26.10.2020

Valtiokonttorin tietosuojaperiaatteet

Vahvistettu 26.2.2018

Päivitetty 26.10.2020

Valtiokonttori
Statskontoret
State Treasury

Sörnäisten rantatie 13, Helsinki | PL 14, 00054 VALTIOKONTTORI
Puh. 0295 50 2000, Faksi 0295 50 3333, www.valtiokonttori.fi

26.10.2020

Version hallinta

Versio	Päiväys	Vastuuhenkilö	Muutokset
1.1	26.10.2020	Riskienhallintajohtaja Heikki Kangas	Tarkastettu ajantasaisuus. Päivitetty mm. - viittaukset lainsäädäntöön - täsmennetty henkilötiedon määritelmää - tarkennettu mm. tietosuojan perehdytystä ja koulutusta käsittelevää osiota (kappale 9) - täsmennetty tietosuojan huomiointia palvelusopimuksissa (kappale 8) sekä tietosuojan raportointia viraston johdolle (kappale 11) - poistettu maininta tietotilinpäätöksestä (kappale 11) - Tarkennettu tietosuojapoikkeamien käsittelyä (kappale 12)

26.10.2020

Sisällys

26.10.2020

1. Yleistä

Tässä asiakirjassa kuvataan Valtiokonttorin tietosuoja-asioissa noudattamia periaatteita sekä rekisteröityjen oikeuksia ja rekisterinpitäjän velvollisuuksia, joita Valtiokonttori noudattaa kaikessa henkilötietojen käsittelyssä. Tehtäviään hoitaessaan Valtiokonttori käsittelee henkilöiden henkilötietoja heille kuuluvia perusoikeuksia ja -vapauksia kunnioittaen.

2. Tavoitteet

Valtiokonttorin tavoitteena on kaikessa toiminnassaan henkilötietoja käsitellessään varmistaa, että rekisteröityjen oikeudet toteutuvat ja henkilötietoja käsitellään lainsäädännön ja näiden periaatteiden mukaisesti.

Ennen henkilötietojen käsittelyn aloittamista ja säännöllisesti käsittelyn aikana Valtiokonttorissa arvioidaan käsittelyyn kohdistuvia riskejä ja tarvittavat hallintatoimenpiteet valitaan arvioidun riskitason mukaan. Lähtökohtana on sisäänrakennettu ja oletusarvoinen tietosuoja.

Valtiokonttori ottaa huomioon tietosuojan vaatimukset hoitaessaan tehtäviään kaikissa olosuhteissa käytetystä teknologiasta riippumatta.

Tietosuojaperiaatteita noudatetaan yhteistyökumppaneiden ja muiden henkilötietojen käsittelijöiden kanssa tehtävissä sopimuksissa ja sidosryhmien käyttäjille laadittavissa ohjeissa.

3. Ohjaavat tekijät

Valtiokonttorin toimintaa ohjaa voimassa oleva lainsäädäntö. Tärkeimpinä tietosuojaa ohjaavina säännöksinä ovat Euroopan unionin yleinen tietosuoja-asetus, Suomen perustuslaki, laki viranomaisen toiminnan julkisuudesta, laki julkisen hallinnon tiedonhallinnasta, tietosuojalaki sekä muu henkilötietojen käsittelyä ja suojaa koskeva kansallinen lainsäädäntö. Osin Valtiokonttorin toimintaan kohdistuu ohjaavia määräyksiä myös Finanssivalvonnan toimesta.

4. Määritelmiä

Henkilötieto
Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen tai hänelle tunnusomaisten tekijöiden perusteella. Henkilötieto voi olla mitä tahansa tietoa, joka koskee esimerkiksi henkilön perhe-elämää, terveyttä, ammatillista toimintaansa taikka hänen taloudellista tai sosiaalista asemaansa. Henkilötietona pidetään esimerkiksi puhelinnumeroa, ajoneuvon rekisterinumeroa tai vaikkapa henkilön käyttämää IP-osoitetta.

Käsittely
Käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti.

Rekisteröity
Rekisteröidyllä tarkoitetaan henkilöä, jota henkilötieto koskee.

Rekisterin pitäjä
Rekisterinpitäjällä tarkoitetaan henkilöä, viranomaista, virastoa tai muuta tahoa, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Henkilötietojen käsittelijä
Luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

5. Periaatteet

Valtiokonttori noudattaa seuraavia periaatteita kaikessa toiminnassaan käsitellessään henkilötietoja:

Lainmukaisuus, kohtuullisuus, läpinäkyvyys
Henkilötietoja käsitellään lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi.

Läpinäkyvyyden periaatteen mukaan rekisteröidylle on:
1. oltava näkyvää, miten henkilötietoja kerätään, käytetään ja muulla tavoin käsitellään
2. oltava näkyvää, missä määrin henkilötietoja käsitellään tai on tarkoitus käsitellä
3. henkilötietojen käsittelyyn liittyvä viestintä oltava helposti saatavilla ja ymmärrettävissä
4. tietoa annettaessa käytettävä selkeää ja yksinkertaista kieltä
5. tiedotettava riskeistä, säännöistä, suojatoimista, oikeuksista ja miten niitä käytetään

Käyttötarkoitussidonnaisuus
Henkilötietoja kerätään nimenomaista ja laillista tarkoitusta varten. Tämä tarkoitus ilmoitetaan rekisteröidylle henkilötietojen keräämisen yhteydessä, eikä kerättyjä tietoja myöhemmin käsitellä tämän tarkoituksen kannalta vieraalla tavalla.

Tietojen minimointi
Kaikki kerätyt henkilötiedot ovat riittäviä, olennaisia ja rajoittuvat siihen, mikä on välttämätöntä käsittelyn tarkoituksen kannalta.

Täsmällisyys
Kerätyt henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä. Epätarkat ja virheelliset tiedot oikaistaan tai poistetaan. Rekisteröidyillä on oikeus päästä tietoihinsa, oikaista tietoja ja poistaa tietojansa lain sallimissa rajoissa.

Säilytyksen rajoittaminen
Henkilötietoja säilytetään tunnistettavassa muodossa vain niin kauan kuin se on tarpeen henkilötietojen käsittelyn tarkoituksen toteuttamista varten. Säilytyksen rajoittamiseksi asetetaan määräaikoja henkilötietojen poistoa tai tarpeellisuuden arviointia varten.

Tietoturvallisuus
Henkilötietoja suojataan luvattomalta tai lainvastaiselta käsittelyltä sekä epätoivotulta häviämiseltä ja tuhoutumiselta.

Osoitusvelvollisuus
Valtiokonttori kykenee tarvittaessa osoittamaan noudattavansa tietosuojavelvoitteita. Henkilötietojen käsittelyyn liittyvät toiminnat suunnitellaan ja dokumentoidaan riittävällä tavalla.

Sisäänrakennettu ja oletusarvoinen tietosuoja
Edellä mainitut periaatteet otetaan tehokkaasti osaksi henkilötietojen käsittelyä niiden käsittelyn kaikissa vaiheissa. Tietosuojaa koskevat kysymykset otetaan huomioon jo henkilötietojen käsittelyä sisältäviä toimintoja suunniteltaessa ja tietojärjestelmiä kehitettäessä.

6. Tietosuojavastuut

Valtiokonttorin pääjohtajalla on kokonaisvastuu tietosuojan järjestämisestä ja sen kehittämisestä, resursoinnista sekä riittävän valvonnan varmistamisesta.

Toimialajohtajat vastaavat oman substanssitoimintansa osalta, että henkilötietojen käsittelyssä noudatetaan Valtiokonttorin tietosuojaperiaatteita ja -ohjeita. Toimialajohtajat nimeävät tarvittaessa toimialojen tietosuojan yhteyshenkilöitä.

Prosessista vastaava esimies tai asiantuntija vastaa, että heidän vastuullaan olevien prosessien henkilötietojen käsittelyssä arvioidaan käsittelyyn liittyvät riskit ja määritellään tarvittavat riskienhallintatoimenpiteet. Prosessista vastaavan esimiehen vastuulla on huolehtia, että henkilötietojen käsittely määritellään näiden periaatteiden ja Valtiokonttorin tietosuojaohjeiden mukaisesti. Erityisen tärkeää on arvioida henkilötietojen käsittelyyn kohdistuvat riskit silloin kun henkilötietoja ryhdytään käsittelemään aiemmasta poiketen, uudessa toiminnossa tai esimerkiksi hyödyntäen uutta teknologiaa. Tällöin kyseeseen voi tulla myös tietosuoja-asetuksen edellyttämä tietosuojan vaikutusten arviointi (DPIA). Toimialojen on syytä olla yhteydessä tietosuojavastaavaan arvioitaessa edustamansa toiminnon riskienhallinnallisia tarpeita ja vaatimuksia.

Esimiehet vastaavat siitä, että heidän alaisillaan on riittävä osaaminen, ohjeistus ja asianmukaiset työkalut henkilötietojen lainmukaiseen käsittelyyn. Heidän tehtävänään on valvoa tietosuojan toteutumista henkilöstön työssä ja raportoida tietosuojan vaarantumiset sekä poikkeamat periaatteista tai ohjeistuksesta Valtiokonttorin ohjeiden mukaisesti.

Henkilöstöllä on henkilötietoja käsitellessään velvollisuus toimia lainsäädännön sekä tietosuojaperiaatteiden ja -ohjeiden mukaisesti. Jokaisen vastuulla on noudattaa erityistä huolellisuutta henkilötietojen käsittelyssä sekä tarvittaessa raportoida havaitsemansa tietosuojan vaarantuminen tai poikkeamat periaatteista tai ohjeistuksesta Valtiokonttorin ohjeiden mukaisesti.

Valtiokonttorissa toimii tiedonhallintaryhmä, joka toimii myös tietosuoja-asioiden yhteistyöryhmänä.

7. Tietosuojavastaava

Valtiokonttorissa on pääjohtajan nimeämä tietosuojavastaava, jonka tehtävänä on antaa neuvoja ja ohjeita koskien tietosuojasäännösten mukaisia velvollisuuksia. Tietosuojavastaava seuraa osaltaan, että henkilötietoja käsiteltäessä noudatetaan tietosuojaan kohdistuvia säännöksiä. Tietosuojavastaava on toiminnassaan riippumaton. Tietosuojavastaavan tehtävät määritellään tarkemmin tietosuojavastaavan tehtäväkuvauksessa.

8. Palveluntuottajien vastuut

Palveluntuottajina käytetään ainoastaan sellaisia tahoja, jotka toteuttavat riittävät suojaamistoimenpiteet rekisteröidyn oikeuksien suojelemiseksi. Palvelusopimuksen liitteeksi laaditaan erillinen tietosuojaliite, kun sopimuksen perusteella käsitellään henkilötiedoiksi katsottavia tietoja. Sopimuk-

sessa tai tietosuojaliitteessä kuvataan mm. tietosuojalle asetetut vaatimukset ja määritellään palveluntuottajien tietosuojavastuuhenkilöt. Palveluntuottajien henkilöstön kanssa voidaan tehdä erilliset salassapitosopimukset, jonka lisäksi Valtiokonttori tekee tarvittaessa turvallisuusselvitykset henkilötietojen käsittelyyn osallistuvalle palveluntuottajan henkilöstölle.

9. Tietosuojaan liittyvä koulutus ja ohjeet

Tietosuojavastaava huolehtii, että Valtiokonttorissa on riittävät ja ajantasaiset tietosuojaohjeet, jotka ovat henkilöstön saatavilla sisäisessä intrassa.

Tietosuojavastaava organisoi henkilöstölle säännöllisesti tietosuojakoulutusta. Periaatteena on, että jokainen Valtiokonttoriin tuleva työntekijä suorittaa osana henkilökohtaista perehtymissuunnitelmaansa vähintään tietosuojan verkkokurssin.

Henkilöstöltä edellytetään tietosuojaosaamisen ylläpitoa määrävälein suoritettavilla kursseilla, pääsääntöisesti kurssi edellytetään suoritettavan vuosittain.

Esimiesten velvollisuutena on huolehtia, että alaiset perehdytetään tietosuoja-asioihin erityisesti substanssitoiminnan näkökulmasta sekä varmistaa, että alaiset osallistuvat tarvittaviin koulutuksiin ja perehdytykseen.

Tarvittaessa tietosuojavastaava tukee toimialoja kohdennettujen tietosuojan erityiskurssien järjestämisessä tunnistettujen koulutustarpeiden mukaisesti.

Valtiokonttori osallistuu säännöllisesti valtionhallinnon yhteisiin harjoituksiin tietosuojansa kehittämiseksi.

10. Tiedottaminen

Valtiokonttorin verkkosivuilla annetaan tietoa rekisteröityjen oikeuksista ja tietosuojan toteutumisesta Valtiokonttorin toiminnoissa. Muu tiedottaminen toteutetaan yhteistyössä Valtiokonttorin johdon, viestinnän ja tietosuojavastaavan kanssa.

Tietosuojapoikkeamiin liittyvästä ulkoisesta viestinnästä vastaa Valtiokonttorin pääjohtaja tai hänen nimeämänsä henkilö.

11. Tietosuojan seuranta ja raportointi

Tietosuojavastaava raportoi tietosuojan toteutumisesta Valtiokonttorin johtoryhmälle pääsääntöisesti kerran vuodessa. Tietosuojaan kohdistuvat merkittävät poikkeamat saatetaan kuitenkin johdon tietoon välittömästi.

Tiedonhallintaryhmä ja tietosuojavastaava seuraavat säännöllisesti tietosuojan toteutumista Valtiokonttorin toiminnoissa.

Jokainen Valtiokonttorin henkilökuntaan kuuluva on velvollinen ilmoittamaan havaitsemistaan tietosuojaan liittyvistä puutteista, uhkista tai menettelyvirheistä lähimmälle esimiehelleen, joka tarvittaessa ilmoittaa ne edelleen tietosuojavastaavalle.

Sisäinen tarkastus tarkastaa Valtiokonttorin tietosuojan toteutumista oman tarkastusohjelmansa mukaisesti.

Valtiokonttori ja sen toimialat arvioivat tietosuojan toteutumista vuosittain annettavan sisäisen valvonnan arviointi- ja vahvistuslausuman yhteydessä.

12. Tietosuojapoikkeaminen käsittely

Jokainen henkilökuntaan kuuluva on velvollinen ilmoittamaan havaitsemistaan tietosuojapoikkeamista välittömästi esimiehelleen, joka ilmoittaa ne tietosuojavastaavalle.

Valtiokonttori arvioi poikkeamasta aiheutuvan riskin ja tarvittaessa ilmoittaa viipymättä tietosuojaloukkauksista valvontaviranomaisille ja/tai rekisteröidyille erikseen laaditun ohjeistuksen mukaisesti (Valtiokonttorin ohje tietosuojaloukkausten ilmoittamisesta ja käsittelystä). Pääsääntöisesti ilmoituksen tekee Valtiokonttorin tietosuojavastaava käsiteltyään asian yhdessä viraston pääjohtajan kanssa. Toimiala, johon poikkeama on kohdistunut, tukee tietosuojavastaavaa ilmoituksen laadinnassa. Rahoitustoimiala ilmoittaa merkittävät tietosuojaan kohdistuvat poikkeamansa Tietosuojavaltuutetun toimiston lisäksi myös Finanssivalvonnalle.

Toimialojen tulee käsitellä havaitut tietosuojapoikkeamat tarvittavassa laajuudessa yhdessä tietosuojavastaavan ja muiden poikkeamaan liittyvien olennaisten henkilöiden kanssa. Käsittelyn tavoitteena on määrittää tarvittavat toimenpiteet tietosuojariskin hallitsemiseksi ja pyrkiä oppimaan tapahtumasta niin, ettei vastaavaa tapahdu muissa vastaavissa toiminnoissa.

Pääjohtaja Timo Laitinen

Tietosuojavastaava Heikki Kangas

SIGNATURES **ALLEKIRJOITUKSET** **UNDERSKRIFTER** **SIGNATURER** **UNDERSKRIFTER**

This documents contains 8 pages before this page
Tämä asiakirja sisältää 8 sivua ennen tätä sivua
Detta dokument innehåller 8 sidor före denna sida
Dokumentet inneholder 8 sider før denne siden
Dette dokument indeholder 8 sider før denne side

Heikki Tapani Kangas
93a1b8f9-ca6b-4ca9-8beb-cbe6cb750174 - 2020-10-27 13:51:26 +02:00
BankID / MobileID - 7d8c1a4f-4a59-4ab5-975c-2b309fbf1bcb - FI

TIMO SAKARI LAITINEN
9af21e4f-4a6b-45a7-8e21-22442cfeccb0 - 2020-10-27 13:53:33 +02:00
BankID / MobileID - 58c21b25-28c8-47c9-b3d5-ebc8b39eac5e - FI

authority to sign	asemavaltuutus	ställningsfullmakt	autoritet til å signere	myndighed til at underskrive
representative	nimenkirjoitusoikeus	firmateckningsrätt	representant	repræsentant
custodial	huoltaja/edunvalvoja	förvaltare	foresatte/verge	frihedsberøvende