CSC-Tieteen tietotekniikan keskus Oy

Lausunto

07.09.2017 1/41/2016

Asia: 1/41/2016

Lausuntopyyntö yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietinnöstä ja työryhmän ehdotuksesta hallituksen esitykseksi uudeksi tietosuojalaiksi

1 luku. Yleiset säännökset

Yleiset kommentit

-

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

CSC Tieteen tietotekniikan keskus Oy kiittää mahdollisuudesta saada lausua yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietinnöstä ja työryhmän ehdotuksesta hallituksen esitykseksi uudeksi tietosuojalaiksi. CSC on suomalainen tutkimuksen, koulutuksen ja julkishallinnon ICT osaamiskeskus, joka ylläpitää opetus ja kulttuuriministeriön toimeksiannosta korkeakoulujen valtakunnallista keskitettyä tietotekniikkainfrastruktuuria ja tarjoaa sen avulla kansallisia tietotekniikkapalveluita tutkimuksen, tieto-, opetus- ja tutkimushallinnon sekä kirjastojen, arkistojen, museoiden ja kulttuurin tarpeisiin.

Yleisen tietosuoja-asetuksen toimivuuden kannalta on ensiarvoisen tärkeää, että pyritään mahdollisimman yhtenäiseen eurooppalaiseen ratkaisuun. Tiedon liikkuvuuden mahdollistamisen ja vastuullisuuden tulee näkyä asetuksessa keskeisinä asiakohtina.

Erityistä huomiota tulee kiinnittää siihen, että henkilötietojen riittävän joustava käsittely tieteellisessä tutkimuksessa on mahdollista, ja että henkilötiedot on suojattu asianmukaisesti ja vastuullisesti. Henkilötietojen riittävän joustava käsittely tutkimuksessa on keskeinen menestystekijä suomalaiselle tieteelle ja Suomen kilpailukyvylle. Näin ollen on tärkeää huomioida että lainsäädännöllä ei suojata henkilötietojen käsittelyä siten, että suojauksesta aiheutuu perusteetonta haittaa tieteelliselle tutkimukselle. Kansalaisten oikeuksien kannalta erityistä huomiota tulee kiinnittää arkaluontoisten henkilötietojen asianmukaiseen suojaamiseen. Arkaluontoisia henkilötietoja ovat mm. henkilön terveyteen, mielipiteisiin, kulutustottumuksiin sekä viestintään liittyvät tiedot.

EU:n yleistä tietosuoja-asetusta täydentävän kansallisen tietosuojalain suurimpia käytännön haasteita ovat vastuukysymykset, sekä hallinnollisten ja teknisten suojaamiskeinojen määrittely. Vastuiden määrittelyt ovat sekä tietosuojan että tietoturvallisuuden osalta usein käytännössä epäselviä. Vastuukysymysten selkiyttäminen on ensiarvoisen tärkeää, ja vastuu tulee selkeästi kohdistaa henkilötietojen turvaamisesta tietoja käsittelevän organisaation ylimpään johtoon sekä toiminnasta vastaavaan työnjohtoon. Yksittäisen suorittavaa työtä tekevän työntekijän tai virkamiehen vastuu siitä, että hän noudattaa annettuja ohjeita tietosuojaan liittyen, tulee olla selvästi rajattu ja ilmaistu. Ohjeiden merkittävä tai törkeä laiminlyönti tulee olla rangaistava teko. Kansalaisen ja tietojärjestelmien käyttäjän tulee noudattaa annettuja käyttöehtoja ja – ohjeita, ja tuottamuksellinen tietosuojarikos ja sen yritys tulee olla rangaistava teko.

Tietosuojalaki tulee valmistella rinnakkain ns. toisiolain (Hallituksen esitys laiksi sosiaali- ja terveystietojen tietoturvallisesta hyödyntämisestä sekä eräiksi siihen liittyviksi laeiksi) kanssa siten, että molemmat lait ovat keskenään toisiaan täydentäviä mutta eivät ristiriitaisia.

2 luku. Käsittelyn oikeusperuste eräissä tapauksissa

Yleiset kommentit käsittelyn lainmukaisuutta koskevasta 3 §:stä.

-

Yleiset kommentit erityisiä henkilötietoryhmiä koskevasta 5 §:stä ja rikostuomioita ja rikkomuksia koskevasta 6 §:stä.

-

Tietoyhteiskunnan palvelujen tarjoamiseen lapselle sovellettavan ikärajan tulisi olla:

-

Ikärajaa koskevat perustelut

-

3 luku. Valvontaviranomainen

Yleiset kommentit suullista käsittelyä seuraamuslautakunnassa koskevasta 16 §:stä

Seuraamuslautakunnan tulisi käsittelyssään arvioida, onko henkilötiedot suojattu noudattaen hyvää tiedonhallintatapaa, riittävää tietoturvallisuuden tasoa hallinnollisten ja teknisten suojaamiskeinojen osalta.

Muut yleiset kommentit valvontaviranomaista koskevasta 3 luvusta.

Valvontaviranomaisella tulee olla riittävät resurssit tunnistaa, täsmentää ja viestiä, mikä on hyvä tiedonhallintatapa ja riittävä tietoturvallisuuden taso sekä hallinnollisten että teknisten suojaamiskeinojen osalta.

4 luku. Oikeusturva ja seuraamukset

Yleiset kommentit käsittelyn viivästymistä koskevasta 23 §:stä.

-

Tulisiko yleisen tietosuoja-asetuksen 83 artiklan mukaisia hallinnollisia sakkoja voida kohdistaa myös viranomaisiin ja julkishallinnon elimiin?

ei

Perustelut

CSC:n näkemyksen mukaan hallinnollisten sakkojen kohdistaminen viranomaisiin ja julkishallinnon elimiin ei ole perusteltua.

Valtio joutuu viime kädessä itse kattamaan hallinnollisten sakkojen kustannukset tai perimään vastaavat varat esimerkiksi korotettuina käyttömaksuina kansalaisilta. Tämän lisäksi viranomaiset toimivat jo virkavastuulla tietoja käsitellessään, ja tätä kautta on jo olemassa toimiva käytäntö seuraamuksista virkavelvollisuuden rikkomisesta.

Mikäli vastaus hallinnollisten sakkojen kohdistamista viranomaisiin koskevaan kysymykseen on ei, pyydetään esittämään näkemys vaihtoehtoisesta seuraamusjärjestelmästä.

Laissa tulee selkeästi kohdistaa vastuu henkilötietojen turvaamisesta tietoja käsittelevän organisaation ylimpään johtoon sekä tämän lisäksi myös toiminnasta vastaavaan työnjohtoon. Tietosuojaa ja tietoturvallisuutta koskevien vastuiden selkiyttäminen on tärkeää. Yksittäinen suorittavaa työtä tekevä työntekijä tai virkamies tulee voida asettaa vastuullinen siitä, että hän noudattaa annettuja ohjeita tietosuojaan liittyen. Ohjeiden merkittävä tai törkeä laiminlyönti tulee olla rangaistava teko kuten tietosuojarikoksesta säädetään (katso tarkempi näkemys kohdasta laki rikoslain 38 luvun 9 §:n ja 10 §:n 3 momentin muuttamisesta).

Esimerkiksi työsuojeluun liittyvissä vakavissa laiminlyönneissä on muodostunut selkeä oikeuskäytäntö, jossa usein toimitusjohtaja sekä vastaava työnjohtaja voi joutua oikeudelliseen edesvastuuseen.

Muut yleiset kommentit oikeusturvaa ja seuraamuksia koskevasta 4 luvusta.

Oikeusturvan kannalta on oleellista, että tietosuojaviranomainen määrittelee ja viestii riittävän selkeästi mitkä ovat ajantasaiset vaatimukset turvata henkilötiedot hallinnollisin ja teknisin suojaamistoimenpitein. Suojaamistoimenpiteiden tulee perustua olemassa oleviin ja tunnettuihin kansainvälisiin sekä kansallisiin varmennettaviin tietoturvallisuuskäytäntöihin, kuten tunnetut kansainväliset tietoturvallisuus sertifionnit (esim. ISO/IEC 27001) . Ei ole suositeltavaa, että tietosuojaviranomainen määrittelee itse virastokohtaisesti erillisnormeja tähän liittyen.

5 luku. Tietojenkäsittelyn erityistilanteet

Yleiset kommentit henkilötietojen käsittelyä journalistisia, akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten koskevasta 27 §:stä.

Tiedon luovuttajan, tiedon käyttäjän, tiedon prosessointialustan ja tiedon haltijan tai lupaviranomaisen roolit on tärkeä selkiyttää. Esimerkiksi CSC arkaluonteisen datan käsittelee genomidataa ja siihen liittyvää metadataa ainoastaan tiedon haltijan toimeksiannosta ja ohjeiden mukaisesti. Tiedon prosessoinnin alustoille ei siis pidä syntyä omistajuutta tai edes käsittelyperustetta vain sillä perusteella, että data sijoitetaan tietylle alustalle. Arkaluontoisen datan prosessoinnin alustoja on yksityisellä ja julkisella sektorilla. Oikeudet arkaluonteisen datan käsittelyyn tulee erikseen pyytää alkuperäiseltä tiedon omistajalta.

Tietoteknisten palveluntarjoajien vastuu tietosuojan osalta rajautuu sen mukaan, miten vastuut palvelun käyttöehdoissa on määritelty. Mikäli vastuu palvelun tietystä osasta, kuten käyttäjähallinta tai sovelluksen ylläpito, ei ole palveluntarjoajan vaan asiakkaan tai kolmannen osapuolen vastuulla, tulee viimeksi mainittu taho myös olla vastuullinen kyseisten toimintojen henkilötietojen suojaamisesta.

Yleiset kommentit tieteellisiä ja historiallisia tutkimustarkoituksia sekä tilastollisia tarkoituksia varten tapahtuvaa käsittelyä koskevista poikkeuksista ja suojatoimista

CSC pyytää kiinnittämään huomiota erityisesti siihen, että tutkimustarkoituksiin tapahtuva henkilötietojen tietojenkäsittely on suojattava hyvän tiedonhallintatavan mukaisesti riittävän tietoturvallisuuden varmistamiseksi. Henkilötietojen suojaamisesta sekä hallinnollisten että teknisten suojaamiskeinojen osalta vastaava taho tulee myös olla selkeästi määritelty. Suojaamisesta vastaava tahon tulee viime kädessä olla tutkimustoiminnasta vastaava taho, esimerkiksi tutkimusryhmän johtaja, mutta suojaamiskeinojen toteuttamisen voi osittain tai laajasti ulkoistaa asiantuntijoille tai toimittajille.

CSC pyysi lausunnossaan EU:n yleisen tietosuoja-asetuksen vaikutuksesta tieteellisen tutkimuksen ja tilastoinnin kansalliseen sääntelyyn (OM 1/41/2016) kiinnittämään huomiota siihen, että on tärkeää luoda periaatteet tietojen minimoinnille, pseudonymisoinnille ja anonymisoinnille tavalla, jossa säilytetään tasapaino tieteen vapauden ja avoimuuden toteuttamisessa sekä tutkittavien henkilöiden yksityisyyden suojaamisessa. Tärkeää on myös se, että tiedot minimoidaan mahdollisimman aikaisessa vaiheessa. Tutkimuskäytössä, joka tehdään ilman tutkittavan henkilön

suostumusta, tietojen tulee aina olla vähintään pseudonymisoituja siten, että tietoa ei voi yhdistää yksittäiseen henkilöön. Jos suostumus on saatu, pseudonymisointi ei ole välttämätön, mikäli pääsy tietoon on valvottua koko tiedon elinkaaren ajan sekä rajattu ainoastaan valtuutetuille toimijoille. Tämä koskee myös rekisteritutkimusta ja arkaluontoisia henkilötietoja kuten terveystietoja. CSC pitää tärkeänä tämän huomioimista.

Muut yleiset kommentit tietojenkäsittelyn erityistilanteita koskevasta 5 luvusta.

Lähtökohtana on oltava se, että tieteellinen tutkimus henkilötietojen ja arkaluonteisten tietojen käsittelyperusteena turvataan. EU:n yleistä tietosuoja-asetusta täydentävässä kansallisessa tietosuojalaissa tulee mahdollistaa tutkijoiden sekä tutkimuksen tietojen siirtäminen automaattisesti rekisteristä ja varannoista toiseen, sekä tietojen rikastaminen tai kytkeminen muihin tietoihin. Tieteen uusiutumisen kannalta peruslähtökohta on, että tieteelliset tulokset ja niiden tekijätiedot ovat julkisia ja vapaasti jaettavissa. Tietojen sujuva liikkuminen rekisterien välillä mahdollistaa tieteen avoimuuden ja julkisuuden toteutumisen. Tutkijat meritoituvat ja saavat mainetta, kun toiset tutkijat viittaavat heihin ja hyödyntävät heidän tutkimustuloksiaan. Tutkijoiden urakehitys sekä menestyksekäs tutkimusrahoituksen saanti riippuu keskeisesti heidän meriiteistään (Tutkimushallinnon verkoston koordinaatioryhmän (TUHA) lausunto EU:n tietosuoja-asetuksen kansallisesta soveltamisesta).

Pitkäaikaissäilytyksen kannalta on tärkeää, että datan säilyttäjillä ja säilytyspalveluita tuottavilla on oikeus pitää aineisto saatavilla, mikä edellyttää tarvetta muokata ylläpitosyistä aineistoa teknisesti. Tekninen muokkaaminen ei kuitenkaan koske aineiston sisältöä. Tämä on tärkeää, koska uuden tekniikan myötä aineistoa joudutaan siirtämään täysin uuteen formaattiin.

Tieteellistä tutkimustarkoitusta varten tietosuoja-asetusta tulee tulkita laajasti, kuten hallituksen esityksessä mainitaankin. On syytä tarkentaa, mitä EU:n yleisen tietosuoja-asetuksen resitaaliin 33 kirjatut tutkimusalueet ("areas of research") tarkoittavat, jotta varmistetaan, että tietoja voidaan käsitellä tutkimustarkoituksissa siinä laajuudessa, kuin niiden luovuttaja on toivonut ja pyrkinyt luvallaan mahdollistamaan. Tämän tutkimusalueiden määrittelyn tulisi olla yhtenäinen Euroopan tasolla, sillä tutkimus on lähtökohtaisesti monikansallista. Suostumusprosessin tulee olla läpinäkyvä ja huomioida se, ettei tieteellisen tutkimuksen lopputulemaa voida määritellä ennakkoon. Suostumuksen muuttamiseen tai laajentamiseen jälkikäteen suostumuksen antajan luvalla pitäisi olla yksinkertainen ja selkeä prosessi, jonka avulla tutkimusaineistojen hyödyntäminen uuteen tutkimusaiheeseen on mahdollista. Tähän liittyen on huomioitavaa myös sosiaali- ja terveystiedon toissijaisen käytön lakimuutos, jonka myötä sosiaali- ja terveydenhuollon asiakastietoja sekä muita terveyteen ja hyvinvointiin liittyviä henkilötietoja voitaisiin käyttää aiempaa laajemmin muussakin kuin siinä ensisijaisessa käyttötarkoituksessa, jonka vuoksi ne on alun perin tallennettu.

CSC ehdottaa, että EU:n yleistä tietosuoja-asetusta täydentävään kansalliseen tietosuojalakiin sisällytettäisiin viittaus ns. toisiolakiin (Hallituksen esitys laiksi sosiaali- ja terveystietojen tietoturvallisesta hyödyntämisestä sekä eräiksi siihen liittyviksi laeiksi).

Laki rikoslain 38 luvun 9 §:n ja 10 §:n 3 momentin muuttamisesta

Yleiset kommentit tietosuojarikosta koskevasta 9 §:stä.

CSC ehdottaa, että tietosuojarikos tulisi määritellä samoin tavoin kuin datavahingonteko:

Joka oikeudettomasti jakaa, hävittää, turmelee, kätkee, vahingoittaa, muuttaa, saattaa käyttökelvottomaksi tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen taikka tietojärjestelmässä olevan henkilötiedon, on tuomittava tietosuojarikoksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Törkeä tietosuojarikos tulee määritellä seuraavasti:

Jos tietosuojarikoksessa

1) aiheutetaan erityisen tuntuvaa haittaa tai taloudellista vahinkoa,

2) rikos tehdään osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa,

3) rikos tehdään osana toimintaa, jossa on vaikutettu merkittävään määrään henkilötietoja

4) rikos kohdistuu tietojärjestelmään, jonka vahingoittaminen vaarantaisi energiahuollon, yleisen terveydenhuollon, maanpuolustuksen, oikeudenhoidon taikka muun näihin rinnastettavan yhteiskunnan tärkeän toiminnon

5) kohdistuu erityisen luottamuksellisiin henkilötietohin

Ja tietosuojarikos on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä datavahingonteosta vankeuteen vähintään neljäksi kuukaudeksi ja enintään viideksi vuodeksi.

Yritys on rangaistava.

Muut mahdolliset kommentit

Muita huomioita työryhmän mietinnöstä ja ehdotuksesta hallituksen esitykseksi

Perustuslakiin liittyvät kysymykset ovat hallituksen esityksessä epäselviä siltä osin, että tietosuojalain suhdetta perustuslain 16 § mainittuun tieteen, taiteen ja ylimmän opetuksen vapauteen ei ole käsitelty. Lakiehdotuksessa on asioita, jotka voivat vaikuttaa perustuslaissa turvattuun tieteen vapauteen. CSC pitää tärkeänä, että EU:n yleistä tietosuoja-asetusta täydentävässä kansallisessa tietosuojalaissa kiinnitetään erityistä huomiota tähän sekä huomioimaan TUHA-verkoston lausunnon asiasisällöstä EU:n tietosuoja-asetuksen kansallisesta soveltamisesta perusoikeuskäsittelyyn liittyen.

Lisäksi CSC pitää tärkeänä, että EU:n yleistä tietosuoja-asetusta täydentävässä kansallisessa tietosuojalaissa huomioidaan suomalaisten kulttuuriperintöorganisaatioiden (arkistot, kirjastot, museot) toiminta, kuten Suomen museoliiton lausunnossa tietosuojalakiin liittyen painotetaan (http://www.museoliitto.fi/jasentiedotteet.php?aid=12960). Erityishuomiota tulee kiinnittää lakiluonnoksen määritelmään, joka koskee vain eläviä henkilöitä. Laajempi määritys tässä asiayhteydessä on tarpeen, sillä nykyisellään museoinnissa ja arkistoinnissa syntyy ongelmia elävien ja kuolleiden erittelyn puitteissa. Lausunnolla oleva lakiluonnos toteaa yksiselitteisesti, että laissa mainitut rajaukset koskevat vain eläviä henkilöitä. Tämä on selkeä ja tärkeä rajaus. Käytännössä museoiden on kuitenkin mahdotonta tietää esimerkiksi sitä, ovatko valokuvissa olevat henkilöt tietojen käsittelyn aikaan eläviä vai kuolleita.

Kaila Urpo
CSC-Tieteen tietotekniikan keskus Oy