

# EU:n tietosuoja-asetuksen mukanaan tuomat vaatimukset Oodi-järjestelmässä – Toimenpide-esitys

## Johdanto

Oodi-konsortio päätti syksyllä 2017 perustaa erillisen työryhmän valmistelemaan esityksen Oodi-konsortion johtoryhmälle koskien tarvittavia toimenpiteitä Oodi-järjestelmään erityisesti EU:n tietosuoja-asetuksen johdosta. Tässä esityksessä käydään läpi työryhmän käsittelemät asiat ja tehdään toimenpide-ehtotuksia koskien Oodi-järjestelmän tietosuoja-asioita. Ryhmän toimeksiantoon ei kuulu järjestelmän ulkopuolella tapahtuva työ.

Web- ja WinOodin käyttäjäryhmät poikkeavat toisistaan siten, että WinOodia käyttävät pääasiassa tukitoimintojen henkilökunta (opintohallinto) ja WebOodia niin opiskelijat, opetushenkilökunta kuin tukitoimintojen henkilökuntakin sekä jossakin määrin myös ylioppilaskunnat. Erilaiset käyttötarpeet ja käyttäjäryhmät tulee huomioida työn edetessä – esim. WinOodissa järjestelmän pääkäyttäjät käsittelevät suuria tietomassoja, ja henkilötietojen käsittely ei välttämättä kohdistu tiettyyn henkilöön vaan usean henkilön tietojen yhdistelmään. Tällaista työtä tehdään esim. tietojen laadunvarmistuksessa, ja se tulee huomioida erityisesti lokituksessa.

Työn tarkoituksena on rakentaa kustannustehokkaasti järkevä kokonaisuus, joka on tietosuoja-asetuksen vaatimusten mukainen mutta joka myös huomioi sen, että ratkaisun käyttöaika ei ole kovin pitkä. Työn pohjana käytetään Synergiaryhmän työn tuloksia, joissa otetaan kantaa tietosuoja-asetuksen vaatimukseen opiskelijarekistereille. Sen mukaisesti moni tietosuoja-asetuksen vaatimus on voimassa jo nykyainsäädännöllä. Tämän lisäksi on katsottu, että henkilön oikeus tulla unohdetuksi, oikeus siirtää tiedot järjestelmästä toiseen sekä oikeus vastustaa käsittelyä ja automaattista päätöksentekoa eivät koske lakisääteisen tehtävän suorittamiseen liittyviä rekistereitä. Oikeus vastustaa profilointia koskee myös yliopistoja, mutta tällaista profilointia Oodi-järjestelmässä ei tehdä. Muilta osin tässä esityksessä otetaan kantaa tarvittaviin toimenpiteisiin.

## Lokitusasiat

EU:n tietosuoja-asetuksessa ei määrätä suoranaisesti lokitusvaatimuksia opiskelijarekisterin osalta. Asetuksessa edellytetään kuitenkin tietoturvaloukkausten raportointia, joka edellyttää henkilötietojen käsittelemisen lokittamista. Lisäksi lokitusvaatimus on sisäänrakennettuna edellytyksenä esim. tietosuoja-asetuksen sisäänrakennetun ja oletusarvoisen tietosuojan periaatteiden sekä tietojen käsittelyn läpinäkyvyyden varmistamisessa.

**Työryhmän näkemyksen mukaan henkilötietojen käsitteleminen tulisi lokittaa laajasti niin tietojen lisäämisen, katselemisen, muuttamisen kuin poistamisenkin osalta.** Tunnistettuja yksittäisiä lokitettavia kokonaisuuksia ovat opiskelijan ja henkilökunnan perustiedot, opinto-oikeustiedot, suoritustiedot, lukukausi-ilmoittautumistiedot, HOPSiin

liittyvät tiedot, opetukseen ilmoittautumiset, lakiperusteiset poissaolot, kurssipalautetiedot, opinnot muissa oppilaitoksissa -tiedot sekä uuden opiskelijan siirtämiseen (UOTK) liittyvät tiedot. Esim. hakuikkunoiden käyttö ja muutenkin pääkäyttäjätyyppinen suurien tietomassojen käsittely täytyy käsitellä erikseen. Suorien kantahakujen tekeminen jätetään tämän työn ulkopuolelle, mutta työryhmä näkee tarpeelliseksi myös niiden lokittamisen riittävällä tasolla. Lokitietojen käsittelemisestä määrätään yliopistoilla erikseen.

**Lisäksi työryhmä suosittelee arkaluonteisten tietojen erottamista omaan ikkunaan** (entinen henkilötunnus, sukupuolen vaihtamiseen liittyvä entinen nimi -tieto sekä vapaatekstikenttiä arkaluonteisia tietoja varten), **jolloin niiden käsitteleminen pystytään lokittamaan erikseen.** Samalla voidaan välttää tilanne, jossa arkaluonteisia tietoja näytetään virkailijalle, vaikka hän tarvitsee pääsyn vain perustietoihin.

### **Vanhojen tietojen poistamisen automatisointi**

Nykylainsäädännölläkään ei ole sallittua käsitellä henkilötietoja, jotka ovat vanhentuneita ja joiden käsittelemiselle ei ole enää lain vaatimaa perustetta. Työryhmä katsoi kuitenkin tarpeelliseksi käydä asian läpi tässä yhteydessä. Mahdollisesti poistettavia tietoja tunnistettiin seuraavasti:

- Opetustapahtumien ilmoittautumiset voidaan tietyin ehdoin poistaa opinto-oikeuden päättymisen jälkeen. Ilmoittautumisten poistamisen osalta vanhoillekin tiedoille saattaa olla tarvetta, jos opiskelija ottaa yhteyttä ja viittaa osallistumiseensa opetukseen. Ilmoittautumistietoja täytyy voida säilyttää opinto-oikeuden päättymisen jälkeen yliopistolla sisäisesti säädetyin ajan. Ilmoittautumisen yhteydessä opiskelijan kirjoittamat lisätiedot tulee erityisesti huomioida tietojen poistamisen yhteydessä, koska niiden osalta tietojen säilytysaika voi olla lyhyempi. Täytyy myös arvioida, että voiko ilmoittautumistietojen teknisestä poistamisesta aiheutua ongelmia.
- HOPS:t voitaisiin poistaa X vuotta sen jälkeen, kun opiskelija on valmistunut kyseisestä opiskeluoikeudesta. Erityistä huomiota tulee kiinnittää HOPSeihin liittyviin kommenttikenttiin, joihin opiskelijat voivat kirjoittaa vapaasti mitä haluavat.
- Yhteystiedot: Postiosoitetiedot voidaan poistaa sen jälkeen, kun opiskelijalla ei enää ole opinto-oikeutta yliopistoon. Sähköpostiosoite ja puhelinnumero eivät vanhene niin nopeasti kuin postiosoite, joten niitä voidaan säilyttää pidemmän aikaa.
- Opintojaksopalautteet poistetaan nykyisten käytäntöjen mukaisesti palauteOodin rekisteriselosteen mukaisesti.
- Väliaikaiset tiedot (esim. SORA-lainsäädäntöön liittyvät) poistetaan sen jälkeen, kun tieto vanhenee.

**Työryhmä suosittelee, että luodaan yhteinen ratkaisu, jonka avulla voidaan poistaa vanhentuneet yhteystiedot Oodista.** Vanhenemisaika tulee voida säätää yliopistokohtaisesti ja erikseen postiosoitteen sekä puhelinnumeron ja matkapuhelinnumeron ja sähköpostiosoitteen osalta. **Opetustapahtumien ilmoittautumisten ja HOPSien osalta on myös syytä toteuttaa yhteinen poistoajo, jonka avulla yliopistot voivat poistaa vanhentuneet tiedot.** Opintojaksopalautteiden osalta on jo olemassa poistoajo. Väliaikaiset tiedot poistetaan manuaalisesti.

**Työryhmän näkemys on, että väliaikaisten tietojen sekä opintojaksopalautteiden poistaminen rekisteriselosteessa määritellyllä tavalla ovat pakollisia.** Muiden tietojen osalta poistamista suositellaan, jos se voidaan toteuttaa teknisesti turvallisesti ja kustannuksiltaan maltillisesti. Ennen tietojen poistamista täytyy varmistaa, että se ei ole ristiriidassa Kansallisarkiston määräyksen kanssa. Yliopistokohtaisesti täytyy myös arvioida, että ovatko tiedot esim. hallinnollisen päätöksen perusteena, jolloin tietoihin voi kohdistua erityisiä arkistointivaatimuksia

## **Muut toimenpiteet**

**Työryhmä näkemys on, että Oodin henkilörekisteriote tulee käydä läpi ja varmistetaan, että tiedot tulostuvat sille riittävän kattavasti ja luotettavasti.** Tässä vaiheessa huomioituja asioita ovat mm. kieliversioiden täydentäminen ja lukuvuosimaksuihin liittyvät tiedot sekä entinen henkilötunnus ja nimitiedot. Lisäksi tulee kiinnittää huomiota raportin luottavuuteen esim. otsikoiden ja käytettyjen lyhenteiden osalta.

**Oodi-järjestelmässä tulee kiinnittää huomiota siihen, missä kohdissa ja kenelle näkyvät sellaiset opiskelijoiden tiedot, jotka ovat salaisia** (esim. turvakiellon alaiset osoite- ja kotikuntatiedot). Tämän osalta työtä on jo aloitettu syksyllä 2017, mutta varmistetaan ja tarvittaessa täydennetään kevään 2018 aikana.

27.10.2017

Työryhmän puolesta

Jukka Kohtanen, pj

[jukka.kohtanen@uva.fi](mailto:jukka.kohtanen@uva.fi)

## **Esityksen perusteella tehdyt päätökset**

Lokitus toteutetaan esitetyllä tavalla eli laajasti. Tekninen toteutustapa määrää tarkemmin, miten ja millaiset tiedot lokitetaan. Arkaluonteiset tiedot erotetaan teknisesti erilleen ja lokitetaan erillisinä ehdotuksen mukaisesti. Tietojen poistaminen tehdään myös esityksen mukaisesti, eli määräaikaiset tiedot sekä rekisteriselosteessa poistettavaksi määrätyt tiedot poistetaan. Muiden tietojen osalta jätetään päätettäväksi asiantuntijoille. Henkilörekisteriote korjataan ja tarvittaessa täydennetään.