisissa häiriötilanteissa etenkin, jos palvelu ja tiedot, tai näiden hallinta tapahtuu Suomen ulkopuolelta.

Henkilötietoja tulee käsitellä sekä niiden hallinta tulee lähtökohtaisesti sallia vain sellaisissa palveluissa, jotka toteuttavat EU:n yleistä tietosuoja-asetusta. Tällöin henkilötietoja tulisi käsitellä vain sellaisten toimijoiden hallinnassa olevissa pilvipalveluissa, jotka noudattavat tietosuoja-asetusta ja jotka pystyvät täyttämään henkilötietojen käsittelyssä edellytettävät vaatimukset (esimerkiksi ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksesta, tarvittavat sopimukset rekisterinpitäjän ja henkilötietojen käsittelijän välillä).

5.1 Tiedon käsittelyn vaatimukset

5.1.1 Tietoturva

Tietoturva on yksi tietosuojan toteuttamisen keino. Sen tarkoitus on suojata tietoaineisto ja tietojärjestelmät. Tietoturva tarkoittaa muun muassa teknisiä, hallinnollisia ja fyysisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus, eheys ja saatavuus sekä varmistetaan järjestelmien tarkoituksenmukainen käytettävyys sekä rekisteröidyn oikeuksien toteutuminen

Tietoturvan toteutuminen edellyttää kaikkien seuraavien näkökulmien tarkastelua:

- Luottamuksellisuus
- Eheys
- Saatavuus
- Autentikointi
- Kiistämättömyys

Luottamuksellisuus tarkoittaa sitä, että tietoon pääsee käsiksi vain ne, joilla siihen on oikeus. Tämä edellyttää esimerkiksi käyttäjien tunnistamista ja käyttöoikeuksien hallintaa ja tarvittaessa tiedon salaamista.

Eheys tarkoittaa tiedon sisällön eheyttä, eli sen varmistamista, että tieto on täydellistä, paikkansapitävää ja että sitä ei ole muutettu ilman valtuuksia tai se ei pääse muuttumaan hallitsemattomasti.

Saatavuus tarkoittaa sitä, että tieto käytettävissä silloin kun sitä tarvitaan.

Autentikointi, käyttäjän tai palvelun identiteetin varmistaminen. Keskinäisessä todennuksessa sekä käyttäjä että palvelu todentavat toisilleen keitä ovat. Pilvipalveluiden yhteydessä niiden globaalista luonteesta johtuen, käyttäjä- ja pääsynhallintaan tulee kiinnittää erityistä huomiota.

Kiistämättömyys tarkoittaa sitä, että tiedon käsittelijä pystytään luotettavasti (kiistämättömästi) todentamaan myös jälkikäteen.

5.1.2 Tietojen luokittelu

Käsiteltäessä suojaustason IV-tietoa, organisaatio voi käyttäen palvelun tuottamiseen liittyvää riskienarviointia päättää, millaisissa palveluissa EU/ETA-alueella sen tietoja on mahdollista käsitellä.

Käsiteltäessä suojaustason III tai turvallisuusluokiteltavaa ST III Luottamuksellinen tai korkeampi tietoa, tietoa saa käsitellä ainoastaan Suomessa ja omassa hallinnassa olevia palveluita hyödyntäen.Tästä on mahdollista poiketa, mikäli tälle löytyy selkeä peruste, tarvittava riskienhallinta on toteutettu sekä palvelun omistaja sekä asiakkaat yhdessä hyväksyvät mahdolliset jäännösriskit.

Kuten kaikissa palveluhankinnoissa, organisaation tulee arvioida palvelun kriittisyys ja tärkeys esimerkiksi yhteiskunnan, organisaation ja sen mahdollisten asiakkaiden näkökulmasta ja tämän perusteella varmistaa palvelun toiminnan turvallisuuteen ja jatkuvuuteen liittyvistä tekijöistä esimerkiksi valmius-, varautumis- ja toipumissuunnittelun näkökulmista.

Mikäli kyseessä on laaja-alainen, esimerkiksi koko julkiseen hallintoon tai valtionhallintoon tarkoitettu yhteinen palvelu, palvelun omistajan tulee ennen palvelun toteuttamista varmistaa sen asiakkailta palvelun tuottamiseen liittyvät edellytykset koskien salassa pidettävien tietojen ja toiminnan jatkuvuudelta edellytettäviä vaatimuksia.

Tietoja voidaan luokitella niiden julkisuuden[5] ja arkaluonteisuuden perusteella seuraavasti:

- Julkinen
- Henkilötieto
- Erityisiä henkilötietoryhmiä koskeva henkilötieto (ns. entinen ”arkaluonteinen henkilötieto”)
- ST IV tai ST IV Käyttö rajoitettu
- ST III tai ST III Luottamuksellinen
- ST II tai ST II Salainen
- ST I tai ST I Erittäin salainen

Julkinen tieto on luonteeltaan julkista.

Henkilötieto tarkoittaa yleisen tietosuoja-asetuksen[6] mukaista tietoa luonnollisista henkilöistä.

Erityisiä henkilötietoryhmät on määritelty tietosuoja-asetuksen 9. artiklassa; Sellaisten henkilötietojen, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely.

[5] Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa
[6] Asetus (EU) 2016/679 – luonnollisten henkilöiden suojelu henkilötietojen käsittelyssä sekä näiden tietojen vapaa liikkuvuus

Viranomaisten luokiteltujen asiakirjojen käsittelyä ohjataan suojaustasojen (ST) avulla.

Suojaustasot ovat:

- suojaustaso I, (ST I), jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle
- suojaustaso II (ST II), jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle
- suojaustaso III (ST III), jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle
- suojaustaso IV (ST IV), jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle

Turvallisuusluokitusmerkinnät: jos asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2 ja 7–10 kohdassa tarkoitetulla tavalla, salassa pidettävän asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta voidaan tehdä erityinen turvallisuusluokitusmerkintä:

- suojaustasoon I kuuluvaan asiakirjaan merkinnällä "ERITTÄIN SALAINEN";
- suojaustasoon II kuuluvaan asiakirjaan merkinnällä "SALAINEN";
- suojaustasoon III kuuluvaan asiakirjaan merkinnällä "LUOTTAMUKSELLINEN";
- suojaustasoon IV kuuluvaan asiakirjaan merkinnällä "KÄYTTÖ RAJOITETTU".

5.1.3 Tietosuoja

Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Tekninen suojaus kattaa kaiken teknisen tietojenkäsittelyn, kuten infrastruktuurin ja ohjelmistot. Myös tietojen salaus ja käyttäjien tunnistaminen lasketaan osaksi teknistä suojausta.

Hallinnollinen suojaus kattaa kaiken organisaation hallinnollisen suojauksen, kuten määritellyt roolit ja valtuutusoikeudet, sekä organisaation jäsenten tietoturvaosaamisen. Lisäksi hallinnalliseksi suojaamiseksi lasketaan erilaiset sopimukset niin oman henkilöstön kuin palvelun tuottajien kanssa.

Fyysinen suojaus kattaa kaiken tiedon fyysisen suojauksen, kuten toimitilojen ja muiden rakenteiden teknisen valvonnan ja suojaamisen, henkilöstön ja asiakkaiden kulunestämisen ja -valvonnan.

5.1.4 Tiedon ja palveluiden sijainti

Tietoa voidaan tallentaa ja sen käsittelyyn liittyviä palveluita tuottaa maantieteellisesti eri sijainneissa osana tiedon elinkaaren hallintaa

Tässä linjauksessa käytettävät tiedon ja palveluiden tuotannon maantieteelliset sijainnit ovat:

- Suomi
- Euroopan Unioni (EU) tai ETA-alue
- Muut maat

Yllä olevan jaottelun lisäksi erilaiset maiden väliset ja muut sopimukset voivat joltain osin muuttaa tilannetta.

5.1.5 Tiedon ja palveluiden hallinta

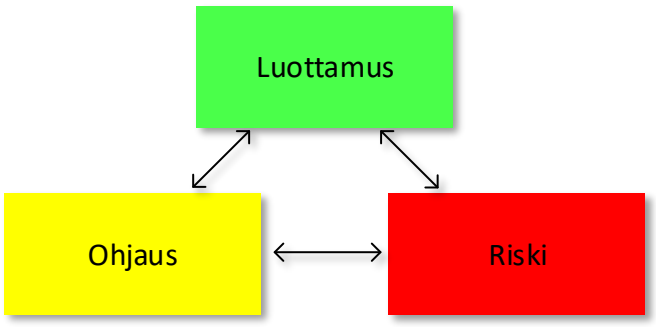
Tietoa ja sen käsittelyyn liittyviä palveluita voi hallita eri osapuolet. Organisaatio voi hallita tietoaan ja palveluitaan itse, tai sitä voi hallita jokin ulkopuolinen taho.

Tietoa ja palveluiden tuotantoa voivat hallita:

- Organisaatio itse
- Muu viranomainen / julkinen toimija
- Yksityinen toimija (kotimainen)
- Yksityinen toimija (EU tai ETA-alue)
- Yksityinen toimija (muut maat)

5.2 Palveluiden ohjaus

Ohjauksen avulla pyritään rakentamaan luottamusta palvelun tuottajiin sekä hallitsemaan palveluihin liittyviä riskejä. Kuvassa 3. on kuvattu luottamuksen, ohjauksen ja riskin välinen kolminaisuus.



Kuva 3. Luottamus, ohjaus ja riski

Kun palvelu toteutetaan itse ja tuotetaan omissa tiloissa, luottamus rakentuu organisaation oman henkilöstön kanssa. Ohjaus tapahtuu organisaation oman johtamisjärjestelmän kautta ja riskien hallinta on täysin omissa käsissä.

Kun palvelu tuotetaan IaaS, PaaS, tai SaaS palvelumalleilla, taikka yksityisellä, julkisella tai hybridi toteutusmalleilla, luottamus rakentuu enenevissä määrin organisaation ja palvelun tuottajan välille. Ohjaus tapahtuu sopimusten ja niihin liittyvän valvonnan avulla.

Riskit riippuvat palvelu- ja toteutusmalleista. Palveluita itse tuotettaessa suurimmat riskit liittyvät palveluiden tuotantoon liittyvään osaamiseen. Pilvipalveluita käytettäessä riskejä ovat muun muassa:

- Palveluhyötyyn liittyvät riskit
- Palvelutakuuseen liittyvät riskit (kapasiteetti, saatavuus, jatkuvuus, tietoturva)
- Neuvotteluasema

Palveluhyötyyn liittyvät riskit tarkoittavat esimerkiksi käytetyn palvelun muuttumista tai lopettamista toimittajan toimesta. Samoin palvelun kehitystarpeiden toteutuminen lasketaan tähän kategoriaan liittyväksi riskiksi. Tämän kategorian riskit ovat osin organisaation hallinnassa, koska organisaatio valitsee itse palvelun ja palveluntarjoajan.

Palvelutakuuseen liittyvillä riskeillä tarkoitetaan palvelun kapasiteettiin, saatavuuteen, jatkuvuuteen, sekä tietoturvaan liittyviä riskejä. Nämä riskit ovat pääosin palveluntarjoajan hallinnassa. Asiakas organisaatio pystyy vaikuttamaan riskeihin pääsääntöisesti palvelutasosopimuksin ja niiden toteutumisen valvonnan kautta.

Neuvotteluasemaan liittyvät riskit tarkoittavat asiakasorganisaation neuvotteluasemaa suhteessa palveluntarjoajaan. Esimerkiksi julkisesta pilvestä tarjottavaan SaaS palveluun liittyen asiakasorganisaation neuvotteluasema on pieni, kun taas itse tuotettuna suuri. Toteutuessaan neuvotteluasemaan liittyvä riski realisoituu palveluhyötyyn tai palvelutakuuseen liittyvänä riskinä.

5.3 Haasteet

Pilvipalveluiden käyttöön liittyy haasteita, jotka on huomioitava hankintaa ja käyttöä suunniteltaessa.

Pilvipalveluiden haasteita ovat muun muassa:

- Salassa pidettävien suojaustasoluokkien ja turvallisuusluokiteltujen ST IV – ST III tietojen käsittely
- Toiminnan jatkuvuuteen liittyvät riskit tietojen sijaitessa ja/tai niiden hallinnan tapahtuessa Suomen ulkopuolella
- Tietoturvan toteutuminen tiedon sijainnista ja hallinnasta riippuen
- Tietosuojan toteutuminen tiedon sijainnista ja hallinnasta riippuen
- Tiedon saatavuuteen ja omistajuuteen liittyvät riskit. Kuka omistaa tiedot? Mahdollistavatko palvelun käyttöehdot tiedon kaupallisen hyödyntämisen? Mikä vastuu palvelun tarjoajalla on, jos tietoa häviää? Mitä tapahtuu sopimuksen päättymisen jälkeen tiedolle?
- Usein yksipuoliset sopimusehdot

Salassa pidettävien tietojen käsittelystä on annettu linjauksia esimerkiksi VAHTI-ohjeissa. Muuta kuin julkista tietoa käsiteltäessä, täytyy varmistaa riittävä tietoturvan ja -suojan taso. Tässä yhteydessä tulee huomata, että valtiovarainministeriössä oleva tiedonhallintalain valmistelu muuttaa tietojenluokittelua, jonka perusteella myös salassa pidettävien tietojen käsittelyyn liittyvä VAHTI-vaatimus- ja arviointikehikko tulee muuttumaan siten, että niissä otetaan huomioon tässä asiakirjassa esitetyt linjaukset.

Toiminnan jatkuvuuteen liittyvät riskit tietojen sijaitessa ja/tai niiden hallinnan tapahtuessa Suomen ulkopuolella tarkoittaa sitä, että organisaation pitää tunnistaa toiminnan kriittisyys ja tärkeys yhteiskunnan, organisaation, sen asiakkaiden tai sidosryhmien näkökulmasta. Mitä kriittisemmästä toiminnasta on kyse, sitä tärkeämpää on varmistaa, että palvelu on saatavilla sille asetettujen vaatimusten mukaisesti. Käytettäessä pilvipalveluita, tämä saattaa edellyttää sitä, että tiedot sijaitsevat myös Suomessa sijaitsevassa konesalissa ja palvelun hallinta voidaan toteuttaa Suomesta.

Tietoturvan toteutumiseen vaikuttaa tiedon ja sen käsittelyyn liittyvien palveluiden sijainti. Kun tieto ja palvelut sijaitsevat organisaation omissa tiloissa Suomessa, organisaatio pystyy varmistamaan omin keinoin sen luottamuksellisuuden, eheyden, saatavuuden ja kiistämättömyyden. Lisäksi tällöin voidaan paremmin varmistua tietojen luotettavasta tuhoamisesta ja sen todentamisesta.

Tieto ja palvelut voivat myös sijaita Suomessa organisaation ulkopuolella, jolloin toimitaan Suomen lakien alaisuudessa. Kun tieto tai palvelut sijaitsevat EU:n tai ETA:n alueella, tai sen ulkopuolella, riski tietoturvan tasosta laskee erityisesti koskien kyseistä palveluntarjoajaa ja maata koskevan lainsäädännön johdosta sekä tietoliikenteen osalta esimerkiksi tiedon saatavuuden osalta. Vastaavasti, tiedon sijoittaminen globaalisti pilvipalveluihin voi parantaa erityisesti julkisen tiedon saatavuutta maailmanlaajuisesti.

Tietosuojan toteutumiseen vaikuttaa tiedon ja sen käsittelyyn liittyvien palveluiden hallinnoijan sijainti, erityisesti henkilötietojen käsittelijän osalta. Kun tieto ja palvelut sijaitsevat organisaation omissa tiloissa Suomessa, organisaatio

pystyy varmistamaan omin keinoin sen teknisen, fyysisen ja hallinnollisen tietosuojan pohjautuen riskienhallintaan. Jos käytetään toisen viranomaisen palveluita, organisaatio ei enää pysty suoraan vaikuttamaan fyysiseen tietoturvaan.

Palvelusta riippuen, myös tekniseen tietoturvaan ei pystytä kaikilta osin vaikuttamaan. Esimerkiksi palvelua voidaan tuottaa palveluntarjoaja valitsemalla infrastruktuurilla, mutta asiakas voi salata tietonsa haluamallaan tavalla. Kun tieto ja palvelut ovat yksityisen toimijan hallinnassa, tietoturvallisuuteen vaikuttaa erityisesti toimijaa koskeva lainsäädäntö.

Maantieteellisestä sijainnista riippuen, toimijoilla ja viranomaisilla saattaa olla Suomen ja EU:n lainsäädännöstä poikkeavia oikeuksia käsitellä ja luovuttaa tietoa. Tällöin erityisesti teknisen ja hallinnollisen tietoturvan merkitys korostuu. Esimerkiksi tiedon tekninen salaaminen käyttäen viranomaisen hyväksymää ja varmistamaa salausratkaisua varmistaa sen, että tietoa voi käsitellä vain valtuutetut tahot.

Riskienhallinnan merkitys korostuu pilvipalveluita käytettäessä. Hankittavaan palveluun saattaa liittyä useita osapuolia, joiden tuottamat palvelut yhdessä muodostavat hankittavan palvelun. Esimerkiksi pilvipalveluita ei voida käyttää ilman tietoverkkoyhteyttä. Erityisesti tietoturvaan ja -suojaan liittyviin riskeihin tulee varautua asianmukaisesti.

Tiedon kriittisyyden luokittelusta riippuen, se tulee olla saatavilla normaaliolojen lisäksi myös poikkeusoloissa, jolloin tiedon sijainti ja hallinta pitää toteuttaa siten, että ne ovat aina saatavilla myös Suomessa.

6. Linjaukset julkisen hallinnon tiedon sijainnista ja hallinnasta

1. Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta

Pilvipalveluita hankittaessa tai kehitettäessä täytyy huomioida samat asiat kuin missä tahansa ICT-palvelun hankinnassa.

Hankinnan valmisteluun on kuitenkin kiinnitettävä tavallista enemmän huomiota. Etenkin tulisi varmistaa, että asianmukainen tietosuoja- ja tietoturvariskien arviointi on tehty ja että markkinakartoitus on tehty perusteellisesti.

Lisäksi varsinaisen hankintamenettelyn valinnassa tulisi kiinnittää huomiota siihen, että tarjoajien kanssa voidaan käydä neuvottelua lain sallimissa rajoissa tekniseen toteutukseen ja tietoturvaan liittyvissä asioissa, jotka ovat merkittäviä riskienhallinnan kannalta.

2. Tiedon sijaitessa Suomen rajojen ulkopuolella erityistä on kiinnitettävä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen

Sopimuksissa on huomioitava millä ehdoille tietoa palvelussa käsitellään ja miten ja missä mahdolliset ristiriitatilanteet hoidetaan. Muiden maiden lainsäädäntö sekä sopimuskäytännöt eroavat Suomen vastaavista, joten tällöin on varmistuttava, että sopimus ja sen tulkinta on ymmärretty riittävällä tasolla.

Palvelun jatkuvuuden osalta on huomioitava palvelun toiminta niin sanotusti päästä päähän, eikä voida keskittyä vain palveluntarjoajan toiminnan jatkuvuuteen. Tähän liittyy muun muassa tietoliikenneyhteyden Suomesta palveluntarjoajaan. Palvelun hankkijalla on oltava suunnitelma, kuinka palvelutaso säilytetään riittävällä tasolla myös häiriötilanteissa.

Palvelun hankkijan on kiinnitettävä varmistettava tiedon saatavuus erilaisissa tilanteissa sekä myös palveluntarjoajaa vaihdettaessa. Palvelun hankkijan on huomioitava myös mahdolliset oman organisaationsa ulkopuoliset käyttäjät ja niiden tarpeet ja vaatimukset tietojen yhteiskäyttötapauksissa.

3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset

Palvelun arvo muodostuu palveluhyödystä ja -takuusta, joiden molempien täytyy toteutua.

4. Mikäli pilvipalvelut tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita

Valitaan aina parhaiten sopiva vaihtoehto. Pilvipalvelujen valinnalle ei ole esteitä, kunhan siinä otetaan vaatimukset huomioon normaalien ICT-hankintojen tapaan.

5. Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti vähintään kerran vuodessa ja oleellisten sopimusehtojen muuttuessa.

Varsinkin julkiset pilvipalvelut kehittyvät jatkuvasti, josta syystä niitä on arvioitava säännöllisesti ja oleellisten sopimusehtojen muuttuessa. Sopimusehtojen muuttamiskäytännöt ja -ehdot vaihtelevat palveluntarjoajien välillä, joten palvelun hankkijan on oltava tietoinen vallitsevista sopimusehdoista koko ajan.

6. Viranomainen ylläpitää listaa hyväksytyistä palveluntarjoajista

Viranomainen määrittelee millä keinoin ja/tai asetuksin tiedon käsittely on sallittua.

Viranomainen ylläpitää listaa vaatimukset todennetusti täyttävistä palveluntarjoajista, joissa muun kuin julkisen tiedon käsittely on sallittua. Listalla olo ei ole ennakkovaatimus hankintoihin osallistumiselle, mutta ennen kuin palvelu voidaan ottaa käyttöön, sen on täytettävä määritellyt vaatimukset.

7. Julkisen tiedon käsittelyä ei rajoiteta

Julkista, tai sellaiseksi tarkoitettua, tietoa voidaan käsitellä vapaasti pilvipalveluissa ottaen huomioon tiedon ja palvelun kriittisyys ja muu tärkeys yhteiskunnalle, organisaatiolle ja sen mahdollisille asiakkaille.

8. Henkilötietoa ja suojaustason IV tietoa voi käsitellä julkisessa pilvessä, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu

Kun tieto on esimerkiksi salattu ja suojattu sekä toiminnan jatkuvuudesta on varmistuttu asianmukaisesti viranomaisen hyväksymällä tavalla tiedon ja palvelun kriittisyys ja muu tärkeys yhteiskunnalle, organisaatiolle ja sen mahdollisille asiakkaille huomioiden, voidaan sitä käsitellä julkisessa pilvessä.

Henkilötietojen käsittelyn ja hallinnan osalta tulee lisäksi varmistua muista EU/ETA-alueen ulkopuolella vaadittavista edellytyksistä.

9. Suojaustason III tietoa voi käsitellä *viranomaisen* hyväksymissä pilvipalveluissa

Tällaisen tiedon käsittelyyn käytettävän pilvipalvelun täytyy sijaita fyysisesti Suomen tai EU:n alueella ja sen täytyy olla Suomessa tai EU alueella sijaitsevan toimijan hallinnassa. Palvelun on täytettävä tiedon käsittelylle asetetut vaatimukset samalla tavalla kuin muiden toteutusmallien.

7. Suosituksia jatkotoimenpiteiksi

- Luodaan prosessit, joilla pystytään välttämään päällekkäisiä arviointeja ja auditointeja yhteisille palveluille
- Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) luo arviointipankin, jossa on saatavilla tietoja tehdyistä arvioinneista helpottamaan uusien hankintojen ja palveluiden suunnittelua ja määrittelyä
- Luodaan hallinnolle ylätason pilviohje, jossa yleisimpien palvelujen soveltuvuutta on tuotu esiin ja jossa huomioidaan myös hankinta-asiat (esimerkkinä vastaavasta https://wiki.eduuni.fi/display/pilviohje/Pilviohje)
- Tarkastellaan linjaukset uuden tiedonhallintalain tultua voimaan ja päivitetään linjaukset ja termistö vastaamaan uutta lakia.
- Neuvotellaan yhteiset sopimus- ja hinnoitteluehdot tärkeimpien palveluntarjoajien kanssa koko julkiselle hallinnolle
- Luodaan riskianalyysipohja ja toteutusmallin valintatyökalu tukemaan palvelujen ja niiden vaatimusten arviointia
- Luodaan ylätason pilviarkkitehtuuri
    - Osana pilviarkkitehtuuria luodaan käyttötapausesimerkkejä helpottamaan hankintojen ja palveluiden suunnittelua ja määrittelyä

Jatkotyössä selvitetään vastuulliset toteuttajat sekä tarkempi sisältö, aikataulu ja seuranta kullekin toimenpiteelle.