

Lausunto

02.03.2021

Asia: VN/3501/2021

Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; lausuntopyyntö (Huom! Lausuntoaika päättyy 3.3.2021)

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Electronic Frontier Finland – Effi ry kiittää mahdollisuudesta tulla kuulluksi asiassa.

Effi on vuonna 2001 perustettu kansalais- ja asiantuntijajärjestö, joka puolustaa perus- ja ihmisoikeuksia digitaalisessa toimintaympäristössä. Näkökulmamme on erityisesti sähköisiä palveluja käyttävän kansalaisen tietosuojaa ja perusoikeuksia painottava.

Effi pitää tietoturvan ja tietosuojan kehittämistä yhteiskunnassa erittäin tärkeänä kansalaisten yksityiselämän suojan ja muiden perusoikeuksien takaamiseksi. Kriittisen infrastruktuurin tietoturvatason nostaminen kokonaisuudessaan on kansalaisten turvallisuuden kannalta elintärkeää. Kriittistä infrastruktuuria vastaan tehdyt hyökkäykset ovat "normalisoituneet" maailmassa ja kynnyksen kyberhyökkäyksen tekoon on laskenut.

Effi korostaa, että tietoturvatason parantaminen yhteiskunnan kriittisillä alueilla on erityisen tärkeä tavoite. Kansalaisten kannalta tämä on yksi parhaista tavoista edistää kriittisen infrastruktuurin resilienssiä kyberhyökkäyksiä vastaan ja parantaa kansalaisten turvallisuutta niin, että kansalaisten perusoikeuksiin ei tarvitse kajota.

Tietoturvan yhteydessä on syytä pohtia myös sitä, mikä on tasapaino kansallisen tietoturvan ja muiden valtioiden ja toimijoiden tietoturvan välillä. Suomen etu ei esimerkiksi ole aina sama kuin muiden valtioiden saati liikeyritysten. Esimerkiksi kysymys siitä, minkä yritysten käsiteltäväksi

henkilötietoja voidaan antaa käsiteltäväksi on tällainen tai se, missä asioissa Suomi voi luottaa edes toisen EU-jäsenvaltion lainsäädännön alla tapahtuvaan henkilötietojen käsittelyyn.

Monet yhteiskunnan käyttämistä kriittisistäkin palveluista on tuotettu Suomen ulkopuolella. Tällöin tulee arvioitavaksi miten luotettava palvelut tuottava organisaatio on ja myös palveluiden tuotantomaan lainsäädäntö esimerkiksi tiedustelua koskevan lainsäädännön osalta. Jotta palvelut toimivat kriisitilanteessa, meidän täytyy voida luottaa sekä palveluntarjoajaan että tietoverkkoyhteyksiin Suomen ja palveluiden tuotantomaan välillä. Pilvipalveluiden yhteydessä on syytä muistaa yksinkertainen nyrkkisääntö: pilvipalvelu on vain jonkun muun tietokone tai joukko niitä.

Tietosuoja-asetuksen takaamien rekisteröidyn oikeuksien toteutumista tulee parantaa huomattavasti. Tällä hetkellä Suomessa ei ole määritelty lainkaan kansallisessa lainsäädännössä, mitä ovat ne tehokkaat oikeussuojakeinot, joita rekisteröity voi käyttää viimekätisesti asiassaan. Tietosuojalakiin tulee tehdä muutos, jossa määritellään mikä oikeusistuin käsittelee tietosuojaan liittyvät asiat. Selvyyden vuoksi mainittakoon että kyse on eri asiasta kuin tietosuojavaltuutetulle tehty valitus ja sen käsittely: jos esimerkiksi tietosuoja-asetuksen määrittelemästä henkilötietojen tietoturvaloukkauksesta aiheutuu rekisteröidylle taloudellista haittaa, tämän täytyy hakea asiassa korvausta oikeusteitse. Tietosuojavaltuutettu ei ole tuomioistuin. Kun tietosuojalajissa ei, lainvalmisteluissa esitetystä asiantuntijalausunnosta huolimatta, ole määrittelyä oikeusistuimesta, Suomi ei tältä osin noudata valtiona tietosuoja-asetuksen mukaisia velvoitteitaan.

Tietosuojan osalta rekisteröidyn oikeuksien toteutumista viranomaistoiminnassa tulee edistää myös muuttamalla tietosuojalakia siten, että tietosuoja-asetuksen artiklan 83 määrittelemiä hallinnollisia sakkoja voidaan määrätä myös viranomaisille.

Kansalaisten oikeuksien parantaminen suhteessa henkilötietojen käsittelyyn edellyttää myös tietosuojavaltuutetun kohtuuttoman pitkien käsittelyaikojen huomattavaa lyhentämistä. Tietosuojavaltuutetun vuosikertomuksissaan esittämät lyhyet keskimääräiset käsittelyajat ovat vain puolet totuutta: sekä oikeuskansleri että eduskunnan oikeusasiamies ovat huomauttaneet useaan kertaan tietosuojavaltuutettua pitkistä, jopa vuosien mittaisista käsittelyajoista. On selvää että rekisteröidyn oikeudet eivät toteudu nykyisessä tilanteessa. Lisäksi olisi toivottavaa että tietosuojavaltuutettu valvoisi oma-aloitteisesti yksityisen sektorin toimintaa. Tiedossamme ei ole ainoatakaan tapausta, jossa tietosuojavaltuutettu olisi oma-aloitteisesti ottanut tutkittavakseen yksityisen sektorin laiminlyönneihin liittyvää tapausta

Erytystä huomiota hankkeessa tulee kiinnittää siihen, että tällä hetkellä viranomaiskentässä on tietoturvaan ja -suojaan liittyen ainakin seuraavat ongelmat:

* Viranomaisen ei tunnista tai ota huomioon pakottavan lainsäädännön vaatimuksia suhteessa toimintaan. Tiedossamme on tapauksia, joissa viranomaisen ei vastaa tiedusteluihin ylläpitämänsä henkilörekisterin tietosuojaselosteesta. Esimerkiksi poliisihallitus ei ole miltei neljässä vuodessa vastannut liikenteenvalvonnan kameravalvontajärjestelmien tietosuojaselostetta tai -selosteita koskevaan, kirjaamon kautta esitettyyn tiedusteluun.

* Viranomaisen tulkitsee toimintansa tai valvontamandaattinsa vain Suomen lainsäädäntöön pohjautuvaksi vaikka Suomea sitoo myös EU:n pakottava lainsäädäntö.

Näistä syistä lakimuutoksia tehtäessä tulee kiinnittää huomiota siihen, että eri viranomaisten velvollisuudet ja tehtävät määritellään laissa siten, että sekä kansallinen että EU-lainsäädäntö otetaan huomioon. Esimerkiksi Traficomien tulkinta siitä, että heidän valvonta- ja neuvontavelvollisuutensa koskien Internet-selainten evästeiden ja jäljittimien käyttöä koskevaa suostumusta perustuu vain kansalliseen lainsäädäntöön, tarkemmin lakiin sähköisen viestinnän palveluiden tarjoamisesta, on esimerkki EU-tason sääntelyn huomioimatta jättämisestä.

Effi pyytääkin linjauksissa kiinnittämään erityistä huomioita seuraaviin asioihin:

* Lainsäädännön ja tietosuojavaateiden tulee tukea pyrkimystä minimoida käsiteltävien henkilötietojen määrä vain välttämättömään tietoon.

* Tietosuoja ei saa rajoittaa hallinnon avoimuutta tai haitata avointa julkista kilpailutusta.

* Jotta tehokas julkinen kilpailutus toimisi, ohjelmistokehityshankkeiden tulisi olla jaettavissa mahdollisimman pieniin osiin ja tiedonkulku hankkeiden välillä on taattava.

* Avointen ohjelmistojen ja rajapintojen käyttöä on edistettävä mm. toimittajariippuvuuden välttämiseksi.

* Lopulta tehokkaat ohjelmistoprojektit edistävät myös tietoturvaa.

* Asiantuntijapulasta johtuen toteutettavien toimien on tähdättävä skaalautuvuuteen.

* Vähintään julkisten toimijoiden on oletuksena minimoitava ihmisten profilointi ja tunnistaminen, esim. käytettävä vain välttämättömiä evästeitä. Turha henkilötietojen käsittely ja tunnistaminen luo aina väärinkäytöksen riskin. On jopa havaittavissa että toimijat antavat ymmärtää olevansa kiinnostuneita tietosuojaan ja tietoturvaan liittyvistä asioista, mutta käyttäytyvät niistä jokseenkin välittämättä.

* On muistettava turvata palveluihin pääsy myös niille, jotka eivät pysty käyttämään tai eivät halua käyttää sähköisiä palveluita.

Romppainen Leena
Electronic Frontier Finland - Effi ry