

Karelia-ammattikorkeakoulun tietosuoja- ja tietoturvaryhmän laatima

Versio: 26.1.2018

Käsitelty 20.2.2018 Karelia-ammattikorkeakoulun yhteistyö- ja työsuojelutoimikunnassa

## Karelia-ammattikorkeakoulun tietosuojapolitiikka

EU:n tietosuoja-asetuksen (EU 2016/679)<sup>1</sup> soveltaminen alkaa 25.05.2018 ja tässä tietosuojapolitiikassa on tämä asetus otettu huomioon.

Tietosuojasta huolehtimisella varmistetaan toiminnan vastuullisuus ja asianmukaisuus niin lainsäädännön kuin eettisten toimintatapojen kannalta. Lisäksi tietosuojasta huolehtiminen on osa ammattikorkeakoulun riskien hallintaa. Tietosuojapolitiikassa määritellään peruseriaatteet, kuinka kaikissa ammattikorkeakoulun toiminnoissa pyritään varmistamaan henkilötietojen lainmukainen käsittely ja tietosuojan korkea taso. Tietosuojapolitiikkaa täydennetään käytännön työohjeistuksilla.

### Tietosuojapolitiikan kattavuus, tavoitteet ja periaatteet

Tietosuojaan kuuluvat henkilöiden yksityiselämän suoja ja yksityisyyden suoja turvaavat muut oikeudet henkilötietoja käsiteltäessä. Tietosuojalla tarkoitetaan henkilötietojen ja muiden henkilön luottamuksellisten tai arkaluonteisten tietojen suojaamista. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattu ja henkilötiedot on suojattava asiattomalta käsittelyltä. Tietojen ja tietojärjestelmien käyttöä seurataan ja väärinkäytöksiin puututaan ammattikorkeakoulun IT-sääntöjen mukaisesti.

EU:n tietosuoja-asetus sisältää sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet.

*Tietosuojaperiaatteet ovat:*

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus
- rekisterinpitäjän osoitusvelvollisuus

”Sisäänrakennetun tietosuojan periaate edellyttää, että edellä mainitut tietosuojaperiaatteet otetaan tehokkaasti osaksi henkilötietojen käsittelyä sisältäviä toimintoja niiden kaikissa vaiheissa.

Oletusarvoisen tietosuojan periaate merkitsee, että rekisterinpitäjän tulee oletusarvoisesti käsitellä vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Velvollisuus koskee kerättyjen henkilötietojen määrää, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Rekisterinpitäjän on toteutettava toimenpiteet, jotka varmistavat etenkin sen, että henkilötietoja

---

<sup>1</sup> Asetuksen sijainti www-sivuilla: [http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L\\_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL](http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL)

ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.” [2]

Ammattikorkeakoulussa kerätään ja käsitellään muun muassa opintoihin, työntekijöihin sekä tutkimus-, kehittämis- ja innovaatiotoimintaan (TKI) liittyviä henkilötietoja sisältäviä rekistereitä. Karelia Ammattikorkeakoulu Oy on näissä rekisterinpitäjänä ja henkilötietoja käsittelevät ovat henkilötietojen käsittelijöitä. Osa käsiteltävästä tiedosta on luottamuksellista, arkaluonteista sekä salassa pidettävää ja voi paljastuttuaan rikkoa yksityisyyden suojan ja heikentää luottamusta ammattikorkeakoulun toimintaa kohtaan.

Henkilötietojen oikeellisuus on varmistettava, niitä on käsiteltävä asianmukaisesti ja niiden on oltava tarpeen mukaan käytettävissä. Väärien, vanhentuneiden ja virheellisten tietojen käsittely on kielletty, ja näiden oikaiseminen on tehtävä tarpeen mukaan.

Tietoja saavat käyttää ainoastaan niitä työssään tai opinnoissaan tarvitsevat henkilöt ja työtehtävänsä tai opintojensa suorittamisen edellyttämässä laajuudessa. Tietoja saa luovuttaa ainoastaan henkilön itsensä suostumuksella tai lainsäädännön nojalla.

Tietosuojalla on kiinteä yhteys tietoturvaan. Ammattikorkeakoulun tietoturvapoliittikka määrittelee, mitä tarkoitetaan tietoturvalla ja kuinka sitä ylläpidetään.

Tietosuojapolitiikka ottaa huomioon myös ammattikorkeakoulun avoimen tieteen politiikan ja periaatteet. Tietosuojan ja tieteen avoimuuden yhteen sovittaminen otetaan huomioon erityisesti tutkimusaineistoja koskevia käytännön ohjeistuksia ja ratkaisuja laadittaessa.

### **Tietojen elinkaari ja käyttö**

Henkilötietojen käsittely perustuu henkilön suostumukseen tai laissa määriteltyyn muuhun perusteeseen. Henkilötietoja käsitellään vain perustellun käyttötarkoituksen johdosta ja vain siinä määrin ja niin kauan, kun se on käyttötarkoituksen kannalta tarpeellista. Käytettävien tietojen oikeellisuus pyritään varmistamaan ja tietoja päivitetään henkilöltä itseltään tai luotettavista lähteistä, joita ovat esim. viranomaiset. Kun tiedot eivät enää ole käyttötarkoituksensa vuoksi tarpeellisia, tiedot tulee tuhota asianmukaisesti.

Tietoja käytetään niitä kerätessä kuvattuihin tarkoituksiin lainsäädännön kulloinkin sallimissa rajoissa. Tietoja luovutetaan vain nimenomaisesti kerrotulla tai laissa mainitulla perusteella ja nimenomaisesti kerrotuille tai laissa mainituille luovutuksen saajille. Tietoja saatetaan siirtää rekisterinpitäjän sijaintivaltion ulkopuolelle tai poikkeustapauksissa EU:n ulkopuolelle. Tällöin noudatetaan siirtoa koskevia, tietosuojalainsäädännössä säädettyjä menettelyitä. EU:n ulkopuolelle henkilötietoja siirrettäessä noudatetaan erityistä huolellisuutta ja siihen liittyviä säännöksiä.

### **Rekisteröityjen informointi**

Rekisterinpitäjänä toimii Karelia Ammattikorkeakoulu Oy. Kustakin henkilörekisteristä laaditaan lainsäädännön edellyttämä rekisteri- ja tietosuojaseloste. Rekisteröidyille tarjotaan laissa tarkoitettu tai muuten tarpeellinen informaatio henkilötietojen käsittelystä tietoja kerätessä.

### **Vastuut ja organisointi**

Vastuu tietosuojan toteuttamisesta ja henkilötietojen käsittelyn lainmukaisuudesta on ammattikorkeakoulun johdolla. Jokaisen työntekijän ja henkilötietoja opinnoissaan käsittelevän opiskelijan tulee tuntea ja hallita oman vastualueensa tietosuojasääntely ja -riskit. Ammattikorkeakoululle on nimitetty **tietosuojavastaava**,

joka ohjaa ja kehittää tietosuojan toteutumista ammattikorkeakoulussa. Tietosuojavastaavan asema ja tehtävät noudattelee EU:n tietuoja-asetuksen artikloja 38 ja 39 (katso liite 1). Tietosuojavastaavan yhteystiedot ovat julkisesti saatavilla.

Tietosuojavastaavan tukena toimii ammattikorkeakoulun **tietuoja- ja tietoturvaryhmä**. Ryhmään kuuluvat tietosuojavastaava, hallinto- ja talousjohtaja, henkilöstöpäällikkö, opiskelijapalvelujen päällikkö ja työsuojeluvastuu. Ryhmän tehtävät on kuvattu liitteessä 1.

Ammattikorkeakoulun yksiköissä ja koulutusvastuissa on nimetyt **tietuojayhdyshenkilöt**, jotka toimintayksikkönsä tasolla edistävät tietosuojan toteutumista ja toimivat yhteistyössä tietosuojavastaavan ja tietuoja- ja tietoturvaryhmän kanssa.

Tietojenkäsittelyä ulkoistettaessa tulee huolehtia, että valittu kumppani noudattaa tätä tietosuojapolitiikkaa. Henkilötietojen käsittelyn ulkoistamisesta laaditaan aina kirjallinen sopimus, jossa osapuolten vastuut ja velvollisuudet määritellään.

### Tietosuojan varmistaminen

Tietosuojan varmistamiseen liittyy oleellisesti riskiperustainen lähestyminen.

”Jotta rekisterinpitäjä voi toteuttaa asetuksen sisäänrakennettua ja oletusarvoista tietuojaa ja muita asetuksessa säädettyjä velvollisuuksia, on rekisterinpitäjän tehtävä perusteellinen arvio henkilötietojen käsittelyyn liittyvistä riskeistä. Tietuoja-asetuksessa riskeillä tarkoitetaan henkilötietojen käsittelystä rekisteröidylle mahdollisesti aiheutuvia fyysisiä, aineellisia tai aineettomia vahinkoja esimerkiksi silloin, kun käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon tai pseudonymisoinnin<sup>2</sup> kumoutumiseen.

Riski voi olla korkeampi silloin, kun käsitellään esimerkiksi erityisiä henkilötietoryhmiin kuuluvia tietoja. Kun henkilötietojen käsittelyyn todennäköisesti kohdistuu korkea riski, on tietuoja-asetuksen mukaan rekisterinpitäjän tehtävä tietuojaa koskeva vaikutustenarviointi. Riskin tasoa arvioitaessa on otettava huomioon henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset edellä selostetun mukaisesti.” [2]

Vaikutustenarvioinnin yhteydessä rekisterinpitäjän on pyydettävä neuvoja tietosuojavastaavalta.

Tietuoja-asiat kuuluvat osana henkilötietoja käsittelevien uusien työntekijöiden perehdytykseen ja niistä järjestetään säännöllisesti koulutusta kaikille työntekijöille. Opiskelijoille tämä sisältyy ammatillisen kasvun opintojaksoon. Kaikkia henkilötietoja käsitteleviä henkilöitä sitoo laissa säännelty tai erikseen sovittu ja dokumentoitu vaitiolovelvollisuus.

Henkilötietoja sisältävien tietojärjestelmien käyttöä kontrolloidaan ammattikorkeakoulun käyttäjähallintaratkaisulla tai muuten dokumentoiduilla menettelyillä.

---

<sup>2</sup> Pseudonymisointi (‘salanimellä julkaiseminen’) Henkilötietojen käsittelemistä niin, että tietoja ei voida enää suoraan yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaiset lisätiedot tulee säilyttää erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei tällaista yhdistämistä tunnustettuun tai tunnistettavissa olevaan henkilöön tapahdu. Lähde: Vahti-raportti 1/2016 [https://www.vahtiohje.fi/c/document\\_library/get\\_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229](https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229)

Ammattikorkeakoulu arvioi ja valvoo tietosuojan toteutumista ja tekee tarkastuksia tietosuoja-asioissa osana normaalia tarkastustoimintaansa. Tietosuojan toteutuminen varmennetaan vuosittain raportoinnilla johdolle ja toimintakertomuksella.

### **Tietosuojan ongelmatilanteet**

Tietosuoja-asetuksessa säädetään rekisterinpitäjän velvollisuudesta ilmoittaa henkilötietojen tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle. Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Osana henkilötietojen käsittelyn suunnittelua ammattikorkeakoululla on prosessi myös mahdollisten tietoturvaloukkausten varalle, jotta tietoturvaloukkaukseen liittyvien ilmoitusvelvollisuuksien täyttäminen on mahdollista. Jokainen ammattikorkeakoulun yhteisöön kuuluva on velvollinen ilmoittamaan havaitsemistaan tietosuojaan liittyvistä puutteista, uhkista tai menettelyvirheistä osoitteeseen [tietosuoja@karelia.fi](mailto:tietosuoja@karelia.fi). Mikäli tietosuojan epäillään tai havaitaan vaarantuneen, asia tutkitaan viipymättä. Lisäksi asiasta ilmoitetaan viipymättä rekisteröidylle, jonka tietosuoja on vaarantunut, edellyttäen, että ilmoittaminen on aiheellista korjaavien toimenpiteiden suorittamiseksi tai vahingon rajaamiseksi.

### **Tiedottaminen henkilöstölle, rekisteröidylle ja sidosryhmille**

Tästä tietosuojapolitiikasta ja sen muutoksista tiedotetaan ammattikorkeakoulun henkilökunnalle ja opiskelijoille intranetissä. Tietosuojapolitiikka päivitetään tarpeen mukaan. Tämän lisäksi annetaan sisäisiä ohjeita tietosuoja-asioista.

Ammattikorkeakoulun tietosuojapolitiikka on voimassa toistaiseksi. Se on asiakirjana julkinen ja saatavissa ammattikorkeakoulun ulkoisilta ja sisäisiltä verkkosivuilta.

### **Tietosuojapolitiikan vahvistaminen**

Tietosuojapolitiikan on vahvistanut Karelian tietosuoja- ja tietoturvaryhmä kokouksessaan 13.3.2018.

### **Lähteet:**

1. Lapin yliopiston tietosuojapolitiikan luonnos 7.9.2017 (iso osa tekstistä perustuu tähän), linkki 6.1.2018 (edellyttää pääsyn ja kirjautumisen eduuniin korkeakoulujen GDPR-yhteistyön materiaaliin): [https://tt.eduuni.fi/sites/kity/EUGDPR/Dokumentteja/\\_Tiimi\\_MP\\_Muut\\_Palvelut/Ryhm%C3%A4%201%20dokumentit/Lapin%20yliopiston%20tietosuojapolitiikka%20LUONNOS.docx?Web=1](https://tt.eduuni.fi/sites/kity/EUGDPR/Dokumentteja/_Tiimi_MP_Muut_Palvelut/Ryhm%C3%A4%201%20dokumentit/Lapin%20yliopiston%20tietosuojapolitiikka%20LUONNOS.docx?Web=1)
2. Tietosuojavaltuutetun ohje ”Miten valmistautua EU:n tietosuoja-asetukseen?” oikeusministeriön ohje 4/2017, linkki 6.1.2018 tietosuojavaltuutetun www-sivuille: <http://www.tietosuoja.fi/fi/index/euntietosujauudistus.html#mitenvalmistautuatietosuoja-asetukseen>

**Linkit:** [Tietoturvapoliittika](#), [IT-säännöt](#)

**Liitteet:** Liite 1 Tietosuoja- ja tietoturvaryhmä, tietosuojavastaava

Liite 1.

**Toimenhaltijapäätös** 13.10.2017 § 30, Karelia-ammattikorkeakoulun tietosuoja- ja tietoturvaryhmän nimeäminen

Karelia-ammattikorkeakouluun muodostetaan ja nimetään toistaiseksi toimiva tietosuoja- ja tietoturvaryhmä, joka:

- valmistelee voimassa olevan EU:n tietosuoja-asetuksen soveltamista Karelia-ammattikorkeakoulussa (siirtymäaika päättyy 25.5.2018)
- käsittelee, kommentoi, antaa lausuntoja sekä hyväksyy tietosuojaan ja tietoturvaan liittyviä Karelia-ammattikorkeakoulun ohjeita ja linjauksia
- käsittelee merkittävät tietosuojaan ja tietoturvaan liittyvät poikkeamat
- kehittää ja edistää Karelia-ammattikorkeakoulun tietosuojan ja tietoturvan toteutumista.

Tietosuoja- ja tietoturvaryhmään kuuluvat:

- hallinto- ja talousjohtaja
- tietoturvavastaava
- henkilöstöpäällikkö
- opiskelijapalveluiden päällikkö
- työsuojeluvaltuutettu.

**Tietosuojavastaavan asema ja tehtävät** ovat EU:n tietosuoja-asetuksen mukaisesti seuraavat.

*38 artikla*

1.Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että tietosuojavastaava otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn.

2.Rekisterinpitäjän ja henkilötietojen käsittelijän on tuettava tietosuojavastaavaa tämän suorittaessa 39 artiklassa tarkoitettuja tehtäviä antamalla tälle resurssit, jotka ovat tarpeen näiden tehtävien täyttämiseksi, samoin kuin pääsyn henkilötietoihin ja käsittelytoimiin, sekä tämän asiantuntemuksen ylläpitämiseksi.

3.Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, ettei tietosuojavastaava ota vastaan ohjeita näiden tehtävien hoitamisen yhteydessä. Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuojavastaavaa sen vuoksi, että hän on hoitanut tehtäviään. Tietosuojavastaava raportoi suoraan rekisterinpitäjän tai henkilötietojen käsittelijän ylimmälle johdolle.

4.Rekisteröidyt voivat ottaa yhteyttä tietosuojavastaavaan kaikissa asioissa, jotka liittyvät heidän henkilötietojensa käsittelyyn ja tähän asetukseen perustuvien oikeuksiensa käyttöön.

5.Tietosuojavastaavaa sitoo hänen tehtäviensä suorittamista koskeva salassapitovelvollisuus unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti.

6.Tietosuojavastaava voi suorittaa muita tehtäviä ja velvollisuuksia. Rekisterinpitäjän tai henkilötietojen käsittelijän on varmistettava, että tällaiset tehtävät ja velvollisuudet eivät aiheuta eturistiriitoja.

### 39 artikla

#### Tietosuojavastaavan tehtävät

1. Tietosuojavastaavalla on oltava ainakin seuraavat tehtävät:

- a) antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle sekä henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat niiden tämän asetuksen ja muiden unionin tai jäsenvaltioiden tietosuojasäännösten mukaisia velvollisuuksia;
- b) seurata, että noudatetaan tätä asetusta, muita unionin tai jäsenvaltion tietosuojalainsäädännöksiä ja rekisterinpitäjän tai henkilötietojen käsittelijän toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan, mukaan lukien vastuunjako, tiedon lisääminen ja käsittelyyn osallistuvan henkilöstön koulutus ja tähän liittyvät tarkastukset;
- c) antaa pyydettyä neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja valvoa sen toteutusta 35 artiklan mukaisesti;
- d) tehdä yhteistyötä valvontaviranomaisen kanssa;
- e) toimia valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, mukaan lukien 36 artiklan mukainen ennakkokuuleminen ja tarvittaessa kuuleminen muista mahdollisista kysymyksistä.

2. Tietosuojavastaavan on tehtäviään suorittaessaan otettava asianmukaisesti huomioon käsittelytoimiin liittyvä riski ottaen samalla huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset.