TIETOSUOJAVALTUUTETUN TOIMISTO

Dnro 165/93/2023

30.1.2023

Hallintovaliokunta
HaV@eduskunta.fi

Hallintovaliokunta tiistai 31.1.2023 klo 13 / HE 133/2022 vp

Apulaistietosuojavaltuutetun lausunto

Eduskunnan hallintovaliokunta on pyytänyt tietosuojavaltuutetun toimistolta kirjallista asiantuntijalausuntoa 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 myös 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 esittämisen käytänteille myös tulevaisuuden kehitystä silmällä pitäen.

Pidän yleisesti ottaen kannatettavana nyt käsillä olevan esityksen tavoitteita, mukaan lukien 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). Hallituksen esityksessä on myös käsitelty tietosuojakysymyksiä monelta osin asianmukaisella tavalla.

Sisäänrakennettu ja oletusarvoinen tietosuoja

Itsehallittavuus digitaalisen henkilöllisyystodistuksen ja ulkomaalaisen digitaalisen asiointivälineen käytössä voi lisätä tiettyjä riskejä henkilön yksityisyyden suojalle ja tietosuojaoikeuksien toteutumiselle. Nämä riskit on välttämätöntä huomioida niin käytännön teknisissä toteutuksissa kuin myös rekisteröidyille annettavassa informoinnissa, ohjauksessa ja tuessa.

Sisäänrakennettua ja oletusarvoista tietosuojaa koskevan tietosuoja-asetuksen 25 artiklan mukaan henkilötietojen käsittelyssä on toteutettava tietosuojaperiaatteiden, kuten tietojen minimointiperiaatteen, vaatimukset tehokkaasti. Minimointiperiaatteen mukaan henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Tietosuoja-asetuksen mukaan on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta käsittely vastaisi tietosuoja-asetuksen vaatimuksia ja rekisteröityjen oikeudet tulevat suojatuiksi.

Hallituksen esityksen mukainen yksilön mahdollisuus rajata niitä henkilötietoja, jotka luottavalle osapuolelle osoitetaan, on itsessään tietojen minimoinnin periaatteen hengen mukainen. Minimointiperiaatteen tosiasiallisen toteutumisen kannalta on syytä kuitenkin kiinnittää itsehallittavan identiteetin mallin käytännön toteutuksessa huomiota tietosuojalainsäädännöstä tuleviin vaatimuksiin. 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 merkittäviä haitallisia seurauksia. Vastaavasti luottava osapuoli ei voi jättää käsittelyn tarkoitukseen nähden tarpeellisia tietoja keräämättä esimerkiksi vahvan sähköisen tunnistautumisen onnistumiseksi.

Tietosuojavaltuutetun toimisto on aiemmassa lainsäädännön valmistelu- ja lausuntovaiheessa kiinnittänyt tähän asiaan 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 luottava osapuoli (esim. viranomainen) ovat usein epätasavertaisessa asemassa.

On huomioitava, että tilannetta 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 asiointivälineen 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

Rekisterinpitäjyys

Hallituksen 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 henkilöllisyyden 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 ovat 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 tärkeää varmistaa, että rekisterinpitäjistä tulee säädettyä riittävän selkeästi ja riittävän tarkalle tasolle ottaen huomioon poliisin organisaatiorakenteen (ei yksi viranomainen).

Turvallisuusvaatimukset ja dokumentointivelvollisuus

Ehdotetussa Digi- ja väestötietoviraston digitaalisen henkilöllisyyden palveluista annettavassa laissa (lakiehdotus 1.) esitetään säädettävän 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 näkemyksen, jonka mukaan 1. lakiehdotuksen 5 §:ssä ei välttämättä ole tarkoituksenmukaista rajoittua vain merkittäviin tietoturvaloukkauksiin ja -uhkiin tai vaihtoehtoisesti tuomaan riittävän selkeästi esiin, että tämä säännös ei poista tai kavenna yleisen tietosuoja-asetuksen 33 artiklan kohdan 5 mukaista velvollisuutta dokumentoida kaikki henkilötietoihin kohdistuneet tietoturvaloukkaukset.

Ehdotetun 1. 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.

Digitaalisen henkilöllisyystodistuksen voimassaolo

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.

Kasvokuvien käsittely

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.

Pitäisin tärkeänä varmistua, että edellä esitetty tulkinta tietojen ei-biometrisestä luonteesta on pitävä ja että asiassa esitetään riittävän selkeät ja kattavat perustelut tulkinnalle ottaen huomioon asian ja sen ymmärrettävyyden haastavuus.

Henkilötietojen käsittely luonnollisen henkilön tunnistusvälineistä perustettavassa rekisterissä ja henkilötietojen säilytysaika

Hallituksen esityksen 7. lakiehdotuksessa esitetään säädettävän 69 f §:n 1 momentti, jossa esitetään säädettävän tiedoista, joita Digi- ja väestötietovirasto tallentaa rekisteriin luonnollisen henkilön tunnistusvälineistä. Ehdotuksen mukaan rekisteriin voitaisiin tallentaa tunnistusvälineen haltijan osalta 1–6 kohdissa määritellyt tiedot. Jo kyseisen momentin kohtien 1–5 kohdassa määritellyt tiedot vaikuttavat niin laajoilta, että voisi jopa perustellusti pohtia, ovatko kaikki kohdissa mainitut tiedot tarpeellisia tähän käyttötarkoitukseen, mutta erityisesti haluan kiinnittää huomiota kohtaan 6). Kyseisessä kohdassa esitetään säädettävän Digi- ja väestötietovirastolle oikeus käsitellä muita kuin 1–5 kohdassa tarkoitettuja tunnistusvälineen tarjoamiseksi tarpeellisia tietoja.

Perustuslakivaliokunta on käytännössään pitänyt henkilötietojen suojan kannalta tärkeinä sääntelykohteina ainakin rekisteröinnin tavoitetta, rekisteröitävien henkilötietojen sisältöä, niiden sallittuja käyttötarkoituksia mukaan luettuna tietojen luovutettavuus sekä tietojen säilytysaikaa (PeVL 14/2018 vp. s 3). Ottaen huomioon perustuslakivaliokunnan linjan katson, että erityisesti esityksen mukainen 69 f §:n kohta 6) jää liian yleiselle tasolle. Henkilötietojen käsittelystä tulee säätää tarkkarajaisesti huomioiden tietosuoja-asetuksen vaatimukset.

Kiinnitän huomiota myös siihen, että hallituksen esityksen yksityiskohtaisissa perusteluissa todetaan sivulla 46: ”*Esityksessä ei määritetä tietojen tai asiakirjojen säilytysai-*

koja, joten Digi- ja väestötietoviraston on määritettävä ne. Perusteena voidaan käyttää esimerkiksi tunnistus- ja luottamuspalvelulain 24 §. Esityksen mukaan asiakirjojen voimassaoloaika perustuu myöntämisen taustalla olevan tunnistusasiakirjan voimassaoloaikaan."

Digitaalisesta henkilöllisyystodistuksesta annettavaksi ehdotetun lain (lakiehdotus 2.) 5 §:ssä esitetään säädettäväksi, että digitaalisista henkilöllisyystodistuksista pidettävästä rekisteristä tiedot poistetaan viimeistään kymmenen vuoden kuluttua siitä, kun henkilön oikeus digitaaliseen henkilöllisyystodistukseen on päättynyt.

Yksi keskeisimpiä tietosuoja-asetuksesta tulevia vaatimuksia on vaatimus henkilötietojen käsittelyn läpinäkyvyydestä. Tähän liittyen haluan kiinnittää ensinnäkin huomiota siihen, ettei välttämättä ole täysin selkeää mihin säilytysaikoihin hallituksen esityksen sivulla 46 viitataan, kun esimerkiksi 2. lakiehdotuksen 5 §:ssä säilytysajasta esitetään säädettävän. Toiseksi haluan kiinnittää huomiota edellä todettuun perustuslakivaliokunnan linjaukseen asioista, joita se pitää tärkeinä sääntelykohteina. Yksi näistä on henkilötietojen säilytysaika.

Vaikutusten arviointi

Riskienarviointi ja tietosuojavaltuutetun ennakkokuulemisvelvollisuus

Henkilön tunnistaminen asianmukaisella ja luotettavalla tavalla on nyky-yhteiskunnassa usein merkittävässä roolissa mm. ohella henkilötietojen luottamuksellisuuden ja turvallisuuden varmistamisessa. Tietosuojavaltuutettu 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 se tuonee parannusta nykytilanteeseen, jossa tunnistamisen käytänteisiin liittyy haasteita.

Esityksen mukaan henkilötietojen laajamittainen käsittely yhdistettynä uusien teknisten ratkaisujen käyttöön merkitsee suurella todennäköisyydellä tietosuoja-asetuksessa tarkoitettua korkeaa riskiä henkilötietojen käsittelylle, mistä johtuen tietosuoja-asetuksen 35 artiklan mukainen tietosuojavaikutusten arviointi on todennäköisesti tarpeen siinä vaiheessa, kun ratkaisujen tekniset suunnitelmat ja käyttömallit tarkentuvat. Myös olemassa olevien rekistereiden osalta ollaan ottamassa käyttöön uusia käyttötapoja, mikä edellyttää tieto-suojavaikutusten arvioinnin päivittämistä (s. 52).

Katson, että kokonaisuus huomioiden on 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.

Kansainväliset tietojen siirrot

Kiinnitän 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 henkilötietojen 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.

Resurssivaikutukset tietosuojavaltuutetun toimintaan

Hallituksen esityksessä on arvioitu vaikutuksia muun muassa kustannusten, henkilöstön ja organisaation sekä toiminnan näkökulmasta. Digi- ja väestötietovirastolle, poliisille ja Traficomille on esityksessä tunnistettu aiheutuvan kustannuksia ja henkilöresurssitarvetta lisätehtävien hoitamisesta. Hallituksen esityksen mukaisilla uudistuksilla tullee olemaan vaikutuksia myös tietosuojavaltuutetun toimiston työmäärään ja sitä kautta resurssitarpeita lisääviä vaikutuksia tietosuojavaltuutetun toimintaan.

Vastaavasti tietosuojavaltuutetulle tulee esityksen mukaisten teknisten ratkaisujen ja prosessien myötä uusia valvottavia kohteita ja myös neuvonnasta ja rekisteröityjen yhteydenottojen lisääntymisestä voidaan arvioida aiheutuvan lisäresurssitarvetta. Ulkomaalaisen asiointitunnus lisää myös henkilöjoukkoa, joka mahdollisesti tulee asioimaan tietosuojavaltuutetun kanssa.

Vähintään vähäiseen lisäresurssin tarpeeseen on tietosuojavaltuutetun tulevaisuudessa syytä varautua. Sääntelystä aiheutuva työmäärä ja siitä johtuvat lisäresurssitarpeet on todella tärkeää voida ottaa huomioon myöhemmin tietosuojavaltuutetun toimiston kokonaisresurssisuunnittelussa.

Apulaistietosuojavaltuutettu Hautala Annina
91286222U