OM 5/043/2014

OIKEUSMINISTERIÖ

Tietohallintoyksikkö

LAUSUNTO

8.8.2014 VM047:21/2007

TIETOTURVALLISUUDEN ARVIOINTIOHJE

Asia: Oikeusministeriön lausunto tietoturvallisuuden arviointiohjeesta

Valtiovarainministeriön Julkisen hallinnon ICT-toiminto on pyytänyt 13.6.2014 lausuntoa tietoturvallisuuden arviointiohjeesta. Oikeusministeriö esittää lausuntona seuraavan.

Ohjeen sivuilla 8 ja 20 läpikäydään lakia viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden arvioinnista. Ohjeeseen ei ole kirjoitettu lain pääsääntöä, jonka mukaan: ”Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain tässä laissa tarkoitettua menettelyä taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaan.” .” Ohjeen jatkovalmisteluissa näyttäisi olevan tarpeen selvittää, voivatko viranomaiset käyttää tietotekniikan kehittämishankkeissa muunlaisia arviointimenettelyjä.

Ohjeen sivuilla 11 ja 23 kerrotaan hankinnoista. Ohjeessa sanotaan, että mikäli hankinnan kohteena on tietojärjestelmä tai tietoliikennejärjestely, määrittelee hankintayksikkö **tarpeen mukaan** näitä koskevat tietoturvallisuusvaatimukset. Tämä on ristiriidassa mm. "VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje" jossa sanotaan: ”Tietoturvallisuuteen liittyvät uudet vaatimukset tulee huomioida ICT-hankinnoissa; niissä tulee huolehtia tietoturvallisuusasetuksen, tietoturvatasojen ja ICT-varautumisen vaatimusten ohella hankinnan kohteeseen liittyvistä substanssikohtaisista vaatimuksista.” Ohjeeseen tulisi täsmentää, milloin tietoturvavaatimusten

Käyntiosoite	Postiosoite	Puhelin	Faksi	Sähköpostiosoite
Eteläesplanadi 10 HELSINKI	PL 25 00023 VALTIONEUVOSTO	02951 6001	09 1606 7730	oikeusministerio@om.fi

määrittely on pakollista, ja koska määrittelyä ei tarvitse tehdä. Tietoturvavaatimusten määrittely on äärimmäisen tärkeää. Oikeusministeriö suosittelee, että ohjeessa korostettaisiin vieläkin vahvemmin tietoturvavaatimusten kattavaa suunnittelua ja määrittelyä niin, että ne saadaan osaksi kilpailutusta.

Sivulla 18 läpikäydään tietoturvamenettelyitä, kun sopijakumppanina on toinen valtiohallinnon viranomainen. Ohjeessa sanotaan: "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." Vahti 2/2010 ohjeessa sanotaan, että luokiteltuja tietoaineistoja voidaan luovuttaa, mikäli vastaanottava taho tuntee käsittelysäännöt ja käsittely-ympäristö on luokitellun asiakirjan suojaustasoa vastaavalla tasolla. Oikeusministeriö suosittelee, että ohjeen kohtaa muutetaan niin, ettei siitä voi vahingossakaan saada sellaista käsitystä, ettei luokiteltuja tietoaineistoja voida luovuttaa sellaisille tahoille, jotka eivät ole tehneet luokittelupäätöstä.

Yksityisiä yrityksiä sopimuskumppanina käsittelevässä jaksossa (s. 18) on todettu, että yksityiset yritykset ja muut vastaavat toimijat eivät olisi velvoitettuja noudattamaan julkisuuslain hyvää tiedonhallintatapaa tai tietoturvallisuusasetuksen vaatimuksia ilman erillistä sopimusta.

Virke voidaan johtaa epätarkkuutensa vuoksi harhaan. Ensinnäkin yksityisen yritykseen voidaan suoraan julkisuuslain nojalla tai erityislaissa olevan säännöksen perusteella soveltaa julkisuuslakia. Toisekseen yksityinen toimija, joka on saanut viranomaiselta salassa pidettäviksi säädettyjä tietoja, kuuluu julkisuuslain salassapito- ja vaitiolovelvollisuutta koskevien velvoitteiden piiriin. Tästä johtuu, että valtionhallinnon tietoturvallisuutta koskevilla menettelyvaatimuksilla voi olla vähintäänkin välillistä vaikutusta sen arviointiin, onko salassapito- ja vaitiolovelvollisuutta noudatettu. On nimittäin selvää, että mainitut velvollisuudet kattavat myös sellaiset tilanteet, joissa salassa pidettävä asiakirja on jätetty sellaiseen paikkaan tai joissa sitä on muutoin käsitelty tavalla, joissa salassa pidettävät tiedot joutuvat tai ovat sivullisten saatavissa.

Sivulla 24 sanotaan, että tietojärjestelmähankkeissa auditointimahdollisuus tulee varmistaa etukäteen jo ennen hankkeen käynnistämistä. Oikeusministeriö suosittelee, että tämän merkitystä korostetaan ohjeessa ja ohjeeseen lisätään, että auditointimahdollisuuden vaatiminen on syytä olla pakollinen tietoturvavaatimus kaikissa tietoliikenne- ja järjestelmähankkeissa.

Sivulla 25 sanotaan, että: "Luonnollisesti auditoinnit jatkuvat tuotantovaiheessa." Oikeusministeriö suosittelee, että ohjeessa korostetaan, että vi-

ranomaisella tulee olla auditointisuunnitelma ja uudet järjestelmät tulee lisätä olemassa olevaan auditointisuunnitelmaan ja auditointeja suorittaa jatkossa sen mukaisesti.

Tietohallintojohtaja Max Hamberg

Riskienhallinnan erityisasiantuntija Matti Aitta