M.NATRI/KA

TIETOTURVALLISUUDEN ARVIOINTIOHJE – Lausunto

s.5: ”Auditoinnit ja arvioinnit ovat lisääntyneet merkittävästi, mutta viranomaisilla on paljon epätietoisuutta siitä milloin arviointeja tulisi tehdä, miten, kenen toimesta ja mitä viitekehyksiä arviointiin pitää käyttää. Tämä ohje pyrkii selventämään näitä kysymyksiä sekä antamaan suosituksia arviointien suorittamiseen.”

Tämä on hyvä huomio, erityisesti omaehtoiset arvioinnit sen jälkeen kun valtionhallinnon virasto on täyttänyt auditointivaatimukset esim. perus- tai korotetulle tasolle (riippuen siitä minkä tason aineistoa ao. virasto toiminnassaan käsittelee) ovat olleet aiemmin ainakin jossain määrin ohjeistamatta.

s.16: ” Tietojärjestelmien arviointia koskevan lain mukaisia arviointeja voivat tehdä Viestintävirasto sekä sen hyväksymät tietoturvallisuuden arviointilaitokset. Viranomaishyväksynnän voi kuitenkin antaa ainoastaan Viestintävirasto. Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä arviointiin 1.6.2015 lähtien vain tämän lain menettelyä. Velvoitteella varmistetaan se, että valtionhallinnon viranomaiset käyttävät vain luotettavia ulkopuolisia tietoturvallisuuden arviointipalveluja, jotka hoitavat arviointitehtävää julkisena hallintotehtävänä. Tämä on tarpeen sen vuoksi, että valtionhallinnon viranomaisten tietojärjestelmien arvioinnit toteutettaisiin yhtenäisillä menettelytavoilla ja siten toimeksiantaja saisi arvioinnista aiheutuvia kustannuksia vastaavan hyödyn valtionhallinnon tietoturvallisuuden kehittämiseksi yhtenäisellä tavalla ja ilman perustaltaan epäasiallisia kustannuksia. Viranomaiset voivat kuitenkin osana normaalia toiminnan kehittämistä tehdä itse viranomaisarviointiin valmistavia sisäisiä arviointeja tai itsearviointeja. Erityisesti muutosten yhteydessä toiminnan arvioiminen on tärkeää. Ohjatuissa sisäisissä arvioinneissa ja itsearvioinneissa voidaan myös hyödyntää ulkopuolisia palveluntuottajia.”

Kannatettavaa, koska yllämainituin keinoin arvioinnit saadaan yhteismitallisiksi eri virastojen välillä.

s.18: ” Valtionhallinnon viranomaisten välisissä sopimuksissa, joissa sopijapuolet luovuttavat salassa pidettävää tietoa, sopijapuolet toteavat minkä suojaustason mukaista tietoa sopimuksen perusteella luovutetaan, tai jos kyseessä on tietojärjestelmää taikka

tietoliikennejärjestelyä koskeva sopimus, minkä suojaustason mukaisia vaatimuksia järjestelmään sovelletaan.

Tietoturvallisuusvaatimusten noudattamisen todentamiseksi tietoja luovuttava taho voi pyytää selvityksen siitä, että tietoja vastaanottava taho on tehnyt asiakirjojen luokittelua koskevan päätöksen ja noudattaa soveltuvaa tietoturvallisuuden tasoa. Tietoturvallisuuden tason noudattaminen voidaan tarpeen mukaan osoittaa myös tiedon vastaanottavan tahon teettämää tietoturvataso- tai tietojärjestelmäarviointia koskevalla raportilla. Jos esimerkiksi valtionhallinnon palvelukeskus hankkii palvelua kaupalliselta palvelutoimittajalta, se voi suorittaa palvelun tietoturvallisuuden arvioinnin ennen palvelun käyttöönottoa. Muilla palvelua käyttävillä viranomaisilla ei silloin ole tarvetta suorittaa tietoturvallisuuden arviointia uudelleen.”

Tämä selkiyttää olennaisesti tämänhetkistä tilannetta.