Tampereen ammattikorkeakoulu

Tietosuojan vaikutustenarviointi (DPIA) oppimisalusta TUNI Moodlesta

Anna Mursunen

OPINNÄYTETYÖ
Huhtikuu 2025

Liiketalouden tutkinto-ohjelma
Juridiikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalouden tutkinto-ohjelma
Juridiikka

MURSUNEN ANNA:
Tietosuojan vaikutustenarviointi (DPIA) oppimisalusta TUNI Moodlesta

Opinnäytetyö 59 sivua
Huhtikuu 2025

Opinnäytetyön tarkoituksena oli tuottaa Tampereen ammattikorkeakoululle (TAMK) tietosuojan vaikutustenarviointi oppimisalusta TUNI Moodlesta. Työn tavoitteena oli tunnistaa Moodlen henkilötietojen käsittelyyn liittyvät riskit ja löytää keinoja niiden hallitsemiseksi sekä selvittää ovatko tunnistetut riskit hyväksyttävällä tasolla. Lisäksi tavoitteena oli tutustua lyhyesti vaikutustenarvioinnin oikeustieteelliseen viitekehykseen, tarkastella mukaileeko TUNI Moodlen henkilötietojen suoja tietosuoja-asetuksen vaatimuksia ja kuinka TUNI Moodlen tietosuojaa voidaan edelleen kehittää ja parantaa. Opinnäytetyössä käytettiin toiminnallisia ja lainopillisia menetelmiä.

Tietosuojan vaikutuksenarvioinnissa tunnistettiin useita TUNI Moodlen henkilötietojen käsittelyyn liittyviä riskejä ja niiden hallitsemiseksi esitettiin erilaisia suojatoimenpiteitä. Avoimen kentän ongelma oli yksi keskeisimmistä tunnistetuista riskeistä. Opiskelijat saattavat itse jakaa oppimisalustalle erityisiä tietoryhmiä koskevia tietoja ja tästä voi aiheutua esimerkiksi mainehaittaa ja ihmissuhdeongelmia henkilökohtaisessa sekä ammatillisessa elämässä sekä altistaa kiusaamiselle. Riskin hallitsemiseksi vaikutustenarvioinnissa esitettiin muun muassa henkilökunnan koulutusta ja TUNI Moodlen toiminnallisuuksien kehittämistä.

Vaikutustenarvioinnin perusteella TUNI Moodlen jäännösriski jäi hyväksyttävälle tasolle. Lisäksi toimeksiantajalle annettiin kehittämisehdotuksia ja jatkotoimenpiteitä TUNI Moodlen tietosuojan parantamiseksi. Toimenpiteisiin kuului esimerkiksi koulutusta ja ohjeistusta, tietosuojaselosteen päivittämistä sekä kansainvälisen tietosuojakehyksen seurantaa.

Opinnäytetyön oheismateriaalina tuotettiin toimeksiantajalle vaikutustenarviointi, joka tehtiin Tietosuojavaltuutetun toimiston laatimaan Excel-työkaluun. Vaikutustenarviointi toimii dokumenttina, jolla voidaan parantaa ja hallita TUNI Moodlen tietosuojaa. Arviointi tulee päivittää lainsäädännön ja toimintaympäristön muuttuessa. Vaikutustenarviointi on TAMKin sisäiseen käyttöön tarkoitettu ja se on poistettu julkisesta raportista. Raportissa kuvattiin kuitenkin vaikutustenarvioinnin sisältö keskeisiltä osin ja tiivistetysti.

Asiasanat: vaikutustenarviointi, DPIA, EU:n yleinen tietosuoja-asetus, GDPR, Moodle

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Administration
Jurisprudence

ANNA MURSUNEN:
Data Protection Impact Assessment (DPIA) of the TUNI Moodle Learning Environment

Bachelor's thesis 59 pages
April 2025

The purpose of this thesis was to produce a Data Protection Impact Assessment (DPIA) of the TUNI Moodle learning environment for Tampere University of Applied Sciences (TAMK). The aim was to identify risks related to the processing of personal data on Moodle, find ways to manage these risks and determine whether the identified risks are at an acceptable level.

Functional and legal methods were applied in this thesis. As supplementary material, a DPIA was produced for the client using the Excel tool created by the Office of the Data Protection Ombudsman. The DPIA is intended for internal use within TAMK and has been removed from the public report. However, the report describes the content of the DPIA concisely and highlights the key aspects.

The Data Protection Impact Assessment identified several risks related to the personal data on TUNI Moodle, and various protective measures were suggested to reduce these risks. One of the main risks was the open field issue, which could be managed through staff training and improving TUNI Moodle functionalities.

Based on the DPIA, the residual risk of TUNI Moodle remained at an acceptable level. Furthermore, development suggestions and follow-up measures were provided to the client to enhance the data protection of TUNI Moodle.

Key words: data protection impact assessment, DPIA, general data protection regulation, GDPR, Moodle

SISÄLLYS

LYHENTEET JA TERMIT

anonymisointi	Henkilötiedon tunnistettavuuden poistaminen niin, että sitä ei voida enää yhdistää rekisteröityyn; peruuttamaton toimenpide. (Tietosuojavaltuutetun toimisto n.d.a.)
biometrinen tieto	Teknisellä käsittelyllä saadut luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvät tiedot, joilla henkilö voidaan tunnistaa ja tunnistaminen voidaan varmistaa, esimerkiksi kasvokuvat tai sormenjälkitiedot. ((EU) 2016/679, 4 artikla.)
DPIA	Data Protection Impact Assessment eli vaikutustenarviointi; prosessi, joka auttaa tunnistamaan, arvioimaan ja hallitsemaan henkilötietojen käsittelyyn sisältyviä riskejä; tulee tehdä, jos käsittely aiheuttaa henkilön oikeuksille ja vapauksille korkean riskin. ((EU) 2016/679, 35 artikla.)
erityiset henkilötietoryhmät	Sellaiset henkilötiedot, joista ilmenee rotu tai etninen alkuperä, uskonnollinen vakaumus, poliittisia mielipiteitä, ammattiliiton jäsenyys, geneettisiä ja biometrisia tietoja henkilön tunnistamista varten, terveyttä koskevia tietoja tai seksuaalinen suuntautuminen; käsittely lähtökohtaisesti kiellettyä. ((EU) 2016/679, 9 artikla.)
GDPR	General Data Protection Regulation; EU:n yleinen tietosuoja-asetus ((EU) 2016/679.)
geneettinen tieto	Henkilötieto, joka koskee luonnollisen henkilön perimää tai elämän aikana tapahtuneita geneettisiä muutoksia, joista selviää yksilöllistä tietoa henkilön fysiologiasta tai

	terveydestä; saadaan biologisesta näytteestä analysoimalla. ((EU) 2016/679, 4 artikla.)
henkilötieto	Kaikki tiedot, josta luonnollinen henkilö (rekisteröity) voidaan suoraan tai välillisesti tunnistaa; esimerkiksi nimi, henkilötunnus, sijaintitieto tai henkilölle tunnusomainen fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä. ((EU) 2016/679, 4 artikla.)
henkilötietojen käsittelijä	Luonnollinen henkilö, oikeushenkilö, viranomainen tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. ((EU) 2016/679, 4 artikla.)
käsittely	Toiminnat, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti; tietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen, hakeminen, käyttäminen, luovuttaminen siirtämällä, levittäminen tai muutoin saataville asettaminen, yhdistäminen, rajoittaminen tai poistaminen. ((EU) 2016/679, 4 artikla.)
Moodle	Modular Object-Oriented Dynamic Learning Environment; verkko-oppimisympäristö. (Moodle n.d.a)
pseudonymisointi	Henkilötietojen käsittely siten, ettei niitä voida enää yhdistää tiettyyn rekisteröityyn ilman lisätietoja; edellyttää, että lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joiden avulla henkilötietojen yhdistämistä luonnolliseen henkilöön ei voi tapahtua. ((EU) 2016/679, 4 artikla.)

rekisteri	Henkilötietoja sisältävä jäsennelty tietojoukko, josta tietoa voidaan hakea ja käyttää tietyin perustein; keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. ((EU) 2016/679, 4 artikla.)
rekisterinpitäjä	Luonnollinen henkilö, oikeushenkilö, yritys, viranomainen tai muu elin, joka määrittelee, millä tavalla ja mihin tarkoitukseen henkilötietoja käsitellään. ((EU) 2016/679, 4 artikla.)
rekisteröity	Luonnollinen henkilö, jota henkilötieto koskee. (Tietosuojavaltuutetun toimisto n.d.b.)
terveystieto	Henkilötieto, joka liittyy luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen. ((EU) 2016/679, 4 artikla.)
tietosuoja	Henkilön yksityisyyden sekä yksilöä koskevien tietojen suojelemista oikeudettomalta käytöltä henkilötietoja käsiteltäessä; henkilötietojen käsittelyä koskevien vaatimusten noudattamista henkilön yksityisyyden suojaamiseksi. (Tieteen termipankki 2025.)
tietoturva	Tietosuojan toteuttamisen keino; tarkoituksena suojata tietoaineisto ja tietojärjestelmät; organisatoriset ja tekniset toimenpiteet tiedon luottamuksellisuuden, eheyden, järjestelmien käytettävyyden ja rekisteröidyn oikeuksien toteutumisen toteuttamiseksi. (Tietosuojavaltuutetun toimisto n.d.b.)
TAMK	Tampereen ammattikorkeakoulu
TUNI	Tampereen korkeakouluyhteisö; Tampere Universities
TUNI Moodle	Tampereen korkeakouluyhteisön käyttämä Moodle; katso myös ”Moodle”.

1 JOHDANTO

Tietosuoja koskee meitä jokaista, mutta silti hyvin harva on siitä erityisen huolissaan tai edes kiinnostunut. Monille tietosuoja näyttäytyy lähinnä pompahtavina evästebannereina ja sivuston alalaidassa vilahtelevina tietosuojaselosteina. Arkikäytössä ja työpaikoilla tietosuoja saattaa tuntua etäiseltä, turhauttavalta ja byrokraattiselta asialta. Todellinen kiinnostus tietosuojaan heräkin usein vasta silloin, kun jotain vakavaa tapahtuu. Psykoterapiakeskus Vastaamon tietomurto vuonna 2020 on varoittava esimerkki siitä, kuinka tietosuojan laiminlyönti voi aiheuttaa merkittäviä vaikutuksia sekä yksilölle että organisaatiolle. Tietomurrossa julkaistiin yli 30 000 ihmisen potilaskertomukset ja osa potilaista on päätynyt itsemurhaan tietojensa vuotamisen takia (Nykänen 2024.) Tietomurron seurauksena Vastaamo asetettiin konkurssiin ja sen entinen toimitusjohtaja tuomittiin Helsingin käräjäoikeudessa tietosuojarikoksesta ehdolliseen vankeusrangaistukseen. (Yle Uutiset 2021, Salumäki 2023.)

Henkilötietojen suoja on nykyaikaisessa yhteiskunnassa keskeinen osa oikeusjärjestelmää ja sen merkitys on kasvanut digitalisaation myötä. Tietoa on tarjolla valtavasti ja oli sitten kyse pienestä tai suuresta yrityksestä tai julkisen puolen organisaatiosta, toimintaan liittyy todennäköisesti henkilötietojen käsittelyä. Tietosuoja on jokaisen henkilön perusoikeus ja siksi henkilötietojen suojaaminen ja asianmukainen käsittely on välttämätöntä yksilön oikeuksien turvaamiseksi sekä luottamuksen säilyttämiseksi. Yksityishenkilöllä ei kuitenkaan ole kansalaisvelvollisuutta perehtyä tietosuojaan, vaan sen toteuttaminen on aina organisaation vastuulla. Tietosuojan tarkoituksena ei ole piilottaa tietoja tai kieltää niiden käyttöä, vaan olennaista on tietosuojan oikeasuhtainen mitoittaminen sekä sen suunnitelmallinen ja hallittu toteuttaminen. (Andreasson & Ylipartanen 2022, luku 1; Korpisaari, Pitkänen & Warma-Lehtinen 2022, XXI.)

Henkilötietojen käsittelyä säätelee Euroopan unionin yleinen tietosuoja-asetus (Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta, EU 2016/679; jäljempänä EU:n yleinen tietosuoja-asetus). Asetus lähestyy tietosuo-

jaa riskiperusteisesti ja sen tarkoituksena on välttää vähäriskisen toiminnan ylisääntelyä ja toisaalta varmistaa yksilön suoja korkean riskin toiminnassa. Kun henkilötietojen käsittely sisältää korkean riskin rekisteröidyn oikeuksille ja vapauksille, tietosuoja-asetus edellyttää organisaatiolta teknisiä ja hallinnollisia toimenpiteitä riittävän tietosuojan takaamiseksi. (Andreasson & Ylipartanen 2022, luku 1.) Yksi näistä toimenpiteistä on tietosuojan vaikutustenarviointi (*Data Protection Impact Assessment*, DPIA), josta säädetään tietosuoja-asetuksen 35 artiklassa.

Tietosuojaosaamisen tarve on EU:n yleisen tietosuoja-asetuksen myötä lisääntynyt, mutta koulutustarjonta on edelleen hajanaista. Kiinnostus tietosuojaan oikeudenalana on kuitenkin korkeakouluopiskelijoiden keskuudessa kasvanut ja osaajia tarvitaan niin julkishallinnossa kuin yksityissektorillakin. (Andreasson & Ylipartanen 2022, Esipuhe.) Tampereen ammattikorkeakoulun lakiasiainpäällikkö ja tietosuojavastaava Niku Hinkan (2025) mukaan yksi tapa tietosuojaosaamisen osoittamiseen on tietosuojan vaikutustenarviointien tekeminen. Tämän opinnäytetyön tarkoituksena onkin tuottaa TAMKille tietosuojan vaikutustenarviointi oppimisalusta TUNI Moodlesta. Opinnäytetyön toimeksiantajana on Tampereen ammattikoulu, joka on sitoutunut noudattamaan voimassa olevaa tietosuojalainsäädäntöä henkilötietojen käsittelyssä. EU:n yleinen tietosuoja-asetus edellyttää tietosuojan vaikutustenarvioinnin laatimista myös TAMKissa laajasti opetuksessa käytettävästä verkko-oppimisympäristö Moodlen kaltaisista ohjelmistoista, jos niiden henkilötietojen käsittelyyn liittyy korkea riski.

Opinnäytetyön tavoitteena on tunnistaa TUNI Moodlen henkilötietojen käsittelyyn liittyvät riskit ja löytää keinoja niiden hallitsemiseksi. Tavoitteena on myös tutustua tietosuojan vaikutustenarvioinnin oikeustieteelliseen viitekehykseen. Työssä pyritään selvittämään, mitä uhkia TUNI Moodlen tietosuojaan liittyy ja ovatko tunnistetut riskit hyväksyttävällä tasolla. Lisäksi tarkastellaan, miten TUNI Moodlen henkilötietojen käsittely mukautuu yleisen tietosuoja-asetuksen vaatimuksiin ja miten TUNI Moodlen tietosuojaa voidaan edelleen kehittää ja parantaa. Opinnäytetyön oheismateriaalina tuotetaan toimeksiantajalle vaikutustenarviointi, joka on tehty Tietosuojavaltuutetun toimiston laatimaan Excel-työkaluun. Vaikutustenarviointi on TAMKin sisäiseen käyttöön tarkoitettu, eikä siten ole julkinen.

Tämä opinnäytetyö on työelämälähtöinen, toiminnallinen ja lainopillinen. Tieteen termipankin (2016) mukaan lainopilla tarkoitetaan voimassa olevien oikeusnormien tulkintaa ja systematisointia. Työssä hyödynnetään muun muassa kansainvälisiä ja kansallisia säädöksiä, oikeuskirjallisuutta, lain esitöitä, tieteellisiä artikkeleita sekä Tietosuojavaltuutetun toimiston linjauksia ja ohjeistuksia. Oikeuskäytäntöä vaikutustenarviointeihin liittyen on raporttia kirjoittaessa niukasti ja sitä sivutaan vain lyhyesti. Toiminnallisen osuuden perustana ovat Moodlen tietosuojaselosteet sekä TAMKin tietosuojavastaava Niku Hinkan asiantuntijahaastattelut. Opinnäytetyön rajatun laajuuden vuoksi kansalliset erityislait, kuten tietosuojalaki, ammattikorkeakoululaki (932/2014) ja laki yksityisyyden suojasta työelämässä (759/2004) rajataan raportin ulkopuolelle. Opinnäytetyössä on käytetty paikoin tekoälyä kieliasun muokkaamisen apuna, esimerkiksi synonyymien etsimiseen usein toistuvien sanojen korvaamiseksi sekä vaihtoehtoisten muotoiluehdotusten saamiseksi.

2 EUROOPAN UNIONIN YLEINEN TIETOSUOJA-ASETUS GDPR

2.1 Tausta ja tavoitteet

Euroopan unionin yleinen tietosuoja-asetus astui voimaan toukokuussa 2016 ja sitä alettiin soveltaa kansallisesti kaksi vuotta myöhemmin toukokuussa 2018. Asetuksesta puhutaan myös usein lyhenteellä GDPR, joka tulee sen englanninkielisestä nimestä *General Data Protection Regulation*. EU:n asetukset ovat suoraan sovellettavaa oikeutta, ja ne ovat ensisijaisia suhteessa kansallisiin säädöksiin. Ne pätevät yleisesti, velvoittavat kaikilta osiltaan ja niitä sovelletaan sellaisinaan kaikissa jäsenvaltioissa, ellei kansallisesti ole säädetty asetuksen sallimista poikkeamista. (Andreasson & Ylipartanen 2022, luku 2; Korpisaari ym. 2022, 41.)

EU:n yleinen tietosuoja-asetus tuli voimaan aiemman henkilötietodirektiivin (Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (95/46/EY)) tilalle. Uuden asetuksen tavoitteena on yhtenäistää jäsenmaiden tietosuojaa koskevaa sääntelyä, nykyaikaistaa ja päivittää henkilödirektiivin periaatteita sekä vahvistaa rekisteröityjen itsemääräämisoikeutta. Asetuksella pyritään myös lujittamaan sisämarkkinaulottuvuutta, huomioimaan tietosuojan kansainvälinen ulottuvuus ja tehostamaan tietosuojasääntöjen täytäntöönpanon valvontaa. Vaikka asetuksen tavoitteena on yhdenmukaistaa tietosuojalainsäädännön soveltamista koko EU:ssa, se jättää jäsenvaltioiden lainsäätäjille myös kansallista liikkumavaraa. (Andreasson & Ylipartanen 2022, luku 2.1.)

Tietosuoja-asetuksen tavoitteena ei ole vain suojata henkilötietoja, vaan myös tukea Euroopan unionin vapautta, turvallisuutta ja oikeusjärjestelmää. Se lähentää sisämarkkinoita ja edistää taloudellista ja sosiaalista kehitystä sekä luonnollisten henkilöiden hyvinvointia. Erityisen huomioitavaa on, että asetuksen pyrkimys on tasapainottaa kahta näkökulmaa: yksilön oikeutta omiin tietoihinsa sekä yritysten ja muiden toimijoiden edellytyksiä käyttää näitä tietoja liiketoiminnassaan. Tietosuoja-asetuksen tarkoituksena ei siis ole haitata henkilötietoihin perustuvaa liiketoimintaa, vaan tukea sitä selkeällä lainsäädännöllä ja määritellä,

miten henkilötietoja saa hyödyntää. Tietosuoja-asetuksessa edistetään sisämarkkinoiden kehitystä toteamalla, että henkilötietojen vapaata liikkuvuutta EU:n sisällä ei saa rajoittaa eikä kieltää henkilötietojen käsittelyyn liittyvistä syistä. (Korpisaari ym. 2022, 41.)

Tietosuoja-asetuksen tavoitteena on myös edistää Euroopan digitaalitalouden kasvua ja edistää yksityisyydensuojaa verkkoympäristössä sekä lisätä kuluttajien luottamusta verkkoympäristöä kohtaan. Tietosuojalainsäädännön uudistamisen on nähty myös tukevan talouskasvua, innovaatioita ja työllisyyttä. Yhtenäisen lainsäädännön tavoitteena on vähentää hallintokustannuksia, mutta tietosuojauudistus on kuitenkin käytännössä aiheuttanut viranomaisille ja yrityksille lisäkustannuksia erityisesti siirtymävaiheessa. Henkilötietojen käsittelytoimien tuominen lainsäädännön vaatimalle tasolle on kuitenkin investointi, jolla voi olla positiivista vaikutusta esimerkiksi liikevaihtoon, asiakastyytyväisyyteen ja asiakkaiden tavoitettavuuteen. (Korpisaari ym. 2022, 42.)

2.2 Soveltamisalue ja keskeinen sisältö

2.2.1 Soveltamisala ja määritelmät

EU:n yleisen tietosuoja-asetuksen soveltamisala jaetaan aineelliseen ja alueelliseen. Tietosuoja-asetuksen 2 artikla käsittelee aineellista soveltamisalaa ja sen 1 kohdan mukaan asetusta sovelletaan henkilötietojen käsittelyyn, joka on kokonaan tai osittain automaattista sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa. Nykyään suurin osa henkilötietojen käsittelystä tapahtuu automaattisesti tietotekniikan avulla, mutta myös manuaalisen käsittelyn yhteydessä tulee soveltaa tietosuoja-asetusta. (Korpisaari ym. 2022, 46.)

Laajaa alueellista soveltamisalaa käsitellään tietosuoja-asetuksen 3 artiklassa. Sen mukaan asetusta sovelletaan henkilötietojen käsittelyyn, jos käsittelijä tai rekisterinpitäjä on unionin alueella tai sijoittautunut paikkaan, jossa sovelletaan jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla. Asetusta sovelletaan myös, jos käsittely liittyy tavaroiden tai palvelujen tarjoamiseen unionin alueella

oleville rekisteröidyille tai on kyse unionissa olevien ihmisten käyttäytymisen seurannasta. Tämä tarkoittaa sitä, että tietosuoja-asetusta sovelletaan myös EU:n ulkopuolella sijaitsevaan verkkokauppaan, jos se myy tavaroita esimerkiksi Suomeen ja samalla käsittelee asiakkaiden henkilötietoja. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 19; Korpisaari ym. 2022, 52–53.)

Tietosuoja-asetuksen 4 artiklassa määritellään 24 asetuksessa käytettyä keskeistä käsitettä, eikä niistä ole mahdollista säätää kansallisesti toisin. Esimerkiksi 4 artiklan ensimmäisessä kohdassa määritellään laaja henkilötiedon käsite. Kohdan mukaan kyse on henkilötiedosta, silloin kun henkilö on sekä suoraan että epäsuorasti tunnistettavissa erityisten tunnistetietojen perusteella. Näitä tunnistetietoja ovat muun muassa nimen, henkilötunnuksen ja sijaintitiedon lisäksi kulttuuriset ja geneettiset tiedot. (Korpisaari ym. 2022, 57.)

2.2.2 Henkilötietojen käsittelyä koskevat periaatteet

Tietosuoja-asetuksen II luvun 5 artiklan 1 kohdassa säädetään henkilötietojen käsittelyä koskevista periaatteista, jotka ovat:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus.

5 artiklan ensimmäisen kohdan periaate lainmukaisuudesta, kohtuullisuudesta ja läpinäkyvyydestä edellyttää muun muassa, että henkilötietojen käsittely on rekisteröidyn kannalta läpinäkyvää ja rekisteröityä informoidaan itseään koskevasta henkilötietojen käsittelystä. Periaatteen mukaan tietojen on oltava ymmärrettäviä ja helposti saatavilla. Käyttötarkoitussidonnaisuuden periaate taas jakautuu kahteen näkökulmaan: henkilötiedot tulee kerätä laillista ja nimenomaista tarkoitusta varten, eikä henkilötietoja saa käyttää myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. (HE 9/2018, 28; Korpisaari ym. 2022, 103.)

Tietojen minimointia koskeva periaate edellyttää, että kerättävät henkilötiedot ovat asianmukaisia, tarpeellisia ja olennaisia niiden käyttötarkoituksen kannalta. Tämä tarkoittaa sitä, että tietoja tulee kerätä mahdollisimman vähän eikä niitä saa kerätä vastaisuuden varalle. Tiedot on myös poistettava rekisteristä sen jälkeen, kun niistä on tullut tarpeettomia. Täsmällisyyden periaatteen mukaan rekisterinpitäjän tulee huolehtia tietojen täsmällisyydestä ja ajantasaisuudesta sekä poistettava tai oikaistava virheelliset henkilötiedot. (HE 9/2018, 28; Korpisaari ym. 2022, 104, 107.)

Säilytyksen rajoittamista koskeva periaate tarkoittaa, että henkilötietoja saa säilyttää vain niin kauan kuin on välttämätöntä niiden käyttötarkoituksen kannalta. Joissakin tilanteissa rekisterinpitäjällä on kuitenkin lakiin perustuva velvollisuus säilyttää tietoja pitkiäkin aikoja. Esimerkiksi työnantajalla on velvollisuus antaa työntekijälle työtodistus, mikä edellyttää työntekijän henkilötietojen säilyttämistä myös työsuhteen päättymisen jälkeen. Eheyden ja luottamuksellisuuden periaatteella on läheinen yhteys tietosuoja-asetuksen riskiperusteiseen lähestymistapaan. Periaate korostaa, että henkilötietoja tulee käsitellä turvallisesti ja ne on suojattava lainvastaiselta käsittelyltä. (HE 9/2018, 28; Korpisaari ym. 2022, 107–108.)

Tietosuoja-asetuksen 5 artiklan 2 kohdassa rekisterinpitäjälle asetetaan osoitusvelvollisuus, jonka mukaan sen on pystyttävä osoittamaan, että henkilötietojen käsittely tapahtuu 5 artiklan 1 kohdan mukaisesti tietosuojaperiaatteita toteuttaen. Myös osoitusvelvollisuus liittyy tietosuoja-asetuksen riskipohjaiseen lähestymistapaan, jonka keskeinen ajatus on, että henkilötietojen käsittelijä voi mukauttaa henkilötietoja suojaavat toimenpiteet käsittelyyn sisältyvän riskin mukaiseksi. Osoitusvelvollisuus ei luo uusia sisällöllisiä velvoitteita, vaan lisää tietosuojaperiaatteiden vaikuttavuutta. Rekisterinpitäjällä on vapaus valita asetuksen sääntelyn puitteissa sopivat keinot osoitusvelvollisuuden toteuttamiseksi. Käytännössä osoitusvelvollisuutta toteutetaan dokumentoimalla tehtyjä toimenpiteitä, laatimalla vaikutustenarviointi sekä ylläpitämällä asetuksen mukaisia käsittelytoimia koskevia selosteita. (HE 9/2018, 28–29; Korpisaari ym. 2022, 110.)

2.2.3 Henkilötietojen käsittelyn lainmukaisuus

EU:n yleisen tietosuoja-asetuksen 6 artiklassa esitetään henkilötietojen lainmukaisen käsittelyn edellytykset. Sen mukaan henkilötietojen käsittely vaatii oikeudellisen perustan ja käsittelyn lainmukaisuus toteutuu, jos se perustuu rekisteröidyn suostumukseen tai muuhun laissa säädettyyn perusteeseen. 6 artiklan 2 ja 3 kohdat antavat jäsenvaltioille mahdollisuuden säätää tarkemmin kahdesta henkilötietojen käsittelyn perusteesta: lakiperusteisesta velvoitteesta sekä julkisen vallan käytöstä ja yleisestä edusta. Muuten artiklassa ei ole kansallista liikkumavaraa. (Korpisaari ym. 2022, 113–115.)

Tietosuoja-asetuksen 7 artiklassa säädetään tarkemmin suostumuksen edellytyksistä ja sen johdannossa mainitaan erikseen, ettei suostumusta voi antaa vaikenemalla tai jättämällä jokin toimi toteuttamalla tai esimerkiksi valmiiksi rastitetuilla ruuduilla. Asetuksen 8 artiklassa taas säädetään lapsen suostumuksesta ja sitä sovelletaan vain sähköisiin palveluihin, joita tarjotaan suoraan lapselle. (Korpisaari ym. 2022, 146, 158–159.)

Joidenkin henkilötietojen käsittely voi olla erityisen riskialtista ihmisen yksityisyyden kannalta. Tietosuoja-asetuksessa tällaisista tiedoista käytetään nimitystä erityiset henkilötietoryhmät. Aiemmin niitä kutsuttiin arkaluonteisiksi tiedoiksi. Erityisiä henkilötietoryhmiä koskevaa käsittelyä säädetään tietosuoja-asetuksen 9 artiklassa. Sen mukaan erityisiä henkilötietoja ovat tiedot, joista ilmenee esimerkiksi rotu tai etninen alkuperä, uskonnollinen vakaumus tai seksuaalista suuntautumista koskeva tieto. Asetuksen mukaan erityisiä henkilötietoryhmiä koskeva käsittely on lähtökohtaisesti kiellettyä, mutta 9 artiklan 2 kohdassa luetteloidaan tähän joitakin poikkeuksia. Rikostiedot eivät kuulu erityisiin henkilötietoryhmiin, vaan niistä säädetään erikseen asetuksen 10 artiklassa (Korpisaari ym. 2022, 167–168, 188).

2.2.4 Rekisteröidyn oikeudet ja rekisterinpitäjän velvollisuudet

Rekisteröidyn oikeuksien vahvistaminen on yksi EU:n yleisen tietosuoja-asetuksen tavoitteista ja niistä säädetään asetuksen III luvussa artikloissa 12–22. Asetuksen mukaan rekisteröidyllä on oikeus saada läpinäkyvää informaatiota henkilötietojensa käsittelystä ymmärrettävässä muodossa. Rekisteröidyllä on myös oikeus saada rekisterinpitäjältä vahvistus siitä, käsitelläänkö hänen henkilötietojaan. Jos käsittelyä tapahtuu, on rekisteröidyllä oikeus tutustua näihin tietoihin. Rekisteröidyn oikeuksiin kuuluu myös virheellisten tietojen oikaiseminen ja tietyin edellytyksin tietojen poistaminen. Lisäksi rekisteröidyllä on oikeus rajoittaa tietojen käsittelyä ja luottaa siihen, että rekisterinpitäjä ilmoittaa oikaisusta, poistamisesta ja rajoituksista kaikille, joille henkilötietoja on luovutettu. Oikeuksiin kuuluu myös omien henkilötietojen siirtäminen järjestelmästä toiseen, sekä eräissä tilanteissa henkilötietojen käsittelyn vastustaminen. (HE 9/2018, 30; Andreasson & Ylipartanen 2022, luku 2.2.)

Lisäksi tietosuoja-asetuksen 34 artiklassa säädetään rekisteröidyn oikeudesta tulla informoiduksi tietoturvaloukkauksista, silloin kun loukkauksesta aiheutuu luonnollisten henkilöiden oikeuksiin tai vapauksiin kohdistuva korkea riski (Korpisaari ym. 2022, 393). Rekisteröidyllä on myös oikeus saada valvontaviranomaiselta apua ja saattaa asiansa valvontaviranomaisen käsiteltäväksi, jos hänen henkilötietojensa käsittelyssä on toimittu tietosuoja-asetuksen vastaisesti. Rekisteröidyllä on oikeus valittaa valvontaviranomaisen tekemästä päätöksestä hallinto-oikeuteen. Rekisteröity on myös oikeutettu saamaan korvausta tietosuoja-asetuksen rikkomisesta aiheutuneesta vahingosta. (HE 9/2018, 30; Andreasson & Ylipartanen 2022, luku 2.2.)

Rekisterinpitäjän ja henkilötietojen käsittelijän yleisiä velvollisuuksia ja tehtäviä käsitellään tietosuoja-asetuksen IV luvussa. Heidän molempien vastuullaan on huolehtia, että henkilötietojen käsittelyssä noudatetaan asianmukaista turvallisuustasoa. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee myös ylläpitää selostetta vastuullaan olevista käsittelytoimista. Selosteen tarkoitus on auttaa henkilötietojen käsittelytoimien kokonaisvaltaista hahmottamista organisaation sisäisesti ja edesauttaa myös 5 artiklassa mainitun osoitusvelvollisuuden toteuttamista. (Andreasson & Ylipartanen 2022, luku 2.2; Korpisaari ym. 2022, 364.)

Rekisterinpitäjällä on velvollisuus ilmoittaa tietoturvaloukkauksista toimivaltaiselle kansalliselle valvontaviranomaiselle ja tietyissä tapauksissa myös rekisteröidylle itselleen. Henkilötietojen käsittelijällä taas on velvollisuus ilmoittaa tietosuojaloukkauksista rekisterinpitäjälle. Tietosuoja-asetuksessa säädetään myös yksityiskohtaisesti rekisterinpitäjän ja henkilötietojen käsittelijän välisestä sopimuksesta. Lisäksi rekisterinpitäjällä on velvollisuus antaa rekisteröidylle maksutta tiettyjä tietoja hänen henkilötietojensa käsittelystä. Tietosuoja-asetus velvoittaa rekisterinpitäjää tekemään myös korkean riskin tilanteissa tietosuojaa koskevan vaikutustenarvioinnin ja sitä mahdollisesti seuraavan viranomaisen ennakkokuulemisen. (HE 9/2018, 30; Andreasson & Ylipartanen 2022, luku 2.2.)

Rekisterinpitäjällä on myös velvollisuus nimetä organisaatioonsa tietosuojavastaava, jos jokin seuraavista kolmesta edellytyksestä täyttyy: henkilötietojen käsittelystä vastaa viranomainen tai julkishallinnon elin, toiminta edellyttää laajamittaista, säännöllistä ja järjestelmistä seurantaa tai toiminta perustuu laajamittaiseen erityisten henkilötietoryhmien tai rikostuomioihin liittyvien tietojen käsittelyyn. Tietosuojavastaavan tehtävänä on toimia erityisasiantuntijana henkilötietojen käsittelyyn ja tietosuojasääntelyyn liittyvissä asioissa. Tietosuojavastaavan nimike velvoittaa henkilön noudattamaan kaikkia tietosuoja-asetuksen tietosuojavastaavan tehtäviä ja asemaa koskevia säännöksiä. Jos näitä säännöksiä ei jostain syystä haluta noudattaa kaikilta osin, tulee vastuuhenkilön tehtävänimikkeen olla jokin muu. (Korpisaari ym. 2022, 420–421; European Data Protection Board n.d.a.) Tietosuoja-asetuksen 39 artiklan c kohdan mukaan tietosuojavastaavan tehtäviin kuuluu myös antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin laatimisessa ja valvoa sen toteutusta.

2.2.5 Valvonta ja sanktiot

Yksi yleisen tietosuoja-asetuksen tavoitteista on valvontaviranomaisen toimivaltuuksien vahvistaminen ja sen riippumattomuuden edistäminen. Tietosuoja-asetuksen VI luvussa säädetään valvontaviranomaisista ja sen tehtävistä. Asetuksen 51 artiklan mukaan jäsenvaltioiden on varmistettava, että tietosuoja-asetuksen soveltamista valvoo yksi tai useampi riippumaton viranomainen. Lisäksi eri maiden valvontaviranomaisten tulee toimia yhteistyössä, jotta asetusta sovelletaan

mahdollisimman yhdenmukaisesti kaikkialla unionissa. Valvontaviranomaisen perustamista sekä sen pätevyyttä ja kelpoisuutta koskeva sääntely on jätetty tietosuoja-asetuksessa jokaisen jäsenvaltion tehtäväksi. Suomessa kansallinen valvontaviranomainen on Tietosuojavaltuutetun toimisto. (HE 9/2018, 30–31; Korpisaari ym. 2022, 513, 515.)

Tietosuoja-asetuksen soveltamista unionin tasolla valvoo Euroopan tietosuojaneuvosto (EDPB, *European Data Protection Board*). Se kokoaa yhteen jäsenvaltioiden kansalliset tietosuojaviranomaiset ja varmistaa, että tietosuoja-asetusta sovelletaan johdonmukaisesti. Euroopan tietosuojaneuvostolla on toimivaltuudet antaa kiistanratkaisumenettelyssä sitovia päätöksiä, joita kansallisten valvontaviranomaisten tulee noudattaa. (HE 9/2018, 31; European Data Protection Board n.d.b.)

Tietosuoja-asetuksen rikkomisen seurauksena valvontaviranomaisella on asetuksen 58 artiklan 2 kohdan mukaan toimivaltuudet korjaaviin toimenpiteisiin ja hallinnollisiin sakkoihin. Korjaavana toimenpiteenä rekisterinpitäjälle tai henkilötiedon käsittelijälle voidaan esimerkiksi antaa varoitus tai huomautus siitä, että käsittelytoimet ovat asetuksen säännösten vastaisia. Jos varoitus ja huomautus eivät riitä, käsittelyä voidaan myös väliaikaisesti tai pysyvästi rajoittaa tai se voidaan kieltää kokonaan. Valvontaviranomainen voi myös määrätä hallinnollisen seuraamusmaksun korjaavien toimenpiteiden sijasta tai niiden lisäksi. Euroopan tietosuojaneuvosto pyrkii yhdenmukaistamaan korjaavien toimenpiteiden soveltamista ja hallinnollisten sakkojen määräämistä antamalla valvontaviranomaisille suuntaviivoja aiheeseen liittyen. (Andreasson & Ylipartanen 2022, luku 2.2.)

Hallinnollisten seuraamusmaksujen määräämisen yleisistä edellytyksistä säädetään tietosuoja-asetuksen 83 artiklassa. Sen 2 kohdassa on lueteltu useita seikkoja, jotka on otettava huomioon päätettäessä seuraamusmaksun määräämisestä tai sen suuruudesta. Näitä ovat muun muassa rikkomisen luonne, vakavuus ja kesto, rikkomisen tahallisuus ja tuottamuksellisuus sekä sen vahingollisuus ja toistuvuus. Tietosuoja-asetuksessa on määritelty sakolle kaksi enimmäismäärää, jotka ovat 10 ja 20 miljoonaa euroa tai 2 ja 4 prosenttia globaalista liikevaihdosta. Kaksi eri sakon enimmäismäärää osoittavat, että tiettyjen asetuksen säännösten rikkominen voidaan nähdä vakavampana kuin toisten. Korkeimpia

sanktiomahdollisuuksia käytetään kuitenkin vain poikkeuksellisissa tilanteissa, mutta jo mahdollisuus niihin edesauttaa tietosuoja-asetuksen tavoitetta saada organisaatiot kunnioittamaan ihmisten tietosuojaa. (Andreasson & Ylipartanen 2022, luku 2.2; Korpisaari ym. 2022, 632, 636.)

2.3 Henkilötietojen suoja ihmisoikeusnäkökulmasta

Tietosuoja-asetuksen taustalla ovat Euroopan unionin perusoikeuskirja (EUVL C 202, 7.6.2016) ja kansainväliset ihmisoikeussopimukset, kuten Euroopan ihmisoikeussopimus (EIS, 1950) (Andreasson & Ylipartanen 2022, luku 2.1). Euroopan ihmisoikeussopimuksen 8 artiklassa turvataan oikeus nauttia yksityis- ja perhe-elämän kunnioitusta. Euroopan ihmisoikeustuomioistuimen (EIT) mukaan henkilötietojen suoja on tärkeä osa tätä oikeutta, sillä yksityiselämän suojaaminen edellyttää muun muassa, että vähintään siihen kuuluvien henkilötietojen käsittelystä on säädetty riittävän selkeästi ja tarkasti. (Korpisaari ym. 2022, 11.)

Euroopan unionin perusoikeuskirjassa yksityiselämää ja henkilötietoja suojataan sen 7 ja 8 artiklassa. Perusoikeuskirjan 7 artiklan mukaan, jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan ja viestejään kunnioitetaan. Perusoikeuskirjan 8 artikla taas turvaa jokaisen oikeuden henkilötietojensa suojaan. Artiklan mukaan tietojen käsittelyn tulee olla asian- ja tarkoituksenmukaista ja se tulee tapahtua asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on myös oikeus tutustua itsestään kerättyihin tietoihin ja saada ne oikaistuksi. Perusoikeuskirjan 8 artiklan 3 kohdan mukaan riippumattoman viranomaisen tulee valvoa näiden sääntöjen noudattamista. Euroopan unionin tuomioistuin on katsonut, että perusoikeuskirjan 7 ja 8 artiklassa turvattu oikeus yksityiselämän suojaan kattaa henkilötietojen käsittelyssä kaikenlaiset tiedot, jotka koskevat tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä. (Korpisaari ym. 2022, 15.)

Myös Suomen perustuslaissa (731/1999) turvataan jokaisen yksityiselämä. Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu ja henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslain säännöksessä henkilötietojen suoja esiintyy siis yhtenä yksityiselämän suojan

osa-alueena. Tämä rajoittaa perustuslakivaliokunnan käytännön mukaan lainsäätäjän liikkumavaraa henkilötietojen käsittelyn sääntelyssä, sillä henkilötietojen suoja sisältyy osittain samassa momentissa turvatun yksityiselämän piiriin. Lainsäätäjän onkin huomioitava henkilötietojen suoja siten, että se on hyväksyttävissä perusoikeusjärjestelmän näkökulmasta. Perustuslakivaliokunnan mukaan EU:n yleinen tietosuoja-asetus muodostaa riittävän sääntelyn perustuslain 10 §:ssä turvatulle yksityiselämän ja henkilötietojen suojalle, eikä erityislainsäädäntöön ole tarpeen sisällyttää yksityiskohtaista sääntelyä henkilötietojen käsittelystä. (Hallberg 2005, luku III, alaluku 6; Korpisaari ym. 2022, 8–9; PeVL 14/2018 vp, 2.)

Kuten yllä on todettu, henkilötiedot ja yksityiselämän suoja ovat läheisessä suhteessa. Kaikki henkilötiedot eivät kuitenkaan välttämättä kuulu yksityiselämän suojan piiriin, mutta jos yksityiselämää koskevat tiedot voidaan yhdistää tiettyä henkilöä koskeviksi, ne ovat aina henkilötietoja. Kun määritellään henkilötietojen ja yksityiselämän suojan suhdetta, tulee huomioida, että yksityisyyden suoja henkilötietoja käsiteltäessä muodostuu myös muista perusoikeuksista. Näitä ovat oikeudet turvallisuuteen, kunniaan, ihmisarvoiseen kohteluun sekä henkilökohtaiseen koskemattomuuteen, oikeus vaikuttaa itseään koskeviin asioihin sekä yhdenvertaisuus ja syrjinnän kielto. Perustusvaliokunnan mukaan suhde muihin perusoikeuksiin täytyy kuitenkin arvioida tapauskohtaisesti viranomaisissa ja tuomioistuimissa. (Korpisaari ym. 2022, 16; PeVL 14/2018 vp, 8–9.)

3 VAIKUTUSTENARVIOINTI

3.1 Määritelmä

Tietosuojaa koskeva vaikutustenarviointi (DPIA, *Data Protection Impact Assessment*) on prosessi, josta säädetään tietosuoja-asetuksen 35 artiklassa. Sen mukaan vaikutustenarviointi on tehtävä, kun ollaan käsittelemässä henkilötietoja tavalla, mikä todennäköisesti aiheuttaa rekisteröidyn oikeuksille ja vapauksille korkean riskin. Vaikutustenarvioinnin tarkoitus on auttaa näiden riskien tunnistamisessa, arvioinnissa ja hallitsemisessa ja sen tavoitteena on selvittää, onko jäljelle jäänyt riski hyväksyttävissä ja oikeutettu kyseisissä olosuhteissa (Tietosuojavaltuutetun toimisto n.d.c.) Vaikka henkilötietojen käsittely ei olisi korkeariskistä, jokaisen rekisterinpitäjän on noudatettava henkilötietojen käsittelyä koskevaa sääntelyä. Jokaisen rekisterinpitäjän täytyy siis vähintään arvioida, tuleeko heidän tehdä vaikutustenarviointi vai ei. (Hanninen ym. 2017, 115; Tietosuojan vaikutustenarvioinnin ohje 2021, 5.)

Vaikutustenarvioinnissa on tarkasteltava suunniteltuja toimenpiteitä ja suojatoimia, joilla lievennetään tunnistettua riskiä ja varmistetaan henkilötietojen suoja. Se kuvaa henkilötietojen käsittelyä ja arvioi käsittelyn tarpeellisuutta suhteessa riskeihin. Vaikutustenarvioinnilla myös osoitetaan, että tietosuoja-asetusta on noudatettu ja se myös helpottaa tietosuoja-asetuksen 5 artiklan 2 kohdassa säädettyä osoitusvelvollisuutta. Osoitusvelvollisuuden mukaan pelkkä tietosuojaperiaatteiden noudattaminen ei riitä, vaan noudattaminen tulee pystyä myös jatkuvasti osoittamaan. (Hanninen ym. 2017, 115; Korpisaari ym. 2022, 99, 400.)

Tietosuoja-asetuksessa ei ole määritelty, miten tietosuojan vaikutustenarviointi tulisi toteuttaa, mutta 35 artiklassa on lueteltu siihen vähimmäissisältö. Artiklan mukaan arvioinnissa on oltava ainakin järjestelmällinen kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista sekä tarvittaessa rekisterinpitäjän oikeutetut edut. Lisäksi sen tulee sisältää arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden sekä arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä. Viimeisenä vähimmäissisältönä vaaditaan suunnitellut toimenpiteet riskeihin puuttumiseksi. (Korpisaari ym. 2022, 408.)

Tietosuojavaltuutetun toimisto on laatinut ohjeet vaikutustenarvioinnin tekemiseen. Ohjeen mukaan vaikutustenarvioinnissa pyritään vastaamaan seuraaviin kysymyksiin: Mitä, miten ja miksi henkilötietoja aiotaan käsitellä? Jos henkilötietojen käsittely tapahtuu suunnitellusti, miten se vaikuttaa rekisteröityihin? Miten suunniteltu henkilötietojen käsittely voi mennä pieleen ja kuinka todennäköistä se on? Miten tätä todennäköisyyttä voidaan pienentää? Vaikutustenarviointi edellyttää siis riskien ja niiden suojatoimenpiteiden tarkkaa tunnistamista etukäteen. (Tietosuojan vaikutustenarvioinnin ohje 2021, 5.)

Vaikutustenarvioinnin toteuttamisesta vastaa aina rekisterinpitäjä. Henkilötietojen käsittelijän on annettava rekisterinpitäjälle tarpeelliset tiedot vaikutustenarvioinnin tekemiseksi. Rekisterinpitäjän tulee pyytää neuvoja tietosuojavastaavalta vaikutustenarviointia tehdessään ja nämä neuvot tulee sisällyttää vaikutustenarvioinnin tuloksiin. On myös suositeltavaa kuulla henkilötietojen käsittelyn kohteena olevia henkilöitä. (Hanninen ym. 2017, 118; Tietosuojan vaikutustenarvioinnin ohje 2021, 7.)

Tietosuoja-asetuksen 5 artiklan osoitusvelvollisuuden mukaisesti vaikutustenarviointi tulee dokumentoida, jotta valvontaviranomaiselle voidaan tarvittaessa näyttää, miten vaikutustenarviointi on tehty. Tietosuojan vaikutustenarviointi on myös pidettävä ajan tasalla ja sen päivittämisen tarvetta suositellaan arvioitavaksi säännöllisesti. Vaikutustenarviointi tulee päivittää, jos lainsäädäntö, toimintaympäristö tai riskit muuttuvat. Asetuksessa ei vaadita, että vaikutustenarviointi pitäisi julkaista, mutta rekisterinpitäjä voi parantaa luottamustaan julkaistessaan esimerkiksi yhteenvedon arvioinnistaan. (Korpisaari ym. 2022, 409.)

Vaikutustenarviointi kannattaa tehdä, sillä sen avulla voidaan huomata henkilötietojen käsittelyyn liittyvät uhat ennen suurien taloudellisten sijoitusten tekemistä. Suunnitellun käsittelyn muuttaminen on todennäköisesti paljon halvempaa tehdä suunnitteluvaiheessa kuin myöhemmässä vaiheessa. Lisäksi vaikutustenarviointi voi tuoda maine-etuja. Rekisterinpitäjä voi ottaa huomioon rekisteröityjen mielipiteet henkilötietojen suunnitellusta käsittelystä etukäteen ja vaikutustenarviointi voidaan julkaista rekisteröityjen nähtäville. Jos käsittelyyn liittyvä uhka toteutuu, vaikutustenarviointi auttaa osoittamaan, että rekisterinpitäjä on

pyrkinyt asianmukaisesti torjumaan tapahtuman. Tämä voi vähentää riskiä negatiivisesta julkisuudesta ja vahinkovastuusta. Jos tietosuojan vaikutustenarviointi jätetään tekemättä, vaikka se olisi pitänyt tehdä, voi seuraamuksena olla käsittelykielto tai seuraamusmaksu. Rekisterinpitäjän kannattaa siis myös dokumentoida, miksi vaikutustenarviointi on jätetty tekemättä. (Tietosuojan vaikutustenarvioinnin ohje 2021, 6.)

3.2 Velvoite tehdä vaikutustenarviointi

Tietosuojaa koskevaa vaikutustenarviointia ei tarvitse tehdä, jos katsotaan, ettei käsittely todennäköisesti aiheuta korkeaa riskiä luonnollisen henkilön oikeuksille ja vapauksille. Vaikutustenarviointia ei myöskään vaadita, jos tietojen käsittelyn luonne, asiayhteys, tarkoitukset ja laajuus on hyvin samankaltaisia, kuin sellaisen käsittelyn, josta on jo aiemmin tehty vaikutustenarviointi. Lisäksi arviointia ei velvoiteta, jos käsittely perustuu rekisterinpitäjän lakisääteiseen velvoitteeseen, yleisen edun mukaiseen tehtävään tai julkisen vallan käyttöön ja jos tietosuojaa koskeva vaikutustenarviointi on jo tehty kyseisen käsittelyn oikeusperusteen määrittelyn yhteydessä. (Korpisaari ym. 2022, 407.)

Vaikutustenarviointi ei ole pakollinen, mikäli olosuhteet eivät ole muuttuneet sen jälkeen, kun valvontaviranomainen on tarkastanut käsittelytoimet ennen toukokuuta 2018. Mikäli ei ole täysin selvää, vaaditaanko vaikutustenarviointia vai ei, se suositellaan tekemään. (Korpisaari ym. 2022, 407–408.) On kuitenkin tilanteita, jossa tietosuojan vaikutustenarviointi täytyy tehdä. Velvoite voi seurata tietosuoja-asetuksessa määritellyistä käsittelytilanteista, kansallisesta lainsäädännöstä, tai siitä, että käsittelytoimenpide on yksilöity tietosuojaviranomaisen luettelossa. (Tietosuojavaltuutetun toimisto n.d.c.)

Tietosuoja-asetuksen 35 artiklan 1 kohdan mukaan vaikutustenarviointi tehdään silloin, kun henkilötietojen käsittelystä etenkin uutta teknologiaa käytettäessä todennäköisesti seuraa korkea riski luonnollisen henkilön oikeuksille ja vapauksille. Asetuksen 35 artiklan 3 kohdassa listataan käsittelytoimet, jotka erityisesti vaativat vaikutustenarvioinnin. Lista ei ole tyhjentävä. Listan mukaan vaikutustenarvi-

ointi on tehtävä erityisesti, jos rekisteröidyn henkilökohtaisia ominaisuuksia arvioidaan automaattisen käsittelyn avulla järjestelmällisesti ja kattavasti ja tämä arvio johtaa päätöksentekoon, jolla on rekisteröityä koskevia oikeusvaikutuksia. Vaikutustenarvio vaaditaan myös, jos käsitellään laajamittaisesti erityisiä henkilöryhmiä, rikoksia tai rikostuomioita. Vaikutustenarviointi tulee tehdä myös siinä tapauksessa, jos yleisölle avointa aluetta valvotaan järjestelmällisesti ja laajasti.

Tietosuojavaltuutetun toimisto on antanut ohjeen keinoista selvittää, milloin kyseessä on tietosuoja-asetuksen mukainen korkea riski. Ohjeessa on listattu kriteerit korkean riskin arvioimiseksi ja ohjeen mukaan vaikutustenarviointi on tehtävä, mikäli kaksi kriteereistä täyttyy. Mitä useampi kriteeri täyttyy, sitä todennäköisemmin rekisteröidyn oikeudet ja vapaudet ovat uhattuna. (Tietosuojavaltuutetun toimisto n.d.c.) Joissakin tapauksissa rekisterinpitäjä saattaa pitää vaikutustenarviointia tarpeellisena, vaikka kriteereistä täyttyisi vain yksi (Korpisaari ym. 2022, 407).

Tietosuojavaltuutetun toimiston antamat kriteerit korkean riskin arvioimiseksi ovat

- henkilötietojen arviointi tai pisteytys
- automaattinen päätöksenteko, jolla on oikeusvaikutuksia
- järjestelmällinen valvonta
- arkaluontoiset tiedot
- tietojen laajamittainen käsittely
- tietokokonaisuuksien yhdistäminen
- heikossa asemassa olevia rekisteröityjä koskevat tiedot
- uusien teknisten tai organisatoristen ratkaisujen innovatiivinen käyttö tai soveltaminen (Tietosuojavaltuutetun toimisto n.d.c).

Esimerkiksi eräässä yhtiössä oli käytössä ajotietojärjestelmä, jonka antamien sijaintitietojen avulla seurattiin työntekijöiden työaikaa. Itä-Suomen hallinto-oikeuden lainvoimaisen päätöksen mukaan yhtiö oli laiminlyönyt velvollisuutensa tehdä vaikutustenarviointi työntekijöiden sijaintitietojen käsittelytoimista. Kyseessä oli heikommassa asemassa olevien työntekijöiden järjestelmällinen valvonta, joka aiheutti työntekijöiden eli rekisteröityjen oikeuksille ja vapauksille korkean riskin. Tietosuoja-asetuksen rikkomuksen luonne ja vakavuus, tuottamuksellisuus sekä rekisteröityjen heikompi asema rekisterinpitäjään nähden olivat

sellaisia, että yhtiölle määrättiin huomautuksen lisäksi 16 000 euron hallinnollinen seuraamusmaksu. (Itä-Suomen HAO 20.05.2021 21/0231/2.)

Tietosuoja-asetuksen 35 artiklan 4 kohdan mukaan valvontaviranomaisen on julkaistava luettelo erilaisista käsittelytoimien tyypeistä, jotka vaativat vaikutustenarvioinnin tekemistä. Luettelo täydentää tietosuoja-asetuksen 35 artiklan 1 kohtaa ja sekä ylempänä lueteltuja Tietosuojaryhmän kriteereitä korkean riskin arvioimiseksi (Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista 2017). Luettelon mukaan vaikutustenarviointi on tehtävä, mikäli käsitellään biometrisiä, geneettisiä tai sijaintitietoja ja vähintään yksi korkean riskin kriteereistä täyttyy. Myös poikkeaminen rekisteröidyn informoinnista tietosuoja-asetuksen 14.5 artiklan nojalla, sekä yhden kriteerin täyttyminen velvoittaa vaikutustenarvioinnin tekemiseen. (Tietosuojavaltuutetun toimisto 2018.)

Vaikutustenarviointia voidaan edellyttää myös erikseen kansallisessa lainsäädännössä. Esimerkiksi tietosuojalain (1050/2018) 31 §:n mukaan voidaan rekisteröidyn oikeuksista tarvittaessa poiketa, kun henkilötietoja käsitellään historiallisessa ja tieteellisessä tutkimuksessa sekä tilastoinnissa. Edellytyksenä tälle voi olla tietosuojaa koskevan vaikutustenarvioinnin tekeminen ja sen toimittaminen tiedoksi tietosuojavaltuutetulle ennen käsittelyyn ryhtymistä. Vaikutustenarviointi vaaditaan 31 §:n mukaan tilanteessa, jossa rekisterinpitäjä käsittelee erityisiin henkilötietoryhmiin kuuluvien tietoja tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja.

3.3 Riskienarviointi

Rekisterinpitäjän tulee tietosuojan vaikutustenarvioinnissa analysoida suunnitellusta käsittelystä aiheutuvat riskit yksityiskohtaisesti. Riskienarvioinnissa on kaksi eri näkökulmaa: rekisteröidyn oikeuksiin ja vapauksiin kohdistuvat riskit sekä organisaatiota kohtaavat riskit. Tietosuojan vaikutustenarvioinnissa arvioidaan ensisijaisesti riskejä rekisteröidyn oikeuksiin ja vapauksiin ja riskiä arvioitaessa henkilön oikeudet ja velvollisuudet tulee ymmärtää laajasti. Tämä tarkoittaa myös sitä, että tietosuojaoikeuksien lisäksi myös esimerkiksi sananvapaus ja liikkumisvapaus tulee ottaa tarvittaessa huomioon. Organisaatioon liittyvät riskit liittyvät

pohjimmiltaan organisaation julkisuuskuvaan ja mahdollisiin sanktioihin. (European Data Protection Supervisor 2018, 8; Korpisaari ym. 2022, 400.) Vaikutustenarvioinnissa huomioidaan riskit, jotka aiheutuvat siitä huolimatta, että henkilötietojen käsittely suoritettaisiin suunnitellusti. Myös esimerkiksi mahdollisen tietoturvaloukkauksen aiheuttamat riskit on arvioitava. Toisin sanoen vaikutustenarvioinnissa arvioidaan hypoteettista riskiä ja sen hallintaa. (KHO:2022:131.)

Riski jaetaan neljään osatekijään, joita ovat uhka, uhan vaikutukset rekisteröidylle, vaikutusten vakavuus rekisteröidylle sekä uhan todennäköisyys. Riskien arviointi aloitetaan kartoittamalla henkilötietojen käsittelyyn kohdistuvat uhat. Uhalla tarkoitetaan henkilötietojen käsittelyyn liittyvää tapahtumaa, joka vaikuttaa haitallisesti tietosuojaperiaatteisiin tai rekisteröidyn oikeuksiin ja vapauksiin. Uhalla tarkoitetaan myös henkilötietojen käsittelyn haavoittuvuutta, heikkoutta tai puutetta. Kun uhkia kartoitetaan, tulee huomioida, että uhat voivat syntyä organisaation sisäisesti tai sen ulkopuolelta ja ne voivat aiheutua ihmisten toiminnasta tai ei-inhimillisistä syistä. Lisäksi uhat voivat syntyä joko tahallisesta tai huolimattomasta toiminnasta. Esimerkiksi harjoittelija voi vahingossa luovuttaa tiedon väärälle henkilölle, organisaatio voi joutua rikollisen kyberhyökkäyksen kohteeksi tai konehuoneessa voi syttyä tulipalo. (Tietosuojan vaikutustenarvioinnin ohje 2021, 26–27, 30–31.)

Tietosuojan vaikutustenarvioinnissa olennaisia ovat sellaiset vaikutukset, jotka aiheutuvat toteutuneesta uhasta henkilötietojen käsittelyn yhteydessä ja kohdistuvat yksilön tietosuojaan. Sen sijaan vaikutukset, jotka kohdistuvat pelkästään muihin perusoikeuksiin olematta suoraan yhteydessä henkilötietojen käsittelyyn, jätetään arvioinnin ulkopuolelle. Uhan vaikutukset voivat olla aineettomia, aineellisia tai fyysisiä ja ne voivat aiheuttaa rekisteröidylle monenlaista vahinkoa, kuten mainehaittaa, identiteettivarkauden, taloudellista menetystä, syrjintää, väkivallan uhkaa tai häirintää. (Tietosuojan vaikutustenarvioinnin ohje 2021, 27; Andreasson & Ylipartanen 2022, luku 5.3.)

Henkilötietojen käsittelystä aiheutuvien uhkien ja niiden aiheuttamien vaikutusten tunnistamisen jälkeen, rekisterinpitäjän on arvioitava vaikutusten vakavuus ja uhan toteutumisen todennäköisyys. Vaikutusten vakavuuden arvioinnissa tulee huomioida esimerkiksi henkilötietojen luonne ja kuinka helposti tiedot voivat tulla

väärinkäytetyksi. Vakavuutta voivat lisätä muun muassa erityisiin henkilötietoryhmiin kuuluvien tai alaikäisten tietojen käsittely sekä sellaisten henkilötunnisteiden käsittely, joita voidaan käyttää rikollisiin tarkoituksiin. Uhan toteutumisen todennäköisyyttä arvioidaan tunnistamalla tietosuojaan liittyvät mahdolliset heikkoudet ja haavoittuvuudet ja selvittämällä, mitkä tekijät voivat aiheuttaa uhan. Lisäksi tulee arvioida, kuinka todennäköistä on, että nämä tekijät pystyvät ja haluavat hyödyntää kyseisiä heikkouksia ja haavoittuvuuksia. Käytännössä organisaatioissa on jo usein käytössä uhkien todennäköisyyttä pienentäviä suojatoimia, joita tietosuoja-asetus edellyttää. Tällöin uhan todennäköisyyden arvioinnissa otetaan huomioon nämä olemassa olevat suojatoimenpiteet. (Tietosuojan vaikutustenarvioinnin ohje 2021, 28, 31–35.)

Uhkien todennäköisyyksistä ja vaikutusten vakavuuden arvioinnista laaditaan yhteenveto, jonka avulla arvioidaan riskien tasot ja pohditaan keinoja niiden pienentämiseksi. Jos riskin taso jää lisätoimenpiteiden toteuttamisesta huolimatta erittäin korkeaksi, tulee ryhtyä valvontaviranomaisen ennakkokuulemiseen. Jos riskit jäävät hyväksyttävälle tasolle, rekisterinpitäjä voi hyväksyä tietosuojan vaikutustenarvioinnin ja siihen sisältyvät riskit ja riskitasot sekä valitut korjaavat toimenpiteet. Organisaatioissa päätetään itse menettely, minkä mukaisesti hyväksyntä tehdään. Esimerkiksi johdolle voidaan laatia yhteenveto vaikutustenarvioinnin lopputuloksesta. (Tietosuojan vaikutustenarvioinnin ohje 2021, 37, 39; Andreasson & Ylipartanen 2022, luku 5.3.)

3.4 Valvontaviranomaisen ennakkokuuleminen

Tietosuojan vaikutustenarviointi on keskeinen työkalu henkilötietojen käsittelyä koskevassa riskienhallinnassa, mutta kaikkia riskejä ei kuitenkaan aina saada poistettua kokonaan tai niitä ei ole mahdollista pienentää riittävän matalalle tasolle. Jos jäännösriskiä ei voida pienentää kohtuullisin toimenpitein ja kustannuksin saatavilla oleva teknologia huomioiden, tulee rekisterinpitäjän kuulla tietosuojavaltuutettua ennen henkilötietojen käsittelyn aloittamista. Valvontaviranomaisen ennakkokuulemisesta säädetään yleisen tietosuoja-asetuksen 36 artiklassa. Huomioitavaa on, että ennakkokuuleminen ei ole niin sanottu lupaprosessi. (Tietosuojan vaikutustenarvioinnin ohje 2021, 39; Korpisaari ym. 2022, 416–417.)

Tietosuojaviranomaisen ennakkokuulemiseen tulee ryhtyä esimerkiksi silloin, kun henkilötietojen käsittely voisi aiheuttaa rekisteröidylle huomattavia tai pysyviä seurauksia, joita he eivät välttämättä pysty estämään. Tällaisia tilanteita voisivat olla esimerkiksi luvaton pääsy tietoihin, joka voisi vaarantaa henkilön hengen, johtaa irtisanomiseen tai aiheuttaa taloudellisia menetyksiä tai kun riskin toteutuminen on ilmeistä, eikä rekisterinpitäjällä ole keinoja rajoittaa niiden henkilöiden lukumäärää, joilla on pääsy tietoihin tai korjata tiedossa olevia haavoittuvuuksia. (Tietosuojan vaikutustenarvioinnin ohje 2021, 39.) Tietosuoja-asetuksen 36 artiklan mukaan tietosuojaviranomaista on myös kuultava aina, jos valmistellaan henkilötietojen käsittelyä koskevaa lainsäädäntöä (kohta 4) tai jos jäsenvaltion lainsäädännössä niin erikseen vaaditaan (kohta 5).

Valvontaviranomaisen on vastattava ennakkokuulemispyyntöön pääsääntöisesti kahdeksan viikon kuluessa. Tietosuojavaltuutetun on annettava tarvittaessa rekisterinpitäjälle tai henkilötietojen käsittelijälle kirjalliset ohjeet toimenpiteistä, joilla riskiä voidaan alentaa. Samalla tietosuojavaltuutettu voi käyttää sille tietosuoja-asetuksen 58 artiklan mukaisia valtuuksia, kuten varoitusta, huomautusta tai tietojen käsittelyn kieltämistä. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee toteuttaa tietosuojavaltuutetun ohjeen mukaiset lisätoimenpiteet, ennen henkilötietojen käsittelyn aloittamista, jotta käsittely olisi lainmukaista. (Korpisaari ym. 2022, 417; Tietosuojavaltuutetun toimisto n.d.d.)

4 OPPIMISALUSTA MOODLEN TIETOSUOJAOMINAISUUDET

4.1 Moodle yleisesti

Moodle (*Modular Object-Oriented Dynamic Learning Environment*) on maksuton, avoimen lähdekoodin verkko-oppimisympäristö, joka on saatavilla ilmaiseksi GNU General Public License -lisenssillä. Se on yksi maailman suosituimmista oppimisalustoista akateemisella sekä yritystasolla ja sillä on noin 435 miljoonaa käyttäjää ympäri maailman. Moodlea käyttävät niin suuret kuin pienetkin organisaatiot ja oppilaitokset. Sen tunnetuimpiin käyttäjiin kuuluvat muun muassa Lontoon kauppakorkeakoulu (*London School of Economics*), New Yorkin osavaltionyliopisto (*State University of New York*), Google sekä öljy-yhtiö Shell. Moodle on saatavilla yli 120 kielelle. (Moodle n.d.a; Moodle 2024a.)

Moodlen perusti 20 vuotta sitten australialainen Martin Dougiamas tavoitteenaan luoda verkkopohjainen oppimisratkaisu, joka olisi joustava, saavutettava ja mahdollistaisi jokaisen oikeuden koulutukseen (Moodle n.d.b). Nykyisin Moodlen toiminnasta vastaa yksityinen osakeyhtiö Moodle Pty Ltd ja sitä rahoitetaan muun muassa Moodle-yhteisön avulla ja vapaaehtoisilla lahjoituksilla (Moodle 2024a). Suomessa Moodle on yksi käytetyimmistä verkko-oppimisympäristöistä. Esimerkiksi Tampereen korkeakouluyhteisössä käytettävä Moodle tunnetaan nimellä TUNI Moodle ja kaikilla korkeakouluyhteisön henkilökunnan jäsenillä ja opiskelijoilla on pääsy tähän oppimisympäristöön. (TUNI Moodle n.d.a.).

Moodlea käytetään opintojaksojen kotisivuna, lähiopetuksen tukena sekä etäopiskelussa (Moodle 2024b). Moodle tarjoaa opettajille erilaisia työkaluja oman kurssialueen luomiseen ja sen hallintaan. Kurssialueelle voi lisätä kurssiin liittyvät materiaalit, linkit, oppimistehtävät ja vuorovaikutusta edistävät aktiviteetit, kuten keskustelualueet. Moodlessa voi myös pitää tenttejä, ohjata ja seurata opiskelijoiden oppimisprosessia, tukea opiskelijoiden ryhmätyöskentelyä sekä tehdä tekstin alkuperäisyystarkistuksia. Moodle mahdollistaa myös tehtävien palautuksen, tenttien automaattisen arvioinnin sekä vertaisarvioinnin. (TUNI Moodle n.d.a; Moodle 2024b.)

4.2 Moodlen tietosuoja

4.2.1 Käsittelyn tarkoitus ja oikeusperuste

Moodlen on kerättävä käyttäjien henkilötietoja voidakseen tarjota palvelujaan. Se on sitoutunut rakentamaan turvallisen oppimisympäristön, joka suojaa käyttäjien tietosuojaa ja turvallisuutta. Moodlen ohjelmistosovellus LMS:ään (*Learning Management System*) upotetut tietosuojaominaisuudet varmistavat, että Moodle on yhteensopiva EU:n yleisen tietosuoja-asetuksen kanssa ja että se noudattaa paikallisten tietosuojalainsäädännön vaatimuksia. Osa rekisteröidyn tietosuojan toteuttamisen vastuusta kuuluu kuitenkin organisaatiolle, joka hallitsee omaa Moodle-asennustaan. Organisaatioiden vastuulla on esimerkiksi laatia tietosuojaseloste, kiinnittää erityistä huomiota alaikäisten käyttäjien suojaamiseen, varmistaa rekisteröidyn oikeuksien toteutuminen ja nimetä tietosuojavastaava. (Moodle 2024c.)

TUNI Moodle noudattaa henkilötietojen käsittelyssä EU:n yleistä tietosuoja-asetusta. Henkilötietojen käsittelyn oikeusperuste on tietosuoja-asetuksen artikla 6.1 e, jonka mukaan käsittely on sallittua, kun se on tarpeen julkisen vallan käyttöön perustuvan tehtävän suorittamiseksi tai yleisen edun vuoksi. Lisäksi perusteena on tietosuojalain 4.1 §:n alakohta 2, jonka mukaan käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi. TUNI Moodlen tapauksessa tämä tarkoittaa, että tietoja käytetään opetuksen kehittämiseen ja tutkimukseen. TUNI Moodle käyttää kerättäviä henkilötietoja opetukseen, käyttöoikeuksien hallintaan, oppimisen ohjaukseen sekä opintosuoritusten arviointiin. Lisäksi henkilötietoja käytetään yhteydenottojen mahdollistamiseen, opiskelijan identiteetin varmistamiseen, Moodleen liitettyihin palveluihin kirjautumiseen, oppimisanalytiikkadatan tuottamiseen sekä ongelmatilanteiden ratkaisemiseen. (TUNI Moodle n.d.b.)

TUNI Moodlen rekisteri sisältää tietoa opettajista, opiskelijoista, opintojaksoista sekä opintosuorituksista. Rekisterin pakolliset henkilötiedot käyttäjistä ovat käyttäjätunnus, etu- ja sukunimi, sähköpostiosoite, opiskelijanumero, kotiorganisaatio ja maa. Käyttäjä voi myös tallentaa henkilökohtaiseen profiiliinsa seuraavat vapaaehtoiset tiedot: valokuva, vapaamuotoinen kuvaus itsestään, verkkosivun

osoite, pikaviestiohjelmien käyttäjätunnukset, puhelinnumero sekä osoitetiedot. Lisäksi rekisteri sisältää TUNI Moodlen käytössä syntyviä tietoja, kuten tehtäväpalautuksia, keskustelualueviestejä sekä muihin Moodle-aktiviteetteihin käyttäjän itse syöttämiä tietoja. (TUNI Moodle n.d.b.)

EU:n tietosuoja-asetuksen 10 artiklan mukaista rikostuomioihin ja rikkomuksiin liittyvää henkilötietojen käsittelyä ei tapahdu, mutta 9 artiklan mukainen erityisiä henkilötietoryhmiä koskeva käsittely saattaa tulla kyseeseen. Moodlen tietosuojailmoituksen mukaan on kyse erityistä henkilötietoryhmää koskevan tiedon käsittelystä, jos rekisteröity lataa kasvokuvan ja Moodle tallentaa tämän biometrisen tiedon. Lisäksi kyseeseen voi tulla työntekijöiden terveystietojen käsittelyä, mikäli he kertovat TUNI Moodlessa sairauspoissaolonsa syyn. Tampereen ammattikorkeakoulun tietosuojavastaava Niku Hinkan (2025) mukaan opiskelijat saattavat myös vapaaehtoisesti antaa erityisiin henkilötietoryhmiin kuuluvia henkilötietoja palveluja käytettäessä esimerkiksi keskustelualueilla. (TUNI Moodle n.d.b; Moodle 2024c; TUNI järjestelmäsalkku 2024.)

4.2.2 Rekisterin suojauksen periaatteet

Tietojen suojaus perustuu käyttövaltuushallintaan, tietokantojen ja palvelinten tekniseen suojaukseen, tilojen fyysiseen suojaukseen, kulunvalvontaan, tietoliikenteen suojaukseen sekä tietojen varmuuskopiointiin. Moodle tarjoaa eri roolit opiskelijoille ja opettajille ja näillä rooleilla on eri käyttövaltuudet ja näkymät. Kurssikohtaiset opettaja- ja opiskelijaroolit saadaan osittain suoraan opintotietojärjestelmä Sisusta tai Pepistä, mutta useimmin niitä hallitaan manuaalisesti kurssikohtaisesti kurssin opettajan toimesta. Ulkopuolisten toimijoiden pääsy TUNI Moodleen edellyttää TUNI-resurssisopimusta, jolla varmistetaan tietosuojavaatimusten toteutuminen. (TUNI järjestelmäsalkku 2024.) Käyttäjärekisteriä voivat käsitellä vain tehtävään nimetyt henkilöt ja henkilötietoja käsittelevillä on salassapitovelvollisuus (TUNI Moodle n.d.b).

TUNI Moodlea suojataan korkeakouluyhteisössä yleisesti käytössä olevien tietoturvaperiaatteiden mukaisesti. Tiedonsiirto palvelimen ja käyttäjän välillä salataan SSL (*Secure Sockets Layer*) -turvatekniikalla ja pääsy palveluihin vaatii kaksivaiheisen kirjautumisen (MFA, *Multi-Factor Authentication*). Lisäksi jokainen korkeakouluyhteisön järjestelmien käyttäjä allekirjoittaa tietojen ja tietojärjestelmien tietoturva- ja vaitiolositoumuksen kirjautuessaan ensimmäistä kertaa TUNI-yhteisöön. Laitetilat ja tiedot sijaitsevat fyysisesti Suomessa ja toiminnan asianmukaisuuden valvontaan käytetään hallinnollisia kontrolleja. Järjestelmien sisältämät tiedot myös varmuuskopioidaan säännöllisin väliajoin. (TUNI järjestelmäsalkku 2024.)

4.2.3 Henkilötietojen elinkaari ja kolmannet osapuolet

Seuraavat henkilötiedot kerätään säännönmukaisesti suoraan kotiorganisaation opintotietojärjestelmästä (Pepistä tai Sisusta) Haka- tai TUNI-kirjautumisen yhteydessä: nimi, sähköpostiosoite, kotiorganisaatio, rooli kotiorganisaatiossa, opiskelijanumero sekä koulutusohjelma. Jos henkilölle luodaan erillinen Moodle-tunnus, koulutuksen järjestäjä toimittaa tarvittavat tiedot. Muut henkilötiedot rekisteröidyt antavat itse lisäämällä sisältöä tai julkaisuja oppimisalustalle. (TUNI Moodle n.d.b.)

TUNI Moodlessa voidaan hyödyntää joitakin ulkoisia palveluja, joissa henkilötietoja luovutetaan palvelukohtaisesti. Kun henkilö avaa tai tallentaa Panopto-videopalvelun sisältöjä Moodle-kurssilla tai avaa Zoom-videotapaamispalvelun linkin, luovutetaan rekisteröidyn käyttäjätunnus sekä nimi- ja sähköpostiosoitetietoja. Kun henkilö lataa dokumentin Turnitin-alkuperäisyystarkistuspalveluun, luovutetaan rekisteröidyn nimi- ja sähköpostiosoitetiedot. Zoom- ja Turnitin-palveluja käytettäessä henkilötietoja siirretään myös Tampereen yliopiston tietoturvakäytäntöjä ja -poliitikkoja noudattaen kolmanteen maahan tai kansainväliselle järjestölle Euroopan unionin (EU) tai Euroopan talousalueen (ETA) ulkopuolelle. Tietoja ei luovuteta ulkopuoliseen käyttöön, paitsi viranomaisen erillisestä pyynnöstä. (TUNI Moodle n.d.b.)

TUNI Moodlen sisäisessä käytössä rekisteröidyn nimitiedot ovat oppimisalustan muiden käyttäjien nähtävissä. Käyttäjä voi halutessaan näyttää myös sähköpostiosoitteensa muille ja lisätä profiiliinsa muita itseään koskevia lisätietoja muiden nähtäväksi. Käyttäjien opiskelijanumero näkyy ainoastaan Moodlea opettajaroolissa käyttäville henkilöille. Lisäksi rekisterin henkilötietojen käsittelyä on ulkoistettu toimeksiantosopimuksella, jonka palveluntarjoajana toimii Mediamaisteri Oy. (TUNI Moodle n.d.b.)

Käyttämättömien kurssialueiden poistamiseen on käytössä automaatiinen poistoprosessi. Kurssialueet, joiden päättymispäivämäärästä on yli 12 kuukautta tai joilla ei ole lainkaan käyntejä yli 24 kuukauteen poistetaan automaattisesti. Myös manuaalinen poistaminen on mahdollista, mutta poistamisessa tulee ottaa huomioon TAMKin tiedonohjaussuunnitelman ohje, jonka mukaan opiskelijatöitä tulee säilyttää 6–12 kuukautta loppuarvioinnin jälkeen. (TUNI Moodle n.d.c.) Moodleen kytketyissä ulkoisissa palveluissa saattaa olla myös muunlaisia säilytysaikoja. Opiskelutietoja säilytetään Tampereen korkeakouluyhteisön asiakirjahallinnon suunnitelman mukaisesti ja ne perustuvat voimassa olevaan lainsäädäntöön. Esimerkiksi pysyvästi säilytetään rekisteröidyn opiskelijanumero, etu- ja sukunimi, käyttäjätunnus, sähköpostiosoite ja maa. (TUNI Moodle n.d.b; Opiskelijan tietosuojailmoitus 2024, 6.)

5 TUNI MOODLEN TIETOSUOJAN VAIKUTUSTENARVIOINTI

5.1 Vaikutustenarvioinnin tarpeen arviointi ja toteutus

Tietosuojan vaikutustenarviointi tulee tehdä, jos henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille. Tietosuojavaltuutetun toimisto on määritellyt kriteerit, joiden avulla voidaan arvioida, onko kyseessä tietosuoja-asetuksen mukainen korkea riski. (Tietosuojavaltuutetun toimisto n.d.c.) Näitä kriteereitä on tarkasteltu luvussa 3.2. TUNI Moodlen henkilötietojen käsittely täyttää ainakin kolme korkean riskin kriteeriä, minkä vuoksi vaikutustenarviointi on tarpeen. Ensinnäkin Moodlea käytetään opiskelijoiden arviointiin ja pisteytykseen. Toiseksi käsiteltävät henkilötiedot koskevat heikossa asemassa olevia rekisteröityjä, sillä opiskelijat ovat opettajiin nähden ja opettajat työnantajaan nähden heikommassa asemassa.

Kolmas korkean riskin kriteeri on laajamittainen henkilötietojen käsittely, sillä Moodlessa on noin 10 000 käyttäjäprofiilia (TUNI Järjestelmäsalkku 2024). Tietosuoja-asetuksessa ei ole määritelty termiä ”laajamittainen”, mutta sen aiemmassa versioluonnoksessa katsottiin laajamittaiseksi toiminta, jossa 12 kuukauden aikana käsitellään yli 5000 rekisteröidyn henkilötietoja (Bu-Pasha 2020, 399). Lisäksi tietosuojavastaava Hinkka (2025) tuo esiin seikan, jota ei ole mainittu Tietosuojavaltuutetun toimiston kriteereissä, mutta saattaa aiheuttaa korkean riskin rekisteröidyn oikeuksille. Moodlessa on avoimen kentän ongelma erityisesti erityisiin tietoryhmiin liittyviin henkilötietoihin liittyen. Moodlea käyttäessään opiskelijat saattavat itse jakaa arkaluonteista sisältöä esimerkiksi keskustelualueilla.

Vaikutustenarvioinnin toteutustapa on vapaa ja moni yritys tarjoaa niiden toteutukseen ja päivittämiseen erilaisia palveluja ja työkaluja. Tietosuojavaltuutetun toimisto on laatinut kaikille saatavilla olevan ohjeistuksen sekä Excel-työkalun vaikutustenarvioinnin tekemiseen. Tässä opinnäytetyössä tehty vaikutustenarviointi Moodlesta on laadittu Tietosuojavaltuutetun toimiston ohjeita noudattaen ja kirjattu heidän laatimaansa Exceliin. Excel-tiedosto on tarkoitettu TAMKin sisäiseen käyttöön ja ei ole julkinen. Raportissa kuvataan kuitenkin vaikutustenarvioinnin sisältö keskeisiltä osin ja tiivistetysti.

Kirjaamistyökalussa vaikutustenarviointi on jaettu eri vaiheisiin. Ensin kuvataan vaikutustenarvioinnin kohteena oleva ohjelmisto Moodle. Kuvauksessa käydään läpi tämän raportin neljännessä luvussa käsiteltyjä aiheita: Moodle yleisesti, henkilötietojen käsittelyn oikeusperuste, tarkoitus ja tavoite, käsiteltävät henkilötiedot ja niiden elinkaari sekä käsittelyn tekninen toteutus. Seuraavaksi arvioidaan, onko käsittely tietosuoja-asetuksen mukaista. Tähän vaiheeseen sisältyy henkilötietojen käsittelyn tarpeellisuuden ja oikeasuhtaisuuden sekä tietosuojaperiaatteiden ja -oikeuksien toteutumisen tarkastelu. Vaikutustenarvioinnin seuraavassa vaiheessa tunnistetaan henkilötietojen käsittelyyn liittyvät riskit tunnistamalla uhat ja arvioimalla niiden vaikutukset ja vakavuus rekisteröidylle. Lopuksi käydään läpi jatkotoimenpiteet vaikutustenarvioinnissa ilmenneiden havaintojen pohjalta ja nimetään vastuutahot toimenpiteiden toteuttamiseksi.

Vaikutustenarvioinnin tekemisessä on hyödynnetty EU:n tietosuoja-asetusta sekä muuta soveltuvaa lainsäädäntöä, kuten tietosuojalakia ja ammattikorkeakoululakia. Lähdemateriaalina on käytetty TUNI Moodlen sekä Moodlen yleistä tietosuojaselostetta (*Moodle Privacy Notice*), TUNIn opiskelijoiden ja henkilöstön tietosuojailmoituksia sekä Turnitin tietosuojaselostetta. Lisäksi arvioinnissa on hyödynnetty TUNIn verkkosivujen tietosuojaosiota sekä TAMKin sisäistä järjestelmäsalkkua, johon on kirjattu Moodlen käsittelytoimet. Tietosuoja-asetuksen 39 artiklan mukaan tietosuojavastaavan tulee auttaa vaikutustenarvioinnin laatimisessa. TUNI Moodlen vaikutustenarviointiin tuokin syvyyttä ja käytännön näkökulmaa tietosuojavastaava Hinkan asiantuntijahaastattelut.

5.2 Tietosuojasääntelyn noudattamisen arviointi

5.2.1 Tietosuojaperiaatteiden noudattaminen

TUNI Moodlessa henkilötietojen käsittely on välttämätöntä, jotta opettajille voidaan tarjota työvälineitä työtehtävien hoitamiseksi ja opiskelun mahdollistamiseksi. Henkilötietojen käsittely on välttämätöntä käyttäjätilien hallinnoimiseksi, opintosuoritusten kirjaamiseksi ja viestinnän mahdollistamiseksi kurssien sisällä. Moodlessa arvioidaan myös opintosuorituksia, joten opiskelijoiden identiteetti tu-

lee varmistaa. Moodlessa henkilötietojen käsittely perustuu oppilaitoksen lakisääteisiin velvoitteisiin sekä rekisteröidyn suostumukseen. Suostumus tapahtuu, kun korkeakouluyhteisön järjestelmien käyttäjä hyväksyy tietojen ja tietojärjestelmien tietoturva- ja vaitiolositoumuksen kirjautuessaan ensimmäistä kertaa TUNI-ympäristöön.

TAMKilla on erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelylle poikkeusperuste, kun käsitellään henkilökohtaisiin opintojärjestelyihin liittyviä tietoja yhdenvertaisuuslain (1325/2014) 6 § toteuttamiseksi (Opiskelijan tietosuojailmoitus 2024). Moodlessa erityisiin henkilötietoryhmiin kuuluvia tietoja ei saa käsitellä lainkaan ja kyseessä on virhe, jos oppilas ohjataan kertomaan tai oppilas omaaloitteisesti kertoo arkaluonteista tietoa. Hinkka (2025) mainitsee, että esimerkiksi opettajakoulutuksen puolella on riski arkaluonteisen tiedon käsittelyyn, sillä opetuksessa käsitellään paljon henkilökohtaista kasvua. Myöskään henkilötunnuksia tai rikostuomioihin liittyviä tietoja ei käsitellä Moodlessa. Hinkan mukaan jälkimmäiseen on sosiaalipuolella teoriassa mahdollisuus, mutta sekin on kiellettyä.

Verkko-oppimisympäristön etuna on, että kaikki kurssimateriaalit, tehtävät, tentit ja keskustelualueet ovat keskitetysti yhdessä paikassa. Tämä parantaa tiedonhallintaa ja tukee opetuksen saatavuutta sekä joustavuutta. Moodlen käyttö vähentää manuaalisen rekisterinhallinnan tarvetta, mikä voi osaltaan vähentää tietoturvariskejä. Kun arvioidaan, voisiko samoihin opetuksellisiin tavoitteisiin päästä henkilötietojen suojaan vähemmän puuttuvilla keinoilla, voidaan todeta, että opetuksen järjestäminen täysin analogisesti ei todellisuudessa vähentäisi henkilötietojen käsittelyä. Sen sijaan digitaalinen ratkaisu tarjoaa organisaatiolle paremmat mahdollisuudet suojata ja hallita henkilötietoja. Kuitenkin tietosuojan parantamiseksi voitaisiin tutkia esimerkiksi pseudonymisoinnin hyödyntämistä tenttitilanteissa, jolloin opettaja voisi arvioida vastauksia ilman opiskelijan henkilökohtaisia tunnistetietoja. (Hinkka 2025.)

Läpinäkyvyydestä huolehditaan informoimalla rekisteröityä henkilötietojen käsittelystä hänen kirjautuessaan ensimmäistä kertaa TUNI-ympäristöön. Jatkoinformointi tapahtuu tietosuojailmoituksilla. Moodlessa oppimisalustan alaosassa on linkki ”Sivuston käytänteet”, jonka kautta saa yhteenvedon käyttöehdoista ja josta

pääsee myös opiskelijan tietosuojailmoitukseen. Moodlen omaan tietosuojaselosteeseen pääsee etusivun ”Tietoja sivustosta” -kohdan kautta. Tiedot ovat helpohkosti löydettävissä, mutta tietosuojaselosteeseen tulisi päästä suosituksen mukaan jokaiselta sivuston sivulta ja linkissä tulee käyttää yleisesti tunnettua nimitystä, kuten tietosuojaseloste, tietosuoja, yksityisyys tai yksityisyyden suoja (Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat 2018, 8).

Tietosuojaseloste on tiivis, selkeä ja helposti ymmärrettävä. Siinä on hyödynnetty kerroksellista rakennetta viittaamalla EU:n tietosuoja-asetukseen ja Tampereen korkeakouluyhteisön asiakirjahallinnon suunnitelmaan. ”Sivuston käytänteet” -välilehden kautta käyttäjät voivat tutustuta TUNin tarkempaan tietosuojainformaatioon ja saavutettavuusselosteeseen. TUNI Moodlen tietosuojaselosteen päivityskäytännöistä ei ole saatavilla tarkkaa tietoa. Sen sijaan Moodlen yleistä tietosuojaselostetta päivitetään yhteisön, asiakkaiden, asiaankuuluvien viranomaisten, teollisuuden tai muiden sidosryhmien palautteen perusteella. Päivityksiä tehdään myös tuotteiden, palveluiden ja tietojenkäsittelykäytäntöjen muuttuessa. (Moodle 2024c.)

Henkilötietojen käsittelyn käyttötarkoitus on yksilöity ja dokumentoitu TAMKin järjestelmäsalkkuun ”Rekisterinpitäjän selosteeksi käsittelytoimista” ja niiden kriittisyys on arvioitu (TUNI Järjestelmäsalkku 2024). Käsittelyn pysyminen käyttötarkoituksen mukaisena varmistetaan opettajien koulutuksella ja tietojenkäsittelysopimuksilla. Lisäksi opiskelijat pystyvät matalalla kynnyksellä ilmiantamaan organisaatiossa ylöspäin mahdolliset tietosuojarikkeet. Henkilötietojen jatkokäsittelyä ei käytännössä pitäisi olla, mutta korkeakouluyhteisössä tapahtuu yleisen edun mukaista arkistointia. (Hinkka 2025.)

Moodlen käyttöön tarvittavat henkilötiedot on minimoitu, eikä palvelun toteuttaminen ole mahdollista ilman niitä. Lisäksi henkilöstöä ohjeistetaan ja koulutetaan minimoimaan henkilötietojen tarpeeton käsittely. Moodlessa on käytössä vapaakenttiä esimerkiksi keskustelualueilla ja tehtävän palautusten yhteydessä. Koska niiden käyttöä ei ole erikseen ohjeistettu, on mahdollista, että käyttäjät syöttävät niihin tarpeettomia henkilötietoja. Oppilaille toisilleen näkyviä aineistoja voidaan pseudonymisoida esimerkiksi tilanteessa, jossa opettaja haluaa havainnollistaa

ryhmän arvosanojen jakautumisen ilman, että yksittäisiä opiskelijoita voidaan tunnistaa. Moodlessa ei ole tiedossa, miten henkilötietojen anonymisointia voitaisiin toteuttaa. (Hinkka 2025.)

Henkilötietojen käsittelyä minimoidaan myös ajallisesti. Moodlessa itsessään ei ole lakisääteisiä henkilötietojen säilytysaikoja, mutta esimerkiksi opiskelutietoja säilytetään voimassa olevaan lainsäädännön mukaisesti. Käyttämättömien kurssialueiden poistamiseen käytetään automaattista poistoprosessia, joka on kuvattu aiemmin raportissa luvussa 4.2.3. Koska kurssien poistoajat ovat lyhyitä, tietojen ajantasaisuuden ja täsmällisyyden varmistaminen ei muodostu haasteeksi. Rekisteröidyt vastaavat itse siitä, että heidän korkeakoululle ilmoittamansa tiedot ovat oikeat ja ajantasaiset. Tietojen oikaisua koskevissa tilanteissa noudatetaan TAMKin tietopyyntöprosessia. Moodleen ei myöskään syötetä tietoja opiskelijan puolesta ainakaan tunnetuissa käyttötarkoituksissa. (TUNI n.d.a; TUNI n.d.b; Hinkka 2025.)

Moodlen henkilötietojen luottamuksellisuus ja eheys turvataan luvussa 2.3.3. käsiteltävillä suojausperiaatteilla, jotka estävät tietojen luvattoman katselun ja käsittelyn. Vaikutustenarvioinnissa tulee myös ottaa huomioon tietojen käytettävyys, vaikka sitä ei erikseen mainita tietosuojaperiaatteena. Rekisterinpitäjän tulee varmistaa, että henkilötiedot ovat käytettäessä aina, kun niitä tarvitaan. (Tietosuojan vaikutustenarvioinnin ohje 2021, 16.) Moodlen käytettävyyttä tukee sen pilvipalveluominaisuus, joka muun muassa mahdollistaa Moodlen käytön missä tahansa maailmaa sekä parantaa sen tietoturvaa varmuuskopioinneilla, palautuspalveluilla ja suojausprotokollilla (Mollik n.d.). Lisäksi TUNIlla on oma tietohallinto, jonka etuna on nopea reagointikyky ongelmatilanteissa ja syvällinen ymmärrys organisaation toiminnasta ja kulttuurista (It-ulkoistus vs. sisäinen tiimi. n.d.) Jos Moodle joutuu tietoturvaloukkauksen kohteeksi, toimitaan TUNIn ennalta määritellyn menettelytavan mukaisesti. Tietoturvaloukkauksen seurauksena järjestetään selvitystilaisuus ja tietosuojavastaava tekee riskiarvioinnin koskien ilmoitusvelvollisuutta tietosuojaviranomaisille ja/tai rekisteröidylle. (TUNI n.d.c.)

5.2.2 Henkilötietojen käsittelijät ja kansainväliset siirrot

Henkilötietoja käsittelevät pääasiassa koulutus ja jatkuva oppiminen- sekä tieto ja digitalisaatio -palvelualueiden henkilöstö (Opiskelijan tietosuojailmoitus 2024, 4). Henkilötietojen käsittelyä on myös ulkoistettu toimeksiantosopimuksella Mediamaisteri Oy:lle (TUNI Moodle n.d.b). Lisäksi henkilökuntaan kuulumaton voi olla resurssisopimuksella käsittelijä ja ulkoisten käsittelijöiden, eli Zoomin, Turnitin ja Panopton kanssa on tehty tietojenkäsittelysopimukset (Hinkka 2025). Sopimuksilla varmistetaan, että henkilötietojen käsittelijät täyttävät EU:n tietosuoja-asetuksen heille asettaman velvoitteet. Käsittelijät sitoutetaan myös korkeakouluyhteisön edellyttämiin tietoturvavaatimuksiin ja heidän toimintatapojaan arvioidaan säännöllisesti. Käsittelyyn osallistuvat vain ne henkilöt, joiden osallistuminen on tarpeen käsittelytoimen tarkoituksen toteuttamiseksi ja käyttöoikeudet rajataan asianmukaisesti. (TUNI n.d.a.) Rekisterinpitäjän alaisuudessa toimivia työntekijöitä, jotka käsittelevät henkilötietoja osana työtehtäviään, ei lueta käsittelijöiksi (Tietosuojan vaikutustenarvioinnin ohje 2021, 18.)

Moodlen tietosuojaselosteen mukaan henkilötietoja siirretään ETA-alueen ulkopuolelle käytettäessä Zoom-videotapaamispalvelua ja Turnitin-alkuperäisyystarkastuspalvelua. Järjestelmien käyttöliittymät sijaitsevat EU:n ja ETA:n ulkopuolella, mutta ne noudattavat Tampereen korkeakouluyhteisön tietoturvakäytäntöjä. TUNIn käytössä oleva Zoom-palvelu on lisäksi toteutettu yhdessä NORDUnetin kanssa, mikä toimii kokonaisuudessaan EU:ssa (Zoom-palvelun tietosuoja ja turvallisuus 2024). Turnitin Feedback Studio -instanssi sen sijaan siirtää tietoja Yhdysvaltoihin. Turnitin suojaa henkilötietoja EU-U.S. Data Privacy Frameworkin mukaisesti, joka täyttää Euroopan komission 10.7.2023 antaman päätöksen mukaisesti Yhdysvaltojen tietosuojan riittävästä tasosta. (Turnitin-järjestelmän tietosuojaseloste 2020.) Yhdysvaltojen presidentti Trump on kertonut purkavansa kyseisen järjestelyn (O’Regan & Ng 2025).

5.2.3 Rekisteröidyn oikeuksien toteuttaminen

TUNI Moodlen käyttäjillä on EU:n yleisen tietosuoja-asetuksen mukaiset rekisteröidyn oikeudet. Jos rekisteröity haluaa käyttää oikeuksiaan, ensisijaisesti tulee olla yhteydessä henkilötietoja käsittelevään organisaatioon eli rekisterinpitäjään. TUNI Moodlen tapauksessa noudatetaan rekisterinpitäjän tietopyyntöprosessia ja pyynnöt toimitetaan Tampereen ammattikorkeakoulun tai yliopiston asiointipalveluun. Rekisteröidyn pitää toimittaa tietopyyntö itse ja hänen henkilöllisyytensä varmistetaan ennen pyynnön toteuttamista. Pyyntöön on vastattava ilman aiheetonta viivytystä viimeistään kuukauden kuluttua sen vastaanottamisesta. Jos tietopyyntöä ei voida toteuttaa, tulee kieltäytyminen perustella. (Tietosuojavaltuutetun toimisto n.d.e; TUNI n.d.d.)

Rekisteröidyllä on oikeus saada pääsy henkilötietoihin eli oikeus saada tietää muun muassa käsitelläänkö hänen henkilötietojaan, mitä henkilötietoja hänestä on tallennettu ja mistä henkilötiedot on saatu. Omien tietojen tarkastusoikeus mahdollistaa myös muiden tietosuojaoikeuksien käytön, kuten oikeuden tietojen oikaisemiseen tai poistamiseen. (TUNI n.d.d.) TUNI Moodlessa käyttäjä pääsee henkilökohtaisilla tunnuksillaan itse tarkastelemaan kootusti omia käyttäjätietojaan sekä keskustelunavauksiaan ja keskusteluviestejään.

Rekisteröidyllä on myös oikeus vaatia ilman aiheetonta viivytystä häntä koskevien virheellisten, puutteellisten tai epätarkkojen henkilötietojen oikaisua tai täydennystä. TUNI Moodlessa käyttäjä voi omilla tunnuksillaan oikaista kaikkia muita tietojaan, paitsi Haka-kirjautumisen yhteydessä haettuja tietoja. Poikkeustapauksissa rekisteröidyllä on myös oikeus saada henkilötietonsa kokonaan poistettua rekisterinpitäjän rekisteristä. Oikeutta tietojen poistoon ei ole, kun tietojen käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. (TUNI n.d.d; TUNI Moodle n.d.b.) TUNI Moodlessa käyttäjä voi poistaa osan tiedoista itse. Esimerkiksi tehtävien palautuksia voi poistaa, mutta keskustelualueen viestejä ei. Jos rekisteröity haluaa poistaa tietoa, mitä ei itse pysty poistamaan, tulee hänen tehdä rekisteröidyn oikeuksien käyttämistä koskeva pyyntö.

Jos rekisteröity on ilmoittanut virheellisistä tai puutteellisista tiedoista, hänellä on oikeus pyytää henkilötietojensa rajoittamista, kunnes hänen tietonsa ovat asianmukaisesti tarkastettu, korjattu tai täydennetty. Rekisteröidyllä on myös henkilökohtaiseen erityiseen tilanteeseen perustuva oikeus vastustaa henkilötietojensa käsittelyä. Tällöin tietoja voidaan käsitellä edelleen vain, jos käsittelylle voidaan osoittaa huomattavan tärkeä ja perusteltu syy. Tietyissä tilanteissa rekisteröidyllä on lisäksi oikeus siirtää tiedot järjestelmästä toiseen. Henkilöllä on tällöin oikeus saada hänen toimittamansa henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa. Oikeus ei koske sellaista henkilötiedon käsittelyä, joka on tarpeen rekisterinpitäjän lakisääteisen velvoitteen täyttämiseksi tai yleistä etua koskevan tehtävän suorittamiseksi. (TUNI Moodle n.d.b; Opiskelijan tietosuojailmoitus 2024, 8.)

Jos rekisteröity katsoo, että hänen henkilötietojensa käsittelyssä toimitaan EU:n yleisen tietosuoja-asetuksen vastaisesti, hänellä on oikeus tehdä valitus valvontaviranomaiselle eli tietosuojavaltuutetulle. Lisäksi rekisteröidyllä on oikeus käyttää hallinnollisia muutoksenhakukeinoja ja muita oikeussuojakeinoja. Rekisteröidyllä on myös oikeus saada rekisteröidyn oikeuksiin liittyvää neuvontaa tietosuojavastaavalta. (TUNI n.d.d; TUNI Moodle n.d.b.)

5.3 Riskien arviointi

5.3.1 Uhkien tunnistaminen

TUNI Moodlen uhkia kartoitettiin perehtymällä yleisimpiin käytännön tietosuojariskeihin, joita ovat käyttöoikeuksien ja käsittelyvaltuuksien hallinnan puutteet, liian vähäinen henkilötietojen ja niiden käsittelyssä käytettävien tietojärjestelmien käyttökoulutus henkilöstölle, huono sopimus- ja hankintaosaaminen, tietojen luovutukset sekä tietosuojattavan jätteen käsittelyprosessin puutteet (Andreasson & Ylipartanen 2022, luku 4.2.) Lisäksi hyödynnettiin tietosuojavastaava Hinkan asiantuntijahaastattelua.

Tämän jälkeen uhkien tunnistamisessa hyödynnettiin Tietosuojavaltuutetun toimiston Excel-työkalun uhkataulukkoa (taulukko 1). Kokonaan täytetty taulukko on ainoastaan TAMKin sisäiseen käyttöön ja raportissa esitetty osittain täytetty uhkataulukko on tarkoitettu selventämään uhkien tunnistamisen prosessia. Taulukossa esitetään henkilötietojen käsittelyn elinkaaren eri vaiheet sekä tietosuojaperiaatteet, joiden toteutumiseen mahdolliset uhat voivat kohdistua. Uhkataulukko käytiin systemaattisesti läpi kohta kohdalta, arvioiden mahdollisia riskejä kunkin tietojen käsittelyn vaiheen osalta. Kaikissa kohdissa ei tunnistettu uhkia, kun taas tietyt uhat koskivat useampaa tietosuojaperiaatetta tai käsittelyn vaihetta. Esimerkiksi uhka ”Opettaja ei osaa soveltaa tietosuojasääntelyä yleisellä tasolla.” voi vaikuttaa lainmukaisuus- ja kohtuullisuusperiaatteeseen useassa eri elinkaaren vaiheessa, kuten tietojen keräämisvaiheessa tai niiden käytön ja muokkaamisen vaiheessa.

TAULUKKO 1. Uhkataulukko (Tietosuojan vaikutustenarvioinnin työkalu n.d.).

	Tietosuojaperiaatteet							
Tietojen käsittelyn elinkaaren vaihe	Lainmukaisuus ja kohtuullisuus	Läpinäkyvyys	Käyttötarkoitus-sidonnaisuus	Minimointi ja säilytysaikojen rajoittaminen	Täsmällisyys	Eheys	Luottamuk-sellisuus	Käytettävyys
Kerääminen	Opettaja ei osaa soveltaa tietosuojasääntelyä .							
Tallentaminen								
Yhdistäminen								
Käyttö ja muokkaaminen	Opettaja ei osaa soveltaa tietosuojasääntelyä .							
Luovutus ja saataville asettaminen								
Siirtäminen 3. maihin ja muut siirtotilanteet								
Säilyttäminen								
Hävittäminen								

Uhkien tunnistamisen jälkeen arvioitiin niiden vaikutuksia ja seurauksia rekisteröidyn oikeuksille ja vapauksille. Vaikutusten vakavuus ja todennäköisyys arvioitiin numeerisesti asteikolla, jossa vakavuus vaihteli vähäisestä kriittiseen ja todennäköisyys epätodennäköisestä lähes varmaan (taulukko 2). Näiden arvioiden perusteella muodostettiin riskiluku, joka kuvaa riskin tasoa asteikolla vähäisestä erittäin korkeaan. Taulukossa esitetään riskiluvut ennen suojatoimenpiteitä ja suojatoimenpiteisiin ryhtymisen jälkeen. Suojatoimenpiteiden jälkeisistä riskiluvuista voidaan päätellä, että Moodlen tietosuojaan kohdistuvat riskit jäävät vähäiselle tasolle. Tämän vuoksi tietosuoja-asetuksen 36 artiklan mukaiseen tietosuojaviranomaisen ennakkokuulemiseen ei ole tarpeen ryhtyä.

TAULUKKO 2. Moodlen riskien tunnistaminen ja arviointi.

Vakavuus: 1 = vähäinen 2 = kohtalainen 3 = merkittävä 4 = kriittinen **Todennäköisyys**: 1 = epätodennäköinen 2 = mahdollinen 3 = todennäköinen 4 = lähes varma **Riskiluku** 1–6 = vähäinen tai kohtalainen riski 7–12 = korkea tai erittäin korkea riski	**Ennen suojatoimenpiteitä**			**Suojatoimenpiteiden jälkeen**		
Uhka	**Vakavuus**	**Todennäköisyys**	**Riskiluku**	**Uusi vakavuus**	**Uusi todennäköisyys**	**Uusi riskiluku**
Erityisiin tietoryhmiin kuuluvaa tietoa kirjoitetaan keskustelualueelle.	3	2	6	3	1	3
Vapaaehtoisiin tietokenttiin syötetään tarpeettomia henkilötietoja. (Näkyvissä vain opettajalle.)	2	2	4	2	1	2
Opiskelija tallentaa materiaalia itselleen.	3	3	**9**	3	1	3
Toinen Haka-verkon jäsen saa oikeudetta haltuunsa jonkin kurssialueen avaimen.	3	2	6	3	1	3
Opettaja pseudonymisoi julkisella opiskelijanumerolla.	3	3	**9**	3	1	3
Opettaja ei osaa soveltaa tietosuojasääntelyä yleisellä tasolla.	3	1	3	2	1	2
Opettaja arvioi syrjivällä tai muutoin laittomalla perusteella.	3	2	6	2	1	2
Kansainvälisistä siirroista ei ole siirtojen vaikutustenarvioita.	3	2	6	3	1	3
Moodle joutuu tietomurron kohteeksi.	3	1	3	3	1	3
Moodle joutuu palvelunestohyökkäyksen kohteeksi.	2	2	4	1	1	1

Uhkien kartoittamisen jälkeen havaittiin, että TUNI Moodlen kohdistuvat uhat voidaan jakaa organisaation sisäisiin ja ulkopuolisiin aiheuttajiin. Sisäiset aiheuttajat tarkoittavat tässä tapauksessa organisaation henkilökuntaa ja opiskelijoita. Ulkoisilla aiheuttajilla taas tarkoitetaan esimerkiksi valtuutettuja kolmansia osapuolia sekä rikollisia ja hakkereita.

5.3.2 Sisäiset uhat

Vaikeimmin ennakoitavat riskit Moodlen henkilötietojen käsittelyssä liittyvät aiemmin mainittuun avoimen kentän ongelmaan. Opiskelijat saattavat itse syöttää keskustelualueille tai vapaaehtoisiin tietokenttiin tarpeettomia tai erityisiin tietoryhmiin kuuluvia henkilötietoja. Opiskelijat saattavat jakaa terveystietojaan kertomalla esimerkiksi omista mielenterveysongelmistaan alueilla, jotka ovat muille opiskelijoille nähtävissä. Tietojen jakamisella voi olla merkittäviä seurauksia rekisteröidylle, kuten mainehaittaa ja ihmissuhdeongelmia henkilökohtaisessa sekä ammatillisessa elämässä. Tietojen päätyminen muille opiskelijoille voi myös altistaa kiusaamiselle, häirinnälle tai jopa kiristämisen uhriksi joutumiselle.

Riskiä voidaan pienentää lisäämällä avoimiin kenttiin tarkentavaa ohjeistusta, kuten kehotus välttää arkaluonteisen tiedon sekä tarpeettomien henkilötietojen kirjoittamista. Uhan toteutumisen todennäköisyyttä voidaan hallita myös kouluttamalla opettajia siten, että he ottavat riskin huomioon opetuksen suunnittelussa ja välttävät sellaisia harjoituksia ja tehtäviä, joissa opiskelija saattaisi jakaa henkilökohtaisia tietojaan. Taulukosta 2 nähdään, että näillä suojatoimenpiteillä riskiluku saadaan laskettua vähäiselle tasolle.

Merkittävänä riskinä voidaan pitää myös tilanteita, jossa opettaja ei osaa soveltaa tietosuojasääntelyä. Tämä voi altistaa vahingossa tapahtuville tietosuojaloukkauksille, heikentää oppilaitoksen mainetta ja jopa velvoittaa organisaation sanktioihin. Opettaja voi esimerkiksi pseudonymisoida käyttämällä opiskelijanumeroa havainnollistaessaan kurssin arvosanojen jakautumista. Opiskelijanumerot ovat julkisia, joten pseudonymisointi on helppo purkaa. Käytäntö on joillakin opettajilla yleisesti käytössä, eli uhan toteutuminen on todennäköistä. Arvosanojen paljastuminen voi tuoda rekisteröidylle niin ikään mainehaittaa ja altistaa kiusaamiselle.

Lisäksi se voi aiheuttaa yksityisyyden loukkaamisen tunnetta. Riskiä opettajien tietosuoja-asetuksen vastaiselle toiminnalle voidaan merkittävästi alentaa pakollisilla tietosuojakoulutuksilla ja käytännön soveltamisen ohjeistuksella. Erikseen tulee myös kieltää pseudonymisointi opiskelijanumerolla ja neuvoa opettajille pseudonymisoinnin oikeaoppinen toteutus.

TUNI Moodlen käytössä voi olla riski myös opettajien syrjivästä arvioinnista, mikä voi aiheuttaa opiskelijan oikeusturvan heikentymistä ja epätasa-arvoista kohtelua. Epäoikeudenmukainen arviointi voi aiheuttaa myös oppimistulosten vääristymää ja siten heikentää opiskelijan tulevaisuuden mahdollisuuksia. Uhka liittyy tietojen minimoinnin periaatteeseen, sillä tenttiä tai tehtävää arvioidessa opettajan ei ole tarpeen tietää esimerkiksi suorituksen tekijän nimeä. Verkkoympäristössä riskiä voitaisiin hallita teknisin ratkaisuin, kuten toteuttamalla tenttien ja tehtävien arviointi siten, että opiskelijan henkilöllisyys varmistetaan, mutta se pysyy opettajalle anonyymina. Lisäksi riskiä voidaan vähentää määrittelemällä arviointikriteerit selkeästi ja läpinäkyvästi sekä varmistamalla opiskelijoiden asianmukaiset oikeusturvakeinot. (Hinkka 2025.)

Uhkamaisemaan kuuluu myös säilytyksen rajoittamiseen liittyviä ongelmia: opiskelijat saattavat tallentaa opetusmateriaalia tai muiden opiskelijoiden lisäämiä tiedostoja ja viestejä itselleen. Jotkin tiedostotyypit latautuvat avatessa automaattisesti laitteeseen. Nämä materiaalit saattavat sisältää henkilötietoja tai ne saattavat olla tekijänoikeuden alaisia. Tähän uhkaan liittyy samoja jo aiemmin mainittuja riskejä rekisteröidylle, mutta myös organisatorinen riski. Tekijänoikeuden alaisten tietojen luvaton tallentaminen ja jakaminen saattaa rikkoa immateriaalioikeuksia ja aiheuttaa erilaisia oikeudellisia ja taloudellisia seuraamuksia organisaatiolle tai rekisteröidylle. Kuten taulukosta 2 nähdään, riskiluku nousee korkealle tasolle. Riskiä voidaan alentaa estämällä tekijänoikeuden alaisten tiedostojen lataus teknisesti tai vesileimaamalla materiaalit ja lisäämällä niihin muistutus käyttöehdoista. Tietosuojakoulutukseen tulee sisällyttää myös tekijänoikeudellinen ja vastuullisen tiedonhallinnan näkökulma.

Kohtalaisen riskin rekisteröidyn oikeuksille ja vapauksille voi myös muodostaa tilanne, jossa kurssin ulkopuolinen Haka-verkon jäsen saa haltuunsa kurssialueen avaimen ja pääsee luvatta tarkastelemaan toisten tietoja. Riskiä voidaan hallita tehokkaammin rajoittamalla pääsy vain niille, joilla on perusteltu syy osallistua kurssille. Vilpillinen kurssialueelle liittyminen lisää tietojen väärinkäytön todennäköisyyttä. Riskin minimoimiseksi kurssiavaimet tulee vaihtaa säännöllisesti ja jakaa vain rajoitetulle joukolle. Suositeltavaa on, että kurssialueelle pääsee vain kurssi-ilmoittautumisen kautta tai opettajan lisäämänä. Jos kurssiavainta käytetään, tulee opiskelijoita erikseen kieltää jakamasta sitä.

5.3.3 Ulkoiset uhat

10 000 käyttäjäprofiilin tietokanta saattaa olla kiinnostava kohde tietomurtoyrityksille (TUNI järjestelmäsalkku 2024). Nykyisten suojaustoimenpiteiden ansiosta tietomurron todennäköisyys on vähäinen, mutta sen tapahtuessa vaikutukset rekisteröityyn voivat olla merkittävät. Rekisteröidylle voi lievimmillään aiheutua esimerkiksi asian selvittämisestä johtuvaa ajanhukkaa ja hän voi saada suuria määriä roskapostia. Vakavia seurauksia voi olla esimerkiksi identiteettivarkaus, muiden käyttäjätilien murtaminen sekä tietojen yhdistäminen muihin vuodettuihin tietoihin. Tietomurron riskiä voidaan vähentää monilla teknisillä toimenpiteillä, kuten monivaiheisella tunnistautumisella, tiedonsiirron salauksella ja varmuuskopioinnilla. Lisäksi tietosuojakoulutus ja selkeä toimintasuunnitelma tietomurron varalta alentavat riskilukua. Suojausta voidaan myös arvioida haavoittuvuustestauksilla, joiden avulla voidaan tunnistaa ja korjata järjestelmän mahdollisia tietoturvaheikkouksia.

Traficomin Kyberturvallisuuskeskuksen (2024) mukaan palvelunestohyökkäykset ovat lisääntyneet Suomessa. Palvelunestohyökkäyksien tarkoituksena on estää käyttäjien pääseminen verkkopalveluun ja myös TUNI Moodle voi joutua niiden kohteeksi. Uhan toteutuminen voi häiritä tai estää opiskelijoiden ja opettajien työskentelyä ja aiheuttaa opintojen viivästymistä. Palvelunestohyökkäyksiä voidaan ennaltaehkäistä suojaamalla palvelut torjuntaohjelmistoilla ja laatimalla sel-

keät toimintaohjeet hyökkäystilanteita varten. Lisäksi tulee varmistaa vaihtoehtoisten järjestelmien tai menetelmien saatavuus opetuksen jatkamiseksi sekä viestiä niistä käyttäjille tietoturvapoikkeaman sattuessa.

Rekisteröidyn henkilötietoja siirretään EU- ja ETA-alueen ulkopuolelle Zoom-videotapaamispalvelun ja Turnitin-alkuperäisyystarkastuspalvelun käytön yhteydessä. Näille siirroille ei ole kuitenkaan tehty vaikutustenarviointeja, mikä muodostaa rekisteröidyn oikeuksille ja vapauksille kohtalaisen riskin (Taulukko 2). Puuttuvat vaikutustenarvioinnit tarkoittavat, että kansainvälisistä siirroista aiheutuvia riskejä ei ole tunnistettu ja dokumentoitu asianmukaisesti. Tämän seurauksena henkilötietojen tekniset suojakeinot eivät ole välttämättä tarkoituksenmukaisia ja riittäviä ja henkilötietoja voi esimerkiksi päätyä maihin, joissa ei ole riittävää tietosuojan tasoa. (Hinkka 2025.) Riskilukua voidaan alentaa vähäiselle tasolle laatimalla vaikutustenarvioinnit ja suorittamalla niiden vaatimat toimenpiteet.

5.4 Kehittämisehdotukset ja jatkotoimenpiteet

TUNI Moodlen vaikutustenarvioinnissa havaittiin muutamia jatkotoimenpiteitä oppimisalustan tietosuojan parantamiseksi. Näihin toimenpiteisiin kuuluu muun muassa koulutusta ja ohjeistusta, Moodlen toimintojen parantelua, tietosuojaselosteen päivittämistä ja kansainvälisen tietosuojakehyksen seurantaa. Jatkotoimenpiteet on kirjattu Excel-kirjaamistyökaluun, joka jää TAMKin sisäiseksi dokumentiksi. Excel-tiedostossa on listattu tarvittavat toimenpiteet ja niiden vastuutahot. Toimenpiteille ei ole asetettu tarkkaa määräaikaa, vaan tietosuojavastaava määrittää määräajat tietosuojan hankintamalliin keskusteltuaan prosessinomistajien kanssa (Hinkka 2025).

Opettajille tulee järjestää tietosuojakoulutus koskien Moodlen käyttöä. Koulutuksessa tulee käsitellä tietosuoja-asetuksen soveltamista käytännössä ja korostaa erityisesti vapaan kentän ongelmaa. Opettajien on huomioitava opetuksen suunnittelussa, että erityisiin tietoryhmiin kuuluvia tietoja ei saa käsitellä ja vältettävä tehtäviä, joissa opiskelijat saattaisivat jakaa arkaluonteista tietoa. Lisäksi heille tulee ohjeistaa pseudonymisoinnin oikeaoppinen toteutus. Koulutuksessa tulee

myös käsitellä tietojen minimointiperiaatetta ja opastaa käytännössä, miten tenttitulokset voidaan arvioida niin, että opiskelija pysyy opettajalle anonyymina. Lisäksi tulee käsitellä kurssiavainten hallintaa, kurssille pääsyn käytäntöjä sekä tekijänoikeudellisia näkökohtia. Myös opiskelijoille tulee tarjota ajantasaista tietosuojakoulutusta erityisesti liittyen arkaluonteisten tietojen käsittelyyn ja tekijänoikeuksiin. Samalla on tärkeää käydä läpi opiskelijan tietosuojaoikeudet ja niiden käyttäminen käytännössä. Tietosuojakoulutusten ja ohjauksen vastuutahona toimii tietosuojavastaava Hinkka.

TUNI Moodlen vapaakenttien yhteyteen tulee tehdä lisäohjeistus, joka estää käyttäjiä jakamasta erityisiin tietoryhmiin kuuluvia tietojaan tai muitakaan henkilötietoja. Tämä voitaisiin toteuttaa esimerkiksi varoituskolmiolla ja kehotuksella ”Älä kirjoita kenttään erityisiin tietoryhmiin kuuluvia tietoja.” Kehotukseen yhteyteen voitaisiin myös lisätä ”Lue lisää” -kohta, jonka päälle vietäessä hiiren kursori avaisi lyhyen infotekstin erityisiin henkilötietoryhmiin kuuluvista tiedoista. Näin käyttäjät saisivat selkeän ja ymmärrettävän ohjeistuksen, joka ei jäisi huomaamatta ja tukisi läpinäkyvyysperiaatetta. Lisäksi vapaakenttien määrää tulee minimoida tilanteissa, joissa ne eivät ole välttämättömiä.

Moodleen tulee myös lisätä linkki tietosuojaselosteeseen jokaiselta Moodlen sivulta ja linkin nimitys tulee muuttaa yleisesti tunnetuksi, kuten ”TUNI Moodlen tietosuojaseloste”. Tällä hetkellä tietosuojaselosteeseen ei ole pääsyä lainkaan opiskelijoiden eniten käyttämältä välilehdeltä ”Työpöydältä”. Etusivulta tietosuojaselosteeseen pääsee vain ”Tietoa sivustosta” -linkin takaa, eikä tämä nimitys viittaa mitenkään tietosuojaan. Suosituksen mukaan, rekisteröidylle pitäisi olla välittömästi selvää mistä ja miten rekisteröidylle suunnattu tieto löytyy eikä hänen pidä joutua etsimään tietoa. Lisäksi linkki pitää nimetä yleisesti tunnettua nimitystä käyttäen. (Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat 2018, 8.) TUNI Moodlen tietosuojaseloste tulee siis olla helpommin saatavilla. TUNI Moodlen toiminnallisuuksien päivittämisen vastuutahona toimii Tampereen korkeakouluyhteisön tiedonhallintatiimi.

TUNI Moodlen tietosuojaseloste vaatii myös jatkokehittämistä ja ajantasaistamista. Tietosuojaselosteessa ei ole lainkaan tietoa sen laatimis- tai päivittämisajankohdasta. Tällä hetkellä koko tietosuojaseloste esitetään tiiviissä muodossa,

mutta kuitenkin näytöllä yhdellä kertaa. Suosituksen mukaan tietosuojaselosteissa tulisi hyödyntää monitasoista esitystapaa, jotta vältetään rekisteröidyn informaatioähkyä. Monitasoisuus tarkoittaa sitä, että lukijaa autetaan esimerkiksi linkeillä siirtymään selosteessa suoraan haluamaansa kohtaan. (Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat 2018, 18–19.) Tietosuojaselosteessa voitaisiin myös hyödyntää kerroksellisuutta lisäämällä lukijalle linkkejä, joiden kautta hän saa lisätietoa. Esimerkiksi rekisteröidyn oikeuksien käyttämistä koskevissa pyynnöissä voitaisiin ohjata rekisteröity suoraan oikeaan paikkaan. Tietosuojaselosteen ajantasaisuudesta vastaa tietosuojavastaava Hinkka.

Kuten aiemmin luvussa 5.3.3 kävi ilmi, TUNI Moodle voi olla houkutteleva kohde tietomurtoyrityksille sekä palvelunestohyökkäyksille. Koska Kyberturvallisuuskeskuksen (2024) mukaan erityisesti palvelunestohyökkäykset ovat Suomessa yleistyneet, tulee jatkotoimenpiteenä tarkistaa, että ulkopuolisia hyökkäyksiä koskevat toimintasuunnitelmat ovat ajan tasalla ja tarkoituksenmukaiset. Toimintasuunnitelmien ajantasaisuudesta vastaa TAMKIn tietohallinto. Lisäksi tietohallinto vastaa kansainvälisten tietosiirtojen vaikutustenarviointien tekemisestä. Kuten luvussa 5.2.2 käsiteltiin, kansainvälisiä siirtoja suojataan tällä hetkellä EU-U.S. Data Privacy Frameworkin mukaisesti, mutta sen voimassaolo on epävarmaa. Tietosuojavastaava Hinkka seuraa tämän tietosuojakehyksen voimassaoloa ja ryhtyy tarvittaessa toimenpiteisiin.

Tietosuoja-asetuksen 35 artiklan 11 kohdan mukaan rekisterinpitäjän on tarvittaessa tehtävä vaikutustenarvioinnille uudelleentarkastelu ainakin silloin, jos käsittelytoimien sisältämät riskit muuttuvat Vaikutustenarvioinnin päivittämisen tarvetta suositellaan arvioitavan säännöllisesti ja arviointi on päivitettävä, jos lainsäädäntö tai toimintaympäristö muuttuvat (Korpisaari ym. 2022, 409). Jatkotoimenpiteenä tietosuojavastaava Hinkka vastaa TUNI Moodlen vaikutustenarvioinnin ajantasaisuudesta ja päivittämisen tarpeellisuudesta.

JOHTOPÄÄTÖKSET JA POHDINTA

EU:n yleinen tietosuoja-asetus on monimutkainen ja laaja kokonaisuus, jonka täydellinen noudattaminen vaikuttaa käytännössä mahdottomalta. Yritysten ja organisaatioiden on kuitenkin ollut pakko ottaa sääntely tosissaan, sillä asetuksen rikkomisesta voidaan määrätä huomattavia sakkoja. Esimerkiksi Vastaamon tapauksessa tietosuojavaltuutetun toimiston seuraamuskollegio määräsi psykoterapiakeskukselle 608 000 euron hallinnollisen sakon tietosuoja-asetuksen rikkomisesta (TSV 07.12.2021). Asetus mahdollistaa jopa 20 miljoonaan euron suuruiset sakot, mikä voi olla yritykselle taloudellisesti kestämätöntä. Viimeistään tietosuojan laiminlyönnistä seuraava vakava mainehaitta voi osoittautua kohtalokkaaksi.

Jos tietosuojaan liittyviä ongelmia ilmenee, valvontaviranomaiselle on pystyttävä osoittamaan, että uhka on pyritty asianmukaisesti torjumaan. Tietosuojan vaikutustenarviointi on tässä tärkeä työkalu, sillä se kattaa lähes koko tietosuoja-asetuksen ja ohjaa organisaatioita tarkastelemaan henkilötietojen käsittelyyn liittyvää toimintaansa kokonaisvaltaisesti. Vaikka vaikutustenarvioinnin tekemiseen ei olisi asetuksen määräämää velvoitetta, se voi olla erinomainen keino tietosuoja-asetuksen 5 artiklan mukaisen osoitusvelvollisuuden täyttämiseksi. Arviointi auttaa myös varmistamaan, että henkilötietojen käsittelyssä huomioidaan asianmukaisesti rekisteröidyn oikeudet, tietosuojaperiaatteet sekä käsittelyyn liittyvät riskit ja niiden hallintakeinot. Vaikutustenarvioinnilla voidaan myös osoittaa rekisteröidylle ja muille sidosryhmille, että organisaatio suhtautuu vakavasti ja kunnioittaen henkilötietojen suojaan. Vaikutustenarvioinnin tekeminen ei siis ole koskaan turhaa, vaan se edistää tietosuoja-asetuksen noudattamista, selkeyttää organisaation tietosuojakäytäntöjä ja vahvistaa luottamusta organisaation toimintaan.

Tietosuojan vaikutustenarviointi on kuitenkin prosessi, joka vaatii rahaa, työpanosta ja aikaa. Vaikutustenarvioinnin kustannukset voivat vaihdella vajaasta tuhannesta eurosta useisiin kymmeniin tuhansiin euroihin riippuen siitä, laaditaanko arviointi organisaation sisäisesti vai ulkoistetaanko sen tekeminen. Vaikutustenarviointi voi vaatia asiantuntijalta jopa useita viikkoja riippuen tapauksesta. (Vandercruysse, Buts & Dooms 2019, 3, 15–16) Dokumentointi ja sidosryhmien

haastattelut tuovat prosessiin huomattavaa hallinnollista taakkaa. Lisäksi vaikutustenarvioinnit tulisi myös tehdä ennen henkilötietojen käsittelyn aloittamista, mikä voi viivästyttää hankkeiden ja liiketoiminnan aloittamista. Arviointien tekeminen saattaa siis olla yrityksille huomattava taloudellinen rasite. Riskinä on, että vaikutustenarvioinnit nähdään organisaatioissa pelkkänä byrokraattisena muodollisuutena, jotka toteutetaan vain näennäisesti velvollisuudesta eikä aidosti tietosuojan parantamiseksi.

Vaikutustenarviointi ei kuitenkaan ole vain muodollinen dokumentti eikä sitä tule tehdä pintapuolisesti. Esimerkiksi Vastaamon tapauksessa vaikutustenarviointi ei ollut täyttänyt tietosuoja-asetuksen asettamia vaatimuksia ja apulaistietosuojavaltuutettu antoi siitä seuraamuksena huomautuksen. Vaikutustenarvioinnissa oltiin muun muassa arvioitu luvatonta käsittelyä ainoastaan terveydenhuollon ammattilaisen suorittamana, mutta mahdollisen ulkopuolisen hyökkääjän hakkeroinnilla suorittama käsittely jätettiin kokonaan huomiotta. (TSV 07.12.2021.) Ei voida myöskään ajatella, että vaikutustenarvioinnin tekemisen jälkeen organisaation tietosuoja-asiat ovat nyt kunnossa ja valmiita. Tietosuojatyö on jatkuvaa ja myös vaikutustenarviointia tulee päivittää muuttuvissa olosuhteissa.

Keskeinen haaste vaikutustenarviointien laatimisessa on löytää keino saada organisaatiot tekemään laadukkaita arviointeja, jotka todella parantavat rekisteröityjen henkilötietojen suojaa ja täyttävät tietosuoja-asteuksen vaatimukset ilman kohtuuttomia resurssipanostuksia. Pitäisikö vaikutustenarviointiprosessia keventää, ja jos, niin missä määrin? Voidaanko riittävä tietosuojan taso saavuttaa kevyemmillä menetelmillä? Olisiko vaikutustenarviointien tekemiseen olemassa vaihtoehtoisia toteutustapoja? Jos vaikutustenarvioinneissa keskityttäisiin vain olennaisiin riskeihin ja taustatyö suoritettaisiin kevyemmin, voitaisiinko saavuttaa jopa parempi tietosuojan taso? Toisaalta onnistutaanko kaikkia riskejä tunnistamaan ilman huolellista taustatyötä? Entä voidaanko kaikkia riskejä koskaan täysin tunnistaa, vaikka taustatyö olisi kuinka perusteellista? Vaikutustenarvioinnin toteuttamiseen liittyy monia kysymyksiä, joihin ei ole vielä selkeitä vastauksia ja jotka edellyttävät lainsäädännön kehittämistä.

Tämän opinnäytetyön tarkoituksena oli laatia vaikutustenarviointi TAMKille oppimisalusta TUNI Moodlesta. Tavoitteena oli tunnistaa TUNI Moodlen henkilötietojen käsittelyyn liittyvät riskit ja löytää keinoja niiden hallitsemiseksi. Riskien tunnistamisprosessissa kävi ilmi, että kaikkien mahdollisten riskien kattava kartoittaminen on käytännössä mahdotonta. Tietosuojavaltuutetun laatima uhkataulukko (taulukko 1) oli kuitenkin hyödyllinen uhkien paljastamisen apuväline, sillä sen avulla henkilötietoihin kohdistuvia riskejä pystytiin havaitsemaan kokonaisvaltaisesti ja järjestelmällisesti koko tietojenkäsittelyn elinkaaren ajalta. Lisäksi tietosuojavastaava Hinkan asiantuntemus ja kokemus olivat arvokas lisä riskien tunnistamisessa ja arvioinnissa. Opinnäytetyön kirjoittaja arvioi riskejä myös rekisteröidyn näkökulmasta.

Uhkien tunnistamisessa olisi voitu hyödyntää myös muita TAMKin asiantuntijoita esimerkiksi haastattelemalla tietohallinnon henkilökuntaa. Laajemmalla asiantuntijoiden joukolla uhkia olisi voitu tunnistaa kattavammin eri näkökulmista. Myös mahdollisista tietovuo- ja työkulkukaavioista olisi voitu konkreettisesti havaita uhkille alttiit kohdat. (Tietosuojan vaikutustenarvioinnin ohje 2021, 30.) Opinnäytetyön rajattu laajuus asetti kuitenkin omat reunaehtonsa työn toteutukselle. On siis todennäköistä, että joitakin riskejä jäi tunnistamatta. Tästä huolimatta työssä on pyritty käsittelemään TUNI Moodlen henkilötietoihin liittyvät oleellisimmat riskit.

Yksi keskeisimmistä riskeistä TUNI Moodlen käytössä liittyi avoimen kentän ongelmaan, jota Tietosuojavaltuutetun toimiston vaikutustenarvioinnin ohjeessa tai sen määrittämissä kriteereissä korkean riskin arvioimiseksi ei kuitenkaan juurikaan käsitellä. Vaikka on opiskelijan valinta, kirjoittako hän erityisiin tietoryhmiin kuuluvaa tietoa Moodleen, ei voida edellyttää, että hänellä olisi syvällistä tietosuojaosaamista tai riittävää ymmärrystä tiedon leviämisen mahdollisista vaikutuksista. Tästä syystä vastuu erityisiin tietoryhmiin kuuluvien tietojen suojauksesta kuuluu ensisijaisesti organisaatiolle. On organisaation tehtävä kehittää toimenpiteitä, jotka estävät erityisiin tietoryhmiin kuuluvien tietojen tallentumisen oppimisalustalle.

Suojatoimenpiteiden suunnittelussa riskien pienentämiseksi onnistuttiin löytämään keinoja, jotka alensivat kaikkien riskien todennäköisyyttä vähäiselle tasolle. Sen sijaan riskin vakavuuteen oli haastavampi vaikuttaa, sillä uhan toteutuessa

sen vaikutukset olisivat samanlaiset riippumatta toimenpiteistä. Vaikutustenarviointia voitaisiin kuitenkin vielä täydentää suojatoimenpiteiden osalta tietoteknisellä osaamisella. Teknisten toimien ansiosta myös uhkien vakavuutta voitaisiin saada alennettua, jolloin riskiluvut pienenisivät entisestään. Kokonaisuudessaan vaikutustenarvioinnissa tunnistettu jäännösriski vaikuttaa kuitenkin jäävän hyväksyttävälle tasolle. Suunnitellut toimenpiteet eivät aiheuta organisaatiolle merkittäviä toteuttamiskustannuksia, eivätkä riskiluvut nousseet niin korkeiksi, että suuria taloudellisia panostuksia tarvittaisiin.

Tulevaisuudessa TUNI Moodleen saatetaan liittää tekoälyä ja chatbotteja, mikä edellyttää uuden tietosuojan vaikutustenarvioinnin laatimista. Tekoälyn käyttöön liittyy uudenlaisia riskejä, joita ei ole käsitelty tässä vaikutustenarvioinnissa. Näihin riskeihin voivat kuulua esimerkiksi vääristyneen tiedon tuottaminen, manipulointi, koneiden inhimillistäminen sekä automatisoinnin passivoiva vaikutus, joka voi ilmetä esimerkiksi vähentyneenä fyysisenä aktiivisuutena ja lisääntyvänä yksinäisyytenä. (Tekoälyn vastuullinen hyödyntäminen 2025.) Tekoälyn liittäminen TUNI Moodleen toisi erityisesti opettajille paljon mahdollisuuksia opintojen suunnitteluun ja kurssialustan hallinnointiin, mutta siihen liittyy myös paljon eettisiä kysymyksiä ja haasteita. Siksi tekoälyyn liittyvien riskien arviointi ja niiden hallintakeinojen kehittäminen Moodlen yhteydessä voisi olla hyödyllinen jatkotutkimuksen kohde.

TUNI Moodlen vaikutustenarvioinnissa saatiin konkreettista hyötyä opinnäytetyön tilaajalle TAMKille, sillä sen tekemisen yhteydessä havaittiin jatkotoimenpiteitä, joiden toteuttaminen parantaa rekisteröityjen tietosuojaa. Työn luotettavuutta arvioitaessa, voidaan kiinnittää huomiota useisiin eri tekijöihin. Ennen vaikutustenarvioinnin tekemistä perehdyttiin syvällisesti EU:n yleiseen tietosuoja-asetukseen ja erityisesti sen 35 artiklaan vaikutustenarvioinnista. Vaikutustenarviointi tehtiin myös järjestelmällisesti ja tarkasti kansallisen valvontaviranomaisen Tietosuojavaltuutetun toimiston laatiman ohjeen mukaan ja sen tekemisessä hyödynnettiin monipuolisesti ajantasaista lainsäädäntöä, organisaation tietosuojamateriaalia sekä muita viranomaisten ohjeistuksia. Vaikka vaikutustenarviointi toteutettiin huolellisesti, on huomioitava, että henkilötietojen suoja on oikeudenalana uusi ja esimerkiksi EU:n yleistä tietosuoja-asetusta on sovellettu

vasta seitsemän vuotta. Tämän vuoksi vaikutustenarviointiin liittyvää oikeuskäytäntöä ja ennakkotapauksia on edelleen niukasti eikä monia asetuksen soveltamiseen liittyviä kysymyksiä ole vielä ratkaistu. On mahdollista, että tulkintakäytäntö vaikutustenarvioinnin osalta muuttuu ja kehittyy tulevaisuudessa.

TUNI Moodlen vaikutustenarvioinnin luotettavuutta vahvistaa erityisesti TAMKin tietosuojavastaavan asiantuntijahaastattelut, jotka tuovat työhön syvyyttä ja varmistavat arvioinnin perusteellisuuden. Kaikki vaikutustenarviointiin kirjatut tiedot sisältävät asianmukaiset viittaukset luotettaviin lähteisiin. Lisäksi vaikutustenarvioinnissa on käytetty selkeää kieltä, jotta se on helposti ymmärrettävä kaikille dokumentin tarkastelijoille. Jäännösriskin hyväksyttävyys on tarkastettu tietosuojavastaavalla.

Vaikutustenarvioinnin tekeminen osoitti, että tietosuoja-ala vaatii todellisia moniosaajia. Arvioinnin onnistunut toteuttaminen edellyttää juridista osaamista sekä tietoturvan, ohjelmistojen ja sovellusten teknisten ratkaisujen ymmärtämistä. Lisäksi hyötyä on hyvistä projektinhallintataidoista, selkeästä kirjallisesta ilmaisusta, tarkkuudesta ja organisaation toimintaympäristön syvällisestä tuntemuksesta. Korkeakoulutasoiselle tietosuojakoulutukselle olisi ilmeinen tarve, jotta kaikissa organisaatiossa voidaan varmistaa laadukas tietosuojaosaaminen. Yritysten ja organisaatioiden tulisi myös vaalia osaavia tietosuoja-asiantuntijoitaan mahdollistamalla riittävät resurssit työn tekemiseen sekä tarjoamalla palkkauksen, joka vastaa työn tosiasiallista vaativuutta. Työhönsä intohimoisesti ja sitoutuneesti suhtautuva tietosuojan asiantuntija voi olla organisaatiolle merkittävä kilpailuetu, joka vahvistaa organisaation tietosuojan toteutumista ja parantaa sen mainetta.

LÄHTEET

Andreasson, A. & Ylipartanen, A. 2022. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus (GDPR). E-kirja. 2., päivitetty laitos. Helsinki: Tietosanoma. Viitattu 16.1.2025. Vaatii käyttöoikeuden. https://www.elibslibrary.com/book/9789518854817

Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat. 2018. Tietosuojaryhmä. Pdf-dokumentti. Annettu 29.11.2017. Päivitetty 11.04.2018. Viitattu 6.3.2025. https://tietosuoja.fi/documents/6927448/8316711/L%C3%A4pin%C3%A4kyvyys+fi/c102605b-e386-4661-9b51-bf427875c8db/L%C3%A4pin%C3%A4kyvyys+fi.pdf?t=1535696089000

Bu-Pasha, S. 2020. The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city. Information & communications technology law 29 (3), 391–402. Viitattu 14.3.2025. Vaatii käyttöoikeuden. https://www.tandfonline.com/doi/epdf/10.1080/13600834.2020.1790092?needAccess=true

(EU) 2016/679. Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus. Euroopan unionin virallinen lehti 4.5.2016. Viitattu 14.3.2025. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679

European Data Protection Board. n.d. a. Tietosuojavastaava. Verkkosivu. Viitattu 16.2.2025. https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-officer_fi

European Data Protection Board. n.d. b. The European Data Protection Board. Verkkosivu. Viitattu 16.2.2025. https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en

European Data Protection Supervisor 2018. Accountability on the ground Part II: Data Protection Impact Assessment & Prior Consultation. Pdf-dokumentti. Viitattu 17.2.2025. https://www.edps.europa.eu/sites/default/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf

Hallberg, P. 2005. Perusoikeudet. Päivittyvä hakuteos. Helsinki: WSOYpro. Viitattu 19.3.2025. https://verkkokirjahylly-almatalent-fi.libproxy.tuni.fi/teos/EAHBGXCTDG#kohta:PERUSOIKEUDET/piste:t2jY

Hanninen, M., Laine, E., Rantala, K., Rusi, M., & Varhela, M. 2017. Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset. E-kirja. Helsinki: Kauppakamari. Viitattu 16.1.2025. https://kauppakamaritieto-fi.libproxy.tuni.fi/ammattikirjasto/teos/henkilotietojen_kasittely#kohta:Henkil((f6)((ad)tietojen((20)k((e4)sittely

HE 9/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Eduskunta. Viitattu 4.2.2025. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_9+2018.pdf

Hinkka, N. tietosuojavaltuutettu. 2025. Teams-haastattelut 25.2.2025 – 18.3.2025. Haastattelija Mursunen, A. Tampereen ammattikorkeakoulu.

It-ulkoistus vs. sisäinen tiimi. n.d. E-it. Verkkosivu. Viitattu 15.3.2025. https://www.e-it.fi/it-ulkoistus-vs-sisainen-tiimi/

Itä-Suomen HAO 20.05.2021 21/0231/2. Hallinto-oikeuden ratkaisu. Viitattu 27.3.2025. https://finlex.fi/fi/oikeuskaytanto/hallinto-oikeudet/2021/ita-suomi/231

KHO:2022.131. Korkeimman hallinto-oikeuden ennakkopäätös. Annettu 23.11.2022. Viitattu 27.3.2025. https://finlex.fi/fi/oikeuskaytanto/korkein-hallinto-oikeus/ennakkopaatokset/2022/131

Korpisaari, P., Pitkänen, O., & Warma-Lehtinen, E. 2022. Tietosuoja. E-kirja. 2. uud. painos. Helsinki: Alma Talent. Viitattu 16.1.2025. https://verkkokirjahylly-almatalent-fi.libproxy.tuni.fi/teos/CAIBCXETEB#kohta:Tietosuoja/piste:b1

Mollik, A. n.d. 7 hyvää syytä, miksi kannattaa hankkia kustannustehokkaat pilvipalvelut yritykselle. Altoros. Verkkosivu. Viitattu 15.3.2025. https://altoros.fi/7-hyvaa-syyta-miksi-kannattaa-hankkia-pilvipalvelut-yritykselle/

Moodle. 2024a. About Moodle. Verkkosivu. Viitattu 24.2.2025. https://docs.moodle.org/405/en/About_Moodle

Moodle. 2024b. Moodle Docs Suomi. Verkkosivu. Viitattu 24.2.2025. https://docs.moodle.org/4x/fi/Etusivu

Moodle. 2024c. Privacy Notice. Verkkosivu. Viitattu 25.2.2025. https://moodle.com/privacy-notice/

Moodle. n.d.a. Statistics. Verkkosivu. Viitattu 24.2.2025. https://stats.moodle.org/

Moodle. n.d.b. The Moodle Story. Verkkosivu. Viitattu 24.2.2025. https://moodle.com/about/the-moodle-story/

Nykänen, P. 2024. Vastaamo-uhrien juristi A-studiossa: Osa pystyy jatkamaan elämäänstä kohtalaisen normaalisti, osa ei ole enää keskuudessamme. Yle Uutiset 30.4.2024. Viitattu 20.3.2025. https://yle.fi/a/74-20086539

Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu "korkea riski”. 2017. Tietosuojaryhmä. Pdf-dokumentti. Annettu 4.4.2017. Päivitetty 4.10.2017. Viitattu 23.1.2025. https://tietosuoja.fi/documents/6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9debe21bdd2e0a63/Vaikutustenarviointi+fi.pdf?t=1527059635000

Opiskelijan tietosuojailmoitus. 2024. Tampereen yliopisto. Pdf-dokumentti. Viitattu 27.2.2025. https://content-webapi.tuni.fi/proxy/public/2024-12/opiskelijan-tietosuojailmoitus-20240607.pdf

O'Regan, E. & Ng, A. 2025. Trump dismantles surveillance watchdog, triggering Europe's privacy PTSD. Politico. Verkkosivu. Viitattu 6.3.2025. https://www.politico.eu/article/usa-donald-trump-privacy-watchdog-dismantle-personal-data/

PeVL 14/2018 vp. Perustuslakivaliokunta. 2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Eduskunta. Viitattu 27.3.2025. https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/PeVL_14+2018.pdf

Salumäki, T. 2023. Syyttäjä ja ex-toimitusjohtaja Ville Tapio valittivat Vastaamo-tuomiosta. Yle Uutiset 19.5.2023. Viitattu 20.3.2025. https://yle.fi/a/74-20032508

Tekoälyn vastuullinen hyödyntäminen 2025. Suomi.fi kehittäjille. Verkkosivu. Viitattu 20.3.2025. https://kehittajille.suomi.fi/oppaat/vastuullinen-tekoaly/huomioi-turvallisuus/punnitse-riskeja

Tieteen termipankki. 2016. Oikeustiede. Verkkosivu. Viitattu 4.3.2025. https://tieteentermipankki.fi/wiki/Oikeustiede:oikeustieteellinen_tutkimus/laajempi_kuvaus

Tieteen termipankki. 2025. Tietosuoja. Verkkosivu. Viitattu 19.3.2025. https://www.tieteentermipankki.fi/wiki/Nimitys:tietosuoja.

Tietosuojalaki. 5.12.2018/1050. Viitattu 24.2.2025. https://www.finlex.fi/fi/lainsaadanto/saadoskokoelma/2018/1050

Tietosuojan vaikutustenarvioinnin ohje. 2021. Tietosuojavaltuutetun toimisto. Pdf-dokumentti. Viitattu 16.1.2025. https://tietosuoja.fi/documents/6927448/66036250/TVA+ohje.pdf/ff0b6e1b-5b89-e85e-a2e5-6c4bd4c0ccfc/TVA+ohje.pdf?t=1639729535787

Tietosuojan vaikutustenarvioinnin työkalu. n.d. Tietosuojavaltuutetun toimisto. Excel-tiedosto. Viitattu 19.3.2025. https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto. 2018. Tietosuojavaltuutetun päätös luetteloksi käsittelytoimista, joiden yhteydessä on tehtävä vaikutustenarviointi. Verkkosivu. Viitattu 23.1.2025. https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista

Tietosuojavaltuutetun toimisto. n.d.a. Aineiston hävittäminen, anonymisointi tai arkistointi tutkimuksen päättyessä. Verkkosivu. Viitattu 4.3.2025. https://tietosuoja.fi/aineiston-havittaminen-anonymisointi-tai-arkistointi-tutkimuksen-paattyessa

Tietosuojavaltuutetun toimisto. n.d.b. Tietosuoja. Verkkosivu. Viitattu 4.3.2025. https://tietosuoja.fi/tietosuoja

Tietosuojavaltuutetun toimisto. n.d.c. Vaikutustenarviointi. Verkkosivu. Viitattu 16.1.2025. https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto. n.d.d. Ennakkokuuleminen. Verkkosivu. Viitattu 23.2.2025. https://tietosuoja.fi/ennakkokuuleminen

Tietosuojavaltuutetun toimisto. n.d.e. Ilmoitus tietosuojavaltuutetulle. Verkkosivu. Viitattu 27.2.2025. https://tietosuoja.fi/ilmoitus-tietosuojavaltuutetulle

Traficom Kyberturvallisuuskeskus. 2024. Palvelunestohyökkäystilanne Suomessa. Verkkosivu. Viitattu 14.3.2025. https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaystilanne-suomessa

TSV 07.12.2021. Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen. Apulaistietosuojavaltuutetun päätös. Viitattu 20.3.2025. Vaatii käyttöoikeuden. https://www-edilex-fi.libproxy.tuni.fi/tsv/20211183?

TUNI n.d.a. Korkeakoulun tietosuojapolitiikka. Verkkosivu. Viitattu 11.3.2025. https://www.tuni.fi/fi/tutustu-meihin/tietosuoja/korkeakoulun-tietosuojapolitiikka

TUNI n.d.b. Tietosuoja ja henkilötietojen käsittely Tampereen korkeakouluyhteistössä. Verkkosivu. Viitattu 11.3.2025. https://www.tuni.fi/fi/tutustu-meihin/tietosuoja

TUNI n.d.c. Ilmoita henkilötietojen tietoturvaloukkauksesta. Verkkosivu. Viitattu 11.3.2025. https://www.tuni.fi/fi/tutustu-meihin/tietosuoja/ilmoita-henkilotietojen-tietoturvaloukkauksesta

TUNI. n.d.d. Henkilötietojen käsittelyyn liittyvät tietosuojaoikeutesi. Verkkosivu. Viitattu 27.2.2025. https://www.tuni.fi/fi/tutustu-meihin/tietosuoja/henkilotietojen-kasittelyyn-liittyvat-tietosuojaoikeutesi

TUNI järjestelmäsalkku. 2024. Rekisterinpitäjän selosteeksi käsittelytoimista. Vaatii käyttöoikeuden.

TUNI Moodle. n.d.a. Mikä on Moodle? Pikaohjeet. Verkkosivu. Viitattu 24.2.2025. https://moodle.tuni.fi/mod/book/view.php?id=229

TUNI Moodle. n.d.b. Tietosuojaseloste. Verkkosivu. Viitattu 25.2.2025. https://moodle.tuni.fi/mod/book/view.php?id=434489&chapterid=7058

TUNI Moodle. n.d.c. Kurssialueiden automaattinen poistaminen. Pikaohjeet. Verkkosivu. Viitattu 24.2.2025. https://moodle.tuni.fi/mod/book/view.php?id=229&chapterid=25087

Turnitin-järjestelmän tietosuojaseloste. 2020. Turun yliopisto. Laadittu 27.3.2019. Päivitetty 14.9.2020. Viitattu 11.3.2025. https://www.utu.fi/fi/turnitin-jarjestelman-tietosuojaseloste

Vandercruysse, L., Buts, C. & Dooms, M. 2019. Economic costs of the DPIA. A report in the framework of the SPECTRE research project. Pdf-dokumentti. https://spectreproject.be/output/downloads-1/deliverable-d3-1-economic-costs-of-the-dpia.pdf

Yle Uutiset. 2021. Psykoterapiakeskus Vastaamo asetettiin konkurssiin. 15.2.2021. Viitattu 28.3.2025. https://yle.fi/a/3-11790537

Zoom-palvelun tietosuoja ja turvallisuus. 2024. TUNI Intra. Verkkosivu. Julkaistu 1.2.2019. Päivitetty 25.6.2024. Viitattu 11.3.2025. Vaatii käyttöoikeuden. https://intra.tuni.fi/fi/it-palvelut/videopalvelut/videotapaamiset-ja-etaopetustilanteet-teams-ja-zoom/zoom-palvelun-tietosuoja-ja-turvallisuus