Tuomioistuinvirasto
Domstolsverket

Dnro 196/00.00.02.00/2021

5.3.2021

Liikenne- ja viestintäministeriö

kirjaamo@lvm.fi

Viite: Lausuntopyyntö VN/3501/2021 Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla

Asia: Tuomioistuinviraston lausunto

Yleinen osio

Tuomioistuinvirasto kiittää mahdollisuudesta lausua ja pitää erittäin kannatettavina periaatepäätöksessä ehdotettuja toimenpiteitä, joiden avulla on tarkoitus turvata tietosuojan ja tietoturvan korkeaa tasoa kriittisillä toimialoilla, ja osin laajemminkin valtionhallinnossa.

Periaatepäätöksessä ei oli linjattu tyhjentävästi sitä, mitä kriittisillä toimialoilla käytännössä tarkoitetaan. On tärkeää, ettei tietosuojaan ja tietoturvaan liittyviä tukitoimia sidottaisi liikaa vain määrättyihin toimialoihin, koska voi syntyä myös sellaisia tietoturvaloukkaustilanteita, joiden osalta niiden kriittisyys ja tosiasiallinen merkitys yhteiskunnan toiminnan kannalta tunnistetaan vasta silloin, kun itse loukkaustilanne aktualisoituu. Esimerkiksi tietosuojan näkökulmasta arvioituna korkean riskin käsittelytoimia toteutetaan huomattavasi laajemminkin viranomaistoiminnassa, kuin pelkästään nyt tarkoitetuilla kriittisillä toimialoilla. On myös tärkeää, että myös tällaisissa tilanteissa osaaminen ja erityisesti vahingon rajoittamiseen liittyvät tukitoiminnot ovat pikaisesti saatavilla viranomaistoiminnan osalta riippumatta siitä, kohdistuu vahinko määrättyyn toimialaan.

On kannatettavaa, että turvallisuuden tasolle pyritään kriittisissä toiminnoissa määrittämään konkreetteja minimivaatimuksia. Tietosuojan ja tietoturvan riittävän tason määrittäminen on kuitenkin jatkuvaa ja dynaamista työtä, jota tosiasiallisesti tehdään subjektiivisen arvion pohjalta sen hetkisessä toimintaympäristössä ja valittuun parametriin heijastaen. Myös tarkastelukohteen rajaus voi olennaisesti vaikuttaa siihen, millaisia huomioita tarkasteltavasta kohteesta tehdään. Tiedon, käsittelyprosessien ja teknisen ympäristön kokonaissuojauksen todellinen tarve konkretisoituu usein vasta riskiperusteisen arvion kautta. Koska työn tulee olla viranomaisessa jatkuvaa, on varmistettava, että tätä työtä todella tehdään dynaamisesti, tarpeeksi kattavasti sekä toimialaan sopivia parametrejä vasten (esimerkiksi ISO 27000 sopivuutta voi olla tarpeen arvioida tilanne- ja toimialakohtaisesti). Tälle työlle on myös varattava riittävät resurssit myös käytännön tasolla, koska pelkkä vaatimusten esittäminen ilman toteuttamiseen varattavia lisäresursseja ei vielä muuta tietosuojan tai tietoturvan tosiasiallista tilaa.

Niiltä osin, kun on tärkeää määrittää tietosuojaan ja tietoturvaan kohdistuvien vaatimusten kohdistuminen määrättyjen toimialojen toimijoihin, on myös välttämätöntä tunnistaa linkitykset muihin tahoihin sekä varmistaa vaatimustason toteutuminen esimerkiksi ulkoistettujen ja muihin toimijoihin liittyvien prosessien yhteydessä.

Yksityiskohtaiset huomiot

1. Usein tietoturvan ja tietoturvatilanteiden selvittäminen ja niistä seuraavien vahinkojen torjuminen edellyttää viranomaisten välistä tiedonvaihtoa. Luovutusten yhteydessä yhteensovitettavaksi tulevat usein luovutusta koskevan lainsäädännön ohella henkilötietojen käsittelyyn oikeuttava tietosuojalainsäädäntö. Tiedonvaihtoa koskevaa lainsäädäntöä tulee tarkistaa siten, että tietojen luovutusta ja käsittelyä koskevat säännökset luovat yhtenäisen, yksiselitteiden ja selkeän kokonaisuuden. Nyt tietojen luovutuksiin liittyvä harkinta on monivaiheista ja eri lakien säännöksiin hajautunutta, joka osaltaan voi hidastaa toimintaa myös tietoturvaloukkauksiin liittyvissä tilanteissa.

4. On erittäin tärkeää ja kannatettavaa, että Kyberturvallisuuskeskus pystyy tukemaan ja antamaan neuvontaa kaikille hallinnonaloille. Esimerkiksi tuomioistuinten toiminta on erittäin tietointensiivistä ja suuri osa käsiteltävistä henkilötiedoista ovat korkeampien suojausvaatimusten piirissä, koska loukkaustilanteista voi aiheutua erittäin korkea riski rekisteröidyn oikeuksille ja vapauksille.

6. Tietoturvallisuuden kartoituspalveluita tulisi tarjota myös muille toimijoille, kuin kriittisten alojen toimijoille, erityisesti silloin, kun muutoin on pääteltävissä ja osoitettavissa, että henkilötietojen käsittelytoimet ovat luonteeltaan sellaisia, että niihin liittyy korkea riski (esimerkiksi laaja-alainen erityisten henkilötietojen tai rikostuomioituihin ja rikkomuksia koskeva käsittely).

7. Tuomioistuinvirasto pitää erittäin kannatettavana sitä, että selvitetään viranomaisten tarpeet teknologisille ratkaisuille salassa pidettävän ja turvaluokitellun tiedon käsittely-ympäristöjen luomiseen. Erityisen tärkeitä tuomioistuintenkin toiminnan kannalta ovat viranomaisten yhdenmukainen salattu sähköpostiviestintä, turvalliset neuvotteluyhteydet ja -palvelut sekä turvallinen tiedonsiirtopalvelu. Todettakoon, että tällaisen tiedon käsittelylle on tarvetta sellaisissa tilanteissa, joissa viranomainen pitää yhteyttä tai viestii yksittäisen kansalaisen tai yksityisen tahon toimijan kanssa, ei ainoastaan viranomaisten keskinäisessä viestinnässä. Tämän vuoksi myös palveluiden saatavuuteen ja häiriöttömyyteen on kiinnitettävä erityistä huomioita, luottamuksellisuuden ohella.

24 – 25. Kappaleessa tunnistetaan Valtori keskeiseksi toimijaksi tieto- ja viestintäpalvelujen tuottajana ja sen osalta ehdotetaan lisätoimenpiteitä tietosuojan ja tietoturvan toteuttamiseksi. Oikeushallinnon alalla tietojärjestelmien ylläpidosta vastaa pääosin Oikeusrekisterikeskus. Tuomioistuintoiminnan osalta kriittisten tietojärjestelmien, kuten lainkäyttöön liittyvien tietojärjestelmien ylläpito ja kehittämistehtävät on tuomioistuinlaissa osoitettu Tuomioistuinvirastolle. Molempien toimijoiden järjestelmiä voidaan pitää kriittisinä yhteiskunnan toiminnan kannalta ja vastaavalla tavalla periaatepäätöksen tulisi tukea tietosuojan ja tietoturvan toteutumista asianmukaisin keinoin myös tässä kontekstissa.

Todettakoon, että tuomioistuimilla voi olla erittäin merkittävä rooli tietosuojaan ja tietoturvaan liittyvien tilanteiden selvittämisessä ja tätä kautta myös mahdollisen vahingon rajoittamisessa, koska poliisin käyttämien salaisten pakkokeinojen käyttö edellyttää lupaa tuomioistuimelta (kts. periaatepäätöksen kohdat 20 – 22).

28. Tietosuojan ja tietoturvan integroiminen kiinteäksi osaksi julkisia hankintoja on erittäin tärkeää, koska näissä tapauksessa usein hankitaan palveluja yksityisiltä toimijoilta. Viranomaisten tulee voida varmistua siitä, että tietosuojan ja tietoturvan taso pysyy korkeana läpi alihankintaketjun. On myös tärkeää, että palveluntarjoajat osaavat ja pysyvät osaltaan todentamaan ja osoittamaan, että palvelut tosiasiallisesti täyttävät kaikki viranomaistoimintaa koskevat vaatimukset, kuten tiedonhallintaa sekä tietosuojaa koskevat vaatimukset silloin, kun ne tarjoavat palvelujaan viranomaisille.

Ylijohtajan sijaisena, Johtaja Tiina Kukkonen – Suvivuo

Tietosuojavastaava Raisa Leivonen