



SUOMEN AKATEMIA

AKA/7/07.01.10/2018

5.12.2018

SUOMEN AKATEMIAN TIETOSUOJAPOLITIIKKA

Sisällys

Johdanto	3
Vastuut ja organisoituminen	3
Tietosuojaperiaatteet	4
<i>Lainmukaisuus, kohtuullisuus ja läpinäkyvyys</i>	4
<i>Käyttötarkoitussidonnaisuus ja tietojen minimointi</i>	4
<i>Täsmällisyys, rajoittaminen, eheys ja luottamuksellisuus</i>	4
<i>Riskienhallinta</i>	5
<i>Sisäänrakennettu ja oletusarvoinen tietosuojaja</i>	5
<i>Osoitusvelvollisuus</i>	5
<i>Hankinnat</i>	5
<i>Henkilötietojen siirto ja luovutus</i>	6
<i>Rekisteröidyn oikeudet ja informointi</i>	6
<i>Vaikutustenarviointi</i>	6
<i>Menettely tietosuojan vaarantuessa</i>	6
<i>Tiedottaminen</i>	6

Johdanto

EU:n yleisen tietosuoja-asetuksen (2016/679) soveltaminen alkoi kaikissa jäsenmaissa 25.5.2018. Asetus on sellaisenaan suoraan sovellettavaa oikeutta sekä viranomaisissa että yritystoiminnassa. Tietosuojalla tarkoitetaan luonnollisten henkilöiden yksityisyyden suojaamista henkilötietojen käsittelyssä. Yksityisyyden suoja on Suomen perustuslain (731/1999) takaama perusoikeus.

Rahoituksen hakijoiden, sidosryhmien edustajien sekä muiden yhteistyökumppaneiden luottamuksen säilyttäminen ja vastuullinen henkilötietojen käsittely on tärkeää Akatemialle. Akatemia sitoutuu kaikessa toiminnassaan noudattamaan EU:n yleistä tietosuoja-asetusta ja muuta tietosuojalainsäädäntöä.

Tämä tietosuojapolitiikka koskee kaikkia Akatemian palveluksessa olevia henkilöitä sekä Akatemian toimielinten luottamushenkilöitä. Lisäksi Akatemia toimii tämän tietosuojapolitiikan mukaisesti suhteessa palveluntuottajiin ja vastaaviin sidosryhmiin niiltä osin, kun ne tuottavat palveluja Akatemialle ja käsittelevät Akatemian toimintaan liittyviä henkilötietoja joko suoraan tai välillisesti.

Vastuut ja organisoituminen

Ylimmällä johdolla on kokonaisvastuu Akatemian tietosuojasta.

Akatemiassa on lähtökohtana, että jokainen työntekijä tuntee tietosuojaan liittyvät perusasiat, osallistuu koulutuksiin, noudattaa työnantajalta saatuja ohjeita sekä raportoi välittömästi esimiehelle tai tietosuojavastaavalle havaitsemistaan henkilötietojen tietoturvaloukkauksista tai niiden epäilyistä sekä puutteista tietosuojaan liittyen.

Akatemiassa on toiminut vuodesta 2007 tietoturvaryhmä, jonka tehtäviin lisättiin tietosuoja-asetukseen liittyvät tehtävät. Ryhmän nimi muutettiin tietoturva- ja tietosuojaryhmäksi ja se koostuu seuraavista: hallinnosta vastaava ylijohdaja, tietohallinnon vastuualueen johtaja, tietoturvavastaava ja tietosuojavastaava. Akatemian tavoitteena oli, että henkilötietojen käsittely Akatemiassa on toukokuussa 2018 tietosuoja-asetuksen mukaista. Tavoite saavutettiin.

Tietoturva- ja tietosuojaryhmän säännöllisiin tehtäviin tästä eteenpäin kuuluvat tietosuojadokumentointi ja päivitys, koulutustarpeen arviointi, riskiarvio, tietosuojan ja tietoturvan kehittäminen sekä seuranta, johdon raportointi ja valtionhallinnon antamien tietoturva- ja tietosuoja-asioiden valmistelu sekä täytäntöönpano Akatemiassa. Ryhmän tapaamisissa käsiteltäviin asioihin kuuluvat esimerkiksi tärkeimpien järjestelmä-hankkeiden ja muutosten tilanne, rekisteröidyiltä ja valvontaviranomaisilta tulleet yhteydenotot, tietosuojavaikutuksia sisältävien merkittävien tietoturvatapahtumien käsittely, henkilöstön koulutus sekä yleisesti havaitut puutteet ja tarpeet tietosuojaan liittyen. Säännöllisten ja määrämuotoisten tehtävien lisäksi tietosuojajärjestelmien vastuulle kuuluvat

operatiiviset tietosuojatehtävät, kuten rekisteröityjen pyyntöihin vastaaminen, vaatimusmäärittelyt tuotekehityksessä ja hankinnoissa, sopimusvaatimusten määrittelyt sekä käsittelyn seurannan tehtävät.

Johdon nimeämänä tietosuojavastaavana Akatemiassa toimii tietosuojakysymyksistä vastaava lakimies. Tietosuoja-asetuksen mukaisesti tietosuojavastaavan tehtäviin kuuluvat muun muassa asetuksen vaatimusten täytäntöönpano ja soveltaminen organisaatiossa, neuvonta ja ohjaus kaikissa tietosuojakysymyksissä, dokumentaation laatiminen, saataavuuden ja säilyttämisen valvonta, ilmoitusvelvollisuuden toteutumisen seuranta, yhteistyö valvontaviranomaisen kanssa sekä rekisteröityjen oikeuksien toteuttamisen tukeminen. Tietosuojavastaava toimii tietosuojan yhteyspisteenä organisaation sisällä ja ulkoisille tahoille. Tietosuojavastaavan osaamista kehitetään jatkuvasti ja tälle taataan resurssit osaamisensa kehittämiseen.

Tietosuojaperiaatteet

Akatemiassa noudatetaan seuraavia tietosuojaan liittyviä periaatteita henkilötietojen käsittelyssä.

Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Tietosuoja-asetuksen mukaan henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Akatemia noudattaa toiminnassaan avoimuuden periaatetta. Henkilötietoja kerätään ja käsitellään asetuksen ja muun tietosuojalainsäädännön mukaisesti. Akatemian henkilörekistereistä on laadittu asetuksenmukaiset tietosuojaselosteet. Asetuksen vaatimat tiedot, muun muassa käsittelyn oikeusperuste, kuvataan selosteissa.

Käyttötarkoitussidonnaisuus ja tietojen minimointi

Akatemia kerää henkilötietoja tiettyjä, nimenomaisia ja laillisia tarkoituksia varten, eikä käsittele niitä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Kerättävän tiedon määrä minimoidaan ja rajoitetaan siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten kyseisiä tietoja käsitellään.

Täsmällisyys, rajoittaminen, eheys ja luottamuksellisuus

Akatemia huolehtii, että käsiteltävät henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä. Akatemia toteuttaa kaikki toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä. Akatemia säilyttää henkilötietoja muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Aka-

temia käsittelee tietoja tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvottomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia. Näiden periaatteiden toteutumista valvotaan, poikkeuksiin puututaan ja niiden toteutuminen pystytään osoittamaan dokumentaation avulla. Esimiehet huolehtivat alaistensa osaamisesta sekä ohjeistuksesta työssä ja työvälineiden käytössä.

Riskienhallinta ja tietoturva

Akatemian tietosuojan osalta noudatetaan riskilähtöistä lähestymistapaa. Luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvia riskejä tarkastellaan säännöllisesti ja niiden perusteella tehdään korjaavat toimenpiteet. Riskeistä raportoidaan ylimmälle johdolle. Tietoturva toimii tietosuojan periaatteiden toteutumisen mahdollistajana. Säännöllinen todentaminen, arviointi ja kehittäminen muodostavat toiminnan perusrungon. Tarkemmin tietoturvan periaatteita kuvataan Akatemian tietoturvadokumentaatiossa.

Sisäänrakennettu ja oletusarvoinen tietosuoja

Akatemian tietosuojapolitiikan lähtökohtana on sisäänrakennettu ja oletusarvoinen tietosuoja. Tietosuojavaatimukset asetetaan jo palvelun tai järjestelmän suunnittelu- ja hankintavaiheessa. Akatemia toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ennen palvelun käyttöönottoa, jotta rekisteröityjen oikeudet ja vapaudet voidaan turvata eikä näiden yksityisyys vaarannu. Akatemia huolehtii tietosuojavaatimuksista tiedon koko elinkaaren ajan.

Osoitusvelvollisuus

Tietosuoja-asetuksen mukaan ei riitä, että organisaatio noudattaa asetusta, vaan tämä on pystyttävä myös osoittamaan. Akatemia pystyy toimenpiteiden ja käytäntöjen dokumentoinnilla sekä erilaisten tietosuoja-asiakirjojen laatimisella osoittamaan, että asetuksen mukaisten tietosuojaperiaatteiden vaatimuksia noudatetaan. Tämä tietosuojapolitiikka on osa osoitusvelvollisuuden toteuttamista. Tietosuojaorganisaation tehtävänä on valvoa, ohjata ja kehittää Akatemian käytäntöjä osoitusvelvollisuuden täyttämiseksi. Tietosuojasta myös raportoidaan säännöllisesti tietotilinpäätöksen muodossa.

Hankinnat

Akatemia varmistaa henkilötietojen käsittelyn lainmukaisuuden tilanteissa, joissa ulkoinen sopimuskumppani käsittelee Akatemian henkilötietoja hankintasopimuksen perusteella. Henkilötietoihin liittyvät riskit arvioidaan hankinnan suunnitteluvaiheessa. Tietosuojavaatimukset yksilöidään jo tarjouspyyntövaiheessa. Akatemia vastaa tietosuojasta

ulkoistaessaan henkilötietojen käsittelyä sekä siitä, että valittu kumppani sitoutuu noudattamaan tietosuojaja-asetusta ja muuta tietosuojalainsäädäntöä. Tietosuojan alaisia hankintoja katselmoidaan säännöllisesti. Akatemian ja henkilötietojen käsittelijän välillä laaditaan aina tietosuojaja-asetuksen edellyttämä kirjallinen henkilötietojen käsittelysopimus.

Henkilötietojen siirto ja luovutus

Akatemian henkilötietojen siirrot ja luovutukset tapahtuvat lainsäädännön sallimissa ja velvoittamissa rajoissa ja tästä mainitaan tietosuojaselosteessa. Akatemian osalta viranomaisen asiakirjojen ja tietojen julkisuudesta säädetään viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999). Yksityisyyden suojan lisäksi myös oikeus saada tieto julkisesta asiakirjasta on Suomen perustuslain takaama perusoikeus. Akatemialle on tärkeää, että sen toiminnassa tehdään jokaisessa yksittäistapauksessa huolellista ja perusteltua punnintaa näiden oikeuksien yhteensovittamiseksi.

Julkisia asiakirjoja luovutetaan pyydettyessä julkisuuslain 13 § ja 16 §:n edellytysten mukaisesti. Julkinenkin asiakirja saattaa sisältää salassa pidettävää tietoa tai tietoja, joiden luovuttamista on rajoitettu (yleensä henkilötietoja). Salassa pidettäviä tietoja annetaan nähtäväksi ja luovutetaan vain asianomaisen suostumuksella, asianosaiselle tai lakiin perustuvan oikeuden nojalla.

Rekisteröidyn oikeudet ja informointi

Akatemian henkilörekisterien tietosuojaselosteet ovat Akatemian verkkosivuilla. Asiakkaat saavat informaatiota tietosuojasta myös tilannekohtaisesti viestinnän yhteydessä ja tarvittaessa tietosuojavastaavalta.

Vaikutustenarviointi

Mikäli hankittavan sovelluksen katsotaan aiheuttavan merkittäviä riskejä tietosuojalle, kohdistetaan siihen vaikutustenarviointi.

Menettely tietosuojan vaarantuessa

Mikäli oman valvonnan tai ilmoituksen perusteella tietosuojaja todetaan vaarantuneeksi, tehdään riskiarvio rekisteröidyn oikeuksien näkökulmasta. Vakavista tietosuojaja- ja tietoturvaloukkauksista Akatemia ilmoittaa tietosuojaja-asetuksen mukaisesti rekisteröidylle itselleen, tietosuojaviranomaiselle ja poliisille.

Tiedottaminen

Tämä tietosuojapolitiikka on julkaistu Akatemian verkkosivuilla.

Tämä tietosuojapolitiikka tulee voimaan 5.12.2018.

Tietoturva- ja tietosuojaryhmä arvioi tietosuojapolitiikan ajanmukaisuutta ja tekee ehdotuksia sen kehittämiseksi.

Heikki Mannila
Pääjohtaja