Valtionhallinnon kehittämisosasto

Valtion talous- ja henkilöstöhallinnon tiedon luokittelusuositukset

Sisällys

1. Johdanto

Talous- ja henkilöstöhallinnon tiedon luokittelukokonaisuuden kehittämisen lähtökohtana on ollut valtion strategisen tason pilvisiirtymä ja tiedon luokitteluun liittyvien säännösten ja tulkintojen soveltamistarpeet. Pilvisiirtymässä on kyse valtion talous- ja henkilöstöhallinnon keskeisten ja olemassa olevien tietojärjestelmien ja tietovarantojen siirtämisestä pilvipohjaisiin ratkaisuihin. Siirtymällä ei välttämättä ole suoraa vaikutusta tietosisältöihin tai tietojen käsittelyyn, mutta kuitenkin yhteinen ymmärrys tiedon luokittelun perustasta on edellytys sille, että valtion yhteiset talous- ja henkilöstöpalvelut voidaan järjestää vaatimusten mukaisesti ja kustannustehokkaasti kirjanpitoyksiköt mahdollisimman yhtenäisiin prosesseihin. Riskinä suositusten mukaisten toimintatapojen käyttöönotolle voi olla kirjanpitoyksiköiden ja palvelukeskuksen erilaiset näkemykset tiedosta ja sen luokittelusta ja tiedon luokittelun edellyttämästä käsittelyprosessista ja toisaalta se, että tietoa luokitellaan korkeammalle tasolle kuin mitä normit edellyttävät. Eroavaisuudet näkemyksistä monimutkaistavat toimintaa ja heikentävät kustannustehokkuutta.

Julkisen hallinnon talous- ja henkilöstöhallinnon teknologisten kehittämisnäkymien vuoksi on merkittävää, että valtionhallintoon on luotu yhteiset pilvilinjaukset. Tavoitteena on kehittää talous- ja henkilöstöhallinnon palveluita kohti pilvitransformaatiota siten, että pystymme lisäämään prosesseissa automatisaatiota ja hyödyntämään tekoälyä mahdollisimman turvallisesti sekä turvaten tietoon liittyvä riskienhallinta ja palveluiden jatkuvuus (Valtionhallinnon pilvipalvelulinjaukset).

Pilvipalvelujen laajaan käyttöön siirtyminen on muutos, jossa hankintaa, käyttöönottoa ja hyödyntämistä tulee käsitellä kuin mitä tahansa muutakin tietojärjestelmän hankintaa tai muutosta. Hankintojen yhteydessä arvioidaan muun muassa teknologinen muutos, kasaantuvat tietomassat (mm. koko valtionhallinnon virastojen tiedot, kirjanpitoyksiköiden tietovarannot), riskipohjainen päätöksenteko, (ml. lainsäädäntöjohdannaiset riskit), tietosuojasäännöksiä ja näihin em. liittyy roolien ja vastuiden uudelleenajattelua sekä uudenlaisia osaamistarpeita. Kuten valtionhallinnon pilvilinjauksiin on kirjattu, riskejä voidaan vähentää tiedon sijoittamisella sellaiseen pilvipalveluun, johon sovelletaan Suomen lainsäädäntöä, palvelutuottajan yritysturvallisuustodistuksella sekä huolehtimalla tiedon salaamisesta luotettavasti koko sen elinkaaren ajan.

Valtiovarainministeriö asetti 10.11.2022 – 31.1.2023 työryhmän tarkastelemaan valtion yhteisten talous- ja henkilöstöhallinnon palveluiden toimintaympäristössä tapahtuneita muutoksia (Valtion yhteisten talous- ja henkilöstöhallinnon palvelujen toimintaympäristömuutosten selvitys). Työryhmä piti tärkeänä, että valtionhallinnossa muodostetaan yhtenäinen näkemys tietojen luokittelusta valtion talous- ja henkilöstöhallinnon yhteisissä, keskitetyissä palveluissa ja tietojärjestelmäratkaisuissa, jossa tärkeässä osassa on yhteiset prosessit eri kirjanpitoyksiköiden kanssa. Yhteinen näkemys tietojen luokittelusta on edellytys palvelujen järjestämiselle, kehittämiselle ja jatkuvuuden turvaamiselle mm. automaation lisäämiseen ja tekoälyn hyödyntämiseen.

Yhteisen näkemyksen saamiseksi talous- ja henkilöstöhallinnon tietojen luokitteluun liittyvä suositusten valmistelutyö tehtiin virkatyönä valtiovarainministeriön valtionhallinnon kehittämisosastolla 1.9.2023-30.4.2024 välisenä aikana. Suositusten valmisteluun osallistuneiden kirjanpitoyksiköiden kanssa käytiin useita keskusteluja talous- ja henkilöstöhallinnon tiedon luokittelusta, kerättävän tiedon perusteista ja rakenteesta. Tietojen keruu tapahtui Palkeiden henkilöstö- ja talouspalvelujen tietoalueiden ja

tietosisältöjen jaottelun mukaisesti. Kerätyistä tiedoista muodostui hyvä kokonaisuus kirjanpitoyksiköiden toimintaan kohdistuvan lainsäädännön tunnistamiseksi, tietoihin kohdistuvien riskien arvioinnista ja niiden hallintakeinoista, tietojen kasaumavaikutuksiin ja tietojen suojaamisen näkökulmiin ja näihin sovellettavasta lainsäädännöstä. Kokonaisuudesta muotoutui suositusten listaus, jonka perusteella kirjanpitoyksiköiden ja palvelukeskuksen on tärkeä huomioida talous- ja henkilöstöhallinnon tietojen käsittelyn arvioinnissa ja suojaamisessa.

Selvitystyön aikana kuultiin useita valtiovarainministeriön ja ministeriön ulkopuolisia asiantuntijoita ja asiantuntijaryhmiä. Erityisenä selvitystyön kohderyhmänä olivat turvallisuusviranomaiset.

Suositusluonnokset ovat olleet lausuntokierroksella ministeriössä, virastoissa ja laitoksissa 19.3.-19.4.2024 välisenä aikana. Lausuntokierroksen perusteella suositusmuistiota muokattiin ja täsmennettiin vastaamaan lausunnoissa esitettyjen erittäin hyvien kommenttien perusteella. Tämän jälkeen valtiovarainministeriön valtionhallinnon kehittämisosaston johtoryhmä on käsitellyt suositukset ja hyväksynyt suositukset.

2. Ohjaavaa lainsäädäntöä ja ohjeistusta

Viranomaisten hallussa on valtion talous- ja henkilöstöhallinnossa käsiteltävää tietoa, jonka keräämistä, säilyttämistä, käsittelyä ja suojaamista koskevat useat säädökset. Keskeisiä talous- ja henkilöstöhallinnon osalta ovat henkilötiedoissa EU:n yleinen tietosuoja-asetus ja tietosuojalaki sekä tiedon luokittelun osalta julkisen hallinnon tiedonhallintalaki sekä julkisuuden osalta laki viranomaisten toiminnan julkisuudesta. Tässä kappaleessa luetellut säännökset ja ohjeluettelo ei ole tyhjentävä, mutta antaa kuvaa siitä, millaiseen sääntelyyn talous- ja henkilöstöhallinnon tiedon käsittely täytyy osata soveltaa.

Perustuslain 12 § 2 momentissa säädetyn julkisuusperiaatteen mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Perustuslain mukaan jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta. Tämän julkisuusperiaatteen mukaisesti valtionhallinnon tieto ja asiakirjat ovat salassa pidettäviä vain, jos salassapidosta on säädetty julkisuuslaissa tai muussa laissa, tai jos se pitää sisällään tietoa, josta on lailla säädetty vaitiolovelvollisuus. Turvallisuusluokiteltujen tietoaineistojen käsittelyyn sovelletaan yleisiä hyvää tiedonhallintatapaa koskevia velvoitteita sekä julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, jäljempänä *tiedonhallintalaki)* yleisiä tiedonhallinnan järjestämistä koskevia velvoitteita. Turvallisuusluokiteltujen asiakirjojen käsittelystä säädetään valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019).

EU:n yleinen tietosuoja-asetus (EU2016/679, GDPR) koskee luonnollisten henkilöiden suojelua henkilötietojen käsittelyssä sekä näiden tietojen vapaata liikkumista. EU:n yleinen tietosuoja-asetus sisältää säännökset suojelluista erityisiin henkilötietoryhmiin kuuluvista tiedoista sekä säädökset kansallisesta liikkumavarasta, jonka puitteissa kansallisesti voidaan täydentää asetuksen säännöksiä, mutta ei säätää sen kanssa ristiriitaisesti. EU:n yleisessä tietosuoja-asetuksessa ja kansallisessa tietosuojalainsäädännössä tunnistetaan eri tavalla luokiteltaviksi tiedoiksi erityisryhmiin kuuluvat henkilötiedot (GDPR 9 artikla), rikosasioihin ja rikkomuksiin liittyvät henkilötiedot (GDPR 10 artikla) sekä henkilötunnus (tietosuojalain 29 §). Ensin mainittujen käsittelyä on säännelty tietosuojalain 6 § 2 momentilla sekä 7 §:llä. EU:n yleisessä tietosuoja-asetuksessa edellytetään henkilötietojen käsittelyä EU-

lainsäädännön mukaisesti, vaikutusvaltaa sopimusehtoihin ja alihankintaketjuihin, sekä sitä, että palveluntarjoaja ei saa ryhtyä käsittelemään henkilötietoja omiin tarkoituksiinsa. Henkilötiedoissa on tärkeää huomioida mm. turvakielto-osoitteet, sillä henkilöstöön voi kohdistua maalittamista, uhkailua ja vaaratilanteita. Lisäksi on syytä huomata, että tietosuoja-asetuksessa edellytetään ennakollista tietosuojaa koskevaa vaikutustenarviointia tehtäväksi etenkin silloin, kun laajamittainen käsittely kohdistuu erityisiin henkilötietoryhmiin. Kansallisesti yksityiselämän suojasta on säädetty perustuslain 10 §:n 1 momentissa, jossa todetaan myös, että henkilötietojen suojasta säädetään tarkemmin lailla.

Yksityisyyden suojasta työelämässä annetun lain (759/2009) tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. Laki asettaa vaatimuksia työntekijöiden henkilötietojen käsittelylle. Laissa yksityisyyden suojasta työelämässä (759/2009) säädetään, että työnantajan on säilytettävä hallussaan olevat työntekijän terveydentilaa koskevat tiedot erillään muista keräämistään henkilötiedoista. Terveydentilaa koskevat tiedot on poistettava välittömästi sen jälkeen, kun käsittelylle ei ole 1 momentissa tarkoitettua perustetta (4 §). EU:n yleisessä tietosuoja-asetuksessa korostetaan riskiperusteisuutta. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi (GDPR 32.2.). Riskiä arvioidaan rekisteröityjen ihmisten kannalta. Tiedot, joiden käsittely voi aiheuttaa rekisteröityjen ihmisten kannalta erityisen riskin, on tunnistettu. Tällaisia tietoja ovat ainakin turvakiellon alaiset kotiosoitteet, henkilötunnukset, joiden vuotaminen aiheuttaa riskin identiteettivarkauksille ja petoksille; sairauspoissaolotiedot, myös pelkät päivien lukumäärät, jotka kuvaavat ihmisen terveydentilaa sekä ulosottotiedot, jotka kuvaavat ihmisen taloudellista asemaa.

Tietosuojalaki (1050/2018) täsmentää ja täydentää EU:n yleistä tietosuoja-asetusta ja sen kansallista soveltamista. Laissa säädetään muun muassa henkilötietojen käsittelystä eräissä tapauksissa sekä tietosuojaa valvovasta viranomaisesta.

Hallintolaissa (434/2003) säädetään hyvän hallinnon perusteista ja hallintoasiassa noudatettavasta menettelystä. Lakiin sisältyy säännökset muun muassa asian vireillepanosta ja käsittelystä sekä päätöksen tiedoksiannosta. Hallintolaissa säädetään myös menettelystä oikaisuvaatimuksen käsittelyssä.

Julkisuuslaki (621/1999) 1 §:n mukaan viranomaisen asiakirjat ovat julkisia, jollei julkisuuslaissa tai muussa laissa erikseen toisin säädetä. Julkisuuslaissa säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassa pidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista samoin kuin viranomaisten velvollisuuksista tämän lain tarkoituksen toteuttamiseksi. Julkisuuslaki on viranomaistoimintaa säätelevä yleislaki, joiden lainkohdissa on tarkemmin säädetty muun muassa tietojen luovutuksesta ja salaamisesta. Talous- ja henkilöstöhallinnossa on muun muassa huomioitava Julkisuuslain 24 §:n kohdissa esimerkiksi 5, 7-10, 20, 23, 25, 29 ja 31 tarkoitetut asiakirjat tai tiedot. Julkisuuslain 24 § 1 momentin 32 kohdassa säädetään tiedoista, joiden salassapidon perusteena on yksityiselämää koskevat tiedot ja henkilökohtaiset olot. Tietosuoja-asetuksessa säädetään erityisistä henkilötietoryhmistä, jotka voivat olla salassa pidettäviä muidenkin julkisuuslain 24 § 1 momentin kohtien mukaan. Julkisuuslaki on parhaillaan uudistettavana.

Julkisen hallinnon tiedonhallintalaki (906/2019, TihL tai tiedonhallintalaki) on julkisen hallinnon tiedonhallintayksiköitä velvoittava laki, jossa kuvataan miten tietoja tulisi käsitellä ja kuvata. Tiedonhallintalain tarkoituksena on varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi. Lisäksi siinä määritellään viranomaisten tietoaineistojen turvallinen ja tehokas hyödyntäminen, jotta viranomainen voi hoitaa tehtävänsä ja tarjota palvelunsa hyvää hallintoa noudattaen tuloksellisesti ja laadukkaasti, kuin myös edistää tietojärjestelmien ja tietovarantojen yhteentoimivuutta. Tiedonhallintalaki koskettaa kaikkea viranomaistoimintaa kuten esimerkiksi yleishallintoa, henkilöstöhallintoa, asianhallintaa, asiakirjahallintoa, arkistointia, kehittämistä, kokonaisarkkitehtuuria, sisäistä tarkastusta, tietohallintoa, tietosuojaa ja tietoturvaa. Tiedonhallinnan järjestämisessä on olennaista riskienhallintaperusteisesti suunnitella keskeiset toimet ja tietoturvallisuustoimenpiteet. Tiedonhallintalain 18 §:ssä säädetään turvallisuusluokiteltavista asiakirjoista valtionhallinnossa. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä julkisuuslain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle. Tiedonhallintalain 18 §:n 4 momentin nojalla annetussa *turvallisuusluokitteluasetuksessa (1101/2019)* on säädetty tarkemmin asiakirjojen turvallisuusluokittelusta ja turvallisuusluokiteltujen asiakirjojen käsittelystä.

Talous- ja henkilöstöhallinnon asiakirjat ovat osa viranomaisen arkistoa. *Arkistolaki (831/1994)* pitää sisällään arkistointiin liittyviä säännöksiä. Asiakirjojen säilytysaikojen määrääminen ja tarpeettoman aineiston hävittäminen kuuluvat viranomaisen arkistotoimen tehtäviin. Kansallisarkisto taas määrää, mitkä asiakirjat tai asiakirjoihin sisältyvät tiedot säilytetään pysyvästi. Tiedon luokitukset ja käyttörajoitukset ovat tärkeitä myös arkistovaiheessa, mutta salassapito pitää myös pystyä purkamaan, kun salassapitoaika umpeutuu.

Viranomaisen tietojärjestelmien turvallisuutta voidaan arvioida viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1406/2011), ns. *arviointilaki*, mukaisilla arvioinneilla. Lisätietoja arviointi- ja hyväksymisprosessista löytyy ohjeesta ”Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit”.

Talousarviolain (Laki valtion talousarviosta 423/1988) mukaisesti Valtiokonttori määrää ne viraston tai laitoksen palkanlaskentaa koskevat tehtävät, jotka hoidetaan keskitetysti ja joista vastaa keskitettyjä taloushallintotehtäviä hoitava virasto tai laitos. Talousarviolaki ja -asetus koskee taloustietoja, mutta niiden lisäksi myös kirjanpitolaki koskee taloustietoja ja myös Valtiokonttorin määräykset ja ohjeet on huomioitava taloustietojen osalta. Taloustietojen avoimuuteen vaikuttavat myös hankintalaki (1397/2016), verotukseen liittyvä lainsäädäntö (esim. tuloverolaki; 1535/1992) ja valtionavustuslaki (688/2001). Kaikissa näissä on vaateita julkaista tietoa avoimesti ja moni näistä päätyy sitten erinäisiin ”tietopankkeihin”, vaikka käsittelyjärjestelmä olisi eri. Tarpeen on tunnistaa ja määritellä, kenelle kuuluu vastuu tietojen kasaantumisesta, kun käsittely ei tapahdu yhdessä järjestelmässä. Taloustietoja päätyy esimerkiksi julkisiin palveluihin kuten tutkihallintoa.fi, tutkihankintoja.fi tai tutkiavustuksia.fi.

Valtion talous- ja henkilöstöhallinnon palvelukeskus Palkeet toimii keskitettyjä taloushallinnontehtäviä hoitavana virastona. Palkeilla on talousarviolain 12 b §:n mukaisesti salassapitosäännösten estämättä

oikeus saada kirjanpitoyksiköihin kuuluvilta virastoilta ja laitoksilta ja muilta toimielimiltä tehtäviensä hoitamiseksi välttämättömät salassa pidettävät asiakirjat lukuun ottamatta julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) tai sen nojalla annettujen säännösten nojalla luokiteltuja turvallisuusluokan I, II ja III asiakirjoja tai muita sellaisia salassa pidettäviä asiakirjoja, joihin sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää tai erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle. Jos esimerkiksi valtion talous- ja henkilöstöhallinnon palvelukeskus Palkeilla ei ole talousarviolain mukaan oikeutta saada välttämättömiä tietoja sille määrättyjen tehtävien hoitamiseksi, kyseisestä tehtävästä vastaa Palkeiden sijasta asianomainen kirjanpitoyksikkö, elleivät Palkeet ja kirjanpitoyksikkö taloushallintotehtävän hoitamisesta toisin sovi.

NI2-direktiviin myötä palveluiden kyberturvallisuudelle asetetaan EU:n laajuiset minimivaatimukset. Valtion pilvipalvelulinjauksissa on todettu, että EU-lainsäädäntö saattaa yksittäistapauksissa asettaa rajoitteita globaalien pilvipalveluratkaisujen käytölle. Esimerkiksi datanhallinta-asetuksen (Euroopan parlamentin ja neuvoston asetus (EU) 2022/868, annettu 30 päivänä toukokuuta 2022, eurooppalaisen datan hallinnoinnista ja asetuksen (EU) 2018/1724 muuttamisesta) mukaista suojattua dataa ei saa siirtää kolmanteen maahan eikä siihen saa päästä käsiksi kolmannesta maasta, jos siirto tai pääsy olisi ristiriidassa unionin lainsäädännön tai kansallisen lain kanssa. Samoin *EU:n digi- ja datasääntelyssä* asetetaan tietoturvaan ja tietosuojaan liittyviä vaatimuksia, joihin on hyvä varautua ennakkoon.

Viranomaisten hallussa olevaa tietoa koskevia säännöstöjä on paljon. Muun muassa *Sähköisen viestinnän palveluista annetussa laissa (917/2014)* asetetaan rajoituksia sille, kuinka ja missä laajuudessa verkkoliikennettä voidaan valvoa viestinnän luottamuksellisuus ja yksityisyyden suoja säilyttäen. Lain asettamat vaatimukset tulee huomioida määriteltäessä ja otettaessa käyttöön tiedon käsittelyyn liittyviä riskienhallintatapoja ja -keinoja. Lisäksi talous- ja henkilöstöhallinnon tietoihin sovellettavia säännöksiä löytyy *Valmiuslaista* (1552/2011), *Nimikirjalaista* (1010/1989), *Työsopimuslaista* (55/2001), *Valtion virkamieslaista* (750/1994), EU:n tietoturvasäätelystä ja valmisteilla olevat NIS2 ja CER-laeista. Yhteiskunnan kriittisen palveluiden häiriönsietokykyyn liittyvää CER-direktiiviä ja niiden vaikutusta pilvipalveluihin on tärkeä huomioida ennakkoon.

Valtiovarainministeriön tuottama riskienhallinnan käsikirja (Riskienhallinnan käsikirja valtionhallinnon toimijoille) antaa kattavat ohjeet tietoaineistojen luokittelua varten.

Talous- ja henkilöstöhallinnon tiedon käsittelyssä voidaan hyödyntää mm. julkisen hallinnon tietoturvallisuuden arviointikriteeristöä (Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) : Suositus ja kriteeristö) ja pilvipalveluiden turvallisuuden arviointikriteeristöä (PiTuKri) (Pilvipalveluiden turvallisuuden arviointikriteeristö) . PiTuKri on liikenne- ja viestintävirasto Traficomin ohjeellinen kriteeristö, joka soveltuu salassa pidettävän ja turvallisuusluokka IV:n tietojen käsittelyyn pilvipalveluissa. Ko. ohje sisältää myös teknisiä kriteerejä. Arviointikriteeristöt tukevat osaltaan koko julkishallinnon tietoturvallisuuden kehittämisen ja arvioinnin tarpeita. Kriteeristöjä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä. Meneillään oleva Cirrus-hankkeessa tuotetaan riskienhallintaan liittyviä mallipohjia, joita voi arvioinnissa hyödyntää.

Valtiovarainministeriö on antanut suosituksen tiedonhallintalain vaatimasta tiedonhallintamallista. Suositus tukee kirjanpitoyksiköitä kuvaamaan sekä hallinnoimaan kokonaiskuvaa tietojen siirtymisestä eri toimijoiden välillä. Tiedonhallintamalli antaa kirjanpitoyksiköille perusrakenteet, jolla varmistetaan, että oikea tieto on oikeaan aikaan oikeassa paikassa oikein koostettuna ja muodostettuna oikeiden henkilöiden välillä. Tiedonhallintamallia on ylläpidettävä aina, kun tiedonhallintayksikön tiedonhallinnassa tapahtuu muutoksia, jotka vaikuttavat sen sisältöön.

3. Julkinen tieto, salassa pidettävä tieto ja turvaluokiteltu tieto

Valtiovarainministeriön tiedonhallintalautakunnan antama Suositus salassa pidettävien asiakirjojen käsittelystä pitää sisällään lainsäädännön vaatimuksia, suosituksia sekä käytännön esimerkkejä salassa pidettävien asiakirjojen käsittelystä. Suosituksessa on esitetty tietojen käsittelylle säädettyjä vaatimuksia sekä hyviä käytäntöjä, joita viranomaiset voivat hyödyntää tietojen käsittelyä koskevien toimenpiteiden toteuttamisessa sekä käsittelyä koskevissa ohjeissaan. Suositus salassa pidettävien asiakirjojen käsittelystä kuvaa suhdetta Valtiovarainministeriön suositukseen turvallisuusluokiteltavien asiakirjojen käsittelystä (Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä) seuraavasti: ”*Suositukset sisältävät turvallisuusluokiteltujen asiakirjojen käsittelyä koskevia suosituksia, joita suositellaan sovellettavaksi riskilähtöisesti ja tilannekohtaista harkintaa käyttäen myös salassa pidettävien tietojen käsittelyssä”* ja ”*salassa pidettävät tiedot voivat myös sisältää turvallisuusluokiteltavia tietoja, jotka on jaettu eri turvallisuusluokkiin.”* Asiakirjassa suositellaan lisäksi, että ”*organisaatiot arvioivat, mitkä turvallisuusluokan TL IV tasolle luokiteltujen tietojen tietoturvallisuustoimenpiteistä ovat tarpeellisia myös organisaation salassa pidettäville tiedoille”.*

Valtionhallinnon tietoja luokitellaan eri turvallisuusluokkiin kunkin eri kirjapitoyksikön toiminnan asettamista tarpeista lähtien, kuitenkin sen mukaan miten tiedonhallintalain 18 §:ssä tai sen nojalla annetuissa säännöksissä säädetään. Valtiovarainministeriön suosituksessa turvallisuusluokiteltavien asiakirjojen käsittelystä (2021:5) kuvataan seuraavaa ”*Erilaisiin tietoaineistoihin kohdistuu erilaisia riskejä. Esimerkiksi viranomaisten turvallisuusluokitellut tiedot ovat yleensä miellettävissä valtion turvallisuuden (yleisen edun) näkökulmasta suojattaviksi. Turvallisuusluokiteltuihin tietoihin voidaan toisaalta usein olettaa kohdistuvan eri tahojen kiinnostus, kuin esimerkiksi turvallisuusluokittelemattomiin henkilötietoihin. Riskien eroavaisuus tulee huomioida myös salausratkaisujen valinnassa.”* Valtiovarainministeriön salassa pidettävien asiakirjojen käsittelystä annetun suosituksen (2023:4) mukaan ”*Henkilötiedot eivät ole salassa pidettäviä, ellei niitä laissa tai asetuksessa ole erikseen säädetty salassa pidettäväksi. On kuitenkin huomioitava, että tietosuojasääntelystä tulee lisävaatimuksia henkilötietojen suojaamisen osalta. Osa erityisiin henkilötietoryhmiin kuuluvista tiedoista on julkisuuslain mukaan 24 § 1 momentin mukaan salassa pidettäviä. Organisaation tuleekin tunnistaa, mitä tietoja se käsittelee ja mitkä säädökset kyseisiä tietoja koskevat. Tietojen tunnistamisella ja luokittelulla voidaan helpottaa tietoturvaan liittyvien investointien priorisointia. Salassa pidettävät tiedot vaativat lisäsuojaustoimia verrattuna julkisiin tietoihin.”* Esimerkiksi TL-luokiteltujen tietojen osalta on suositeltu, että tallentaminen ilman salausta on hyväksyttävää, jos palvelussa käytetään vahvaa tunnistautumista. Vaikka esimerkiksi erityisiin henkilötietoryhmiin liittyvä tieto on julkista, niihin voi liittyä tietosuojanäkökulmia, joiden huomioiminen on

tarpeen kokonaisuutta arvioitaessa ja suunniteltaessa muun muassa ay-jäsenyys, siviilipalvelus, perhevapaat.

Turvallisuusluokiteltujen tietojen suojaaminen perustuu riskienhallintaan, jonka perusteella turvatoimet suunnitellaan. Kirjanpitoyksikön tuleekin oman riskiarvioinnin keinoin varmistaa, että asiakirjat turvallisuusluokitellaan asianmukaisesti. Yli- ja aliluokittelun välttämiseksi tulee organisaation tuntea omaan toimialaansa liittyvä erityissääntely sekä huolehtia henkilöstön salassapito- ja turvallisuusluokittelusääntelyn osaamisesta.

4. Riskienhallinta

Valtionhallinnon eri tiedonomistajien on tärkeä tiedostaa talous- ja henkilöstöhallinnon tiedoista muodostuva kokonaisuus. Yleisesti kuvattuna, tieto koostuu kirjanpitoyksiköiden tiedoista, jotka siirtyvät yhteisesti käytössä olevissa talous- ja henkilöstöhallinnon eri tietojärjestelmissä tai kirjanpitoyksiköiden omista tietojärjestelmistä palvelukeskuksen käsiteltäväksi. Lopputuotoksena syntyvät palkanlaskentaan ja taloushallintoon liittyvät suoritteet, joista siirtyy tietoa edelleen esim. tilinpäätökseen, kirjanpitoon, verottajalle, Kansaneläkelaitokselle sekä yksityisen sektorin eri toimijoille, esimerkiksi pankeille ja vakuutusyhtiöille.

Tiedon luokittelua voidaan käyttää riskien hallinnassa muun muassa tietoaineistoon liittyvien vaatimusten tunnistamiseen ja käsittelyrajoitusten osoittamiseen, riskien arviointiin ja tietoturvallisuusvaatimusten määrittelyyn. Lähtökohtana on, että keskitettyihin järjestelmiin voidaan tuoda kaikki julkiset tiedot ja myös salassa pidettävät tiedot sekä TL IV-luokan tiedot.

Riskienhallintaprosessi koostuu toimintaympäristön määrittämisestä, riskien arvioinnista (tunnistaminen, analysointi, merkityksen arviointi), riskien käsittelystä, riskien hyväksynnästä, riskejä koskevasta viestinnästä ja tiedonvaihdosta sekä riskien seurannasta ja katselmoinnista. Tiedon luottamuksellisuuden lisäksi on tärkeää tunnistaa tiedon eheyteen ja saatavuuteen liittyvät riskit.

Tiedon luokittelu tehostaa riskien hallintakeinojen käyttöä ja siten myös tietosuojatoimenpiteiden vaikutuksia. Kuvan 1 mukaisesti valtion talous- ja henkilöstöhallinnon toimintaympäristön riskien hallintakeinoja voidaan tarkastella kolmesta eri näkökulmasta; tiedon, tiedon käsittelijän ja tiedon käsittely-ympäristön näkökulmista. Kuva ja sitä tukevat lyhyet selitteet eivät ole tyhjentäviä listauksia riskien hallintakeinoista.

Kuva 1. Valtion talous- ja henkilöstöhallinnon toimintaympäristön riskien hallintakeinoja (mitigointikeinoja).

Alla lyhyet selitteet kuvassa (Kuva 1.) oleville erilaisille riskien hallintakeinoille.

Tieto

- Karkeistus: tieto karkeistetaan sellaiselle tasolle, jolla sen taltioiminen keskitettyyn tietojärjestelmään on mahdollista tai sen käsittelyprosessi eri tahojen ja henkilöiden toimesta on mahdollista.
- Lukotus: osassa tietojärjestelmiä tietoa voidaan suojata erillisillä lukoilla, jolloin tiedon näkevät vain ”avaimenhaltijat”.
- Organisaatiorajaukset ovat käytössä kaikissa yhteisissä järjestelmissä ja palveluissa. Tieto - luonti, pääsy, käsittely, muutokset, poistot - rajataan organisaatioittain. Perusolettamana on yleensä kirjanpitoyksikkökohtainen rajaus esim. kirjanpito, tai työantajavirasto esim. palkat.
- Tiedon säilytysajoilla määritellään ja kuvataan tiedon säilytysaikoja.

Tiedon käsittelijä (henkilötietojen käsittelijä)

- Vähimmäisoikeuksien periaatteen mukaisesti käyttäjälle myönnetään aina vain sellaiset oikeudet, joita hän tehtävänsä suorittamisessa tarvitsee.
- Käyttövaltuushallinta: käyttövaltuudet ja -oikeudet myönnetään aina henkilökohtaisesti, käyttövaltuudet myönnetään rooli- ja tehtäväkohtaisesti, kun se teknisesti on mahdollista. Käyttövaltuuksien säännöllinen validointi (tehtävien muuttuessa, henkilöt lähtiessä jne.). Käyttövaltuuksien haku ja myöntö tehdään ohjatusti vain nimettyjen tahojen toimesta (kontrolloitu prosessi).
- Identiteetinhallintaa hallinnoidaan mm. toimikorteilla, Kieku-numerolla, vahvalla tunnistautumisella.

- Ohjeistuksilla ja koulutuksilla varmistetaan tiedon käsittelyiden (virkamiehet/käyttäjät/henkilöt) osaamista.
- Tiedon luovuttamiseen liittyvät ohjeistukset ja koulutukset, joilla varmistetaan (virkamiehet/käyttäjät/henkilöt) osaaminen.

Tietojen käsittely-ympäristö

- Tiedonsiirrot: yhteyksien varmistaminen, salaus, varajärjestelyt, suojaaminen, esim. virukset yms. saastuminen.
- Valvonta: esim. palvelu on käytettävissä kuten suunniteltu, epäilyttävän liikenteen jatkuva skannaus.
- Pääsynhallinta: kontrollit kuten esimerkiksi käyttäjätunnusten ja salasanojen säännöstöt ja validoinnit, pääsy vain sallituista paikoista, esim. vain tietystä verkosta tai vain tietyistä fyysisistä paikoista.
- Arvioinnit: tietoturva-arvioinnit, tietosuojan vaikutusten arviointi, riskiarvioinnit.
- Tekniset ratkaisut: salausalgoritmit, tietoliikenteen salaaminen, avaintenhallinta, jatkuvuuden turvaamisen ratkaisut, esim. kahdennukset, hajautukset, turvasatamat, varmistukset.

Tiedon hävittäminen: prosessit ja menetelmät tiedon arkistoinnille tai poistamiselle/tuhoamiselle, kun säilytysaika päättyy. Valtion talous- ja henkilöstöhallinnossa käsitellään tietoja, joihin liittyy sekä velvoitteita että valvontaa. Talous- ja henkilöstöhallinnossa tietosuojaan ja -turvaan liittyvät säännökset ovat keskeisiä, sillä talous- ja henkilöstöhallinnossa käsitellään muun muassa henkilöstön terveystietoja tai muita luottamuksellisia tietoja. Tiedon luottamuksellisuuden lisäksi on tärkeää tunnistaa tiedon eheyteen ja saatavuuteen liittyvät riskejä mm. tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja vaaditulla tavalla, tietoa ei ole muutettu luvatta tai että se ei ole muuttunut vahingossa ja että mahdolliset muutokset voidaan todentaa. Esimerkiksi riskitarkastelussa on myös hyvä arvioida miten riskiä salassa pidettävän tietojoukon päätymisestä tahoille, jolle sen ei kuuluisi päätyä, voidaan pienentää tai arvioida tietojärjestelmässä olevan tietoturva-aukon vuoksi riskit tiedon paljastumisen seurausvaikutuksista.

Riskienhallintakeinoilla ja -toimilla tähdätään joko riskin poistamiseen, pienentämiseen tai riskin toteutumisen vaikutusten pienentämiseen. Tunnistettuihin riskeihin liittyvät hallintakeinot ja -tavat liittyvät usein tietojen käsittelyyn, käyttöön ja luovuttamiseen. Myös tietojen arkistointiin ja tietojen poistamiseen sekä hävittämiseen liittyvät riskit tulee tunnistaa.

Tietosuojaan liittyviä riskejä voidaan hallinnoida esimerkiksi tietosuojaan liittyvillä sopimusliitteillä. Tietosuojaliitteen sisältö määräytyy hyvin pitkälle tietosuoja-asetuksen 28 artiklan vaatimuksista. Asetus edellyttää siten henkilötietojen käsittelijän suorittaman käsittely määrittämistä sopimuksella tai muulla vastaavalla sitovalla oikeudellisella asiakirjalla. Sisältö kattaa ne osa-alueet, jotka jäävät teknisten toimenpiteiden ulkopuolelle. Riskejä madaltavia toimenpiteitä ovat tietosuojaliitteen sijasta ensisijaisesti

tekniset tietoturvatoimenpiteet, fyysisten toimitilojen turvallisuuteen liittyvät toimenpiteet sekä hallinnolliset tietoturvatoimenpiteet, kuten koulutus, ohjeistus, tiedotus ja dokumentointi.

Talous- ja henkilöstöhallinnon tiedon käsittelyn riskipohjainen tarkastelu tulee tehdä toimintalähtöisesti ja hallinnointikeinot huomioiden. Virasto tai laitos itse päättää jäännösriskeistä mitä ovat valmiita hyväksymään. Ei-hyväksyttävän jäännösriskin osalta tieto on karkeistettava sallitulle tasolle ja sallittu taso pitäisi määritellä talous- ja henkilöstöhallinnon osalta prosessi- ja tietojärjestelmäkohtaisesti. Salassa pidettävän ja turvaluokitellun tiedon käsittelyyn tarkoitettujen tieto- ja käsittelyjärjestelmien osalta tulisi arvioida mahdollinen tarve hyödyntää teknisiä kriteeristöjä järjestelmien tietoturvallisuuden arvioinnissa. Muodostettavaa, luokiteltavaa tietoa ja luokitteluperiaatteita varten on tärkeää tunnistaa suojattavat kohteet, vastuut ja velvollisuudet, vaatimuksenmukaisuus, tietoturva, riskienhallinta ja elinkaaren hallinta. Tiedon luokittaminen ei saa muodostaa estettä tietojen myöhemmälle hyödyntämiselle mm. arkistoinnin yhteydessä.

Riskien hallintakeinona tulee ottaa huomioon pakollisena vaatimuksena myös henkilötietojen käsittelyn riittävä lokitietojen käsittely. ”Lokitus” tulee toteuttaa EU-oikeuskäytännön mukaisesti rekisteröityjen oikeudet huomioiden Laki julkisen hallinnon tiedonhallinnasta (906/2019) 17 § mukaisesti. EU-tuomioistuimen ratkaisun C 579/21 mukaan lokimerkinnöistä tulisi selvitä henkilötietojen käsittelyn tarkastelun ajankohta ja tarkoitukset. Lisäksi yksi tietojen hallintakeino on henkilötietojen pseudonymisointi.

Suunnitteluvaiheessa tulee arvioida huolellisesti mm. lainsäädäntöjohdannaiset riskit, joka edellyttävät erityistä huolellisuutta tiedon suojaamisen suunnittelussa valtionhallinnon pilvilinjausten mukaisesti. Lainsäädäntöjohdannaisilla riskeillä tarkoitetaan esimerkiksi eri maiden lainsäädännössä mahdollisesti olevia säännöksiä, jotka voivat velvoittaa pilvipalveluntuottajaa tai muuta henkilötietojen käsittelijää toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suoran tai epäsuoran pääsyn palveluun tai järjestelmään tallennettuihin tietoihin. Lainsäädäntöjohdannaisten riskien tunnistamiseen ja tietoturvalliseen hallitsemiseen velvoittavaa lainsäädäntöä sisältyy lakiin viranomaisen toiminnan julkisuudesta (621/1999), lakiin julkisen hallinnon tiedonhallinnasta (906/2019) ja asetukseen asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) sekä tietosuojalainsäädäntöön. Lainsäädäntöjohdannaisten riskien huomioiminen on merkityksellistä erityisesti turvallisuusviranomaisen tietojen käsittelyn näkökulmasta. Esimerkiksi käsiteltäessä poliisin henkilötietomassaa on huomioitava, että se sisältää myös ns. erityisiä henkilöstöryhmiä.

Erityisen merkityksellinen on yleisen tietosuoja-asetuksen V luvun mukainen velvollisuus varmistua siitä, että organisaation rekisterinpito – tai käsittelyvastuulle kuuluvia henkilötietoja ei siirretä EU/ETA-alueen ulkopuolelle siten, että henkilötietojen tietosuojan taso siirron myötä vaarantuisi. Tietojen siirto EU/ETA-alueen ulkopuolelle edellyttää muiden tietosuojalainsäädännön vaatimusten noudattamisen lisäksi erityistä siirtoperustetta, jotka määritellään tietosuoja-asetuksen V luvussa. Varmistuminen edellyttää sen tunnistamista, millaisia riskejä rekisteröidylle mihinkin valtioon siirrettäessä aiheutuu. Koska näitä riskejä voidaan hallita osin tietoturvallisuustoimenpitein, ja koska kolmasmaasiirrot ja niiden osalta tehtävät selvitykset palvelevat osaltaan myös lainsäädäntöjohdannaisten riskien tunnistamista ja hallintaa, liittyvää vastuujakoa muun ohella siirtovaikutusarviointien (TIA) tekemisen osalta.

Tiedon kasaumavaikutus

Tietojen kasautumisvaikutuksen tapauskohtainen arviointi edellyttää aina kyseessä olevan tietovarannon nykyisen ja arvioidun tulevan asiasisällön selvittelyä ja arviota siitä, onko asiakirja tai tieto sekä siihen liittyvä tietokasauma turvallisuusluokiteltava ja mahdollisesti mille tasolle. Jokin tietoalkioiden joukko voi kuitenkin muodostaa yhdistettynä tietokasauman, jonka joutuminen ulkopuolisten käsiin voisi aiheuttaa vahinkoa esimerkiksi maanpuolustukselle, huoltovarmuudelle tai poikkeusoloihin varautumiselle. Tällaisen tietokasauman asiasisältö saattaisi olla myös valtion turvallisuuden (yleisen edun) näkökulmasta suojattavaa ja turvallisuusluokittelun perusteet täyttävää.

Erityisesti turvallisuusviranomaisissa tulee kiinnittää huomiota henkilöstön tietojen luokitteluun eri tietoaineistoympäristöissä ja tietoyhdistelmissä sekä niiden julkistamisessa ja luovuttamisessa. Eli yksittäisenä tietona tieto voi olla JulkL 1 §:n mukaisesti julkista, mutta kasaumavaikutuksen vuoksi (esimerkiksi yhdistelemällä tietoja eri tietosisällöistä; nimi, toimipaikka ja työtehtävä tai sotilasarvo tms.) tieto voi muodostua salassa pidettäväksi tai harkinnanvaraisesti luovutettavaksi, mikä on otettava huomioon tietoa käsiteltäessä ja sitä luokiteltaessa.

Salassapidon ja turvallisuusluokittelun tulee kuitenkin aina perustua lakiin, eikä asiakirjoja voi määritellä salassa pidettäväksi tai turvallisuusluokitelluksi ilman lainmukaista perustetta. Tieto voi kuitenkin muuttua ja tiedon arviointi sekä sen luokitus on syytä pysyä ajassa mukana. Ja vaikka tieto pysyisi samana, niin luokitus voi muuttua, kun alkuperäinen salausperuste poistuu.

Talous- ja henkilöstöhallinnon tietoja voidaan käsitellä turvallisesti TL IV- turvallisuusluokkaan määritellyissä tietojärjestelmissä. Mikäli talous- ja henkilöstöhallinnon tietoihin ei sisälly turvallisuusluokiteltuja tietoja, ei niiden käsittelyyn käytettävältä tietojärjestelmältä tarvitse edellyttää hyväksyntää TLIV-tason tietojen käsittelyyn.

Ehdotonta lainsäädännöllistä estettä ei ole sijoittaa TLIV-tietoja julkisiin pilvipalveluihin. Turvallisuusluokan IV asiakirjoja ja tietoja voidaan käsitellä julkisessa pilvipalvelussa, kunhan tietoturva, tietosuoja ja jatkuvuudenhallinta on turvaluokan vaatimuksenmukaisesti toteutettu, todennettu ja käyttöönotettu tiedonhallintayksikön tai kirjanpitoyksikön johdon riskiperusteisella päätöksellä. Julkisessa pilvessä syntyvä tietojen kasauma tulee aina käsitellä tapauskohtaisesti ja tiedon määrästä riippumatta kohteeseen soveltuvalla riski- ja vaikutuksenarvioinnilla.

5. Johtopäätökset ja suositukset

Työn tavoitteena on luoda suositukset talous- ja henkilöstöhallinnon tiedon luokitukselle, jotka antavat kirjapitoyksiköille ja palvelukeskukselle suuntaa yhtenäisten prosessien ja yhteisten tietojärjestelmien käyttämiselle sekä luo perustaa riskienhallinnan kehittämiseen ja jäännösriskien asianmukaiseen arviointiin. Perustan tiedon luokittelulle muodostavat lakien ja säännösten noudattaminen.

Suositukset kuvaavat pilvipalveluihin siirtymiseen liittyviä varautumistekijöitä, mutta myös perinteisissä on premise -ratkaisuissa huolehdittavista asioista, jotka kirjanpitoyksiköiden on syytä ennakoida ja sisällyttää osaksi siirtymisprosessia. Erityisesti varautumiseen liittyen, keskeisten talous- ja henkilöstöhallinnon

tietojärjestelmien pilvisiirtymässä tulee ottaa tarkasteluun samanaikaisesti ns. turvasatama-konseptin mukaiset tai samankaltaiset ratkaisut.

Talous- ja henkilöstöhallinnon yhteisissä tietojärjestelmäratkaisuissa palvelun tuottaja vastaa suojauskeinoista ja jatkuvuudesta tietojärjestelmien osalta. Yhteisissä tietojärjestelmissä palveluntuottaja tai kirjanpitoyksikkö omien erillisten tietojärjestelmien osalta käyttää tiedon hallinnointikeinoina esimerkiksi tietojärjestelmään tehtävillä salassapitomerkinnöillä, käyttövaltuushallinnalla, käyttäjärajauksilla, erilaisilla koodauksilla, tietoa karkeistamalla sekä hajauttamalla tieto eri tietojärjestelmiin (Kuva 1). Esimerkiksi käyttäjien käyttöoikeuksien hallinta ja ajantasaisuuden varmistaminen säännöllisesti ovat osa viraston sisäistä valvontaa ja riskienhallintaa. Lisäksi riskienhallintakeinoina voivat toimia palvelun koko elinkaaren aikainen riskienarviointi, henkilöstön koulutus sekä korvaavien hallintakeinojen arviointi ja suunnittelu häiriötilanteita varten.

Valtiovarainministeriö suosittaa talous- ja henkilöstöhallinnon tietojen luokitteluun seuraavanlaisesti:

1. Virasto tai laitos tunnistaa toimintaansa ja palveluihinsa liittyvät ICT-varautumista ohjaavan kansallisen ja EU-lainsäädännön sekä muut ICT-varautumiseen liittyvät normit, ja huomioi oman toimintansa erityispiirteistä nousevat tarpeet. Erityisen tärkeää on, että sekä palvelua hankkiva, että palvelua tuottava organisaatio tuntevat tietojärjestelmiin ja palveluihin vaikuttavat määräykset ja pitävät toisensa näistä tietoisina.
2. Virasto tai laitos arvioi olennaiset talous- ja henkilöstöhallinnon tietoihin kohdistuvat riskit ja dokumentoi ne. Tässä yhteydessä tarkoitetaan riskien arviointia ja siihen perustuvaa päätöksentekoa, joka kohdistuu yhteisessä tietojärjestelmässä olevaan tietoon ja niiden käsittelyyn sekä mahdollisiin tietoon liittyviin riskienhallintatoimiin. Riskienhallintatoimenpiteet mitoitetaan riskiarvioinnin perusteella riskien toteutumisen vaikuttavuuden ja todennäköisyyden mukaisesti. Riskienhallinta tulee suunnitella ja ohjeistaa siten, että siinä käsitellään systemaattisesti ja suunnitelmallisesti erilaisia tiedonhallintaan ja tietoturvallisuuteen liittyviä riskejä (mm. SFS:ISO 31000 Riskienhallinta –standardin ja Riskienhallinnan käsikirja valtionhallinnon toimijoille mukaisesti).
3. Talous- ja henkilöstöhallinnon keskitettyihin tietojärjestelmiin voidaan tuoda korkeintaan TLIV-tason tietoja. Yksittäisenä tietona tieto voi olla JulkL 1 §:n mukaisesti julkista, mutta tietokokonaisuus voi muodostua salassa pidettäväksi tai harkinnanvaraisesti luovutettavaksi, mikä on otettava huomioon tietoa käsiteltäessä. Pelkkä kasaumavaikutus ei kuitenkaan ole peruste tietojen salassapidolle tai turvallisuusluokittelulle, vaan salassapidon ja turvallisuusluokittelun tulee aina perustua lakiin. Tieto voi kuitenkin muuttua ja tiedon arviointi ja sen luokitus on syytä pysyä ajassa mukana. Julkisuuden rajoitus saattaa tarkoittaa sitä, että tiedon luokitus voi muuttua TLIV-III salassapidon ja turvaluokituksen perusteella osittain salassa pidettäväksi tai kokonaan salassa pidettäväksi. Jokainen tiedon omistaja arvioi oman riskienhallintakeinojen mukaisesti kyseisen tietoluokkamuutoksen tarpeellisuuden, lainsäädäntöperustan sekä vastaa yhteisten tietojärjestelmien ulkopuolella olevien tietojen käsittelyn asianmukaisuudesta ja kustannuksista.

   Kasaumavaikutusten arviointi on tehtävä tapauskohtaisesti riski- ja vaikutusten arvioinnin keinoin tiedon määrästä riippumatta, sillä tietosuoja-asetus ei tee eroa yksittäisen henkilötiedon tai kasautuneen tiedon välillä. Yleinen tietosuoja-asetus tunnistaa kuitenkin suuresta

henkilötietomäärästä koostuvan datan, johon tulee soveltaa suojausmenetelmiä. Julkisessa pilvessä syntyvä tietojen kasauma tulee aina käsitellä tapauskohtaisesti kohteeseen soveltuvalla riski- ja vaikutuksenarvioinnilla. Kasaumavaikutusten arvioinnissa olennaista on, että yksittäisiä tietoja yhdistelemällä voi muodostua tietoa, jolla on merkitystä riskienhallinnan näkökulmasta.

4. Talous- ja henkilöstöhallinnon tiedot tulee suojata riskienhallintakeinoilla. Talous- ja henkilöstöhallinnon yhteisissä tietojärjestelmäratkaisuissa palvelun tuottaja vastaa suojauskeinoista ja jatkuvuudesta tietojärjestelmien osalta. Hallintakeinoina käytetään esimerkiksi tietojärjestelmään tehtäviä tarvittavien asiakirjojen salassapitomerkintöjä, käyttövaltuushallintaa, käyttäjärajauksia, erilaisia koodauksia, tiedon karkeistamista sekä hajauttamista tieto eri tietojärjestelmiin (katso kuva 1). Lisäksi riskienhallintakeinoina voivat toimia palvelun koko elinkaaren aikainen riskienarviointi, henkilöstön (sekä viraston ja laitoksen, palvelukeskuksen että sen toimittajien) koulutus sekä korvaavien hallintakeinojen suunnittelu häiriötilanteita varten. Riskien hallintakeinoista organisaatioilla on tärkeää olla omat ohjeet.

Jakelu	ministeriöt, virastot ja laitokset Palkeet Valtiokonttori
Tiedoksi	Kansliapäällikkö Juha Majanen Alivaltiosihteeri Susanna Huovinen ICT-johtaja Jarkko Levasma