15.3.2023

Valtion yhteisten talous- ja henkilöstöhallinnon palvelujen toimintaympäristömuutosten selvittäminen

1. Taustaa

Suomi on tunnettu EU:n alueella digitalisaation ja datatalouden edistäjä. Julkisen hallinnon strategian ja Valtiovarainministeriön 2030 strategian mukaisena tavoitteena on rakentaa julkista hallintoa entistä tehokkaammaksi, vaikuttavammaksi ja uudistumiskykyisemmäksi sekä edistää ihmislähtöistä digitalisaatiota ja tiedon parempaa hyödyntämistä yhteiskunnassa. Suomen digitalisaatiokehitystä suuntaa ja johtaa Suomen digitaalinen kompassi Valtioneuvoston selonteko : Digitaalinen kompassi - Valto. Digitalisaatiota vauhditetaan digitalisaation edistämisen ohjelman mukaisilla toimenpiteillä Digitalisaation edistämisen ohjelma - Valtiovarainministeriö (vm.fi).

Digitalisaatiota ja datataloutta vauhdittamaan tarvitaan investointeja ja toimialarajat ylittäviä käytänteitä. Digitalisaation edistämisen ja kehittämisen edellytyksenä on avoimen datan alustojen ja julkisen sektorin datan yhtenäistämiseen liittyviä lukuisia toimenpiteitä. Teknologian kehittyessä dataan pääsystä ja datan yhteistoimivuudesta tulee yhteiskunnan kehityksen kannalta yhä tärkeämpää. Yhtenäistämistavoitteeseen päästäksemme tarvitsemme samanaikaisesti säädösmuutoksia, joilla mahdollistetaan toimenpiteiden onnistuminen.

Valtion taloushallinnon osalta on tarve verkottuneeseen toimintatapaan yli organisaatio- ja valtiorajojen. Taloushallinnon digitalisointi ja automatisointi ovat välineitä, joita hyödyntämällä haetaan kilpailuaseman parantamista ja kulujen vähentämisen kautta tuloksen parantamista. Digitalisoinnin ja automatisoinnin vaikutukset tulevan pidemmällä aikajänteellä näkymään valtion budjettisäästöinä, toisin sanoen budjettilisäysten pienentymisenä.

Valtion taloushallinnosta lähetetään mm. myyntilaskuja niin henkilö- kuin yhteisöasiakkaille osin valtion rajojen ulkopuolelle. Ostolaskuja vastaanotetaan verkkolaskumuodossa ja tulevaisuudessa enemmän myös sähköisiä kuitteja niin ikään osin myös valtion rajojen ulkopuolelta. Henkilöstöhallinnon osalta tilanne on osin toinen. Valtion henkilöstöhallinnon tietojen tarkoitus ei ole liikkua vapaasti vaan pysyä tiukkaan rajatun käytön piirissä.

Globaali kilpailu uusimmista teknologioista, osaamisesta ja osaajista kiihtyy ja leimaa digitalisaatiokeskustelua. Toimintaympäristön muutostekijät ja digitalisaatiokehitys vaikuttavat eri ammattialojen monitasoisiin ja –laatuisiin uusiin osaamistarpeisiin ja työvoiman saatavuuteen tulevaisuudessa. Digitaalinen turvallisuusosaaminen, digitaaliset kommunikointi- ja yhteistyötaidot, digitaalinen lukutaito, digitaalisuuden perusteiden hallinta ja digitaaliset ongelmanratkaisutaidot ja digitaalisen sisällön luominen haastavat meitä kaikkia. Osaamisvaatimuksissa on katse kohdistunut mm. digiturvallisuusosaamiseen, johon liittyvää osaamista tarvitaan uuden digiajan sisäänrakennetuissa toiminnoissa, prosesseissa ja järjestelmissä. Perusdigitaidot eivät enää riitä. Esimerkiksi osaamisen ennakointifoorumin 2021–2024 laaja-alainen osaaminen 2030 –raportin tuloksissa kiinnitetään huomio talous- ja rahoitusalan työntekijöiden kasvaviin osaamisvaatimuksiin. Näissä tehtävissä työskennellään yleensä henkilötietojen tai -suojan parissa. Lisäksi regulaation yleisenä trendinä lisääntyy taloushallinnossa (esim. kansainväliset standardit, maksuliike) ja taloushallintoon vaikuttavissa prosesseissa (esim. pakotteet) kaikilla tasoilla. Nämä kaikki lisäävät henkilöstön osaamisvaatimuksia. Automatisaatio ja robotisaatio tulevan entisestään vähentämään rutiininomaisia tehtäviä ja lisäävät digitaalista osaamista edellyttäviä tehtäviä. Tästä esimerkkinä valtiovarainministeriössä meneillään oleva hanke elämäntapalähtöisen digitalisaation edistämisestä Infotilaisuus: Elämäntapahtumalähtöisen digitalisaation edistäminen - Valtiovarainministeriö (vm.fi) jonka tuotokset tulevat ulottumaan myös taloushallinnon tehtäviin. Muutosten myötä valtion talous- ja henkilöstöhallintoon saattaa muodostua esimerkiksi uusia työmuotoja ja tarve tiedon avaamiselle ja reaaliaikaisuudelle todennäköisesti kasvaa.

Digitaalisiin osaamisvaatimuksiin sisältyy myös mm. digitaalisten välineiden ja sisältöjen suojeluosaaminen, henkilökohtaisen tiedon ja yksityisyyden suojeluosaaminen sekä digitaalisten teknologioiden ja niiden ympäristövaikutusten tiedostamiseen liittyvät osaamiset. Kestävyysajattelu on myös osa nykyajan osaamisvaatimuksia, joka tarkoittaa alan työskentelytapojen kriittistä arviointia ja tietoisuutta vaihtoehtoisista toimintatavoista. Lisääntynyt etä- ja hybridityö kasvattavat osaltaan digitaalisen turvallisuusosaamisen tarvetta. Digiosaamisissa ja kestävyysosaamisissa tarvitaan edistynyttä tai korkean asiantuntijuuden taitotasoa (Laaja-alainen osaaminen 2030-luvulla (oph.fi).

Tekoäly mahdollistaa automaation lisäämistä entisestään. Tekoälynkin kehitys on ymmärrettävä suhteessa teknologian kehityksen kokonaisuuteen. Tekoälyyn liittyy kuitenkin uhkakuvia. Tekoälyä saatetaan käyttää mm. automaattiseen kyber- ja informaatiovaikuttamiseen. Esimerkiksi sosiaalisessa mediassa voi olla haastavaa erottaa tekoälyä inhimillisistä keskustelijoista. Silloinkin kun ihminen tietää keskustelevansa tekoälyn kanssa, saattaa ihmistä jäljittelevä käyttöliittymä luoda väärän vaikutelman inhimillisen kaltaisesta älystä. Yhteiskuntamme voi täyttyä epämääräistä dataa käyttävistä ja huolimattomasti suunnitelluista tekoälyjärjestelmistä, joiden käyttäjät eivät ymmärrä niiden toimintaa. Tekoälyä ja digitalisaatiota

on kuitenkin kehitettävä ja edistettävä palvelulähtöisesti. Tälläkin hetkellä talous- ja henkilöstöhallinnossa tekoälyä käytetään apuna esimerkiksi menotositteiden tiliöinnissä. Palvelujen kehittäminen on myös konkreettinen tapa toteuttaa EU:n tavoitetta ihmis- ja kansalaiskeskeisestä digitalisaatiota ja tekoälystä (Tekoälyratkaisut tänään ja tulevaisuudessa (eduskunta.fi).

Talous- ja henkilöstöhallinnon tehtävät tulevat kehittymään strategisemmiksi ja tiedolla johtamisen tavoitteita entistä paremmin palveleviksi. Talous- ja henkilöstöhallinnon tietojärjestelmissä tulee hyödyntää nykyaikaista teknologiaa ja tietojärjestelmien kehittämisessä nykyaikaisia menetelmiä. Monet merkittävät ohjelmistotalot ovat siirtäneet kehityspanoksensa pilvipohjaisiin toteutuksiin ja on-premise eli konesaliratkaisujen hankkiminen on jo nykyhetkessä vaikeutumassa. Pilviteknologian käyttöönottoa haastaviin asioihin tulee yhdessä löytää yhteisesti hyväksytyt ratkaisut, mikäli halutaan käyttää moderneja toiminnan kehittämistä tukevia tietojärjestelmäratkaisuja ja asiantuntijapalveluita.

Valtiolla on jo nyt käytössään erilaisia pilvipalveluratkaisuja ja automaattisia päätöksentekoprosesseja ja näiden tarve tulee tulevaisuudessa todennäköisesti lisääntymään. Digitalisaatio mahdollistaa uudenlaisia automatisoidumpia, tehokkaampia ja resurssiviisaampia ratkaisuja. Näihin uusiin ratkaisuihin sisältyvät muun muassa pilvipalveluiden käytön laajentaminen ja automaattisen päätöksenteon mahdollistaminen.

2. Työryhmä ja tavoitteet

Valtiovarainministeriö asetti marraskuussa 2022 työryhmän, jonka tehtävänä oli selvittää pilvipalvelun ja automaattisen päätöksenteon käyttömahdollisuuksia valtion talous- ja henkilöstöhallinnossa. Työryhmän selvittämistyön tavoitteena oli turvata hyvää hallintoa, hallintoasian käsittelyä ja viranomaisten toiminnan lainmukaisuutta koskevat vaatimukset sekä pilvipalvelun käytössä toiminnan jatkuvuus- ja varautumistarpeet.

Työryhmän tehtävänä oli

1. tunnistaa pilvipalveluiden käytön edellytyksiä talous- ja henkilöstöhallinnon palveluiden palvelutuotannossa,

2. tunnistaa pilvipalveluiden käytön edellyttämiä lainsäädännön muutostarpeita,

3. tunnistaa automaattiseen päätöksentekoon sopivia talous- ja henkilöstöhallinnon palveluita ja

4. tunnistaa mahdollisia muita toimintaympäristön muutoksia, jotka edellyttävät palvelukeskukseen tai talous- ja henkilöstöhallinnon palveluihin liittyvää sääntelyn kehittämistä.

Työryhmän jäsenet

Virpi Mustonen, neuvotteleva virkamies, valtiovarainministeriö, pj
Timo Kallio, johtaja, Palkeet (varajäsen Helena Lappalainen, Palkeet)
Tanja Wistbacka, apulaisjohtaja, Valtiokonttori
Matti Hyytinen, johtava erityisasiantuntija, valtiovarainministeriö (31.12.2022 asti)
Peppiina Huhtala, hallitussihteeri, valtiovarainministeriö
Timo Hattinen, budjettineuvos, valtiovarainministeriö

Työryhmän työskentelykausi oli 10.11.2022 – 31.1.2023.

Työskentelykautenaan työryhmä on kuullut useita eri asiantuntijoita valtionhallinnosta ja yksityiseltä sektorilta.

3. Yleistä pilvipalveluista

Pilvipalvelu on kokonaisuus, jossa organisaation sovellukset sijaitsevat fyysisten palvelinten sijaan skaalautuvalla pilvipalvelimella. Pilvipalveluilla tarkoitetaan palvelumallia, jossa helposti säädettäviä usean käyttäjän kesken jaettuja tietoteknisiä resursseja tarjotaan tietoverkkojen yli.

Pilvipalvelut voidaan pääpiirteittäin jaotella julkiseen ja yksityiseen pilveen, hybridipilveen sekä monipilveen. *Julkinen pilvi* on periaatteessa kolmannen osapuolen tarjoama palvelu. Julkinen pilvi on avoin kaikille tilaajille ja samanaikaisesti eri asiakkaiden käytettävissä. *Yksityinen pilvi* on organisaatiokohtainen pilvipalveluratkaisu. Tyypillisesti yksityinen pilvi ei ole lainkaan saatavilla julkisesta internetverkosta ja sitä hallinnoidaan ainoastaan suoraan organisaation sisäverkosta tai suojattujen etäyhteyksien kautta. Yksityinen pilvi voidaan rakentaa joko organisaation omilla palvelinlaitteilla omia laitetiloja hyödyntäen tai ulkoistaa sekä laitehallinta että laitteiden sijoituspaikka omalle pilvipalvelua tarjoavalle kumppanille. Yksityinen pilvi voi olla tietosuoja-, datan sijainti-, konesalin luokittelu- ym. syistä myös ainoa vaihtoehto. Yksityistä pilvipalvelua käyttävät usein julkisen sektorin toimijat, rahoitusalan toimijat sekä muut keskisuuret ja suuret organisaatiot. Yksityinen pilvi ei rajaa pois mitään palveluita, vaan sen kautta voidaan tuottaa organisaation palvelut eri pilvipalveluteknologioita hyödyntäen.

Hybridipilvi on pilvipalveluiden ratkaisu- ja toteutusmalli, joka yhdistää julkisen pilven ja on-premise-ratkaisun (konesalin) tai yksityisen pilven, kuitenkin niin, että nämä kaksi ratkaisu- ja toteutusmallia säilyvät erillisinä. Yhdistelmä julkisen ja yksityisen välillä arvioidaan tietosuojan ja tehdyn riskiarvioinnin perusteella. *Monipilvi* (multi-cloud) viittaa toimintaympäristöön, jossa organisaatio käyttää useampaa pilviympäristöä. Nämä voivat olla niin julkisen pilven kuin yksityisen pilven palveluita useissa eri ympäristöissä.

Pilvipalveluiden tunnistettuja hyötyjä on listattu alle mm. konsernitoimijoilta saatujen käyttäjäkokemusten ja selvitysten perusteella

- automaattinen versionhallinta ja teknisen velan välttäminen,
- skaalautuvuus tarpeiden mukaan,
- yhteensopivuus ja –toimivuus muiden pilviratkaisujen kanssa,
- käyttöönoton suoraviivaisuus sekä integraatioiden kustannustehokkuus,
- automaattiset tietoturvapäivitykset ja -ominaisuudet,
- kehittyneet ratkaisut salaus- ja kulunvalvontaan ja yhtenäiseen identiteetin hallintaan sekä
- automatisaatiomahdollisuudet, koneälyn ja koneoppimisen hyödyntäminen ja älykkäät kehityssuunnat automatisoituun analytiikkaan pohjautuen.

Pilvipalveluiden haasteita

- EU-tason tietosuojalainsäädännön tulkinnat,
- julkishallinnossa erilaiset näkemykset turvallisuusluokitellun materiaalin käsittelystä,
- organisaation valmius muuttaa toimintatapoja merkittävästi,
- pilviympäristöjen auditointiin liittyvät haasteet,
- mahdollisuudet palveluiden räätälöintiin ja sopimusehtoihin rajalliset,
- toimittajan palveluhintamuutokset tai pois siirtymisen problematiikka,
- kriittisiin toimintoihin tai versiopäivityksiin liittyvät rajalliset vaikutusmahdollisuudet,
- mahdolliset tarpeet lainsäädännön muutoksille.

Edellä mainitut listat hyödyistä ja haitoista eivät ole tyhjentäviä. Kyse on kuitenkin varsin haasteellisesta toimintaympäristöstä, jossa digitalisaatiota edistetään ja pilvipalveluista on jo kokemusta. Kaikki näkökulmat ja riskit on arvioitava erityisellä huolellisuudella, jotta digikyvykkyytemme pysyy ja kehittyy kokonaisturvallisella tasolla.

4. Valtion pilvipalveluiden linjauksia, ohjeita ja kriteeristöjä

Julkisen hallinnon pilvipalvelulinjaukset määrittävät, miten julkisen hallinnon organisaation omistamaa tietoa voidaan käsitellä pilvipalveluissa. Linjausten tavoitteena on tukea ICT-palveluiden suunnittelua ja päätöksentekoa. Linjaukset käsittelevät jaettuja resursseja tarjoavia ICT-palveluita, kuten laskentatehoa sekä tallennus-, varmuuskopiointi- ja tiedonsiirtokapasiteettia. Julkisen hallinnon pilvipalvelulinjaukset ovat parasta aikaa uudistettavana.

Julkisen hallinnon pilvipalveluista on laadittu myös erilaisia ohjeita, kriteeristöjä ja suosituksia.

- Julkisen hallinnon pilvipalvelulinjaukset (valtiovarainministeriön julkaisuja – 35/2018).
- Pilvipalvelujen soveltamisohje - Pilvipalvelujen hyödyntämisen soveltamisohjeita julkisen hallinnon organisaatioille (valtiovarainministeriön julkaisuja – 2020:73).
- Tuottavuutta pilvipalveluilla - Ohje julkisen hallinnon pilvipalvelujen hyödyntämiseen (valtiovarainministeriön julkaisuja – 2020:66).
- Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) (Traficomin julkaisuja 13/2020)
- Kansallinen turvallisuusauditointikriteeristö “Katakri”
- Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (valtiovarainministeriön julkaisuja – 2021:5)
- Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalvelussa (valtiovarainministeriön julkaisuja – 2022:4)

Vuoden 2018 julkisen hallinnon pilvipalvelulinjaukset ja vuoden 2020 pilvipalvelulinjauksien soveltamisohjeiden päivitys on parhaillaan käynnissä. Lausuntopalvelussa on lausuttavana 10.3.2023 asti ehdotus valtionhallinnon pilvipalvelulinjausten päivittämiseksi.

Lisäksi keväällä 2022 käynnistyi 30.6.2024 asti kestävä valtiovarainministeriön ja DigiFinlandin yhteinen Cirrus-hanke, jonka tavoitteena on nopeuttaa julkishallinnon pilvisiirtymää vähentämällä ja poistamalla julkipilvipalveluiden tietosuojaan liittyviä riskejä sekä luomalla julkishallinnon vaatimuksiin yhtenäiset toimintamallit.

5. Työryhmän tehtävät

5.1. Pilvipalveluiden käytön edellytykset talous- ja henkilöstöhallinnon palveluiden palvelutuotannossa

Riippumatta siitä, puhutaanko pilvipalveluista vai muista uusista teknisistä tai toiminnallisista ratkaisuista valtion talous- ja henkilöstöhallinnon palveluissa, tulee varmistua siitä, että hankittavat ja toteutettavat ratkaisut täyttävät lainsäädännön asettamat vaatimukset valtion talous- ja henkilöstöhallinnon palveluille, tietojärjestelmille, prosesseille, tietojen käsittelylle sekä lopputuotoksille. Ratkaisujen kehittämisessä on siis huomioitava säädösmuutostarpeet, taloudelliset vaikutukset, digitaalinen infrastruktuuri, uudet toimintatavat ja –mallit, erilaiset palvelumallit ja kartoitettava kansainväliset referenssit. Lisäksi ratkaisuissa on huolehdittava riittävä sisäinen valvonta ja automaattiset tai vaihtoehtoiset valvontatavat.

Pilviratkaisujen tulee olla tietoturvallisia. Ne eivät saa heikentää tietoturvan tasoa verrattuna käytössä oleviin ratkaisuihin. Ratkaisut eivät saa edes häiriö- ja vikatilanteissa heikentää valtion turvallisuutta tai aiheuttaa vahinkoa yleiselle edulle.

Valtion taloushallinnon ja siihen keskeisesti liittyvien prosessien tulee olla pystyssä viimeisinä yhteiskunnassa. Tämä vaatii varautumista erilaisiin poikkeustilanteisiin ja lisää haasteita prosessien, tietoliikenneyhteyksien ja –järjestelmien suunnitteluun.

Pilviratkaisujen käytön yhteydessä on myös arvioitava turvasatama-konseptin mukaisen ”varaympäristön” käyttötarve ja tehtävä siitä päätös ottaa tai olla ottamatta käyttöön. Ratkaisut eivät myöskään saa vaarantaa valtioon palvelussuhteessa olevien henkilöiden turvallisuutta esimerkiksi henkilöön liittyvien tietojen oikeudettoman paljastumisen tai oikeudettoman käytön myötä. Tämä koskee ennen kaikkea turvallisuusviranomaisia, mutta samalla koko valtion henkilöstöä.

Toiminnan jatkuvuus/keskeytysriski- näkökulmat on tärkeä huomioida edellä kuvattujen seikkojen ohella. Huoltovarmuuskriittisten toimintojen osalta on tärkeä varmistaa niiden jatkuvuus.

Ratkaisujen tulee olla myös kustannustehokkaita ja vastata siihen tarpeeseen, jota varten ne hankitaan käyttäjäkokemusta unohtamatta. Ratkaisuissa tulee ottaa huomioon myös vastuullisuus, kestävä kehitys ja ympäristönäkökulmat siten, että hankittava uusi ratkaisu on asianmukaisesti kilpailutettu, ja ettei se aiheuttaisi suurempaa kuormaa ympäristölle kuin käytössä oleva ratkaisu.

Pilviratkaisujen ylläpidettävyyteen tulee myös kiinnittää huomiota. Pilviratkaisun ylläpitoon tulee löytyä riittävästi osaavaa henkilöstöä sekä palvelun toimittajalta, että sen käyttäjäorganisaatiolta. Tärkeää on varmistua myös siitä, että eri osapuolten vastuut ovat selvät niin uuden ratkaisun hankinta-, rakentamis- ja käyttöönotto- kuin tuotantovaiheessa.

Pilviratkaisun käyttöönotto voi myös vapauttaa valtion oman henkilöstön työpanosta. Esimerkiksi valtion yhteishankintayksikkö Hansel Oy:ssä vuoden 2022 IT-kulut per työntekijä laskivat noin 20 prosenttia pilvisiirtymän myötä. Samaan aikaan Hanselin käyttämien IT-palveluiden määrä yli kolminkertaistui. Oman henkilöstön työaikaa siirtyi infran ylläpidosta liiketoiminnalle lisäarvoa tuottavamman työn tekemiseen. Tämä voi olla myös kokonaisturvallisuutta parantava asia, sillä valtion oman henkilöstön työpanosta kohdentuu esimerkiksi tietosuojan kannalta haastavampien ratkaisujen ylläpitoon, kun pilvipalveluun on ulkoistettu muiden, vähemmän kriittisten toimintojen ylläpito.

Valtion keskitetyistä taloushallintotehtävistä vastaavana virastona Palkeiden tulee valtion talousarviosta annetun lain (423/2988) 12 b §:n 4 momentin mukaisesti tarjota talous- ja henkilöstöhallinnon palvelut tiedoille, jotka on korkeimmillaan turvaluokiteltu tasolle TLIV. Erityisesti turvaluokiteltujen henkilötietojen käsittely asettaa vaateita ja rajoitteita pilvipalvelujen keskitettyä hyödyntämistä suunniteltaessa. Turvallisuusluokiteltavien asiakirjojen käsittelystä pilvipalvelussa annetussa

ohjeistuksessa on kuvattu huomioitavat asiat hyvin. Lähtökohtaisesti talous- ja henkilöstöhallinnon tiedot ovat korkeintaan salassa pidettäviä tai alimman turvaluokan eli TLIV-tasoisia tietoja. Joidenkin asiakkaiden osalta osa tiedoista voi kuitenkin olla turvallisuusluokiteltua tasolle TLIII. Näin voi mahdollisesti olla joko yksittäisten tietojen tai tiedon kasautumisen kautta. Tällä hetkellä TLIII-luokiteltujen tehtävien järjestämisestä vastaa kyseinen virasto tai laitos itse, jonka lisäksi keskitettyjen talous- ja henkilöstöhallinnon palvelujen tuottamisesta Palkeiden toimesta voidaan erikseen sopia. Tässä selvitysmuistiossa ei oteta kantaa virastojen omien turvaluokiteltujen aineistojen erilaisiin prosesseihin.

Talous- ja henkilöstöhallinnon tietojen käsittely pilvipalvelussa on pääsääntöisesti mahdollista TLIV-tasolle saakka EU/ETA-alueella toteuttavan pilviratkaisun avulla. Turvaluokitellun tiedon osalta on käytävä läpi yhteistyössä asiakkaiden kanssa turvaluokittelun perusteet ja mahdollisuudet tietojen käsittelyyn talous- ja henkilöstöhallinnon yhteisissä järjestelmissä. Luokittelun perusteena voidaan käyttää prosessikohtaisia asiamatriiseja, joiden kautta tiedon luokittelulle ja käsittelylle voidaan luoda yhtenäiset suositukset.

5.2. Pilvipalveluiden käytön riskit talous- ja henkilöstöhallinnossa

Sekä pilvipalveluihin että on-premise –ratkaisuihin sisältyy riskejä. Riskejä arvioitaessa tulee huomioida erityisen tarkasti kriittisten järjestelmäkokonaisuuksien vaikutus koko tuotantoympäristön toimivuuteen, jatkuvuuteen, vikasietoisuuteen ja palautumiseen. Valtion taloushallinnon jatkuvuuden rooli koko yhteiskunnan huoltovarmuudessa on merkittävä. Taloushallinto ja maksuliike on hoidettava kaikissa olosuhteissa mukaan lukien häiriötilanteet ja poikkeusolot.

Kun järjestelmissä käytettävän tiedon rooli ja sijainti ovat kriittisiä myös tietosuojanäkökulmasta, on olennaista huomioida EU:n yleisen tietosuoja-asetuksen ja tiedonhallintalain vaatimukset kuvaamalla mm. tiedonkäsittelyprosessit. Julkisten organisaatioiden on varmistettava, että niiden arkaluonteiset henkilö- ja taloustiedot ovat turvattuja pilvipalveluissa, koska tietoturvaloukkaukset voivat johtaa merkittävään turvallisuuden vaarantamiseen, taloudellisiin tappioihin ja mainevahinkoihin.

Julkisten organisaatioiden on varmistettava, että niiden pilvipalvelujen tarjoajalla on jatkuvuus- ja valmiussuunnitelmat palvelukatkosten varalta, sillä tämä voi vaikuttaa organisaation kykyyn hoitaa henkilöstö- ja talousprosesseja. Valtion on organisaationa varmistettava koko palveluketjun toimivuus kaikissa olosuhteissa ja varauduttava myös palveluntarjoajan force majoure -tilanteisiin.

Virastot ja laitokset arvioivat valtion yhteisissä talous- ja henkilöstöhallinnon tietojärjestelmissä olevien tietojensa turvallisuustason, jolloin tällä hetkellä katsotaan riskeinä olevan mm. tietojen epäyhtenäinen riskiarviointi ja luokittelu.

5.3. Pilvipalveluiden käytön edellyttämät lainsäädännön muutostarpeet

Lainsäädännössä ei ole asetettu esteitä pilvipohjaisiin palveluihin siirtymiselle, kunhan henkilötietojen suojaa ja tietoturvallisuutta koskevat kysymykset huomioidaan. Pilvipohjaiseen ratkaisuun siirryttäessä huomioitavaksi tulevat ainakin seuraavat säännökset:

- Sellaisenaan sovellettava Euroopan parlamentin ja neuvoston asetus (EU:n yleinen tietosuoja-asetus, (EU) 2016/679) sekä sitä täydentävä tietosuojalaki (1050/2018), jotka sisältävät säännöksiä henkilötietojen käsittelystä.
- Euroopan parlamentin ja neuvoston datanhallinta-asetus (EU) 2022/868, joka sisältää säännöksiä luottamuksellisten tietojen siirtämisestä kolmansiin maihin; Tietoja ei saa siirtää, jos se olisi ristiriidassa unionin tai kansallisen lainsäädännön kanssa.
- Ehdotus Euroopan parlamentin ja neuvoston asetukseksi datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös) COM (2022) 68 final, jolla säädettäisiin pilvipalveluita EU-alueella sijaitseville asiakkaille tarjoavien toimijoiden velvollisuudesta huolehtia tietojen suojaamisesta kolmannen maan viranomaisilta, jos kolmannen maan viranomaisen pääsy tietoihin olisi ristiriidassa unionin tai kansallisen lainsäädännön kanssa. Lisäksi säädöksen tavoitteena on tehdä pilvipalveluiden vaihtamisesta helpompaa ja kustannustehokkaampaa
- Viranomaisen toiminnan julkisuudesta annettu laki (julkisuuslaki, 621/1999).
- Julkisen hallinnon tiedonhallintalaissa annettu laki (tiedonhallintalaki, 906/2019), joissa säädetään muun muassa asiakirjojen salassapitoperusteista sekä tietoturvallisuudesta.
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) sisältää säännökset erityissuojattavan tietoaineiston käsittelyvaatimuksista.
- Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (turvallisuusluokitteluasetus, 1101/2019) sisältää säännökset salassa pidettävien ja turvallisuusluokiteltujen asiakirjojen käsittelyvaatimuksista valtionhallinnossa.

Erityisiä vaatimuksia pilvipohjaisille ratkaisulle asettaa turvallisuusluokiteltavan tiedon käsittely. Turvallisuusluokkaa koskevaa merkintää ei saa käyttää muissa kuin kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 8 §:n 1 momentin tai tiedonhallintalain 18 §:n 1 momentin tarkoittamissa tilanteissa, ellei se ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön.

Valtion talousarviosta annetun lain taloushallintotehtäviä koskevan 12 b §:n 4 momentin mukaan keskitetyistä taloushallintotehtävistä vastaavalla virastolla tai laitoksella on salassapitosäännösten estämättä oikeus saada virastoilta, laitoksilta ja muilta toimielimiltä tehtäviensä hoitamiseksi välttämättömät salassa pidettävät asiakirjat lukuun ottamatta julkisen hallinnon tiedonhallinnasta annetun lain 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 keskitetyistä taloushallintotehtävistä vastaavalla virastolla tai laitoksella ei ole edellä todetun mukaisesti oikeutta saada asiakasvirastolta tai laitokselta välttämättömiä tietoja tehtäviensä hoitamiseksi, kyseisestä tehtävästä vastaa keskitettyjä taloushallintotehtäviä vastaavan viraston tai laitoksen sijasta asianomainen virasto tai laitos itse, ellei toisin sovita.

Pilviratkaisujen käyttöönotto ei edellytä lainsäädännön muutostarpeita, mutta yhtenäistä tulkintaa edistäviä lainsäädännön soveltamisohjeita tarvittaisiin mahdollisesti lisää. Lisäksi pilvisiirtymässä huomioitavaksi tulee EU-tuomioistuimen vuonna 2020 tekemä Schrems II –päätös (C-311/18), jonka seurauksena henkilötietojen siirrot Euroopan talousalueen ulkopuolelle edellyttävät aiempaa kattavampaa riskiarviointia ja mahdollisia lisätoimia. Päätöksen seurauksena EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä annettu aikaisempi päätös (2016/1250) katsottiin pätemättömäksi. Yhdysvaltojen ei toisin sanoen katsottu enää lähtökohtaisesti täyttävän Euroopan tietosuoja-asetuksen kriteerejä. Päätöksen seurauksena tulee aina tapauskohtaisesti arvioida ja neuvotella tietosuoja-asiat kaikkien kolmansien maiden palveluntarjoajien (ml. Yhdysvallat) kanssa siten, että pilviratkaisun turvallisuus on EU-sääntelyn edellyttämällä tasolla.

5.4. Automaattinen päätöksenteko ja talous- ja henkilöstöhallinnon prosessit

Hallitus antoi eduskunnalle 19.09.2022 esityksen julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi (HE 145/2022 vp). Esityksen keskeinen sisältö on tuoda hallintolakiin (434/2003) säännökset, jotka mahdollistavat automaattisen päätöksenteon julkisessa hallinnossa. Automaattisen päätöksenteon pohjana olisivat käsittelysäännöt, jotka ihminen on etukäteen laatinut.

Esitys on tarpeen, koska EU:n tietosuojasääntely kieltää lähtökohtaisesti automaattisen päätöksenteon silloin, kun päätös vaikuttaa yksityisen oikeuteen tai velvollisuuteen. Asiaa koskeva Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta

(yleinen tietosuoja-asetus) tuli voimaan 24.5.2016 ja sen soveltaminen alkoi 25.5.2018.

Asetuksella kielletään pelkästään automaattiseen käsittelyyn perustuvien, merkittäviä oikeusvaikutuksia sisältävien päätösten antamisen. Kieltoon on mahdollista säätää kansallisella lainsäädännöllä poikkeuksia, joita nyt eduskunnassa käsittelyssä olevalla hallituksen esityksellä (HE 145/2022 vp) esitetään.

Talous- ja henkilöstöhallinnon prosessien kannalta keskeistä on ymmärtää, mitä automaattisella päätöksenteolla kansallisessa sääntelyssä tarkoitetaan sekä tunnistaa, mitkä talous- ja henkilöstöhallinnon päätökset kuuluvat automaattista päätöksentekoa koskevan sääntelyn ja yleisen tietosuoja-asetuksen soveltamisalaan.

5.4.1. Päätöksentekoa vai päätöksen täytäntöönpanoa

Kyse on automaattisesta päätöksestä, jos varsinainen käsittelyn päättävä ratkaisu tehdään automaattisella tietojenkäsittelyllä ilman ihmisen tarkastusta ja hyväksyntää. Ihminen voi osallistua johonkin asian käsittelyvaiheeseen, mutta kyse on automaattisesta päätöksenteosta aina, jos varsinainen päätös tehdään ilman ihmisen myötävaikutusta. Toisaalta, tekaistulla ihmisen osallistumisella asiaa ei voida EU:n tietosuojatyöryhmän ohjeistuksen mukaan kiertää.

Automaattista päätöksentekoa koskevaa sääntelyä sovelletaan tilanteeseen silloin, kun kysymyksessä on luonnollisen henkilön oikeuteen tai velvollisuuteen vaikuttava päätös, kuten verotus- tai etuuspäätös. Tällainen automaattista päätöksentekoa koskevan sääntelyn piiriin tuleva päätös on usein myös hallintolain tarkoittama hallintopäätös.

Talous- ja henkilöstöhallinnossa, erityisesti valtion talous- ja henkilöstöhallinnon palvelukeskus Palkeissa, tehdään hallintopäätösten sijaan useammin niin kutsuttua määräyksen tai päätöksen täytäntöönpanoa, kuten palkkasummien koneellista laskemista ja maksatusta. Tällaisen prosessin osan automatisointi on sallittua itsessään ilman erillissääntelyäkin, koska kyse ei ole päätöksestä vaan päätöksen täytäntöönpanosta eli niin kutsutusta tosiasiallisesta hallintotoiminnasta.

Palkeet on kehittänyt prosessiautomatisaatiota talous- ja henkilöstöhallinnossa sujuvoittaakseen toimintaa, tiedon käsittelyä ja tehostaakseen prosesseja. Automaatioratkaisut perustuvat pääosin ohjelmistorobotiikkaan, jonka avulla toteutetaan automaattista laadunvalvontaa, automatisoidaan manuaalisia työvaiheita, tarkastetaan tietoja ja siirretään niitä järjestelmästä toiseen.

Automaattista päätöksentekoa koskeva sääntely ei koske myöskään hallintolain 4 §:n 1 momentin tarkoittamia hallinnon sisäisiä määräyksiä, esimerkiksi yleisiä henkilöstölle osoitettuja ohjeistuksia kuten matkustusohjeita.

Toisaalta on vaikea tietää, mitkä kaikki hallinnolliset toimet voivat olla EU:n yleisen tietosuoja-asetuksen 22 artiklassa tarkoitettuja päätöksiä, koska asiasta ei ole vielä syntynyt EU-tuomioistuimen oikeuskäytäntöä.

5.4.2. Automaattisen päätöksenteon edellytykset

Kun asia on tunnistettu hallintolain uuden 53 e §:n ja EU:n yleisen tietosuoja-asetuksen soveltamisalaan kuuluvaksi, viranomainen voi ratkaista automaattisesti asian, jos kansallisessa sääntelyssä säädetyt edellytykset täyttyvät.

Tapauskohtaista harkintaa sisältävää asiaa ei saa ratkaista automaattisesti, ellei virkamies tai muu asian käsittelijä ole arvioinut tällaisia seikkoja etukäteen. Automaattisen ratkaisemisen edellytyksenä on lisäksi, että luonnollinen henkilö, johon ratkaisu on kohdistettu, voi kaikilta osin vaatia siihen oikaisua maksutta hallintolain 7 a luvun mukaisella oikaisuvaatimuksella tai siihen rinnastuvalla vaatimuksella, joka käsitellään päätöksen tehneessä viranomaisessa tai sen kanssa samaan rekisterinpitäjään kuuluvassa viranomaisessa. Oikaisuvaatimusta tai siihen rinnastuvaa vaatimusta ei voida ratkaista automaattisesti.

Uudenkaan sääntelyn myötä automaattista päätöstä ei voi tehdä tekoälyllä. Tekoälyllä tarkoitetaan tekniikoita, jotka perustuvat esimerkiksi tilastolliseen päättelyyn, joissa tekoälyjärjestelmälle on annettu mahdollisimman suuri määrä olemassa olevaa dataa ja sille on kerrottu, mitä datasta pitäisi löytää. Lopulta tekoäly alkaa luoda säännönmukaisuuksia, joiden tilastollisten sääntöjen perusteella se tuottaa lopputuloksen. Tekoälyllä tehtävien päätösten kohdalla ongelmaksi muodostuu päätösten perusteiden läpinäkymättömyys, sekä se, että lopputuloksen lainmukaisuutta tai siitä syntyvää virkavastuuta ei voi osoittaa yksittäiselle virkamiehelle. Tämä on ongelmallista oikeusturvan kannalta.

Pelkästään tekoälypohjainen hallinnollisen päätöksenteon automatisointi ei käytännössä ole nykylainsäädännön pohjalta mahdollista, mutta tulee huomioida, että EU:ssa on valmisteilla tekoälyasetus (2021/0106 (COD)), jossa selvitetään, millaisia velvoitteita tekoälyjärjestelmiin voisi liittää. Tällä voi olla vaikutusta sääntelyyn tulevaisuudessa.

Tekoälyasetuksessa ei kuitenkaan tulla näillä näkymin säätämään poikkeusta EU:n yleisen tietosuoja-asetuksen 22 artiklan kiellosta, joten automaattiseen päätöksentekoon liittyvät kysymykset on aina viime kädessä ratkaistava kansallisessa sääntelyssä päätöksenteossa käytettävästä teknologiasta riippumatta.

5.5. Muita toimintaympäristön muutoksia, jotka edellyttävät talous- ja henkilöstöhallintoon liittyvää sääntelyn kehittämistä

5.5.1. Tiedon kasaumavaikutus

Yhtenä merkittävimpänä ongelmana julkisen pilven käytössä on pidetty niin kutsuttua ”kasaumavaikutusta”, joka aiheuttaa tietosuojaa ja tietoturvaa koskevia haasteita. Kasautumisvaikutuksessa on kyse ilmiöstä, jossa suuri määrä tietoa voi muodostaa yksittäisiä tietoja merkittävämmän asiakokonaisuuden. Tällöin luokittelu ja suojaamistarpeet voivat erota yksittäisten tietoalkioiden luokittelusta ja suojaamistarpeista.

Suuri määrä tietoa voi nousta kasaumaperusteella luokitukseltaan yksittäistä tietoa korkeampaan turvallisuusluokkaan. Esimerkiksi suuri määrä turvallisuusluokan IV tietoa voi kasautuessaan muodostaa turvallisuusluokan III tietovarannon. Kasautumista turvallisuusluokitellun IV tai jopa III-luokkaan voi joissain tilanteissa tapahtua myös turvallisuusluokittelemattomista, salassa pidettävistä tietoalkioista.

Talous- ja henkilöstöhallinnon osalta haasteeksi voi jatkossa muodostua pilvipohjaiseen, kuin myös on-premise –ratkaisuihin pohjautuviin, palveluihin siirtymiseen liittyvistä suojaustarpeista ja riskienhallinta- ja suojaustoimien laajemmista ja syvälle menevistä toimista. Tästä esimerkkinä korkeammalle kuin TLIV-tasolle luokiteltu tieto.

Kasaumavaikutukseen viitataan kansallisissa tai alueellisissa ohjeistuksissa, mutta siitä ei säädetä EU-tason velvoittavassa lainsäädännössä tai kansallisessa lainsäädännössämme. Kasaumavaikutuksen huomioon ottaminen nojautuu näin ollen pitkälti tapauskohtaiseen riski- ja vaikutustenarviointiin sekä annettuihin ohjeisiin (ks. mm. PiTukri ja tiedonhallintalautakunnan suositus turvallisuusluokiteltujen asiakirjojen käsittelystä).

EU:n yleisessä tietosuoja-asetuksessa säädetään henkilötietojen käsittelyä koskevista yleisistä periaatteista, joita ovat lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus. Tietosuoja-asetus ei tee eroa yksittäisen henkilötiedon tai kasautuneen tiedon välillä. Tietosuoja-asetuksen periaatteet ja velvoitteet pätevät tiedon määrästä riippumatta.

Yleinen tietosuoja-asetus kuitenkin tunnistaa tilastollista käyttöä varten kerätyn suuren henkilötietomäärän, johon tulee soveltaa tiettyjä suojausmenetelmiä, kuten anonymisointia. Tällöin käsittelyn kohteena oleva tieto ei olisi enää henkilötietoa, vaan kyseessä on muu data. Samat suojausedellytykset soveltuvat myös pilvipalveluun tilastollista käyttöä varten kerättyyn kasautuneeseen tietoon, jos kasauma muodostuu henkilötietoja sisältävästä datasta.

Eurooppa-neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488) koskee nimensä mukaisesti turvallisuusluokiteltuja tietoja sekä niiden käsittelyä. Kasautunutta tietoa sivutaan lyhyesti sääntöjen 4 artiklassa, jonka mukaan EU:n turvallisuusluokiteltujen tietojen kooste voi edellyttää korkeampaan turvallisuusluokkaan sovellettavaa suojaa kuin yksittäisten tietojen suoja vaatisi.

Suurikaan määrä turvallisuusluokittelematonta, salassa pidettävää tietoa ei tiedonhallintalautakunnan suosituksen mukaan aina johda kasautumisvaikutukseen ja turvallisuusluokittelun perusteiden täyttymiseen. Vastaavasti suurikaan määrä turvallisuusluokiteltua tietoa ei aina johda kasautumisvaikutukseen ja turvallisuusluokan nostoon.

5.5.2. Tekoäly ja tekoälyn sääntely

EU:ssa on valmistelussa tekoälyasetus, jonka tavoitteena on luoda tekoälyn käytölle yhteiset pelisäännöt. Tekoälyasetuksen tavoitteena on varmistaa, että tekoälyn käyttö on turvallista kaikille yrityksille ja ihmisille. Asetuksella säänneltäisiin tekoälyä hyödyntävien tietojärjestelmien suunnittelua ja käyttöä. Pääosa sääntelystä kohdistuisi suuririskisiin käyttötarkoituksiin, joita ei henkilöstö- ja taloushallinnossa juurikaan ole.

Suomelle on tärkeää, että asetuksen tekoälyn määritelmä kattaisi vain aidon tekoälyn. Asetuksen ei tulisi koskea esimerkiksi sääntöpohjaista automaatiota, eli järjestelmiä, jotka soveltavat ihmisen määrittämiä sääntöjä ja ohjeita automaattisesti. Päätösautomaatiosta kerrotaan tarkemmin kappaleessa 5.4. Suomi on ollut aloitteellinen tekoälyn määritelmän kaventamisessa, jotta pystytään esimerkiksi varmistamaan, että tiettyjen jo käytössä olevien automaattisen päätöksenteon järjestelmien käyttöä voidaan jatkaa.

Sääntelyn laatiminen ilmiölle, jota ei voi yksiselitteisesti määritellä, on haastavaa. Sääntelyn taustalle tarvitaankin visiota siitä, mitä digitalisaatiolla ja tekoälyllä halutaan saada aikaan. Yhteinen ja selkeä visio mahdollistaisi halutun tulevaisuuden rakentamisen säädöksillä, piloteilla ja T&K-rahoituksella Tekoälyratkaisut tänään ja tulevaisuudessa (eduskunta.fi).

Asetusehdotuksesta on syntynyt neuvoston yleisnäkemys joulukuussa 2022 ja parlamentti valmistelee kantaansa kevään 2023 aikana.

5.5.3. Muut lainsäädäntöuudistukset

EU:n datastrategiaa toteuttavan sääntelyviisikon (tekoälyasetus, datahallinta-asetus, digimarkkina-asetus, digipalveluasetus, data-asetus) tarkoituksena on lisätä datan hyötykäyttöä EU:n sisämarkkinoilla. Sääntelyllä pyritään myös luomaan

yhtenäiset säännöt ja tasapuoliset olosuhteet kaikille toimijoille. Toisin sanoen tarkoituksena on luoda toimivat datan sisämarkkinat EU-alueelle.

Toukokuussa 2022 voimaan tullut nk. datanhallinta-asetus (EU) 2022/868) sääntelee julkisen hallinnon hallussa olevan luottamuksellisen tiedon luovuttamista tiedon uudelleenkäyttöä varten. Asetuksella pyritään kehittämään digitaalisia sisämarkkinoita sekä ihmiskeskeistä, luotettavaa ja turvallista datayhteiskuntaa ja –taloutta. Datanhallinta-asetuksella ei kuitenkaan perusteta tiedonsaantioikeuksia, vaan niistä tulee olla säännökset kansallisessa lainsäädännössä. Talous- ja henkilöstöhallinnossa ei lähtökohtaisesti ole asetuksessa tarkoitettuja tietoja ja asiakirjoja, jotka tulisivat asetuksen soveltamisalan piiriin.

Valmisteilla oleva data-asetus antaisi julkiselle hallinnolle mahdollisuuden pyytää hätätilanteen tai lakisääteisen tehtävän hoitamiseksi dataa yksityiseltä sektorilta. Tavoitteena on varmistaa datasta saatavan arvon oikeudenmukainen jakaminen datatalouden toimijoiden kesken sekä edistää datan saatavuutta ja käyttöä. Tällä pyritään varmistamaan EU:n yritysten mahdollisuudet innovoida ja kilpailla kaikilla aloilla, lisätään tehokkaasti yksilöiden vaikutusmahdollisuuksia oman datansa suhteen ja annetaan oikeasuhteisen ja ennakoitavissa olevan mekanismin avulla yrityksille ja julkisen sektorin elimille paremmat valmiudet vastata merkittäviin poliittisiin ja yhteiskunnallisiin haasteisiin, kuten yleisiin hätätiloihin ja poikkeustilanteisiin.

Valmisteilla olevan yhteentoimiva Eurooppa- asetuksen tavoitteena on edistää Euroopan laajuisen digitaalisten julkisten palvelujen infrastruktuurin kehittymistä vahvistamalla yhteiset säännöt ja koordinaatiopuitteet julkisen sektorin yhteentoimivuuden varmistamiseksi. Yhteentoimivuudella tarkoitetaan verkko- ja tietojärjestelmien kykyä keskinäiseen vuorovaikutukseen jakamalla dataa sähköisen viestinnän avulla.

Ehdotuksen mukaan jäsenvaltioiden rajat ylittävän yhteentoimivuuden sääntely on perusedellytys digitaalisten sisämarkkinoiden kehittymiselle. Kun prosesseja automatisoidaan ja digitaaliteknologia yleistyy julkisessa hallinnossa, on ratkaisevan tärkeää, että eri maiden julkiset hallinnot pystyvät kommunikoimaan keskenään. Tämän tavoitteen saavuttamisessa yhteentoimivuudella on tärkeä rooli. Yhteentoimivuus ei kuitenkaan toteudu pelkästään teknisin keinoin, vaan tarvitaan sopimuksia ja vakiintuneita prosesseja eri organisaatioiden välillä. Yhteentoimivuus on ratkaiseva tekijä myös unionin ja jäsenvaltioiden kasvavien kyberturvariskien lieventämisessä.

Julkiset hallinnot ovat nykyään kyberhyökkäysten kohteina. Heikko yhteentoimivuus aiheuttaa kansalaisille ja yrityksille tarpeettomia hallinnollisia vaikeuksia ja lisää julkishallintojen kustannuksia. Julkisen sektorin yhteentoimivuuden kehittä-

minen tarjoaa merkittäviä mahdollisuuksia lisätä innovointia, parantaa varautumissuunnittelua (esim. kriisitilanteita varten) ja vahvistaa EU:n teknologista suvereniteettia. Maiden rajat ylittävän yhteentoimivuuden sääntelyssä julkisella sektorilla olisi keskityttävä yleisen edun turvaamiseen käyttäjäkeskeisillä ja avoimilla ratkaisuilla. Yhteentoimivuusratkaisujen tukena käytetään avoimen lähdekoodin toteutuksia.

Kyberturvallisuusdirektiivin eli ns. NIS2-direktiivin tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa tiettyjen kriittisten sektoreiden osalta. Kyberturvallisuudella tarkoitetaan tietojärjestelmien ja tietoaineistojen eheyttä ja loukkaamattomuutta ulkopuolista uhkaa vastaan.

Direktiivissä osoitetaan yhteiskunnan kriittisille sektoreille kyberturvallisuutta vahvistavia riskienhallintavelvoitteita ja raportointivelvoitteet kyberhäiriöistä. Direktiivissä on lueteltu vähimmäistoimenpiteet, jotka kaikkien toimijoiden on toteutettava hallitakseen toimintoihinsa kohdistuvia kyberturvallisuusriskejä.

Direktiivin soveltamisala kattaa entistä laajemmin esimerkiksi energia- ja terveydenhuoltosektorilla toimivia tahoja sekä digitaalisen infrastruktuurin palveluntarjoajia. Direktiivin soveltamisalaa on laajennettu koskettamaan myös uusia sektoreita ja toimijoita, kuten julkista hallintoa, elintarvikealaa ja jätehuoltoa.

Liikenne- ja viestintäministeriössä on käynnissä NIS22-direktiivin kansallinen täytäntöönpanohanke.

Single Digital Gateway –asetus, eli asetus digitaalisesta palveluväylästä, on EU-asetus, jonka tarkoituksena on auttaa ihmisiä ja yrityksiä toimimaan Euroopan unionin alueella entistä helpommin. Asetuksen päämääränä on lisätä, täydentää ja selkeyttää EU:n sisämarkkina-asioita koskevaa verkossa jo olevaa tietoa. Lisäksi halutaan helpottaa EU-kansalaisten ja yritysten sähköistä asiointia myös rajat ylittävissä tilanteissa. Digitaalisen palveluväylän kansalaisille näkyvin osa on portaali, jonka kautta EU-kansalaiset ja yritykset löytävät keskeisen informaation ja sähköiset palvelut (ns. eurooppalainen Suomi.fi-palvelu).

Digitaalisen palveluväylän toimeenpanon koordinaatiohanke on parhaillaan käynnissä työ- ja elinkeinoministeriössä.

Vireillä olevat lukuisat EU:n säädösaloitteet määrittelevät pelisäännöt digitalisaation ja uusien teknologioiden käyttöönotolle. Yhtenäisyyttä tarvitaan, sillä EU:n lainsäädäntö ja jäsenmaiden digitaalinen kyvykkyys ovat varsin hajaantuneet, ja lisäksi kysymys on globaalista ilmiöstä, jonka eteen tuomia haasteita tulee ratkoa yhdessä. Yhtenäisen sääntely-ympäristön ja standardien luominen ovat keskeinen keino myös lunastaa uusien ratkaisujen skaalaedut. Suomen on jatkossakin

tarjottava aktiivisesti ratkaisuja, joilla datatalouden kehitystä ohjataan myös globaalisti demokratiaan ja eurooppalaiseen arvopohjaan perustuvalle uralle. (Valtioneuvoston selonteko: Suomen digitaalinen kompassi).

5.5.4. Yhteenveto

Suomen digitalisaatiokehityksen suuntaamiseksi ja johtamiseksi on digitalisaation, datatalouden ja julkisen hallinnon kehittämisen ministerityöryhmän ohjauksessa ja digitoimiston valmistelussa laadittu Suomen digitaalinen kompassi. Digikompassi luotsaa suuntaa, kun luomme yhteistä etenemissuunnitelmaa digitalisaation ja datatalouden kehitykselle Valtioneuvoston selonteko: Suomen digitaalinen kompassi

Digitalisaatio mahdollistaa palveluiden asiakaslähtöisyyden, paremman laadun ja tuottavuuden kasvun sekä haastaa organisaatiot erityisesti toiminnalliseen muutokseen. Tämä uudistuminen edellyttää organisaatiolta ja sen henkilöstöltä kehittyneitä ongelmanratkaisutaitoja ja kokonaisuuksien hahmottamiskykyä. Henkilöstön osaamisesta tulee huolehtia. Uudenlaiset osaamiset, kuten kyberturvallisuus- ja dataosaaminen, ovat aikaisempaa tärkeämpiä digitalisoituvissa ympäristöissä.

Työryhmän mukaan valtion talous- ja henkilöstöhallintoa tulisi edelleen kehittää kustannustehokkaammaksi, vaikuttavammaksi ja uudistumiskykyisemmäksi. Kehittämistyössä tulisi edistää ihmislähtöistä digitalisaatiota ja tiedon parempaa hyödyntämistä yhteiskunnassa. Datan käsittelyyn ja hallintaan liittyvällä säädöspohjalla, tiedon yhtenäisellä luokittelulla ja prosesseilla tulisi mahdollistaa entistä laajempi automaatio ja nousevien teknologioiden hyödyntäminen. Tavoitteisiin pääsemiseksi, työryhmä esittää toimenpiteitä, joilla kehitettäisiin valtion henkilöstö- ja taloushallinnon datavarantoa kohti yhtenäistä luokittelua ja tietoturvallisia ratkaisuja. Suunnittelu on tärkeää tehdä monipuolisella, kattavalla viranomaisyhteistyöllä asiakasnäkökulmat huomioiden. Tiivis lainsäädäntöyhteistyö jo suunnitteluvaiheessa on mm. kustannustukihankkeessa todettu erityisen tärkeäksi (Yritysten tukena, yhteiskunnan hyväksi - Kuinka kustannustuet auttoivat yrityksiä selviämään koronapandemiasta 2020-2022 - hankkeen loppuraportti - Valtiokonttori). Tärkeään rooliin nousee myös digiajan tiedon jakamisen eri näkökulmat ja sen mukanaan tuomat uudet mahdollisuudet.

6. Työryhmän suositukset

Työryhmä esittää seuraavia suosituksia:

- Turvallisuusluokituksia koskevaan riski- ja vaikutustenarviointiin tulisi laatia ohjeistus, jonka avulla kasaumavaikutusta voidaan arvioida julkisten pilvipalveluiden käyttöönottoa harkittaessa tai niitä myöhemmin auditoita-

essa. Arviointiohjeistus pohjautuisi EU:n yleisen tietosuoja-asetuksen vaikutustenarviointia koskeviin vaatimuksiin sekä kansainväliseen ja kansalliseen turvallisuusluokiteltuja asiakirjoja koskevaan sääntelyyn.

Myös 31.6.2024 loppuun asti työskentelevän Cirrus-hankkeen tavoitteena on nopeuttaa julkisen hallinnon pilvisiirtymää vähentämällä ja poistamalla julkipilvipalveluiden tietosuojaan liittyviä riskejä sekä luomalla julkisen hallinnon vaatimuksiin yhtenäiset toimintamallit.

Työryhmä esittää, että Cirrus-hankkeen tulosten valmistuttua, henkilöstö- ja taloushallinnon kasaumavaikutuksen liittyvä ohjeistustarve arvioidaan. Mikäli ohjeistus tarvitaan, se laaditaan yhteistyössä Cirrus-hankkeen kanssa. Arviointiohjeistus esitellään tiedonhallintalautakunnalle syksyyn 2024 mennessä mahdollista suositusten laadintaa varten. Tiedonhallintalautakunta on työryhmän näkemyksen mukaan oikea taho antamaan asiasta koko julkista hallintoa koskevan suosituksen.

- Valtion talous- ja henkilöstöhallinnon turvaluokitellun tietoaineiston käsittelyyn esim. pilvessä, liittyviä riskejä ja niiden riskien hallintaa ja pienentämistä tulisi tietoaineiston luokittelulle määritellä yhtenäiset suositukset, jotta voidaan varmistaa palvelu- ja järjestelmäratkaisut, jotka ovat taloudellisuuden, teknologian, käyttäjäkokemuksen, yhteiskunnan huoltovarmuuskriittisten toimintojen näkökulmat ja riskienhallinnan näkökulmasta riittävät valtion talous- ja henkilöstöhallinnon toimivuudelle eri olosuhteissa.

  Työryhmä esittää, että valtiovarainministeriö vastaa työryhmätyöstä ja selvitys tehdään tiiviissä yhteistyössä Palkeiden ja Valtiokonttorin kanssa. Muut työryhmätyöhön osallistujat arvioidaan myöhemmin. Tämän kokonaisuuden valmistumisaikataulu syksy 2024.

- Työryhmä suosittelee tarkastelemaan automaation lisäämisen mahdollisuuksia valtion talous- ja henkilöstöhallinnon prosesseissa asiaa koskeva sääntely huomioiden. Tarkastelussa tulisi käydä läpi kaikki ns. päästä päähän -prosessien vaiheet ja hyväksyntäkohdat, jotta voidaan tunnistaa mahdolliset säädös- ja määräysmuutostarpeet.

  Työryhmä esittää tämän kokonaisuuden vetovastuuta Valtiokonttorille. Tämän kokonaisuuden valmistumisaikataulu 31.5.2024 mennessä.

Virastot ja laitokset tulisi ottaa mukaan moniammatillisesti ja laajasti suunnittelemaan pilvipalvelujen käyttöönottoa sekä automaation edistämistä valtion talous- ja henkilöstöhallinnon palveluissa.

Jakelu	Valtiovarainministeriön osastot Palkeet Valtiokonttori
Tiedoksi	Alivaltiosihteeri Susanna Huovinen Osastopäällikkö Juha Sarkio ICT-johtaja Jarkko Levasma