Valtiovarainministeriön lausuntopyyntö valtion talous- ja henkilöstöhallinnon tiedon luokittelusuosituksista (VN/8268/2024)

2. Suositusten valmistelu

Suosituksen tavoitteiksi on asetettu hallittu pilvisiirtymä, yhteinen näkemys talous- ja henkilöstöhallinnon tietojen luokittelusta, yhtenäiset talous- ja henkilöstöhallinnon prosessit ja yhteiset periaatteet tiedon tehokkaamman hyödyntämisen mahdollistamiseksi. Rahoitusvakausvirasto katsoo tavoitteet järkeviksi, ja kannattaa valtionhallinnon toimintaa yhtenäistäviä ja tehostavia uudistuksia.

Rahoitusvakausvirasto painottaa kokonaisturvallisuuden huomioivia ratkaisuja, joissa valtionhallinnon kaikki organisaatiot saataisiin yhtenäisten hyvin suojattujen talous- ja henkilöstöhallinnon järjestelmien piiriin. Nyt suunnitelluissa suosituksissa on vielä riski, että ne eivät täytä kaikkien viranomaisten vaatimuksia, jonka seurauksena osa viranomaisista jää omien ratkaisujen piiriin. Hajaantuneet ja eri tasoisesti suojatut talous- ja henkilöstöhallinnon järjestelmät voivat osaltaan haitata esimerkiksi niihin kohdistuvien uhkien havainnointia ja kansallisen tilannekuvan muodostamista.

3. Ohjaava sääntely

Suositusluonnoksessa kerrataan jo kumottua sääntelyä (henkilötietolaki (523/1999), tiedon suojaustasot). Syy siihen, miksi kumottua sääntelyä käydään läpi, olisi syytä tuoda suositustekstissä selkeästi esiin. Muuten suositus voi jäädä tältä osin harhaanjohtavaksi.

5. Johtopäätökset ja suositukset

Suositusluonnoksessa tuodaan selkeästi esiin virastojen vastuu tiedonluokittelusta, riskiarvioinnista sekä jäännösriskien hyväksymisestä.

Suositusluonnoksesta on kuitenkin häivytetty lähes olemattomiin palveluntuottajan rooli esimerkiksi yhteisrekisterinpitäjänä Tietosuoja-asetuksen 26. artiklan mukaisesti. Palveluntuottajan rooliin ja vastuisiin viitataan oikeastaan vain neljännen suosituksen toisessa virkkeessä, jossa kerrotaan palveluntuottajan vastaavaan suojauskeinoista ja jatkuvuudesta järjestelmien osalta.

Tämä vastuu edellyttää RVV:n näkemyksen mukaan varsin isoa koordinoivaa roolia, sillä vaikka yksittäinen virasto vastaa tiedon luokittelustaan ja riskiarvioinnista, ainoastaan palveluntuottajalla on täysi näkymä esim. koko tietomassan kasautumisvaikutusten arviointiin.

Yksittäisellä virastolla ei juuri ole todellista mahdollisuutta vaikuttaa palveluntuottajan järjestelmissään käyttämiin sopimusteknisiin riskien mitigointikeinoihin tai järjestelmien teknisiin määrityksiin. Erityisesti henkilötietojen siirtoihin liittyvät sääntelyriskit on usein vain hyväksyttävä sellaisenaan, jos yhteistä tietojärjestelmää mielii käyttää.

Rahoitusvakausvirasto
Työpajankatu 13 | PL 70 | 00581 Helsinki | www.rvv.fi | +358 295 253 500 | rahoitusvakausvirasto@rvv.fi

Jos TL IV -tiedonkäsittelyä toteutetaan julkisessa pilvipalvelussa toimivassa järjestelmässä, tulee järjestelmän siihen liittyvine prosesseineen olla auditoitu ulkopuolisen tahon toimesta TL IV -vaatimukset täyttäväksi. Auditoinnissa tulee huomioida etenkin toiminnan jatkuvuus, mikäli kyseessä on ulkomailta käsin toimiva julkinen pilvipalvelu. RVV:n näkemyksen mukaan turvallinen tiedonkäsittely ja tietojen saatavuus tulee varmistaa arvioimalla palveluntuottajan tekninen, fyysinen ja hallinnollinen tietoturvallisuus, sekä sitoumustenhoitokyky, ja auditointi tulisi toteuttaa määrätyn turvallisuusviranomaisen toimesta.

Lisäksi palveluntuottajan koordinointirooli on olennainen sen tavoitteen saavuttamisessa, että talous- ja henkilöstöhallintoon saadaan luotua yhteiset periaatteet tiedon tehokkaammaksi hyödyntämiseksi, sillä analysointi- ja raportointipalveluita tuottavien tahojen on määriteltävä tiedon luovuttamiset yhteistyössä virastojen kanssa tiedonhallintalain (906/2019) 5 luvun mukaisesti.

Jaakko Weuro
ylijohtaja

Taneli Kilpiö
tietoturva-asiantuntija