TIETOSUOJAVALTUUTETUN TOIMISTO

Dnro 8027/91/2022

21.11.2022

Perustuslakivaliokunta

Perustuslakivaliokunta tiistai 22.11.2022 klo 10.45 / HE 133/2022 vp /

Apulaistietosuojavaltuutetun lausunto

Eduskunnan perustuslakivaliokunta on pyytänyt tietosuojavaltuutetun toimistolta kirjallista asiantuntijalausuntoa hallituksen esityksestä eduskunnalle hallituksen esityksestä eduskunnalle digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi.

Kiitän mahdollisuudesta lausua asiassa. Apulaistietosuojavaltuutettuna olen arvioinut kokonaisuutta toimivaltani piiriin kuuluvan henkilötietojen suojan toteutumisen ja tietosuojalainsäädännön valossa ja lausun asiassa kunnioittavasti seuraavaa.

Esityksen tavoitteet ja ehdotetut ratkaisut yleisesti

Hallituksen esityksen tavoitteena on mahdollistaa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluiden sekä laajasti yhteiskunnan palveluissa käytettävän poliisin tarjoaman digitaalisen henkilöllisyystodistuksen tuottaminen. Ehdotuksella on tarkoitus mahdollistaa digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen tuottaminen ja käyttö. Lisäksi esityksellä mahdollistettaisiin vaihtoehtoinen luonnollisen henkilön tunnistusväline sellaisille henkilöille, jotka eivät halua tai voi käyttää digitaalisen henkilöllisyystodistuksen käyttämisen edellyttämää mobiilisovellusta.

Esityksen yhtenä erityisenä tavoitteena on rakentaa edellytyksiä henkilön itsensä toimesta tapahtuvaan henkilöön itseensä liittyvien viranomaisten vahvistamien tietojen jakamiseen ja henkilöllisyyttä koskevien tietojen esittämiseen (ns. itsehallittava identiteetti, Self-sovereign identity), sekä luoda pohja itsehallittavien viranomaistietojen esitämisen käytänteille myös tulevaisuuden kehitystä silmällä pitäen.

Digitalisoituvassa yhteiskunnassa kysyntä erilaisia digitaalisesti saatavilla olevia palveluita kohtaan kasvaa jatkuvasti. Samaan aikaan myös tarve viranomaisen vahvistamien henkilötietojen ja henkilöllisyyden osoittamisen mahdollisuuksille sähköisessä asioinnissa kasvaa, säilyttäen toisaalta vakaan paikkansa myös perinteisemmässä käyntiasioinnissa. Mahdollisuus henkilön luotettavaan tunnistamiseen erilaisten asiointitapahtumien yhteydessä on useissa tilanteissa keskeistä muun ohella henkilötietojen suojan varmistamiseksi. Henkilöllisyystodistusten laaja henkilötietosisältö huomioiden on kuitenkin perusteltua tarkastella myös sitä, missä laajuudessa näiden eri henkilötietojen osoittaminen kussakin tilanteessa on tarpeellista ja oikeasuhtaista, ja millä tavoin mahdollisuuksia eri tietojen osoittamista koskevan valinnan tekemiseen voitaisiin saattaa enemmän henkilön itsensä harkintaan.

Pidän yleisesti ottaen kannatettavana nyt käsillä olevan esityksen tavoitetta luoda edellytyksiä henkilön mahdollisuudelle määrätä itseään koskevista tiedoista. Lähestymistapa on linjassa henkilötietojen suojan kannalta keskeisen tiedollista itsemääräämisoikeutta koskevan periaatteen kanssa, joka kiinnittyy niin perustuslain säännöksiin muun

muassa yksityiselämän suojasta kuin henkilötietojen suojaa koskevaan lainsäädäntöön kokonaisuutena, jonka keskiössä on EU:n yleinen tietosuoja-asetus (EU) 2016/679 (tietosuoja-asetus).

Sisäänrakennettua ja oletusarvoista tietosuojaa koskevan tietosuoja-asetuksen 25 artiklan mukaan henkilötietojen käsittelyssä on toteutettava tehokkaasti tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta ne saataisiin sisällytettyä käsittelyn osaksi ja jotta käsittely vastaisi tietosuoja-asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin. Oletusarvoisesti tulee käsitellä vain käsittelyn tarkoituksen kannalta tarpeellisia henkilötietoja. Henkilötietojen käsittelyssä noudatettavista tietosuojaperiaatteista säädetään tietosuoja-asetuksen 5 artiklassa, jonka 1 kohdan c alakohta koskee tietojen minimointia. Minimointiperiaatteen mukaan henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään.

Ehdotuksen mukainen yksilön mahdollisuus rajata niitä henkilötietoja, jotka luottavalle osapuolelle osoitetaan, on itsessään tietojen minimoinnin periaatteen hengen mukainen. Minimointiperiaatteen tosiasiallisen toteutumisen kannalta kehotamme kuitenkin kiinnittämään itsehallittavan identiteetin mallin käytännön toteutuksessa huomiota tietosuojalainsäädännöstä tulevaan tarpeellisuusvaatimukseen. Digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen asiointivälineen erilaisissa käyttötilanteissa luottavalle osapuolelle ovat tarpeellisia tietyt tapauskohtaisesti vaihtelevat henkilötiedot, joita henkilö ei yleensä voi kyseisessä asiointitilanteessa tosiasiallisesti kieltäytyä antamasta ilman asiointitapahtuman keskeytymistä tai muita haitallisia seurauksia. Vastaavasti luottava osapuoli ei voi jättää käsittelyn tarkoitukseen nähden tarpeellisia tietoja keräämättä esimerkiksi vahvan sähköisen tunnistautumisen onnistumiseksi. Myöskään tähän tarkoitukseen nähden tarpeettomien henkilötietojen kerääminen ei toisaalta ole yleisen tietosuoja-asetuksen vaatimusten mukaista.

Tietosuojavaltuutetun toimisto on jo lausuntovaiheessa kiinnittänyt tähän asiana huomiota, mutta näen tarpeelliseksi edelleen kiinnittää tähän huomiota. Lausuttavana olevan hallituksen esityksen käsittelyssä olisi tarpeen edelleen kiinnittää huomiota siihen, miten voitaisiin toteutuksessa pyrkiä varmistumaan siitä, ettei tarpeettomien tietojen antaminen henkilön itsensä toimesta ja toisaalta kerääminen luottavan osapuolen toimesta olisi mahdollista. Asian merkittävyyttä nostaa se, että usein henkilöllisyyttään todentava luonnollinen henkilö ja siihen luottavan osapuoli (esim. viranomainen) voivat usein olla epätasavertaisessa asemassa.

On huomioitava, että lopputilannetta ei ole pidettävä minimointiperiaatteen mukaisena, mikäli tekninen toteutus mahdollistaisi esimerkiksi sen, että luottava osapuoli voi kerätä tai ratkaisusta riippuen jopa automaattisesti vastaanottaa myös sellaiset käsittelyn tarkoitukseen nähden tarpeettomat tiedot, jotka digitaalisen henkilöllisyystodistuksen tai ulkomaalaisen asiointivälineen haltija sille tietoisesti tai tahattomasti osoittaa. Tekninen toteutus tulisi toisin sanoen rakentaa sellaiseksi, että luottava osapuoli ei voi asiointitapahtuman yhteydessä kerätä tai vastaanottaa muita kuin suorittamansa henkilötietojen käsittelyn tarkoituksen kannalta tarpeellisia henkilötietoja.

Huomiota on niin ikään kiinnitettävä myös tietosuoja-asetuksen 5 artiklan 1 kohdan mukaiseen lainmukaisuusperiaatteeseen sekä käsittelyn lainmukaisuutta koskevassa tietosuoja-asetuksen 6 artiklassa säädettyihin käsittelyn oikeusperusteisiin ja niiden tunnistamiseen erityisesti digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen asi-

ointivälineen eri käyttötilanteissa. Ennen kaikkea on aiheellista huomioida, että 6 artiklan 1 kohdan a alakohdassa tarkoitettu rekisteröidyn antama suostumus ei muun muassa suostumuksen vapaaehtoisuuteen liittyvän vaatimuksen myötä lähtökohtaisesti sovellu tietojen käsittelyperusteeksi henkilön tunnistamista tai henkilöllisyyden osoittamista edellyttävissä tilanteissa. Suostumusta ei myöskään voida käyttää oikeusperusteena tarpeettomien henkilötietojen käsittelylle. Tämä on merkityksellistä itsehallittavan identiteetin toteuttamisessa siltä keskeiseltä osin kuin kysymys on henkilön mahdollisuudesta valita itse luottavalle osapuolelle osoitettavat tiedot.

Sisäänrakennettua ja oletusarvoista tietosuojaa koskevan vaatimuksen mukaisesti toteutuksessa on varmistettava myös muilta osin huolellisesti, että henkilötietojen käsittely vastaa tietosuoja-asetuksessa säädettyä. Minimointiperiaatteen ja toisaalta asetuksen 5 artiklan 1 kohdan b alakohdassa säädetyn käyttötarkoitussidonnaisuuden periaatteen tulee toteutua digitaalisen henkilöllisyyden palvelujen ja digitaalisen henkilöllisyystodistuksen tuottamisen yhteydessä myös muutoin kuin edellä todetuilta osin niin rekisterinpitäjien kuin mahdollisten henkilötietojen käsittelijöiden toteuttamassa tietojenkäsittelyssä rajoittaen henkilötietojen käsittelyn siihen, mikä on käsittelyn tarkoitusten kannalta perustellusti tarpeellista. Tämä on keskeistä huomioida muun ohella esitykseen liittyviä viranomaisten tiedonsaantioikeuksia toteutettaessa. Minimointiperiaatteen näkökulmasta on hyvä kiinnittää huomiota siihen, että nyt käsiteltävässä hallituksen esityksessä toteutusratkaisu on esitetty toteutettavan siten, että tiettyä henkilötietojen käsittelyä tapahtuu passin ja henkilökortin haltijoiden tietojen osalta otti henkilö sähköisen henkilöllisyystodistuksen käyttöönsä tai ei.

Toteutuksessa on aiheellista kiinnittää erityistä huomiota henkilötietojen eheyden, luottamuksellisuuden ja turvallisuuden varmistamiseen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdassa edellytetyllä tavoin. Henkilötietoja on suojattava luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen riittäviä suojatoimia, joista on säädetty tarkemmin muun muassa tietosuoja-asetuksen 32 artiklassa. Nyt kysymyksessä oleva henkilötietojen käsittely on käsittelytoimien ja niiden kohteena olevien henkilötietojen laajuus ja luonne huomioiden omiaan aiheuttamaan riskin käsittelyn kohteena olevien luonnollisten henkilöiden oikeuksille ja vapauksille, minkä vuoksi on keskeistä, että tiedot on asianmukaisesti suojattu koko käsittelyn elinkaaren ajan. On hyvä, että tämä on ehdotettujen säädösten tasolla huomioitu nimenomaisin ja yleiseen tietosuoja-asetukseen nähden osin lisäsuojatoimia sisältävin säännöksin. Korostan vielä tämän asian keskeisyyttä erityisesti lainsäädännön toimeenpanoa ja käytännön toteutusta silmällä pitäen.

Säädösehdotukset ja niiden perustelut

Henkilötietojen käsittelyä koskevat sääntelyratkaisut ja tietosuoja

Esityksen mukaan rekisterinpitäjänä digitaalisen henkilöllisyyden palvelujen osalta toimisi Digi- ja väestötietovirasto (ehdotetun Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annettavan lain 3 §) sekä digitaalisia henkilöllisyystodistuksia koskevan rekisterin osalta poliisi (ehdotetun digitaalisesta henkilöllisyystodistuksesta annettavan lain 5 §). Rekisterinpitäjien rooleja, vastuita ja velvollisuuksia on selvennetty ehdotetuissa laeissa sekä niitä koskevissa yksityiskohtaisissa perusteluissa. Esimerkiksi Digi- ja väestötietoviraston osalta ehdotuksessa on myös nimenomaisesti rajattu rekisterinpitäjän oikeutta palvelujen tuottamisen yhteydessä käsiteltävien henkilötietojen luovuttamiseen kolmannelle osapuolelle. Lisäksi säädöksissä on määritelty tarkemmin esimerkiksi niitä henkilötietoja, joiden käsitteleminen olisi digitaalisen henkilöl-

lisyyden palvelujen tuottamiseksi ja toteuttamiseksi tarpeellista. Yksityiskohtaisissa perusteluissa on niin ikään tarkasteltu henkilötietojen käsittelyn oikeusperustetta, jonka on katsottu molempien rekisterinpitäjien toteuttaman käsittelyn osalta olevan tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohta.

Pidän hyvänä sitä, että rekisterinpitäjät sekä rekisterinpitäjien vastuut nyt kysymyksessä olevien käsittelytoimien osalta on ehdotuksessa määritetty selkeästi ja yleisen tietosuoja-asetuksen sallima kansallinen liikkumavara huomioiden. Hallituksen esityksestä on luettavissa, että tarkoitus on säätää poliisi rekisterinpitäjäksi koskien rekisteriä digitaalisesta henkilöllisyystodistuksesta. Kiinnitän huomiota siihen, että esimerkiksi henkilötietojen käsittelystä poliisitoimessa annetussa laissa (616/2019) rekisterinpitäjyys määritellään tarkemmalle tasolle kuin poliisi; rekisterinpitäjäksi on säädetty esimerkiksi Poliisihallitus. Viitaten edellä olevaan, rekisterinpitäjyyden selkeyden näkökulmasta olisi hyvä varmistaa, että rekisterinpitäjistä tulee säädettyä riittävän selkeästi.

Ehdotetussa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annettavassa laissa säädettäisiin digitaalisen henkilöllisyyden tietojärjestelmää koskevista laatu- ja tietoturvallisuusvaatimuksista. Ehdotuksen 5 §:n mukaan Digi- ja väestötietoviraston olisi huolehdittava hallinnollisilla ja teknisillä toimenpiteillä tietojärjestelmän tietoturvallisuudesta muun muassa siten, että tietojärjestelmään kohdistuvat merkittävät tietoturvaloukkaukset ja -uhat kyetään havaitsemaan. Yksityiskohtaisten perustelujen mukaan pykälän tarkoituksena on säätää ensisijaisesti muiden tietoturvallisuuden varmistamiseksi käsiteltävien tietojen kuin henkilötietojen suojaamisesta, eikä tarkemmista tietoturvavaatimuksista säätäminen vaikuttaisi rekisterinpitäjän tietosuoja-asetuksen mukaiseen velvollisuuteen toteuttaa asianmukaiset tietoturvatoimenpiteet tai tähän liittyvään rekisterinpitäjän vastuuseen henkilötietojen käsittelyn osalta. Siltä osin kuin ehdotetussa pykälässä säädettävät erityiset vaatimukset kuitenkin kohdistuisivat henkilötietoihin, olisi esityksen mukaan kyse tietosuoja-asetuksen 5 artiklan 1 kohdan d ja f alakohdissa tarkoitettujen periaatteiden täsmentämisestä yksittäisessä tilanteessa kansallisen liikkumavaran puitteissa.

Edellä mainittujen laatu- ja tietoturvallisuusvaatimusten osalta on syytä kiinnittää huomiota perusteluissa viitattujen yleisen tietosuoja-asetuksen säännösten lisäksi myös yleisen tietosuoja-asetuksen 33 artiklassa säädettyihin henkilötietojen tietoturvaloukkaustilanteita koskeviin rekisterinpitäjän velvoitteisiin, joihin ei liity kansallista liikkumavaraa. Mainittu 33 artikla sisältää muun muassa velvollisuuden dokumentoida kaikki henkilötietojen tietoturvaloukkaukset ja artiklan 5 kohdassa tarkemmin yksilöidyt tietoturvaloukkaukseen liittyvät tiedot. Dokumentointivaatimus ei siten rajaudu pelkästään merkittäväksi katsottaviin tietoturvaloukkaustilanteisiin. Tämä huomioiden toistan tietosuojavaltuutetun toimiston hallituksen esityksen aiemmassa valmisteluvaiheessa esiin tuoman ehdotuksen sanan ”merkittävät” poistamisesta ehdotetusta lainkohdasta siten, että lopullisen sanamuodon mukaan kaikkbi tietojärjestelmään kohdistuvat tietoturvaloukkaukset ja -uhat olisi kyettävä havaitsemaan tai vaihtoehtoisesti tuomaan perusteluissa riittävän selkeästi esiin, että tämä säännös ei poista tai kavenna yleisen tietosuoja-asetuksen 33 artiklan kohdan 5 mukaista velvollisuutta dokumentoida kaikki henkilötietoihin kohdistuneet tietoturvaloukkaukset.

Hallituksen esityksessä ehdotetaan säädettäväksi, että digitaalisen henkilöllisyystodistuksen voimassaolo päättyy vuoden kuluttua siitä, kun sen perustana olevan henkilöllisyyttä osoittavan asiakirjan voimassaolo on päättynyt. Näkisin tarkoituksen mukaiseksi arvioida, onko hallituksen esityksessä arvioitu ja käsitelty tähän eritahtiseen

voimassaoloon mahdollisesti liittyviä riskejä riittävällä tavalla. Jos riskejä ei ole tunnistettu, niin tämäkin voisi olla selvyyden vuoksi perusteltua todeta.

Lisäksi ehdotetun Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annettavan lain 5 §:n 3 momentissa säädettäisiin Digi- ja väestötietoviraston velvollisuudesta päättää tietojärjestelmän tarkemmista teknisistä vaatimuksista sekä tietoturvavaatimuksista, joiden olisi perustuttava yleisesti tunnettuihin tai kansainvälisiin standardeihin. Yksityiskohtaisten perustelujen mukaan vaatimusten olisi perustuttava nyt ehdotettuun Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annettavaan lakiin, sähköisestä tunnistamisesta ja luottamuspalveluista annettuun EU:n asetukseen ja yleisesti tunnettuihin kansallisiin tai kansainvälisiin standardeihin. Totean tältä osin yleisenä huomiona, että myös tietosuojalainsäädäntö sisältää verrattain runsaasti tietoturvallisuutta koskevia vaatimuksia edellyttäessään käsittelystä aiheutuvaa riskiä vastaavan turvallisuustason varmistamisen edellyttämiä teknisiä ja organisatorisia toimenpiteitä, jotka rekisterinpitäjän velvollisuutena on toteuttaa siltä osin kuin kysymys on henkilötietojen käsittelystä.

Hallituksen esityksen perusteluissa todetaan sivulla 113, että digitaalisessa henkilöllisyystodistuksessa käyttäjän kasvokuva luovutetaan digitaalisessa muodossa hänen itsensä käytettäväksi mobiililaitteessa ja että kuvaa käytetään käyttäjän tunnistamiseen käyntiasioinnin yhteydessä. Kohtaan on kuvattu, että käyttäjän tunnistaminen tapahtuu tunnistajan silmämääräisen arvion perusteella vastaavalla tavalla kuin perinteisten virallisten henkilöllisyyttä osoittavien asiakirjojen osalta. Lisäksi todetaan, että digitaalisen henkilöllisyystodistuksen tarkastussovellus ei sisällä mitään erityisiä teknisiä menetelmiä, joita tunnistamisessa käytettäisiin ja että digitaalinen henkilöllisyystodistus ei itsessään mahdollista erityisten teknisten menetelmien käyttöä. Näin ollen esityksessä katsotaan, ettei kyse ole biometristen tietojen käsittelystä henkilön yksiselitteistä tunnistamista varten. Lisäksi on esitetty, että vaikka kasvokuvia ei katsottaisi tässä yhteydessä käsiteltävän biometrisinä tietoina on niiden käsittelyssä noudatettava erityistä varovaisuutta. Jatkovalmistelussa on syytä varmistua, että esitetty tulkinta tietojen eibiometrisestä luonteesta on pitävä ja että asiassa esitetään riittävän selkeät ja kattavat perustelut tulkinnalle ottaen huomioon asian ja sen ymmärrettävyyden haastavuus.

Vaikutusten arviointi

Henkilön tunnistaminen asianmukaisella ja luotettavalla tavalla on nyky-yhteiskunnassa usein merkittävässä roolissa muun ohella henkilötietojen luottamuksellisuuden ja turvallisuuden varmistamisessa. Tietosuojavaltuutetun toimisto vastaanottaa säännöllisesti kanteluita koskien luonnollisten henkilöiden tunnistamisessa noudatettavia menettelytapoja, kuten tunnistamiskäytäntöjen rakentamista yksinomaan henkilötunnuksen kysymisen varaan, minkä on tietosuojavaltuutetun vakiintuneen linjauksen mukaan katsottu olevan henkilötietojen suojaa koskevan lainsäädännön ja hyvän tietojenkäsittelytavan vastainen toimintatapa. Sitä, että hallituksen esityksessä ehdotetut toimintatavat johtanevat siihen, että nykyistä useampi asiointipalvelu tarjoaisi käyttäjilleen mahdollisuuden vahvaan sähköiseen tunnistamiseen, voidaan pitää hyvänä kehityssuuntana ja tuo parannusta nykytilanteeseen, jossa tunnistamisen käytänteisiin liittyy yhä haasteita.

Esityksen mukaan henkilötietojen laajamittainen käsittely yhdistettynä uusien teknisten ratkaisujen käyttöön merkitsee todennäköisesti tietosuoja-asetuksen mukaista korkeaa

riskiä henkilötietojen käsittelylle, mistä johtuen tietosuoja-asetuksen 35 artiklan mukainen tietosuojavaikutusten arviointi on todennäköisesti tarpeen siinä vaiheessa, kun ratkaisun tekniset suunnitelmat ja käyttömallit tarkentuvat. Myös olemassa olevien rekistereiden osalta ollaan ottamassa käyttöön uusia käyttötapoja, mikä edellyttää tieto-suojavaikutusten arvioinnin päivittämistä (s. 52).

Apulaistietosuojavaltuutettuna katson, että kokonaisuus huomioiden olennaista, että tietosuoja-asetuksen 35 artiklan mukainen tietosuojaa koskeva vaikutustenarviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle toteutetaan jatkovalmistelun yhteydessä ja että sitä päivitetään aina tarvittaessa. Yksityiskohtaisten vaikutustenarviointia edellyttävien käsittelyyn liittyvien elementtien lisäksi voidaan katsoa yleisesti ja myös esityksen sivulla 112 todettuun viitaten, että suunniteltuun kansalaisten identiteettitietojen uudenlaiseen digitaaliseen käsittelyyn liittyy tavanomaista korkeampia riskejä muun muassa tietoturvallisuuden näkökulmasta, minkä vuoksi tietosuojaa koskevien riskien huolellinen arvioiminen on korostuneen tärkeää.

Tietosuojan vaikutustenarvioinnin tarkoituksena on tunnistaa, arvioida ja hallita henkilötietojen käsittelyyn sisältyviä riskejä sekä toimia siten välineenä rekisteröityjen henkilötietojen suojalle aiheutuvien riskien hallitsemiseksi ennakollisesti ja toisaalta jatkuvana osana henkilötietojen käsittelyä. Vaikutustenarviointi on suositeltavaa tehdä riittävän varhaisessa vaiheessa käsittelyn suunnittelua, jotta arvioinnin yhteydessä nousevat havainnot ja kehittämistarpeet on tosiasiallisesti mahdollista ottaa huomioon osana toteutusta. Tämä on tyypillisesti myös kustannustehokkaampi ratkaisu kuin muutosten toteuttaminen jälkikäteen.

Kiinnitän vielä erikseen huomiota toteutukseen mahdollisesti liittyviin tiedonsiirtoihin. Esityksen sivulla 52 on todettu, että kansainvälisten tiedonsiirtojen näkökulmasta toteutuksessa tulisi pyrkiä siihen, että henkilötietoja ei siirretä EU/ETA-alueen ulkopuolelle. Näen tarpeellisena korostaa, että henkilötietojen siirrot kolmansiin maihin (tai kansainvälisille järjestöille) ovat tietosuoja-asetuksen mukaan mahdollisia ainoastaan tietosuojalainsäädännön vaatimuksia ja yleisen tietosuoja-asetuksen V luvussa vahvistettuja erityisiä edellytyksiä noudattaen. Euroopan tietosuojaneuvosto on antanut vaatimuksenmukaisuuden toteuttamisesta tältä osin yksityiskohtaista täsmentävää ohjeistusta. Tiedonsiirtoihin EU/ETA-alueen ulkopuolelle tulee nykyisessä toimintaympäristössä ja vallitseva oikeustila huomioiden suhtautua korostuneella huolellisuudella. Nyt tarkasteltavana olevan käsittelyn osalta on vielä arvioitava huolella ja harkiten, millä edellytyksillä ja missä tilanteissa tietojen siirtäminen kolmansiin maihin olisi mahdollista ylipäänsä, vai onko mahdollista laisinkaan. Tässä arvioinnissa on kiinnitettävä huomiota tiedonsiirtoihin sisältyviin riskeihin ja otettava huomioon yhtäältä käsillä olevan toteutuksen perustavaa laatua oleva luonne henkilötietojen käsittelyn näkökulmasta sekä toisaalta erot tietosuoja-asetuksen V luvussa määriteltyjen eri siirtoperusteiden tehokkuudessa tietosuoja-asetuksen takaaman henkilötietojen suojan tason varmistamiseksi. Ratkaisevaa on, että henkilötietojen siirtäminen EU/ETA-alueen ulkopuolelle on lainmukaista ainoastaan, mikäli siirrettäville henkilötiedoille voidaan jatkuvasti taata Euroopan unionin vaatimuksia vastaava tietosuojan taso. Arvioinnissa olisi siten kiinnitettävä erityisesti huomiota siihen, miten palvelu voitaisiin toteuttaa siinä tapauksessa, että sen pohjalla mahdollisesti oleva komission päätös tietosuojan riittävästä tasossa kolmannessa maassa kumottaisiin Euroopan unionin tuomioistuimessa. Vaikutusten arvioinnin jatkovalmistelussa on syytä kiinnittää huomiota vaatimuksenmukaisuuden varmistamiseen erityisesti näiden seikkojen osalta.

Lakiehdotuksen 9 a §:ssä säädettäisiin muun kuin Suomen kansalaisen tietojen tallettamisesta väestötietojärjestelmään sähköisessä etärekisteröintimenettelyssä.

Vaikka ehdotettu sääntely ei sitä edellytä, menettely on käytännössä tarkoitettu täysin automatisoiduksi menettelyksi, johon ei yleensä osallistuisi lainkaan Digi- ja väestötietoviraston tai muun viranomaisen virkailijaa. Ehdotetussa 9 a §:ssä ei kuitenkaan säädettäisi menettelyn automaattisuudesta, vaan tältäkin osin menettelyyn sovellettaisiin valmisteilla olevia hallintolain automaattista hallintoasian käsittelyä koskevia säännöksiä (HE 145/2022 vp). Koska etärekisteröintimenettelyssä olisi kyse tietosuoja-asetuksen 22 artiklan 2 kohdan b alakohdassa tarkoitetusta automatisoidusta yksittäispäätöksestä, olisi lisäksi huomioitava kyseisen alakohdan edellyttämät asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä oikeutettujen etujen suojaamiseksi. Tietosuoja-asetuksen johdanto-osan 71 kappaleen perusteella toimenpiteisiin olisi kuuluttava muun muassa käsittelystä ilmoittaminen rekisteröidylle ja oikeus vaatia ihmisen osallistumista tietojen käsittelemiseen.

Hallituksen esityksen 9 b §:ssä säädettäisiin siitä, mitä tietoja väestötietojärjestelmään talletettaisiin etärekisteröintimenettelyssä. Lakiehdotuksen 9 c §:ssä säädettäisiin puolestaan etärekisteröintimenettelyssä kerättävien biometristen tietojen käsittelystä. Ehdotetut pykälät ovat sisällöltään asianmukaisia ja tarpeellisia.

Hallituksen esityksen 9 d §:ssä säädettäisiin tunnistamisen tai yksilöinnin tapaa ja tietojen lähdettä kuvaavien tietojen muuttamisestä tai lisäämisestä. Esityksen mukaan mainituilla tiedoilla voisi olla vaikutusta henkilön tosiasiallisiin mahdollisuuksiin hyödyntää VTJ-identiteettiään yhteiskunnan palveluissa, tietojen ajantasaisuudella olisi erityisen suuri merkitys rekisteröidylle.

Käytännössä 9 d § tulisi useimmiten sovellettavaksi silloin, kun väestötietojärjestelmään ehdotetun 9 a §:n mukaisesti etärekisteröitynyt ulkomaalainen ensimmäisen kerran asioisi fyysisesti jonkun mainituista viranomaisista luona tai hänen henkilöllisyydestään varmistuttaisiin Suomen ulkomaan edustuston, toisen Schengen-valtion edustuston tai ulkoisen palveluntarjoajan toimesta ehdotetun 22 §:n mukaisesti ja perustietojen lähteestä tehtäisiin merkitä väestötietojärjestelmään. Henkilön VTJ-tiedoissa oleva merkintä etärekisteröitymisestä olisi tällöin päivitettävä merkinnäksi kasvokkain tunnistamisesta.

Esityksen 34 a § olisi uusi ja siinä säädettäisiin etärekisteröintimenettelyyn perustuvien tietojen luovuttamisesta väestötietojärjestelmästä. Ehdotuksen mukaan etärekisteröintimenettelyssä tunnistetun henkilön tietoja voitaisiin luovuttaa väestötietojärjestelmästä vain yhdessä lain 13 §:n 1 momentin 22 kohdassa tarkoitetun tunnistamisen tai yksilöinnin tapaa kuvaavan tiedon kanssa.

Tältä osin kiinnitän huomiota tietosuojavaltuutetun valtiovarainministeriölle antamaan lausuntoon, jossa on korostettu tietosuoja-asetuksen 19 artiklan mukaista velvoitetta. Tietosuoja-asetuksen 19 artiklan mukaan *rekisterinpitäjän on ilmoitettava kaikenlaisesta 16 artiklan, 17 artiklan 1 kohdan ja 18 artiklan mukaisesti tehdyistä henkilötietojen oikaisuista, poistosta tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa.* Mikäli esityksessä esitetyllä tavalla henkilön tunnistamisen tai yksilöinnin tapaa koskevalla tiedolla olisi vaikutuksia henkilön tosiasiallisiin mahdollisuuksiin hyödyntää VTJ-identiteettiä, tulisi tunnistamisen tapaa koskevasta muutoksesta ilmoittaa niille

vastaanottajille, joille ehdotetun uuden 34 a §:n mukaisesti tieto tunnistamisen tai yksilöinnin tavasta on toimitettu ennen fyysistä asiointia viranomaisessa.

Hautala Annina
Apulaistietosuojavaltuutettu 91286222U

Asiakirja on allekirjoitettu sähköisesti. Allekirjoituksen oikeellisuuden voi tarvittaessa tarkistaa tietosuojavaltuutetun toimiston kirjaamosta.