Varmennepalvelut

1.11.2021

Organisaatiokortin käyttöehdot

Yleistä

Digi- ja väestötietovirasto (DVV) on henkilörekisteriä ylläpitävä ja sähköisen asioinnin tukipalveluita, notaari- ja oikeudellisia vahvistuspalveluita sekä holhoustoimen palveluita tuottava viranomainen, jonka väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetun lain (661/2009) mukainen tehtävä on myös tuottaa varmennettuja sähköisen asioinnin palveluita. Virasto (31.12.2019 asti Väestörekisterikeskus (VRK)) on toiminut myös terveydenhuollon lakisääteisenä varmentajana 1.12.2010 alkaen ja sosiaalihuollon lakisääteisenä varmentajana 1.4.2015 alkaen (laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021), laki sähköisestä lääkemääräyksestä (61/2007) sekä laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista (661/2009)).

Digi- ja väestötietovirasto myöntää organisaatioiden ja yhteisöjen käyttöön tarkoitetut toimikortit ja niiden varmenteet.

DVV:n toimintaa sähköisen tunnistuspalvelun tarjoajana ja hyväksyttynä luottamuspalvelun tarjoajana säätelee syyskuussa 2014 voimaan tullut Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (ns. eIDAS-asetus). eIDAS-asetus on jäsenvaltioissa suoraan sovellettavaa oikeutta ja sitä on sovellettu 1.7.2016 alkaen.

Edellä mainittua EU-sääntelyä täydentää komission täytäntöönpanoasetus (EU) 2015/1502, teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti (ns. varmuustasoasetus). Varmuustasoasetuksen vaatimukset täyttäessään palveluntarjoaja profiloituu Suomessa sähköisten tunnistuspalvelujen osalta korotetun tai korkean varmuustason mukaisena palveluntarjoajana/vahvan sähköisen tunnistuspalvelun tarjoajana.

Kansallisessa laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) säädetään vahvan sähköisen tunnistamisen palvelujen tarjoamisesta ja sähköisistä luottamuspalveluista, mm. sähköisestä allekirjoituksesta, ja niiden oikeusvaikutuksista. Lakia on muutettu vastaamaan eIDAS-asetuksen vaatimuksia ja muutokset ovat tulleet voimaan 1.7.2016 alkaen.

Organisaatiokortin sisältämiä organisaatiovarmenteita voidaan käyttää henkilön vahvaan sähköiseen tunnistamiseen, tiedon salaukseen ja sähköiseen allekirjoitukseen. Todentamis- ja salausvarmenne täyttää vahvan sähköisen tunnistamisvälineen vaatimukset eIDAS-asetuksen mukaisella tasolla ”korkea”. Yksinomaan allekirjoituksen toteuttamiseen tarkoitettu allekirjoitusvarmenne täyttää eIDAS-asetuk-sen mukaiset hyväksytyn allekirjoitusvarmenteen vaatimukset. Varmenteen hakijan henkilöllisyyden oikeellisuuden takaa Digi- ja väestötietovirasto.

Organisaatiovarmenteen voimassaoloaika on enintään viisi vuotta.

Organisaatiokortin sähköisten ominaisuuksien käyttöönottaminen edellyttää organisaatiovarmenteen aktivoimista.

Organisaatiokortin hakeminen

Organisaatiovarmennetta haetaan käymällä henkilökohtaisesti rekisteröijänä toimivassa rekisteröintipisteessä. Hakemuksen tiedot tallennetaan varmentajan varmennetietojärjestelmään.

Organisaatiovarmennehakemus hyväksytään myöntämällä varmenne. Mikäli edellytykset varmenteen myöntämiseksi puuttuvat hakijan osalta, varmennetta ei myönnetä ja hakemus hylätään. Päätöksestä ilmoitetaan viipymättä hakijalle, joka voi tehdä päätöksestä kirjallisen muutosvaatimuksen varmentajalle.

Varmennetta haettaessa organisaatiokortin hakijan henkilöllisyys tarkistetaan voimassa olevasta, poliisin myöntämästä henkilöllisyyden osoittavasta asiakirjasta, joita ovat henkilökortti (1.3.1999 jälkeen myönnetty) ja passi. Hyväksyttäviä tunnistamisasiakirjoja ovat myös Euroopan talousalueen jäsenvaltion, Sveitsin tai San Marinon viranomaisen myöntämä voimassa oleva passi tai henkilökortti, tai muun valtion viranomaisen myöntämä voimassa oleva passi. Jos hakijalla ei ole em. asiakirjoja, poliisi tunnistaa hakijan henkilöllisyyden muilla tavoin.

Uutta varmennetta voidaan hakea myös edellisen varmenteen voimassaolon päättyessä, mikäli varmenteen myöntämisen edellytykset ovat edelleen voimassa. Uutta varmennetta haettaessa noudatetaan samoja menettelyjä kuin varmennetta ensi kertaa haettaessa. Uutta varmennetta voi hakea vain varmenteen haltija.

Uutta varmennetta voidaan hakea myös varmenteen tietosisältöön vaikuttavien varmenteen haltijan tietojen muuttuessa tai varmennekortin rikkoutuessa. Tällöin varmenteen haltijan tulee ottaa yhteyttä rekisteröintipisteeseen ja hakea uutta varmennekorttia ja varmennetta.

Varmentaja toimittaa hakijalle hakijan tiedoilla yksilöidyn:

• organisaatiokortin, joka sisältää kortinhaltijan henkilökohtaiset avainparit ja varmenteet

• aktivointitunnuslukukuoren, jonka avulla organisaatiokortin haltija asettaa kortille PIN1- (todentamis- ja salausvarmenne) ja PIN2-tunnusluvut (allekirjoitusvarmenne).

Lisäksi rekisteröijä toimittaa varmenteen hakijalle toimikortin käyttöoppaan.

Organisaatiovarmenteen käyttöönottoon tarvittava aktivointitunnuslukukirje postitetaan joko hakijan kotiosoitteeseen tai organisaatioon kortinhakijalle osoitettuna noin neljä päivää kortin postittamisen jälkeen.

Organisaatiovarmenteen käyttöön ottaminen

Organisaatiokortilla olevan organisaatiovarmenteen sähköisten ominaisuuksien käyttöönotto edellyttää kortin aktivointia aktivointitunnusluvun avulla. Organisatiokortin ja aktivointitunnusluvun lisäksi organisaatiovarmenteen käyttöönottoa varten tarvitaan tietokone, kortinlukija ja kortinlukijaohjelmisto. Organisaatiovarmenteen aktivointi suoritetaan

kortinlukijaohjelmisto mPollux DigiSign Client avulla. Uusimman kortinlukijaohjelmiston voi ladata ilmaiseksi osoitteesta https://dvv.fi/kortinlukijaohjelmisto.

Kortinlukijaohjelmisto käynnistää aktivointiprosessin automaattisesti, kun organisaatiokortti asetetaan kortinlukijaan ensimmäisen kerran. Aktivointitunnusluvun avulla käyttäjä luo varmenteelle kaksi henkilökohtaista PIN-tunnuslukua, eli perustunnusluvun (PIN1) ja allekirjoitustunnusluvun (PIN2). PIN1-perustunnusluvun avulla kortin käyttäjä voi tunnistautua palveluihin ja PIN2-allekirjoitustunnusluvun avulla käyttäjä voi tehdä sähköisen allekirjoituksen.

Yksityiskohtaiset ohjeet organisaatiovarmenteen käyttöön ottamiseksi löytyvät DVV:n verkkosivulta https://dvv.fi/toimikortin-kayttoonotto.

Varmenteiden neuvontapalvelu palvelee maanantaista perjantaihin klo 8 - 21 ja lauantaina klo 9 - 15 numerosta 0600 96160 (pvm/mpm). Palvelu on suljettu sunnuntaisin ja arkipyhinä. Neuvontapalvelu palvelee suomeksi, ruotsiksi ja englanniksi.

Tunnuslukujen hallinta

Ohjeet lukkiutuneen tunnusluvun vapauttamiseen ja tunnusluvun vaihtamiseen löytyvät DVV:n verkkosivulta https://dvv.fi/pin-tunnuslukujen-hallinta. Jos aktivointitunnusluku katoaa, tilataan uusi aktivointitunnusluku henkilökohtaisen käynnin yhteydessä organisaation omasta rekisteröintipisteestä.

Vastuu organisaatiokortin säilyttämisestä

Organisaatiokorttia ja siihen liittyvää aktivointitunnusta saa käyttää ainoastaan kortinhaltija.

Varmenteen haltijan tulee säilyttää ja hallita huolellisesti omia varmenteitaan ja avainparejaan sekä niihin liittyviä tunnuslukuja ja varmennekorttiaan. Varmenteen haltijan tulee estää varmennekortin katoaminen sekä tunnuslukujen paljastuminen tai luvaton käyttö.

PIN-tunnuslukuja, joita käytetään avainten aktivointiin, ei saa säilyttää samassa paikassa varmennekortin kanssa. Varmenteen haltijan on vaihdettava PIN-tunnusluvut, mikäli on epäiltävissä, että tunnusluvut ovat voineet joutua ulkopuolisten tietoon.

Organisaatiovarmenteen haltijan vastuu varmenteen käyttämisestä päättyy, kun hän on ilmoittanut sulkupalveluun tarvittavat tiedot sen sulkemiseksi ja saanut puhelun vastaanottaneelta virkailijalta sulkemista koskevan ilmoituksen. Tarkemmat ohjeet varmenteen sulkemiseen löydät kohdasta *Organisaatiokortilla olevien varmenteiden mitätöinti*. Vastuun katkaisemiseksi sulkuilmoitus on tehtävä välittömästi, kun syy ilmoittamiseen on havaittu.

Kortinhaltijan on huolehdittava organisaatiokortista näiden käyttöehtojen ja julkisesti saatavilla olevan hyväksytyn varmennepolitiikan mukaisesti. Organisaatiokorttia on säilytettävä huolellisesti siten, ettei se joudu ulkopuolisten käsiin, eikä sitä muuteta tai ettei sitä käytetä luvatta. Tämän käyttöohjeen vastainen menettely vapauttaa Digi- ja väestötietoviraston organisaatiokortin käyttämisestä mahdollisesti aiheutuvista vastuista.

Organisaatiokortin haltijan vastuu

Varmennepalvelut 1.11.2021

Organisaatiovarmenne sisältää eurooppalaisen eIDAS-asetuksen (910/2014) mukaisen henkilön tunnistusvarmenteen sekä sähköisen allekirjoituksen hyväksytyn tason varmenteen.

Organisaatiokortin haltijan tulee sitoutua toimimaan varmennepolitiikan mukaisesti hakiessaan ja käyttäessään organisaatiovarmennetta. Varmenteen haltija vastaa siitä, että varmennetta haettaessa ilmoitetut tiedot ovat oikeita.

Organisaatiovarmenteen hakijan oikeudet ja velvollisuudet ovat saatavilla ennen organisaatiovarmennehakemuksen allekirjoittamista toimikortin käyttöoppaassa (https://dvv.fi/toimikortin-kayttoonotto), toimikortin käyttöehdoissa ja varmennepolitiikassa (https://dvv.fi/cps), joissa on kuvattu kummankin osapuolen (varmentajan ja varmenteen haltijan) oikeudet ja velvollisuudet. Kun organisaatiovarmenteen hakija hakee varmennetta, hän hyväksyy samalla yleiset käyttöehdot ja sitoutuu ohjeiden mukaiseen varmenteiden käyttöön.

Hakemusasiakirjassa ja käyttöehdoissa mainitaan selkeästi, että organisaatiovarmenteen hakija vahvistaa allekirjoituksellaan annettujen tietojen oikeellisuuden sekä hyväksyy organisaatiovarmenteen luomisen ja julkaisun asiakasorganisaation kanssa tehdyn sopimuksen mukaisesti tai julkisessa hakemistossa. Samalla hakija hyväksyy organisaatiovarmenteen käyttöön liittyvät säännöt ja ehdot sekä huolehtii organisaatiovarmenteen ja PIN-tunnusten säilyttämisestä sekä mahdollisen väärinkäytön tai kortin katoamisen ilmoittamisesta.

Organisaatiovarmenne on haltijansa sähköinen henkilöllisyys eikä sitä tämän vuoksi saa luovuttaa toisen henkilön käytettäväksi.

Organisaatiovarmenteen haltija on vastuussa toimikortin käytöstä, kortilla tekemistään oikeustoimista ja niiden taloudellisista seuraamuksista.

Kortinlukijassa olevaa omaa varmennekorttia ei saa jättää valvomatta eikä missään tilanteessa antaa kenenkään muun käyttöön.

Mikrosirun sisältävän kortin jättäminen lukijalaitteeseen saattaa mahdollistaa organisaatiovarmenteen väärinkäytön. Lopettaessaan pääteistunnon tai jättäessään päätelaitteen valvomatta organisaatiovarmenteen haltijan vastuulla on poistaa organisaatiovarmenteen sisältävä mikrosiru lukijalaitteesta ja sulkea käytetyt sovellukset asianmukaisesti tai muuten katkaistava organisaatiovarmenteen käyttämiseksi tarvittava tekninen yhteys.

Jos varmennekortti rikkoutuu, tulee kortinhaltijan sulkea rikkoutuneen kortin varmenteet ja hakea uusi varmennekortti rekisteröintipisteestä. Uuden varmennekortin hakemisessa noudatetaan samoja menettelyjä kuin korttia ja varmennetta ensi kertaa haettaessa.

Varmenteenhaltijan tulee ilmoittaa sulkupalveluun varmennekortin katoaminen tai väärinkäyttöepäily.

Jos tunnusluku on lukkiutunut ja sen avaamiseen tarvittava PUK-/aktivointitunnusluku on kadonnut, tulee kortinhaltijan ottaa yhteyttä oman organisaationsa rekisteröintipisteeseen saadakseen tietoonsa PUK-/aktivointitunnusluvun.

Digi- ja väestötietoviraston vastuu

Varmennepalvelut 1.11.2021

Varmennepalveluiden tuottamiseen liittyvä Digi- ja väestötietoviraston vahingonkorvausvastuu määräytyy asiakasorganisaation kanssa tehdyn sopimuksen mukaisesti. Digi- ja väestötietovirastoa koskevat lain vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain mukaiset varmentajan vahingonkorvausvastuut. Soveltuvin osin sovelletaan myös vahingonkorvauslakia (412/1974) ja sähköisestä asioinnista viranomaistoiminnassa annettua lakia (13/2003).

Digi- ja väestötietovirasto vastaa varmentajana koko varmennejärjestelmän turvallisuudesta. Varmentaja vastaa toimeksiantona hankkimistaan palveluista samoin kuin olisi itse tuottanut palvelun.

Digi- ja väestötietovirasto vastaa siitä, että organisaatiovarmenne on luotu noudattaen väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (661/2009), laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista, laissa sähköisestä asioinnista viranomaistoiminnassa ja varmennepolitiikassa sekä varmennuskäytännössä esitettyjä menettelyjä ja varmenteen hakijan antamien tietojen mukaisesti. Digi- ja väestötietovirasto vastaa ainoastaan niistä tiedoista, jotka se on tallettanut organisaatiovarmenteeseen.

Digi- ja väestötietovirasto vastaa siitä, että kun organisaatiovarmennetta käytetään asianmukaisesti, se on käytettävissä luovutushetkestä koko sen voimassaoloajan, ellei sitä ole asetettu sulkulistalle. Organisaatiovarmenne on luovutettu henkilölle, joka on tunnistettu organisaatiovarmenteelta edellytettävällä tavalla. Varmenteen haltijalle on luovutettu organisaatiovarmenteen käyttöön liittyvät käyttöohjeet.

Varmennetta luodessaan ja allekirjoittaessaan organisaatiovarmenteen yksityisellä avaimellaan varmentaja vakuuttaa tarkistaneensa organisaatiovarmenteessa olevat henkilötiedot varmennepolitiikassa ja varmennuskäytännössä esitettyjen menettelyjen mukaisesti.

Varmentaja vastaa siitä, että sulkulistalle viedään oikean henkilön organisaatiovarmenne ja että ne ilmestyvät varmennepolitiikassa mainitussa ajassa sulkulistalle.

Digi- ja väestötietoviraston vastuun rajoitukset

Digi- ja väestötietovirasto ei vastaa PIN-tunnusten, PUK-/tai aktivointitunnusluvun ja organisaatiovarmenteen haltijan yksityisten avainten paljastumisen seurauksena syntyvistä vahingoista, ellei paljastuminen välittömästi johdu Digi- ja väestötietoviraston välittömästä toiminnasta.

Digi- ja väestötietovirasto vastaa organisaatiovarmenteen haltijalle ja organisaatiovarmenteeseen luottavalle osapuolelle enintään aiheutuneista välittömistä vahingoista, mikäli vahinko johtuu Digi- ja väestötietoviraston välittömästä toiminnasta.

Digi- ja väestötietovirasto ei vastaa organisaatiovarmenteen haltijalle aiheutuneista välillisistä tai seurannaisvahingoista. Digi- ja väestötietovirasto ei myöskään vastaa organisaatiovarmenteeseen luottavan osapuolen tai organisaatiovarmenteen haltijan muun sopimuskumppanin mahdollisesti kärsimistä välillisistä tai seurannaisvahingoista.

Digi- ja väestötietovirasto ei vastaa yleisten tietoliikenneyhteyksien eikä tietoverkkojen, esimerkiksi Internetin toimivuudesta eikä siitä, jos oikeustoimen suorittaminen estyy

organisaatiovarmenteen haltijan käyttämän laitteen tai ohjelmiston toimimattomuudesta eikä siitä, että organisaatiovarmennetta käytetään vastoin sen käyttötarkoitusta.

Varmentajalla on oikeus keskeyttää palvelu muutos- ja huoltotoimien ajaksi. Sulkulistaa koskevista muutoksista tai huoltotöistä ilmoitetaan etukäteen.

Varmentajalla on oikeus kehittää edelleen varmennepalvelua. Organisaatiovarmenteen haltijan tai organisaatiovarmenteeseen luottavan osapuolen on vastattava tämän vuoksi aiheutuvista omista kustannuksistaan eikä varmentaja ole velvollinen korvaamaan organisaatiovarmenteen haltijalle tai organisaatiovarmenteeseen luottavalle osapuolelle tällaisesta varmentajan kehittämistyöstä aiheutuvista kustannuksista.

Varmentaja ei vastaa varmennetta käytettäessä varmenteen haltijalle ja organisaatiolle tarkoitetun varmenteeseen pohjautuvan verkkopalvelun tai sovelluksen virheistä tai niistä aiheutuvista kustannuksista.

Varmentaja ei vastaa vahingosta, joka aiheutuu varmenteen haltijan tai varmennejärjestelmää hyödyntävän tahon lain, varmennepolitiikan, varmennuskäytännön tai muiden ohjeiden vastaisesta toiminnasta.

Ylivoimainen este

Varmentaja ei vastaa luonnonmullistuksista tai muista vastaavista ylivoimaisista olosuhteista johtuvista vahingoista.

Organisaatiokortilla olevien varmenteiden sulkeminen/mitätöinti

Organisaatiokortilla olevat varmenteet suljetaan soittamalla sulkupalveluun 0800 162 622 (maksuton Suomesta soitettaessa), ulkomailta soitettaessa +358 800 162 622 (+ paikallisen operaattorin veloitus).

Varmenteen sulkemista voivat vaatia:

- organisaatiokortin haltija tai hänen lakisääteinen edustajansa kyseisen henkilön oman varmenteen osalta;
- varmentaja alla mainittujen edellytysten täyttyessä.

Varmenne suljetaan kun:

- varmenteen haltija pyytää sulkemista
- varmenteen haltija vaihtaa työpaikkaa
- Varmennekortti on vahingoittunut, kadonnut tai anastettu
- avaustunnusluku sekä varmennekortti ovat kadonneet tai anastettu
- varmenteen haltija on kuollut.

Varmenteen haltijan tulee viipymättä tehdä varmenteen sulkupyyntö sulkupalveluun, kun yllä kuvatut varmenteen sulkemisen edellytykset täyttyvät.

Varmentaja voi sulkea organisaatiovarmenteen, mikäli varmennetta on käytetty varmennepolitiikan, varmennuskäytännön, sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain tai sähköisestä lääkemääräyksestä annetun lain sekä niiden nojalla annettujen säädösten tai niiden nojalla asetettujen vaatimusten ja ohjeiden vastaisesti.

Varmennetta ei saa käyttää tai yrittää käyttää sen jälkeen, kun sitä koskeva sulkupyyntö on tehty.

Digi- ja väestötietovirasto sulkee myöntämänsä varmenteet, mikäli varmenteiden tietosisällössä havaitaan virhe.

Digi- ja väestötietovirasto voi sulkea käyttämällään yksityisellä avaimellaan allekirjoitetut varmenteet, mikäli on syytä epäillä Digi- ja väestötietoviraston yksityisten avainten paljastuneen tai joutuneen vääriin käsiin.

Kaikki paljastuneella avaimella myönnetyt ja voimassa olevat varmenteet on suljettava yhdellä tai useammalla sulkulistalla, joiden voimassaoloaika ei lakkaa ennen kuin viimeisen suljetun varmenteen voimassaoloaika on päättynyt.

Mikäli Digi- ja väestötietoviraston varmenteiden luonnissa käyttämä yksityinen avain tai muu tekninen menetelmä on paljastunut tai tullut muutoin käyttökelvottomaksi, Digi- ja väestötietoviraston on ilmoitettava tapahtuneesta kaikille kortinhaltijoille ja valvontaviranomaisena toimivalle Liikenne- ja viestintävirastolle (Traficomille) asianmukaisella tavalla.

Digi- ja väestötietovirasto voi sulkea varmenteen erityisestä syystä.

Informointi tietojen käsittelystä

Varmentajan järjestelmissä tapahtuvassa yksityisten tietojen käsittelyssä noudatetaan henkilötietojen käsittelyä ja yksityisyydensuojaa koskevaa lainsäädäntöä, mm. väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annettua lakia (661/2009), EU:n yleistä tietosuoja-asetusta (EU) 2016/679 ja tietosuojalakia (1050/2018). Varmentajan järjestelmissä tapahtuvassa julkisten tietojen käsittelyssä noudatetaan lakia viranomaisten toiminnan julkisuudesta (621/1999). Varmentaja vastaa siitä, että varmentajan järjestelmissä käsiteltävät yksityiset tiedot on suojattu asiattomalta käsittelyltä. Viranomaisille luovutetaan tietoja lakien, asetusten taikka niiden nojalla annettujen määräysten perusteella.

Henkilön yksilöintitunnus ja muut hakemuksessa ilmoitetut tiedot talletetaan DVV:n varmennejärjestelmään. Organisaatiokortissa olevat todentamisvarmenteet ja henkilön yksilöintitunnus talletetaan myös DVV:n julkiseen hakemistoon (https://dvv.fi/varmennehakemisto), ellei asiakasorganisaation kanssa ole sovittu toisin. Julkisesta hakemistosta jokaisella on oikeus saada tietoja siten kuin viranomaisten toiminnan julkisuudesta annetussa laissa säädetään. Tietojen arkistointiaika on kortin voimassaoloaika + 5 vuotta.

Varmentaja on julkaissut varmennepalveluiden osalta erityiset tietosuojalainsäädännön mukaiset käytännesäännöt.

Rekisterinpitäjä ja selosteet

Organisaatiokortin sisältämiä henkilötietoja kerätään seuraaviin järjestelmiin: väestötietojärjestelmään, varmennejärjestelmään ja sulkulistaan. Väestötietojärjestelmän osalta

rekisterinpitäjiä ovat DVV ja Ahvenanmaan valtionvirasto, varmennejärjestelmän ja sulkulistan osalta rekisterinpitäjä on DVV.

Rekistereistä on laadittu tietosuojalain mukaiset selosteet, jotka ovat nähtävissä https://dvv.fi/tietosuojaselosteet.

DVV:n palveluiden ja rekisterien tietosuojaselosteet kertovat yksityiskohtaisesti, miten, missä ja miksi henkilötietoja käsitellään.

Varmenteen tietosisältö

Digi- ja väestötietoviraston myöntämään organisaatiovarmenteeseen talletetaan:

- Varmenteen haltijan yksilöintitunnus (entinen SV-numero)
- Varmenteen sarjanumero
- Varmenteen haltijan suku- ja etunimi
- UPN- kenttä
- Organisaation nimi
- Varmenteen voimassaoloaika
- Titteli (valinnainen tieto)
- Organisaatioyksikkö (valinnainen tieto)

Tarkemmat tekniset määrittelyt varmenteiden tietosisällöistä löytyvät https://dvv.fi/fineid-maaritykset -sivustolta.

Varmenteen tiedot ja niiden oikeellisuus vahvistetaan varmenteen myöntäjän sähköisellä allekirjoituksella.

Varmentaja julkaisee varmentajan varmenteet ja sulkulistat maksuttomassa, yleisesti saatavilla olevassa julkisessa hakemistossa. Varmenteesta ja/tai asiakasorganisaation kanssa tehdystä sopimuksesta riippuen varmentaja julkaisee myönnetyt todentamis- ja salausvarmenteet joko julkisessa tai ei-julkisessa hakemistossa. Allekirjoitusvarmenteita ei julkaista hakemistossa.

Tietosuojalainsäädännön mukaisen tarkastusoikeuden ja virheenoikaisun toteuttaminen

Varmenteen haltijalla on oikeus saada häntä koskevia tietoja, esimerkiksi henkilötietoja, voimassa olevan lainsäädännön mukaisesti.

Rekisteröidyn oikeudesta tarkastaa omat rekisteritietonsa ja rekisteröidyn kielto-oikeudesta kieltää rekisterinpitäjää käsittelemästä häntä itseään koskevia rekisteritietoja sekä virheen oikaisusta säädetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 (yleinen tietosuoja-asetus), tietosuojalaissa (1050/2018) ja väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista annetussa laissa (661/2009). Tietosuojalainsäädännön mukaiset tarkastusoikeuspyynnöt ja virheenoikaisut osoitetaan kunkin rekisterin rekisterinpitäjälle.

Rekisterinpitäjän vastuu ja henkilötietojen käsitteleminen

Varmentajan järjestelmissä tapahtuvassa yksityisten tietojen käsittelyssä noudatetaan henkilötietojen käsittelyä ja yksityisyydensuojaa koskevaa lainsäädäntöä. Varmentajan järjestelmissä tapahtuvassa julkisten tietojen käsittelyssä noudatetaan lakia viranomaisten toiminnan julkisuudesta (621/1999). Varmentaja vastaa siitä, että varmentajan järjestelmissä käsiteltävät yksityiset tiedot on suojattu asiattomalta käsittelyltä. Viranomaisille luovutetaan tietoja lakien, asetusten taikka niiden nojalla annettujen määräysten perusteella.

Organisaatiokorttiin liittyvät lisätiedot

Organisaatiokorttia koskevat varmennepolitiikka-asiakirjat löytyvät osoitteesta https://dvv.fi/cps

DVV:n tunnistusperiaatteet löytyvät osoitteesta https://dvv.fi/varmenteet

PIN-tunnuslukujen vaihtamiseen ja lukkiutuneiden tunnuslukujen vapauttamiseen soveltuva ohjelma (mPollux DigiSign Client) on ladattavissa ilmaiseksi osoitteesta https://dvv.fi/kortinlukijaohjelmisto

Valitus- ja riidanratkaisumenetelmät

Hakemuksesta DVV:ssä myönnetty organisaatiokortti on osoitus myönteisestä hallintopäätöksestä, organisaatiokorttihakemuksen hylkääminen on osoitus kielteisestä hallintopäätöksestä. DVV:n päätöksessä on liitteenä oikaisuvaatimusohje ja valitusosoitus.

DVV:n päätökseen tyytymätön voi vaatia päätöksen oikaisua DVV:lta. Oikaisuvaatimus DVV:lle on tehtävä kirjallisesti. Oikaisuvaatimus voi olla vapaamuotoinen, mutta siinä on ilmoitettava ja sen tulee sisältää oikaisuvaatimusohjeessa ja valitusosoituksessa mainitut asiat ja liitteet.

Oikaisumenettelyssä tehdystä päätöksestä voi päätökseen edelleen tyytymätön valittaa hallinto-oikeuteen. Muutosta haetaan hallinto-oikeuteen toimitettavalla kirjallisella valituksella. Valitus voi olla vapaamuotoinen, mutta siinä on ilmoitettava ja sen tulee sisältää oikaisuvaatimusohjeessa ja valitusosoituksessa mainitut asiat ja liitteet. Valitus tehdään sille hallinto-oikeudelle, jonka tuomiopiirissä DVV sijaitsee. Valitusaika alkaa kulua siitä hetkestä, kun valitusosoitus on asianmukaisesti liitetty päätökseen ja annettu tiedoksi hakijalle.

Rekisteröintisopimuksen nojalla sopimusta koskevat erimielisyydet, joista ei Osapuolten välisissä neuvotteluissa päästä sovintoon käsitellään Helsingin käräjäoikeudessa suomen kielellä. Valtionhallinnon sisällä erimielisyydet ratkaistaan neuvotteluin.