2.5.2018

TIETOSUOJA-ASETUKSEN TUOMAT VAATIMUKSET VARMENNETOIMINTAAN

Tämä liite on osa rekisteröintiohjetta ja koulutusmateriaalia. Tietosuoja-asetuksen vaatimukset varmenteiden rekisteröintitoiminnalle on kirjattu tähän liitteeseen. Sopimukseen sisällytettävät henkilötietojen käsittelyn ehdot ja ohje tietoturva- tai tietosuojapoikkeamien käsittelystä liittyvät myös tietoturva-asetuksen mukaisten vaatimusten täyttämiseen.

Oletusarvoisen ja sisäänrakennetun tietosuojan vaatimus tarkoittaa sitä, että tietosuojanäkökulma otetaan huomioon kaikissa rekistereissä, palveluissa, järjestelmissä ja toiminnoissa jo niiden suunnitteluvaiheessa ja erilaiset toiminnallisuudet rakennetaan tietosuojanäkökulma edellä. Vaatimus kytkeytyy osoitusvelvollisuuden periaatteeseen, jonka mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on aktiivisesti pystyttävä osoittamaan, että tietosuoja on huomioitu kaikessa toiminnassa niin organisatorisesti kuin teknisestikin ja tietosuoja todella toteutuu käytännössä.

Varmenteisiin liittyvä henkilötietojen käsittely perustuu lakiin. Laissa on myös säädetty nimenomainen oikeus henkilötietojen käsittelyyn[1)]. Varmennepalvelujen tarjoaminen ja sähköisen identiteetin oikeellisuuden varmistaminen edellyttävät henkilötietojen käsittelyä. Henkilötietoja tulee käsitellä vain siinä laajuudessa kuin varmentajan toiminnalle on tarpeellista. Rekisteröidyn varmennehakemuksen nojalla rekisteröidyn henkilötietoja käsitellään varmenteen myöntämiseksi, tuottamiseksi ja hallinnoimiseksi. Varmennehakemuksen yhteydessä rekisteröityä informoidaan henkilötietojen käsittelystä varmenneprosesseissa.

Tietojen käsittely on VRK:n lakisääteinen tehtävä varmenteiden myöntämiseksi ja hallinnoimiseksi, joten tietojen käsittelyn rajoittamista ei voida vaatia eikä myöskään tietojen siirto-oikeutta toiseen järjestelmään ole.

Rekisteröidyn oikeuksilla tarkoitetaan varmenteenhaltijan oikeuksia, esimerkiksi oikeus saada tietää mitä henkilötietoja on varmennerekisterissä tai korttien ja varmenteiden tilaus- ja hallinnointijärjestelmässä (Vartti) ja mihin tarkoitukseen niitä käsitellään sekä oikeus saada virheelliset tiedot oikaistua. Henkilötietolain (523/1999) 29 §:n mukaisesti rekisteröidyllä on oikeus vaatia oikaistavaksi, poistettavaksi tai täydennettäväksi rekisterissä oleva virheellinen, tarpeeton, puutteellinen tai vanhentunut henkilötieto. Kansallinen henkilötietolainsäädäntö ja tietosuojalainsäädäntö on lähiaikoina uudistumassa. Oikaisua on haettava rekisterinpitäjältä (VRK) kirjallisesti. Oikaisua pyytävä henkilö on tunnistettava, Väestörekisterikeskuksen on varmistuttava oikaisua pyytävän tahon henkilöllisyydestä.

Rekisteröity saa järjestelmässä olevat henkilötietonsa ja tiedon siitä mihin tietoja käytetään asioimalla Väestörekisterikeskuksessa (VRK), rekisteröijän tunnistettua henkilön tai myöhemmin kesällä 2018 WebVartti-sovelluksesta. Kun rekisteröity ottaa yhteyttä rekisterinpitäjään, tiedot tulee luovuttaa 1 kuukauden kuluessa. Vastaus annetaan rekisteröidylle täydellisenä, mukaan lukien mm. rekisterissä olevat henkilötiedot ja tietojen käsittelyn perusteet[2)]. VRK varmistaa, että tietojen pyytäjä saa kaikki pyytämänsä tiedot, ellei tietojen luovutukselle ole estettä.

Mikäli vastaus on kielteinen, eli tietoja ei jostain syystä annettaisi, rekisteröidylle annetaan valitusosoitus. Mikäli henkilötiedot ovat virheellisiä, oikaisupyyntö lähetetään rekisteröintipisteen kautta tai suoraan VRK:lle.

Kaikilta osin tiedot eivät ole oikaistavissa (Väestötietojärjestelmästä tulevat tiedot). Lisätietoa löytyy VRK:n verkkosivuilla olevista rekisteriselosteista, jotka sisältävät VRK:n henkilötietojen käsittelyn periaatteet.

Vartin osalta VRK toimii rekisterinpitäjänä ja organisaatioiden rekisteröijät käsittelevät henkilötietoja VRK:n puolesta ja lukuun. Organisaatioiden rekisteröijät toimivat täten henkilötietojen käsittelijän roolissa. Varmennerekisteröijien tulee täyttää ja toimittaa VRK:lle henkilötietojen käsittelijän seloste käsittelytoimista. Henkilötietojen käsittelijän seloste käsittelytoimista (mallipohja) ohjeineen on saatavilla Tietosuojavaltuutetun verkkosivuilla: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/selostekasittelytoimista.html#mitatietojaselosteessataytyyolla. Lisäksi VRK on laatinut selosteen täyttöohjeen.

Nämä roolit (rekisterinpitäjä, henkilötietojen käsittelijä) on kuvattu henkilötietojen käsittelyä koskevassa dokumentaatiossa (mm. sopimusliite henkilötietojen käsittelyn ehdot ja seloste käsittelytoimista). Aiheesta tiedotetaan, kun dokumentit valmistuvat ja ne on julkaistu VRK:n verkkosivustolla.

VRK huolehtii rekisteröijien säännöllisestä koulutuksesta ja tiedottamisesta rekisteröijätehtävien hoitamiseksi ja rekisteröintipisteelle asetettujen vaatimusten täyttämiseksi. Pidetyistä koulutuksista ja osallistumisista pidetään kirjaa ja koulutustarpeita arvioidaan säännöllisesti, erityisesti muutostilanteissa. Nimetyt VRK:n henkilöt vastaavat, että tarvittavat päivitykset huomioidaan VRK:n dokumentaatioissa, kuten rekisteröijäohje ja koulutusmateriaalit ym.

Tietoturva- ja tietosuojakysymykset on huomioitu ja sisällytetty sopimusliitteisiin ja rekisteröijille suunnattuun ohjeistukseen ja koulutusmateriaaleihin ja jokaisen tulee vastata myös omalla lainsäädännön, sopimusehtojen ja ohjeistusten mukaisella toiminnallaan tietoturvallisesta ja tietosuojakysymykset huomioivasta toiminnasta.

Rekisteröintipisteissä tulee käsitellä vain niitä henkilötietoja ja siinä laajuudessa mikä on hakemuskäsittelyn ja varmennehallinnan kannalta tarpeellista. Varmenneprosesseissa tarpeellisia henkilötietoja ovat hakemuksessa pyydetyt tiedot, väestötietojärjestelmästä (VTJ) ja Valviran rekistereistä haetut tiedot, jotka kirjataan Varttiin ja kortin varmenteeseen. Henkilötietojen käsittelyn käyttötarkoituksia ovat varmenteiden myöntäminen ja hallinnointi, varmenteiden sulkeminen sekä arkistoinnin edellyttämä käsittely. Tietoja ei käytetä muuhun tarkoitukseen. Henkilötietojen käsittelyyn ei sisälly erityisiä henkilötietoryhmiä[3)] koskevaa tietoa.

Käsittelyn tulee tapahtua VRK:n ohjeistuksen mukaisesti luottamuksellisuus, yksityisyys ja arkistointikäytänteet huomioiden. Tämä tarkoittaa esimerkiksi tietojen suojaamista luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia. Toiminnassa on ehkäis-

tävä luvatonta pääsyä tietoihin ja niiden käsittelyyn käytettyihin laitteisiin. Periaate edellyttää tietoturvallisuudesta huolehtimista ja se tulee asianmukaisesti katettua, kun noudatetaan tietoturvallisuutta koskevia määräyksiä, käytäntöjä, ehtoja ja ohjeita.

Tietojenkäsittelyä seurataan ja valvotaan asianmukaisuuden varmistamiseksi. Tietojen käsittelystä sekä Vartissa tehdyistä toimenpiteistä jää merkintä lokitietoihin. Näitä tietoja ei voida jälkikäteen muuttaa. VRK suorittaa valvontaa mm. auditointien ja lokitietojen tarkistuksen muodossa. Rekisteröijien asianmukaisella toiminnalla ja toiminnan seurannalla VRK:n toimesta varmistetaan osaltaan henkilötietojen säilyminen eheänä ja muuttumattomana, virheiden korjaaminen sekä rikkomuksista ilmoittaminen VRK:lle viivytyksettä.

Järjestelmän lokitiedot eivät kuulu omien tietojen tarkastusoikeuden piiriin. Tietojen käsittelyä valvoo tietosuojavaltuutettu/tietosuojan valvontaviranomainen. Väestörekisterikeskus raportoi vuosittain tietosuojavaltuutetulle/tietosuojan valvontaviranomaiselle suoritetusta tietojen käsittelystä.

VRK:n ulkopuolelle tapahtuva tietojen luovuttaminen ja käsittely palvelusta/rekisteristä/tietojärjestelmästä on toteutettu huomioiden tietojen minimointi eli vain ne tiedot luovutetaan ja niitä tietoja käsitellään, joiden osalta se on tarpeellista. Tämä sisältää asiakasorganisaatioiden tietojen käsittelyn, sopimuskumppanien ja alihankkijoiden sekä niiden henkilöstön tietojen käsittelyn, tarpeellisin osin rekisteröidyille itselleen tapahtuvan tietojen luovuttamisen sekä tietojen luovuttamisen korttitehtaalle varmennekortin tuottamista varten.

Lailliset henkilötietojen käyttötarkoitukset on kirjattu Vartin käyttöoikeuksia koskeviin päätöksiin ja seuraamukset käyttötarkoituksen vastaisesta toiminnasta on kirjattu sopimuksiin (sopimusehdot velvollisuuksista ja vastuista sekä sopimuksen korvausehdot sopimuksen vastaisesta toiminnasta).

Henkilötietojen käsittelyssä samaa tietoa ei käsitellä useissa eri järjestelmissä samaan käyttötarkoitukseen, ellei tähän ole löydettävissä selkeitä perusteita.

Rekisterinpitäjän (VRK) tulee ilmoittaa henkilökohtaisesti rekisteröidylle, mikäli on tapahtunut sellainen henkilötietoihin kohdistunut tietoturvaloukkaus, jonka yhteydessä henkilötietojen luottamuksellisuus on vaarantunut, esimerkiksi tietoja on vuotanut ulkopuolisille. Jotta VRK voi tehdä säädetyssä ajassa ilmoituksen rekisteröidylle ja valvontaviranomaiselle, tulee rekisteröijien, toimiessaan VRK:n puolesta ja lukuun, ilmoittaa viivytyksettä VRK:lle saatuaan tiedon tietoturvaloukkauksesta. Ilmoitus- ja yhteistyömenettelystä on tarkempia ehtoja sopimuksen liitteenä olevassa ohjeessa tietoturva- tai tietosuojapoikkeamien käsittelystä.

Palvelun/rekisterin/tietojärjestelmän tietolähteet on määritelty ja kuvattu rekisteriselosteessa. VRK:n rekisteriselosteet ovat saatavilla VRK:n verkkosivuilla. Eri tietojen käsittelyssä hyödynnetään mahdollisuuksien mukaan aina tietojen lähteenä primäärirekisteriä tai tieto pyydetään henkilöltä itseltään.

Varttiin tai rekisteröintiprosessiin liittyvien tietojen osalta epätarkkoja ja virheellisiä tietoja löydetään ja korjataan VRK:n henkilöstön ja rekisteröijien havaintojen sekä rekisteröityjen ilmoitusten

ja korjauspyyntöjen kautta. Rekisteröijä on velvollinen ilmoittamaan viivytyksettä epätarkoista ja/tai virheellisistä tiedoista VRK:lle kirjallisesti sähköpostilla osoitteeseen vartti@vrk.fi. Vartin osalta voidaan korjata rekisteröijän tiedoista nimi, henkilötunnus, sähköpostiosoite tai poistaa tarpeeton tunnus. Kortinhaltijan tiedot tulevat väestötietojärjestelmästä, joten virheellisten/muuttuneiden tietojen korjauspyyntö tulee lähettää väestötietojärjestelmän ylläpitoon. Kortit, joissa on virheellisiä tietoja, tulee sulkea varmenteiden sulkupalvelussa. Näistä ei tarvitse ilmoittaa VRK:lle.

Henkilötietojen säilytys perustuu myönnettyyn varmenteeseen ja varmenteen rekisteröintitoimiin ja tiedot on pystyttävä yhdistämään varmenteenhaltijaan. Säilytettävät tiedot ja säilytysaika perustuvat lakiin (laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 24 §). Säilytettäviä tietoja ovat varmenteen tietosisältö, ensitunnistamisen tiedot/käytetyt asiakirjat/sähköisen tunnistamisen tiedot). Tietojen arkistointiaika on kortin voimassaoloaika + 5 vuotta.

Vartin henkilötiedot on salattu ja suojattu asianmukaisesti huomioiden tietoturvallisuuden vaatimukset muun muassa seuraavin tavoin: Varttiin on rajatut käyttöoikeudet, kaikki tapahtumat tallentuvat lokitietoihin ja tiedonsiirto korttitehtaalle on salattu.

Tietosuojapoikkeamatilanteissa/tietoturvaloukkauksissa rekisteröijien on informoitava viivytyksettä VRK:lle poikkeamatilanteista (ohje tietoturva- ja tietosuojapoikkeamien käsittelystä). Rekisteröijän/VRK:n tulee tehdä tarvittavat toimet (varmenteen mahdollinen sulkeminen ym.) poikkeaman ottamiseksi käsittelyyn ja vahinkojen minimoimiseksi.

[1)] Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista 661/2009, 6 § Väestörekisterikeskuksen varmennettu sähköinen asiointi ja sen tarkoitus, 61 § Varmennetun sähköisen asioinnin palvelut; laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009, 6 § Henkilötietojen käsittely

[2)] Käsittelyn tarkoituksena on varmennepalvelujen tarjoaminen VRK:n lakisääteisenä tehtävänä. Mikäli tietoja luovutetaan, tiedon vastaanottajina ovat varmenteenhaltijat ja korttitehdas. Tietojen säilytysaika on kortin voimassaoloaika + 5v. Henkilöllä on oikeus pyytää rekisterinpitäjältä tietojensa oikaisemista (oikeutta pyytää tietojen poistamista tai tietojen käsittelyn rajoittamista ei puolestaan sovelleta VRK:n lakisääteisiin henkilörekistereihin, eli ei myöskään varmennerekistereihin, koska henkilötietojen käsittely on varmennetoiminnan edellytys). VRK:n varmennerekistereitä pidetään lakisääteisten tehtävien hoitamiseksi (varmennepalvelujen tarjoaminen), joten tietojen siirto-oikeutta toiseen järjestelmään ei tällöin ole. Henkilöllä on oikeus tehdä valitus valvontaviranomaiselle/tietosuojavaltuutetulle (mikäli henkilötietoja ei ole käsitelty lainsäädännön edellyttämällä tavalla). Mikäli henkilötietoa ei ole kerätty rekisteröidyltä, tietojen alkuperästä annetaan tarpeellinen tieto, esim. tietolähteenä organisaation rekisteröijä, VTJ.

[3)] Erityisiä henkilötietoryhmiä koskeva käsittely: Sellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys sekä geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely.