Tampereen ammattikorkeakoulu

Tietosuojan vaikutustenarviointi (DPIA): Rego-järjestelmä

Ida Holm

OPINNÄYTETYÖ
Heinäkuu 2025

Liiketalouden tutkinto-ohjelman
Oikeudellinen asiantuntijuus

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalouden tutkinto-ohjelma
Oikeudellinen asiantuntijuus

HOLM, IDA
Tietosuojan vaikutustenarviointi (DPIA): Rego-järjestelmä

Opinnäytetyö 38 sivua
Heinäkuu 2025

Tämä opinnäytetyö on tehty Tampereen ammattikorkeakoululle (TAMK) tarkoituksena tuottaa kokonaisvaltainen tietosuojan vaikutustenarviointi (DPIA) Rego-järjestelmästä. Työn tavoitteena on varmistaa, että Rego-järjestelmän DPIA vastaa nykytilannetta ja että järjestelmä toimii tehokkaana työkaluna tietosuoja-asetuksen (GDPR) vaatimusten toteuttamisessa sekä helpottaa mahdollisten riskien tunnistamista ja hallintaa. Työssä tarkastellaan DPIA-prosessia kokonaisuutena ja keskitytään sen oikeudelliseen kehykseen sekä prosessin uhkiin ja mahdollisuuksiin. Lisäksi analysoidaan, millaisia vaikutuksia DPIA:lla on rekisteröityihin.

Opinnäytetyö on toiminnallinen, ja sen yhteydessä laadittiin Rego-järjestelmän tietosuojan vaikutustenarviointi excel-muodossa, joka on tarkoitettu vain TAMK:in sisäiseen käyttöön. Tässä opinnäytetyössä käytettiin dokumenttianalyysiä, jonka kohteena olivat Tampereen ammattikorkeakoulun sisäiset raportit, järjestelmään liittyvät dokumentaatiot sekä GDPR:n vaatimuksia koskevat ohjeistukset ja kansalliset aiheeseen liittyvät säädökset.

Vaikutustenarvioinnin perusteella havaittiin, että DPIA-prosessin toteutus Rego-järjestelmän kohdalla on toteutettu noudattaen tietosuojalainsäädännön vaatimuksia sekä organisaation sisäisiä ohjeistuksia. Riskiluvut jäivät huolellisen tarkastelun jälkeen hyväksyttävälle tasolle. Toimenpiteinä jatkoa varten tilanteen ylläpitämiseksi esitettiin esimerkiksi teknisten järjestelmien jatkuvaa seurantaa ja myös automatisoitujen toimenpiteiden varmistamista säännöllisin väliajoin. Suojatoimenpiteenä korostettiin myös henkilöstön jatkuvaa kouluttamista.

Asiasanat: tietosuoja, vaikutustenarviointi, rego, gdpr, dpia

ABSTRACT
Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Administration
Legal expertise

HOLM, IDA
Data Protection Impact Assessment (DPIA): Rego-system

Bachelor's thesis 38 pages
July 2025

This thesis was done for Tampere University of Applied Sciences (TAMK) and its purpose is to produce a Data Protection Impact Assessment (DPIA) for the Rego platform. The goal is to make sure that the previously made DPIA is correct and up to date and that it works as an effective tool to meet the requirements of GDPR, while also helping the company to identify and manage any possible risks. In this thesis, the DPIA process is reviewed from a wide perspective, but mainly focusing on its legal background, the risks and opportunities involved, and also how it might impact data subjects.

This is a functional thesis that includes creating a DPIA for the Rego platform in excel format, intended for internal use only by TAMK. The thesis is based on document analysis and the focus was TAMK's internal reports as well as the program involving documentation, GDPR guidelines, and related national laws.

The DPIA showed that the process for the Rego system followed both data protection laws and internal company rules. The risks were reviewed carefully and were considered acceptable. The DPIA has helped the organization make improvements and handle risks more effectively. In the future the systems should be checked regularly, make sure automated actions work as expected, and keep staff well trained.

Key words: data protection impact assessment, rego, gdpr, dpia

SISÄLLYS

1 JOHDANTO 7
1.1 Tausta ja konteksti 7
1.2 Tavoitteet ja rajaus 7
1.3 Menetelmät ja aineisto 8
2 TIETOSUOJAN VAIKUTUSTENARVIOINTI (DPIA) 10
2.1 DPIA:n käsite ja tarkoitus 10
2.2 DPIA:n lainsäädännöllinen tausta ja vaatimukset 11
2.2.1 EU:n yleinen tietosuoja-asetus (GDPR) 11
2.2.2 Kansallinen sääntely 15
2.2.3 DPIA-velvoitteen syntyminen 16
2.3 DPIA-prosessin vaiheet 17
2.3.1 Kuvaus tietojen käsittelystä 17
2.3.2 Riskien tunnistaminen 18
2.3.3 Ennakoiva riskien hallinta 19
2.3.4 Dokumentointi ja seuranta 20
3 REGO-JÄRJESTELMÄ 21
3.1 Regon käyttötarkoitus 21
3.2 Henkilötietojen käsittely Rego-järjestelmässä 22
3.2.1 Tarkoitus ja oikeusperuste 22
3.2.2 Suojauksen periaatteet 23
3.2.3 Henkilötietojen elinkaari 24
3.2.4 Kolmannet osapuolet ja tietojen siirrot 25
3.3 DPIA-tarpeen arviointi Regon osalta 25
4 REGO-JÄRJESTELMÄN VAIKUTUSTENARVIOINTI 27
4.1 Arviointiprosessin suunnittelu/toteutus 27
4.2 Tietosuojasääntelyn vaatimusten toteutuminen 28
4.3 Riskien tunnistaminen ja analyysi 29
4.3.1 Tekniset uhat 30
4.3.2 Organisatoriset uhat 30
4.3.3 Oikeudelliset uhat 31
4.4 Suojaustoimet ja toimenpide-ehdotukset 31
5 POHDINTA JA YHTEENVETO 33
LÄHTEET 36

LYHENTEET JA TERMIT

anonymisointi	Tunnistetietojen muokkaaminen tai poistaminen niin, ettei henkilöitä voida enää tunnistaa. (Tieteen termipankki 2025.)
arkaluonteiset henkilötiedot	Näiden tietojen huolimaton käsittely voi vaarantaa henkilön oikeudet ja vapaudet, joten ne edellyttävät erityistä suojausta. (Tietosuojavaltuutetun toimisto, n.d.)
DPIA	Data Protection Impact Assessment, tietosuojan vaikutustenarviointi
DPO	Data Protection Officer
GDPR	General Data Protection Regulation, EU:n yleinen tietosuoja-asetus
henkilötietojen käsittelijä	Henkilötietojen käsittelijä on organisaatio tai henkilö, joka toimii rekisterinpitäjän toimeksiannosta ja käsittelee henkilötietoja tämän ohjeiden mukaisesti. (Tietosuojavaltuutetun toimisto, n.d.)
henkilötietojen käsittely	Henkilötietojen käsittely tarkoittaa kaikkia toimenpiteitä, jotka kohdistuvat henkilötietoihin – kuten keräämistä, tallentamista, käyttöä, siirtämistä ja poistamista. (Tietosuojavaltuutetun toimisto, n.d.)
pseudonymisointi	Pseudonymisointi on tapa käsitellä henkilötietoja niin, ettei niitä voi enää suoraan yhdistää yksittäiseen henkilöön ilman erillisiä lisätietoja. (Tietosuojavaltuutetun toimisto, n.d.)
Qreform	Rego-järjestelmän tarjoaja.
Rego Whistleblow	Rego-järjestelmän osa, joka toimii sisäisenä ilmoituskanavana.
Rego-järjestelmä	Rego HSEQ (Health, Safety, Environment, Quality) tarjoaa työkaluja yrityksille koko henkilöstön käyttöön esimerkiksi riskienhallintaan, turvallisuusraportointiin, työvuorojen hallintaan, ympäristöasioiden seurantaan ja laadun valvontaan.

rekisterinpitäjä	Rekisterinpitäjä päättää miksi ja miten henkilötietoja käsitellään. (Euroopan komissio n.d.)
rekisteröity	Rekisteröity tarkoittaa yksilöä, jonka henkilötietoja käsitellään. (Tietosuojavaltuutetun toimisto, n.d.)
TAMK	Tampereen ammattikorkeakoulu
Thinking-portfolio	Järjestelmä, jossa on rekisterinpitäjän käsittelytoimien seloste.
Tietosuojavaltuutetun toimisto	Suomessa GDPR:n ja tietosuojalain valvontaviranomainen on Tietosuojavaltuutetun toimisto.
tietoturvaloukkaus	Henkilötietojen tietoturvaloukkauksessa tiedot voivat esimerkiksi hävitä, vahingoittua, muuttua tai joutua luvattomasti ulkopuolisten käyttöön. (Tietosuojavaltuutetun toimisto, n.d.)
TOS	Tiedonohjaussuunnitelma
vastustamisoikeus	Tietyissä tilanteissa rekisteröity voi käyttää oikeuttaan vastustaa henkilötietojensa käsittelyä. (Tietosuojavaltuutetun toimisto, n.d.)

1 JOHDANTO

1.1 Tausta ja konteksti

Tietosuojan merkitys on korostunut jatkuvasti digitalisoituvassa yhteiskunnassa, jossa henkilötietojen käsittely on olennainen osa monia julkisia sekä yksityisiä palveluita. Euroopan unionin yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR) edellyttää, että rekisterinpitäjät arvioivat henkilötietojen käsittelyyn liittyviä riskejä ja varmistavat riittävät suojaustoimenpiteet yksilöiden oikeuksien turvaamiseksi. Tietosuojaan liittyvät vaikutustenarvioinnit (Data Protection Impact Assessment, DPIA) ovat keskeinen osa tätä prosessia ja tietyissä tilanteissa myös lakisääteinen velvoite.

Tässä raportissa tarkastellaan DPIA:n toteutusta Rego-järjestelmän käyttöönoton yhteydessä. Erityisesti julkisissa organisaatioissa, kuten korkeakouluissa, henkilötietojen käsittely liittyy päivittäisiin toimintoihin kuten opiskelijahallintoon, opintosuoritusten rekisteröintiin ja muihin sähköisiin palveluihin. Näissä ympäristöissä DPIA toimii tärkeänä välineenä riskien hallinnassa sekä tietosuojatietoisuuden lisäämisessä. Vaikutustenarviointi myös tukee päätöksentekoa uusien järjestelmien käyttöönotossa ja auttaa tunnistamaan teknisiä toimenpiteitä, joilla riskejä voidaan hallita ennakoivasti.

Tämä työ on tehty Tampereen ammattikorkeakoulun toimeksiannosta Rego-järjestelmän käyttöönoton ja siihen liittyvän tietosuojan vaikutustenarvioinnin tueksi.

1.2 Tavoitteet ja rajaus

Tämä opinnäytetyö on luonteeltaan toiminnallinen ja sen päätavoitteena on arvioida tietosuojaan liittyvien vaikutustenarviointien (DPIA) toteutusta Rego-järjestelmän käyttöönoton yhteydessä korkeakouluympäristössä. Tarkoituksena on tunnistaa keskeiset tietosuojariskit, arvioida DPIA-prosessin toimivuutta sekä ehdottaa kehitystoimenpiteitä, jotka tukevat riskien tunnistamista, hallintaa ja

GDPR-vaatimusten täyttämistä. Raporttiin on sisällytetty uhkien tarkempi analysointi taulukkomuodossa.

Raportin rajaus kohdistuu ensisijaisesti Rego-järjestelmän henkilötietojen käsittelyyn liittyviin toimintoihin sekä DPIA:n suunnittelu- ja arviointivaiheisiin.

Tavoitteiden pohjalta muotoillut keskeiset kysymykset ovat:

- Kuinka DPIA-prosessi on toteutettu käytännössä Rego-järjestelmän kohdalla?
- Miten DPIA vaikuttaa Rego-järjestelmän henkilötietojen käsittelyyn ihmisoikeuksien turvaamisen näkökulmasta?
- Miten DPIA toimii organisaation kehittämisen työkaluna?

1.3 Menetelmät ja aineisto

Tässä opinnäytetyössä käytettiin dokumenttianalyysiä, jonka avulla tarkasteltiin Rego-järjestelmän tietosuojaan liittyvän vaikutustenarvioinnin (DPIA) toteutusta. Dokumenttianalyysin kohteena olivat Tampereen ammattikorkeakoulun sisäiset raportit, järjestelmään liittyvät käyttöönotto- ja tietosuojadokumentaatiot sekä GDPR:n vaatimuksia koskevat ohjeistukset ja kansalliset aiheeseen liittyvät säädökset.

Dokumenttianalyysi mahdollisti perusteellisen tarkastelun siitä, miten DPIA-prosessi on toteutettu käytännössä ja miten se vastaa lainsäädännön vaatimuksia. Analyysi tehtiin teemallisen analyysin periaatteita noudattaen, jolloin aineistosta tunnistettiin keskeiset teemat liittyen DPIA:n toteutukseen, vaikutuksiin sekä mahdollisuuksiin.

Tutkimuksen rajoituksena on, että pelkkä dokumenttianalyysi ei mahdollista suoraa vuorovaikutusta toimijoiden kanssa, mikä saattaa rajata eri kokemusten ja näkökulmien saamista.

Tässä opinnäytetyössä on käytetty apuna myös aiemmin mainitun lisäksi aiheeseen liittyvää kirjallisuutta, oikeustapauksia sekä Tietosuojavaltuutetun toimiston sivuillaan jakamaa tietoa. Myös Tampereen ammattikorkeakoulun lakiasiainpäällikkö ja tietosuojavastaava Niku Hinkka on avustanut työn tekemisessä. Työssä on paikoittain käytetty tekoälyä pääosin kieliasun ja tekstin jäsentelyn apuvälineenä.

2 TIETOSUOJAN VAIKUTUSTENARVIOINTI (DPIA)

2.1 DPIA:n käsite ja tarkoitus

Data Protection Impact Assessment (DPIA), on tietosuojaa koskeva, etukäteen tehtävä, vaikutustenarviointi. Vaikutustenarvioinnin tarkoituksena on ennakoida ja vähentää henkilötietojen käsittelyn riskejä sekä luoda näyttöä siitä, että tietosuojaa koskevia säädöksiä noudatetaan. Arviointia hyödynnetään jatkuvasti tietosuojan periaatteiden toteuttamisessa ja riskien hallinnassa, erityisesti silloin, kun henkilötietojen käsittelyssä on merkittäviä riskejä rekisteröidyille. (Andreasson & Ylipartanen 2022, luku 5.)

DPIA perustuu EU:n yleiseen tietosuoja-asetukseen, englanniksi The General Data Protection Regulation (GDPR), jossa sitä pidetään paitsi lakisääteisenä vaatimuksena, mutta myös keinona osoittaa tietosuojan toteutumista käytännössä. Se auttaa varmistamaan, että henkilötietojen käsittely tapahtuu lainmukaisesti ja turvallisesti niin, että yksilöiden oikeudet ja vapaudet suojataan asianmukaisesti. DPIA edistää myös organisaation tietosuojakulttuuria lisäämällä tietoisuutta henkilötietojen käsittelyn riskeistä ja vastuista, ja tukee päätöksentekoa niin teknisten kuin hallinnollisten ratkaisujen osalta.

Tietosuojan vaikutustenarviointi on pakollinen vain tietyissä tilanteissa. Jos vaikutustenarviointia ei tehdä, seurauksena voi olla hallinnollinen seuraamus, esimerkiksi sakko valvontaviranomaiselta. (Andreasson & Ylipartanen 2022, luku 5.1.) Euroopan tietosuojaneuvoston EDPB:n ohjeistuksen mukaan vaikutustenarviointi on tarpeen erityisesti silloin, jos henkilötietojen käsittely aiheuttaa merkittävän riskin rekisteröidyn oikeuksille ja vapauksille.
Esimerkiksi automaattinen päätöksenteko, laajamittainen valvonta tai arkaluonteisten tietojen käsittely ovat tällaisia tilanteita. Vaikka lainsäädäntö ei aina edellytä vaikutustenarviointia, sen tekeminen on suositeltavaa ja se voi suojata organisaatiota mahdollisissa tulevissa tarkastuksissa.

DPIA:n ajantasaisuus varmistetaan päivittämällä sitä tarpeen mukaan. Tietosuojavaikutusten arviointi on jatkuvaa toimintaa, eikä vain kertaluontoinen tehtävä. (Andreasson & Ylipartanen 2022, luku 5.1.) Jatkuva seuranta ja arviointi auttavat varmistamaan, että henkilötietojen suoja pysyy riittävänä ja että organisaation toimintatavat ovat sekä lainmukaisia että eettisesti kestäviä.

2.2 DPIA:n lainsäädännöllinen tausta ja vaatimukset

2.2.1 EU:n yleinen tietosuoja-asetus (GDPR)

Yleinen tietosuoja-asetus (GDPR) on säädös, joka koskee tietosuojaa ja yksityisyyttä. Se hyväksyttiin Euroopan unionin (EU:n) parlamentin sekä neuvoston toimesta korvaamaan aiemman tietosuojadirektiivin. Asetus hyväksyttiin virallisesti 25. toukokuuta 2016 ja se tuli voimaan 25. toukokuuta 2018. (Evans 2022, luku 25., suom. tekijä). EU:n yleinen tietosuoja-asetus eli GDPR tuli voimaan Suomessa ja muissa EU-maissa toukokuussa 2018, korvaten aiemman henkilötietodirektiivin. Sen tavoitteena on päivittää henkilötietojen suojaa koskevat säännöt ja yhtenäistää jäsenmaiden tietosuojakäytännöt sekä vahvistaa rekisteröityjen oikeutta hallita omia tietojaan. (Andreasson & Ylipartanen 2022, luku 2.1.) GDPR on suoraan voimassa oleva EU-laki, joka sitoo kaikkia jäsenvaltioita. Sen sääntöjä noudatetaan sellaisenaan, ellei kansallisella tasolla ole hyväksytty asetuksen sallimia poikkeuksia. (Andreasson & Ylipartanen 2022, luku 2.1.)

GDPR suojelee henkilötietoja riippumatta siitä, millaista teknologiaa käsittelyssä käytetään. Asetus on teknologianeutraali, eli soveltuu sekä automatisoituun, että manuaaliseen tietojenkäsittelyyn, kunhan tiedot löytyvät ennalta määriteltyjen kriteerien mukaisesti (esimerkiksi aakkosjärjestys). Tietojen säilytysmuodolla ei myöskään ole merkitystä, vaan kyseessä voi olla IT-järjestelmä, videovalvonta tai paperimuoto; kaikissa tapauksissa henkilötiedot kuuluvat GDPR:n suojausvaatimusten piiriin. (European Comission, n.d., suom. tekijä). Organisaatioiden tulee siis huolehtia aina se, että ne noudattavat tietosuojavaatimuksia riippumatta siitä, miten ja missä henkilötietoja käsitellään. Tietoturvatoimet ja rekisteröityjen oikeuksien toteuttaminen on varmistettava siis

myös esimerkiksi paperidokumenteissa ja valvontajärjestelmissä. Asetuksen teknologianeutraali luonne tekee siitä joustavamman ja tehokkaamman.

GDPR itsessään kattaa laajasti kaikenlaiset henkilötiedot, joilla voidaan suoraan tai epäsuorasti tunnistaa luonnollinen henkilö. Tietoihin lukeutuvat esimerkiksi perustiedot (nimi, henkilötunnus, yhteystiedot), tunnistamiseen soveltuvat tiedot (IP-osoite, geopaikannustiedot, kuvat ja videot), taloudelliset tiedot (pankki- ja tulotiedot), työhön liittyvät tiedot (työsuhteeseen liittyvät tiedot ja koulutustiedot) sekä arkaluonteiset tiedot (terveystiedot, geneettiset ja biometriset tiedot, uskonto, poliittiset mielipiteet). Kaikki tiedot, joita voidaan käyttää henkilön tunnistamiseen siis kuuluvat GDPR:n suojaan.

7 tietosuojaperiaatetta, jotka perustuvat GDPR:n artiklaan 5:

- Lainmukaisuus, kohtuullisuus ja läpinäkyvyys. Henkilötietoja on käsiteltävä lainmukaisesti, kohtuullisesti ja läpinäkyvästi rekisteröidyn kannalta.
- Tarkoitussidonnaisuus. Tietoja saa kerätä vain ennalta määriteltyä ja laillista tarkoitusta varten.
- Tietojen minimointi. Kerättävien tietojen on oltava olennaisia ja rajoituttava vain siihen, mikä on tarpeen.
- Täsmällisyys. Tietojen on oltava oikeita ja ajan tasalla; virheet on korjattava viipymättä.
- Säilytyksen rajoittaminen. Tietoja saa säilyttää vain niin kauan kuin on tarpeen niiden käsittelyn tarkoituksiin.
- Eheys ja luottamuksellisuus. Henkilötiedot on suojattava luvattomalta pääsyltä ja vahingoittumiselta asianmukaisin turvatoimin.
- Vastuullisuus. Rekisterinpitäjän on voitava osoittaa, että kaikkia tietosuojaperiaatteita noudatetaan.

GDPR säätelee henkilötietojen keräämisestä laillista tarkoitusta varten sekä niiden asianmukaisista käsittelyperusteista. Asetus sisältää myös rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet, joihin lukeutuvat esimerkiksi henkilötietojen käsittelemisen asianmukaisuus ja kaikista henkilötiedoille tehdyistä toimenpiteistä tietojen kerääminen sekä niiden säilyttäminen. EU:n yleisen tietosuoja-asetuksen mukaan rekisterinpitäjä on taho,

joka yksin tai yhdessä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjän rooli on keskeinen tietosuojan toteutumisessa, ja sillä on laaja vastuu henkilötietojen lainmukaisesta käsittelystä.
Tietoturvaloukkausten ilmoittaminen sekä valvontaviranomaiselle että rekisteröidyille kuuluu rekisterinpitäjän vastuulle, kun taas henkilötietojen käsittelijän tehtävä on tiedottaa loukkauksista rekisterinpitäjälle. (Andreasson & Ylipartanen 2022, luku 2.2.)

Henkilötietojen käsittelijä on sitoutunut auttamaan rekisterinpitäjää suojaamaan ja toteuttamaan rekisteröityjen oikeuksia erilaisilla toimenpiteillä. Tämä tarkoittaa, että henkilötietojen käsittelijä toteuttaa rekisteröityjen oikeuksia esimerkiksi tarjoamalla pääsyn tietoihin, mahdollistamalla tietojen oikaisun, poistamisen ja käsittelyn rajoittamisen, sekä huolehtii tietoturvasta estäen tietojen luvattoman käsittelyn, häviämisen tai vahingoittumisen. Tällä tarkoitetaan myös asianmukaisia turvatoimia, mahdollisten poikkeamien tai tietoturvaloukkausten raportointia välittömästi sekä esimerkiksi tietosuoja-arviointien tekemisessä avustamista.

Rekisteröidyillä on useita oikeuksia, kuten oikeus saada selkeää ja avointa tietoa koko henkilötietojen käsittelyprosessista aina tietojen keräämisestä niiden käyttöön. Heillä on myös oikeus tarkastaa omat tietonsa ja pyytää niiden korjaamista, oikeus tulla unohdetuksi sekä oikeus vastustaa tietojensa käsittelyä. (Andreasson & Ylipartanen 2022, luku 2.2.) Rekisteröidyn oikeudet ovat keskeisiä, ja niiden toteutuminen edellyttää, että yritykset suunnittelevat henkilötietojen käsittelyprosessit mahdollisimman läpinäkyviksi ja eettisiksi.

Jos henkilötietoja käsitellään yleisen edun mukaisessa tehtävässä, julkisen vallan käyttämiseksi tai rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen vuoksi, rekisteröidyllä on oikeus vastustaa käsittelyä, mikäli hän perustelee vastustuksensa henkilökohtaisilla erityisolosuhteillaan. (Tietosuojavaltuutetun toimisto, n.d.) GDPR:n artiklan 21 mukaan rekisteröidyllä on oikeus vastustaa henkilötietojensa käsittelyä, eli vastustamisoikeus. Vastustamisoikeus ei kuitenkaan ole ehdoton ja rekisterinpitäjä voi jatkaa tietojen käsittelyä, mikäli se pystyy osoittamaan painavat oikeutetut syyt (esimerkiksi

lakisääteinen velvoite), jotka menevät rekisteröidyn intressien, oikeuksien ja vapauksien ohi.

Rekisteröidylle on annettava selkeä ja erillinen tieto oikeudesta vastustaa henkilötietojensa käsittelyä. Tämä tieto tulee esittää erillään muusta tiedottamisesta. (Tietosuojavaltuutetun toimisto, n.d.)

Pakollinen tietosuojavastaavan nimittäminen koskee vain tiettyjä tilanteita. Sosiaali- ja terveydenhuollon alalla tietosuojavastaavan nimittäminen on ollut pakollista jo vuodesta 2007. Moni organisaatio ja yritys on valinnut nimittää tietosuojavastaavan vapaaehtoisesti parantaakseen riskienhallintaa ja tehokkuutta, vaikka se ei ole lain vaatimus. (Andreasson & Ylipartanen 2022, luku 1.) Data Protection Officer (DPO), eli tietosuojavastaava, on organisaatiossa nimetty henkilö, joka vastaa tietosuojan noudattamisen valvonnasta ja organisaation henkilöstön ohjeistamisesta. Hänen tehtävänään on varmistaa, että organisaation henkilötietojen käsittely on lainmukaista ja että rekisteröityjen oikeudet toteutuvat.

Tietosuojavastaava on nimettävä, jos organisaatio kuuluu julkiseen sektoriin, lukuun ottamatta tuomioistuimia niiden tuomiovallan käytössä. Velvollisuus koskee myös tilanteita, joissa organisaation ydintoimintaan kuuluu ihmisten säännöllinen ja laajaksi laskettava seuranta. Tietosuojavastaava on nimettävä myös silloin, kun käsitellään suuria määriä arkaluonteisia tietoja, kuten terveystietoja tai rikoksiin liittyviä tietoja.

GDPR:n rikkomisella voi olla merkittäviä hallinnollisia seurauksia. Tietosuojaviranomaiset voivat asettaa yrityksille tai muille rekisterinpitäjille seuraamusmaksuja, joiden suuruus määräytyy rikkomuksen vakavuuden, keston ja toistuvuuden perusteella. Sakon määräämisestä päättävät tietosuojavaltuutettu ja apulaistietosuojavaltuutettu.

Suurimmat sakot voivat olla siis enintään 20 miljoonaa euroa tai 4 % yrityksen maailmanlaajuisesta liikevaihdosta, riippuen siitä, kumpi on suurempi. Tarpeeksi vakava rikkomus voi kuitenkin johtaa myös siihen, että yritys joutuu lopettamaan toimintansa. (Evans 2022, luku 25. suom. tekijä).

Esimerkkitapauksena voidaan tarkastella Meta (Facebook) vuoden 2023 tapausta, jossa Euroopan unionin tietosuojaviranomaiset määräsivät 1,2 miljardin euron sakon siitä syystä, että yhtiö oli siirtänyt EU-käyttäjien tietoja Yhdysvaltoihin ilman asianmukaista tietojen suojausta. Sakko on korkein, mitä on

ikinä määrätty. Meta valitti päätöksestä ja on saanut aikarajan, jonka puitteissa sen on lopetettava lainvastainen toimintansa, eli tässä tapauksessa EU-käyttäjien tietojen siirtäminen Yhdysvaltoihin. (Time 2023, suom. tekijä).

Tapauksessa korostuu myös GDPR:n mukainen vaatimus riittävästä suojan tasosta ennen henkilötietojen siirtoa.
Euroopan komissio tekee päätöksen siitä, että jokin maa tai organisaatio takaa riittävän suojan tason ennen henkilötietojen siirtämistä EU:n ulkopuolelle. (Evans 2022, luku 25., suom. tekijä). Riittävä suoja tarkoittaa käytännössä sitä, että vastaanottajamaa tai -organisaatio tarjoaa henkilötietojen käsittelyssä vähintään yhtä vahvat oikeudet ja suojamekanismit kuin EU:n alueella.

2.2.2 Kansallinen sääntely

Euroopan unionin yleinen tietosuoja-asetus täydentyy ja tarkentuu kansallisella tietosuojalailla. Tämä laki korvasi aiemman henkilötietolain sekä tietosuojalautakuntaa ja tietosuojavaltuutettua koskevan lain. Tietosuojalaki toimii yleisenä säädöksenä henkilötietojen käsittelyssä, mutta se ei ole itsenäinen tai kattava sääntelykokonaisuus, vaan sitä sovelletaan yhdessä EU:n tietosuoja-asetuksen kanssa. (Andreasson & Ylipartanen 2022, luku 2.3.)

Suomen kansallisessa lainsäädännössä tietosuojalaki toimii EU:n yleisen tietosuoja-asetuksen täsmentävänä sekä täydentävänä sääntelynä. Suomen tietosuojalaki konkretisoi GDPR:n periaatteita ja antaa tarkempia ohjeita erityisesti niissä tilanteissa, joissa on annettu lupa tehdä kansallisia ratkaisuja. Muita kansallisia erityislakeja, jotka sääntelevät eri toimialojen henkilötietojen käsittelyä, ovat esimerkiksi Laki yksityisyyden suojasta työelämässä (759/2004) sekä Laki viranomaisten toiminnan julkisuudesta (621/1999).

Suomessa GDPR:n ja tietosuojalain valvontaviranomainen on Tietosuojavaltuutetun toimisto. Toimisto tarjoaa neuvontaa, käsittelee rekisteröityjen valituksia, voi antaa päätöksiä sekä sakkoja tietosuoja-asetuksen rikkomisesta.
Yhteenvetona voidaan todeta, että kansallinen lainsäädäntö yhdessä valvontaviranomaisen kanssa takaa sen, että Suomessa henkilötietojen käsittely noudattaa sekä EU:n vaatimuksia että kansallisia erityispiirteitä.

2.2.3 DPIA-velvoitteen syntyminen

DPIA-velvoitteen syntyminen perustuu GDPR:n artiklaan 35. Vaikutustenarvioinnin tekeminen on erityisesti pakollista esimerkiksi seuraavissa tilanteissa:

- toteutetaan kameravalvontaa julkisilla, yleisölle avoimella alueella
- käytetään automaattista päätöksentekoa, joka vaikuttaa luonnolliseen henkilöön merkittävällä tavalla tai muuten tekoälypohjaista analytiikkaa
- käsitellään arkaluonteisia henkilötietoja laajasti

DPIA tulee tehdä myös tilanteessa, jossa rajoitetaan rekisteröidyn oikeuksia tai poiketaan niistä. Tämä on mahdollista vain lainmukaisin perustein, esimerkiksi turvallisuuteen liittyvissä tehtävissä. GDPR ei oikeuta poikkeamaan oikeuksista, mutta sitä käytetään työkaluna henkilötietojen käsittelyn lainmukaisuuden osoittamiseksi sekä mahdollisena perusteluna sekä todisteena.

Tietosuojavaltuutetun toimisto voi määrätä hallinnollisia seuraamusmaksuja tietosuojalainsäädännön rikkomisesta. Tietosuojavaltuutetun toimiston seuraamuskollegio määräsi Kymen Vesi Oy:lle 16 000 € seuraamusmaksun DPIA:n tekemättä jättämisestä. Tapauksessa oli kanneltu siitä, että työntekijöiden sijaintitietoja oli käsitelty ajoneuvoja paikantamalla ja käytetty esimerkiksi työajanseurannassa. Tästä ei ollut tehty GDPR:n vaatimusten mukaista vaikutustenarviointia.
Vaikutustenarviointi on suoritettava, mikäli käsittely aiheuttaa todennäköisesti merkittävän riskin rekisteröidyn oikeuksille ja vapauksille. Arviointi on tarpeen esimerkiksi silloin, kun käsitellään haavoittuvassa asemassa olevien henkilöiden, kuten työntekijöiden, sijaintitietoja tai kun sijaintitietoja käytetään jatkuvaan valvontaan. (Tietosuojavaltuutetun toimisto 2020.) Esimerkkitapaus on vuodelta 2020.

2.3 DPIA-prosessin vaiheet

DPIA on systemaattinen ja dokumentoitu prosessi, jonka avulla arvioidaan henkilötietojen käsittelyyn liittyviä riskejä rekisteröidyn oikeuksien ja vapauksien kannalta sekä suunnitellaan toimenpiteet näiden riskien ehkäisemiseksi tai lieventämiseksi. DPIA-prosessissa tulee kuvata vaikutustenarvioinnin kohde, henkilötietojen käsittelyn luonne, laajuus, tarkoitus ja käsiteltävät tietotyypit sekä arvioida riskit yksilöiden oikeuksille. Lisäksi määriteltäviksi tulevat myös toimenpiteet mahdollisten riskien hallitsemiseksi. Prosessi perustuu GDPR:n artiklaan 35.

Kuva 1. Tietosuojavaltuutetun toimiston kuvalliset ohjeet DPIA:n tekemiseen. (Tietosuojavaltuutetun toimisto), lähde: https://tietosuoja.fi/vaikutustenarvioinnin-tekeminen

2.3.1 Kuvaus tietojen käsittelystä

Käsittelyllä tarkoitetaan tässä henkilötietojen keräämistä, tallentamista, käyttöä, muokkaamista, siirtämistä, luovuttamista, säilyttämistä ja poistamista koskevia toimia. Tässä osiossa tulee kuvata tarkasti, mitä henkilötietoja käsitellään, mihin tarkoituksiin niitä käytetään ja millä tavoin sekä miten henkilötiedot ovat tarkoitus

hävittää. Kuvaukseen tulee myös lisätä rekisterinpitäjä ja mahdolliset muut henkilötietojen käsittelijät.

Lisäksi on tärkeää kuvata, millä oikeusperusteella henkilötietojen käsittely tapahtuu (esimerkiksi suostumus, sopimus, lakisääteinen velvoite). Tietojen käsittelyvaiheet tulee dokumentoida koko henkilötietojen käsittelyn elinkaaren ajalta. Kuvauksen tulee olla riittävän kokonaisvaltainen ja yksityiskohtainen, jotta sen perusteella pystytään tekemään luotettavia arviointeja käsittelyyn liittyvistä riskeistä ja niiden hallinnasta.

2.3.2 Riskien tunnistaminen

DPIA:n yksi keskeisimmistä vaiheista on riskien tunnistaminen. Tarkoituksena on havaita jo etukäteen mahdolliset uhat, jotka voisivat johtaa tietosuojaloukkauksiin tai muihin haitallisiin seurauksiin. Uhalla tarkoitetaan henkilötietojen käsittelyprosessin epäkohtia tai mahdollisia huomioita, jotka voivat vaikuttaa rekisteröidyn oikeuksiin ja vapauksiin. Tässä kohdassa tarkastellaan esimerkiksi käsiteltävien tietojen tyyppiä, millä tietoja tarkastellaan ja miten sitä valvotaan, tietojen käsittelyprosesseja sekä henkilöitä, jotka tietoja käsittelevät.

Riskien arvioinnissa tarkastellaan esimerkiksi juridisia uhkia, teknisiä uhkia (esimerkiksi järjestelmän toimivuus ja järjestelmän suojausta) sekä organisatorisia uhkia (esimerkiksi työntekijöiden osaaminen). Lisäksi riskien arvioinnissa tulee huomioida myös henkilötietojen käsittelyn koko elinkaari aina tietojen keräämisestä niiden säilyttämiseen ja lopulta hävittämiseen saakka. On tärkeää arvioida, kuinka pitkään tietoja säilytetään, missä ne sijaitsevat ja miten tietojen poistaminen toteutetaan.

Henkilötietojen käsittelyyn liittyvien riskien arviointi alkaa tunnistamalla, millaisia uhkia käsittelyyn liittyy. Tämän jälkeen arvioidaan, millaisia vaikutuksia uhkien toteutumisella voisi olla, kuinka vakavia ne ovat ja kuinka todennäköisesti uhka toteutuu. (Andreasson & Ylipartanen 2022, luku 5.3.)

Henkilötietojen tietovuoto voi aiheuttaa vakavaa ja monitasoista haittaa, minkä vuoksi riskejä on tarkasteltava huolellisesti osana tietosuojan

vaikutustenarviointia. Mahdollisia seurauksia henkilötietojen vuodosta voivat olla esimerkiksi identiteettivarkaus, väkivallan uhka tai mainehaitta ja näiden vaikutukset voivat ulottua hyvin pitkälle.

2.3.3 Ennakoiva riskien hallinta

Ennakoiva riskien hallinta on DPIA-prosessin keskeinen osa, jossa tunnistetut riskit pyritään minimoimaan tai poistamaan jo ennen henkilötietojen käsittelyn aloittamista. Tämä tarkoittaa, että organisaatio suunnittelee ja toteuttaa teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan tietosuojavaatimusten täyttyminen ja rekisteröityjen oikeuksien turvaaminen.

Riskienhallinnassa toimenpiteitä voivat olla esimerkiksi:

- Kerättävien ja käsiteltävien tietojen minimointi.
- Henkilötietojen pseudonymisointi tai anonymisointi, eli muuttaminen tunnistamiskelvottomiksi.
- Tietoturvatoimet, kuten säilytysaikojen lyhentäminen, käyttöoikeuksien rajoittaminen tai vahvempi salaus.

Jos riski pysyy korkeana, vaikka lisätoimenpiteitä on tehty, rekisterinpitäjän täytyy pyytää tietosuojaviranomaiselta ennakkokuulemista ennen käsittelyn aloittamista. Vastuu toimenpiteisiin ryhtymisestä on rekisterinpitäjällä. Tätä menettelyä tarvitaan esimerkiksi silloin, kun rekisteröityihin saattaa kohdistua vakavia tai peruuttamattomia seurauksia, joita he eivät pysty estämään, kuten luvaton pääsy arkaluonteisiin tietoihin, joka voi uhata heidän henkeään, johtaa irtisanomiseen tai aiheuttaa taloudellisia vahinkoja. Ennakkokuulemista pitää myös pyytää, jos riskin toteutuminen vaikuttaa hyvin todennäköiseltä. (Andreasson & Ylipartanen 2022, luku 5.3.)

Ennakkokuulemisella tarkoitetaan menettelyä, jossa rekisterinpitäjä ottaa yhteyttä tietosuojaviranomaiseen ennen henkilötietojen käsittelyn aloittamista. (Tietosuojavaltuutetun toimisto, n.d.) Jos DPIA:n perusteella jää jäljelle korkea riski rekisteröityjen oikeuksille ja vapauksille, eikä sitä voida lieventää kohtuullisin toimenpitein, rekisterinpitäjän on konsultoitava valvontaviranomaista ennen

henkilötietojen käsittelyn aloittamista. Ennakkokuuleminen perustuu GDPR:n artiklaan 36.

2.3.4 Dokumentointi ja seuranta

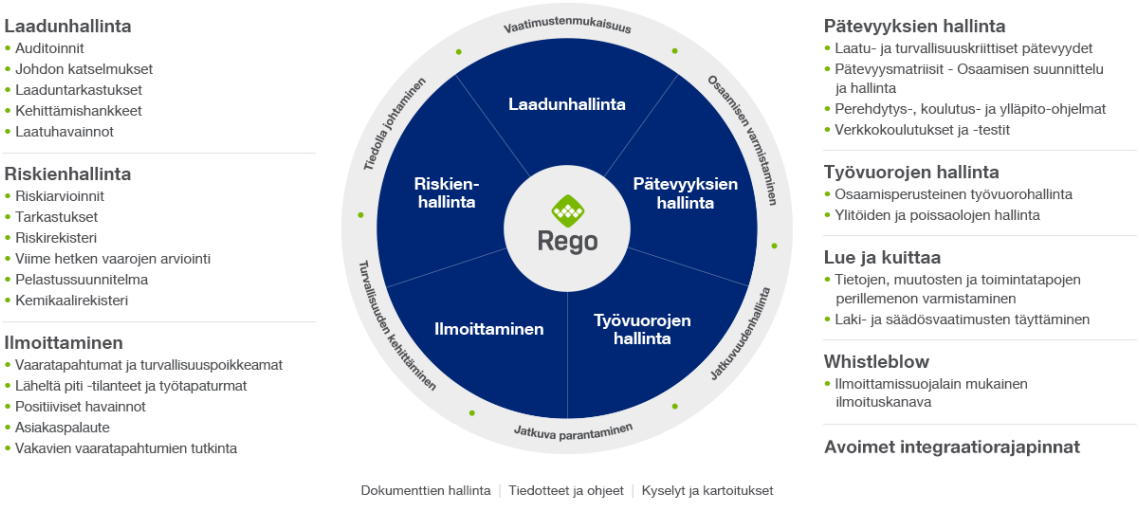
Henkilötietoja käsiteltäessä tulee noudattaa tietosuoja-asetuksen määräyksiä. Osoitusvelvollisuus tarkoittaa sitä, että rekisterinpitäjän on pystyttävä todistamaan, että se noudattaa tietosuojalakeja. (Tietosuojavaltuutetun toimisto, n.d.) Dokumentointi on DPIA:n keskeinen osa, sillä se toimii todisteena siitä, että vaikutustenarviointi on tehty huolellisesti ja systemaattisesti. Hyvin dokumentoitu DPIA auttaa myös tiedon jakamisessa organisaation eri sidosryhmien, kuten johdon, tietosuojavastaavan ja tarvittaessa valvontaviranomaisen kesken. Dokumentointi ei ole vain hallinnollinen muodollisuus, vaan se viestii myös läpinäkyvyyden ja osoitusvelvollisuuden toteutumista. Hyvin laadittu DPIA auttaa osoittamaan, miten riskit on tunnistettu ja miten niihin on vastattu.

Seurannalla tarkoitetaan sitä, että kyseessä ei ole kertaluontoinen raportti, vaan DPIA:a tulee tarkistaa säännöllisesti ja päivittää tarvittaessa. Jatkuva seuranta tukee organisaation kykyä reagoida nopeasti esimerkiksi uusiin tietoturvauhkiin, lainsäädännön muutoksiin tai käsittelytapojen muuttumiseen, mikä on keskeistä tietosuojavaatimusten noudattamisessa. Seurannan tavoitteena on varmistaa, että DPIA pysyy elävänä ja jatkuvana osana organisaation arkea.

3 REGO-JÄRJESTELMÄ

3.1 Regon käyttötarkoitus

Rego HSEQ (Health, Safety, Environment, Quality) tarjoaa työkaluja yrityksille koko henkilöstön käyttöön esimerkiksi riskienhallintaan, turvallisuusraportointiin, työvuorojen hallintaan, ympäristöasioiden seurantaan ja laadun valvontaan. Järjestelmän takana on yritys Qreform ja Regon laajamittainen käyttöönotto on Suomessa tapahtunut vuonna 2021. Myös Tampereen yliopisto ja Tampereen ammattikorkeakoulu valitsivat Qreformin toimittajakseen ja ottivat Regon käyttöön vielä saman vuoden aikana elokuussa 2021.



Kuva 2. Qreform.com oma kuva, jossa on kerrottu enemmän Rego HSEQ -järjestelmän sisällöstä, lähde: https://www.qreform.com/rego/

Rego on monikäyttöinen järjestelmä, jota voidaan käyttää eri toimialoilla esimerkiksi tietoturvavaatimusten täyttämiseen ja monitoimittajaympäristöjen yhdistämiseen.

Ilmoittajien suojaa koskeva laki perustuu EU:n direktiiviin, joka vahvistaa väärinkäytöksistä ilmoittavien henkilöiden suojelua. Tätä direktiiviä kutsutaan usein whistleblower- tai whistleblowing-direktiiviksi. Sen tarkoituksena on taata,

että työntekijät, jotka havaitsevat tai epäilevät väärinkäytöksiä, voivat raportoida niistä turvallisesti ja ilman pelkoa seuraamuksista. (Qreform 2025.)
Ilmoittajansuojelulaki on tullut voimaan 1.1.2023. Laki edellyttää, että vähintään 50 työntekijää työllistävät yksityisen ja julkisen sektorin organisaatiot perustavat sisäisen ilmoituskanavan. Regon Whistleblow on Rego-järjestelmän osa, joka toimii sisäisenä ilmoituskanavana. Regon Whistleblow mahdollistaa ilmoituksen tekemisen työyhteisön sisällä anonyymisti tai omalla nimellään, jonka jälkeen organisaation tulee reagoida siihen. Ilmoituksen tekijälle tulee ilmoittaa kolmen kuukauden aikana ilmoituksen jättämisestä mitä toimenpiteitä on seurannut ilmoituksen vastaanottamisen jälkeen. Whistleblow-järjestelmän osana nostaa yrityksen luottamuksellisuutta ja minimoi vahinkoriskiä, joten siinä korostuu erityisesti vaikutustenarvioinnin tekemisen tärkeys.

Ilmiantojärjestelmä antaa työntekijöille ja muille mahdollisuuden kertoa nimettömästi, jos organisaatiossa tapahtuu jotain epäeettistä tai sääntöjen vastaista. Järjestelmän tavoitteena on varmistaa, että organisaatio toimii reilusti ja noudattaa sovittuja sääntöjä ja käytäntöjä. (Andreasson & Ylipartanen 2022, luku 5.3.)

3.2 Henkilötietojen käsittely Rego-järjestelmässä

3.2.1 Tarkoitus ja oikeusperuste

Rego-järjestelmässä Tampereen ammattikorkeakoulu (TAMK) vastaa rekisterinpitäjän roolista, mikä tarkoittaa, että se määrittelee henkilötietojen käsittelyn tarkoitukset ja prosessit itse. Järjestelmän teknisestä toteutuksesta vastaava Qreform toimii puolestaan henkilötietojen käsittelijänä. Rekisteröityjä ovat ne luonnolliset henkilöt, joiden henkilötietoja järjestelmässä käsitellään, eli TAMKin puolesta näihin kuuluvat organisaation henkilöstö ja opiskelijat sekä mahdollisesti ilmoituskanavan kautta yhteyttä ottavat ulkopuoliset henkilöt.

Qreformin Rego-järjestelmän toiminta perustuu GDPR:n edellyttämiin lainmukaisiin oikeusperusteisiin. Qreform kerää tietoja pääosassa laadunvalvontaprosessia, riskienhallintaa, työvuoronsuunnittelua ja muuta työvuoroliitännäistä sekä poikkeamailmoitusten tekemistä varten, mutta

henkilötietoja käytetään myös lisäkoulutuksiin. Henkilöprofiiliin tallennetaan perustietoja ja laajasti työhön sekä koulutukseen liittyviä tietoja. Perusteena on lakisääteisten velvoitteiden toteutuminen (työturvallisuuslain mukainen tapaturmien kirjaaminen) tai joissakin tilanteissa henkilötietojen käsittely perustuu rekisterinpitäjän oikeutettuun etuun, kuten järjestelmän toiminnan ja turvallisuuden varmistamiseen, kuitenkin siten, että rekisteröidyn oikeudet ja vapaudet eivät vaarannu. Lisätietoja voidaan kerätä myös rekisteröityjen suostumuksella.
Kaikki Rego-järjestelmässä tapahtuva käsittely dokumentoidaan ja sen lainmukaisuus varmistetaan säännöllisesti, jotta tietosuojaperiaatteet toteutuvat asianmukaisesti.

3.2.2 Suojauksen periaatteet

Tietojen suojaus tarkoittaa kaikkia niitä teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, että henkilötiedot pysyvät turvassa ja että niiden luottamuksellisuus, eheys ja saatavuus säilyvät. GDPR edellyttää rekisterinpitäjältä ja käsittelijältä asianmukaisia turvatoimia, jotka perustuvat riskiarviointiin ja tietojen luonteeseen. Suojatoimet Qreform on eritellyt seitsemään eri kategoriaan.

- Sovelluksen ja käyttäjän tietoturvasta huolehditaan esimerkiksi SSL/TLS-suojauksen avulla, joka käyttää palvelintodennuksen lisäksi myös tietojen salausta, käyttäjätunnuksien ja salasanojen avulla sekä tietojen salauksella/minimoinnilla.
- Henkilötietoja käsitellään ja säilytetään vain EU:n alueella olevilla palvelimilla GDPR:n mukaisesti.
- Fyysisestä turvallisuudesta huolehditaan järjestelmäkeskuksen kautta, jossa on ympärivuorokautinen valvonta.
- Käytettävyyden suojaus on toteutettu esimerkiksi sähkönsyötön häiriöiltä suojaamalla, toiminta-ajan jatkuvalla seurannalla sekä kahta eri fyysistä palvelukeskusta käyttämällä.
- Verkon tietoturvasta huolehtii kolmas osapuoli ja tarkastuksia tehdään säännöllisesti. Järjestelmän toimintaa testataan aina ennen käyttöönottoa. Käytössä on myös palomuuri, järjestelmäkirjauksien

valvonta, varmuuskopioinnit ja uusimmat suojauspäivitykset sovelluksiin sekä muihin käyttöjärjestelmiin.

- Organisatorista ja hallinnollista tietoturvaa suojataan käyttöoikeuksia rajaamalla, valvontakirjauksilla, tietoturvakäytäntöjä- ja toimintasuunnitelmia ylläpitämällä sekä tietoja poistamalla.
- Käyttäjällä on velvollisuudet kuitenkin myös itse huolehtia esimerkiksi oman järjestelmänsä tietoturvasta, virussuojasta ja salasanojen suojauksesta.

Qreform on sitoutunut informoimaan rekisterinpitäjää mahdollisista tietoturvamurroista välittömästi. Muihin tietoturvarikkomuksiin liittyvät prosessit vaihtelevat niiden kriittisyyden mukaan. Suurimman riskin tapahtumiin reagoidaan välittömästi, mutta alhaisemman riskin tapaukset käsitellään teknologiatiimin kesken.

3.2.3 Henkilötietojen elinkaari

Qreform tarjoaa sekä ylläpitää järjestelmää, jonka kautta rekisterinpitäjä voi hallita henkilöstön tietoja. Rekisterinpitäjä itse kerää ja muutoin käyttää tietoja asiakastilillään, ellei ole sovittu muuta. Qreform tarkastelee näitä tietoja vain siihen liittyvän järjestelmän sekä muiden palvelujen ylläpitotarkoituksessa. Qreform itse kerää tietoja pääosassa laadunvalvontaprosessia, riskienhallintaa, työvuoronsuunnittelua ja muuta työvuoroliitännäistä sekä poikkeamailmoitusten tekemistä varten, mutta henkilötietoja käytetään myös lisäkoulutuksiin. Henkilöprofiiliin tallennetaan perustietoja ja laajasti työhön sekä koulutukseen liittyviä tietoja.

Tietoja varastoidaan EU-alueella. Henkilötietojen käsittelijä pitää yllä lokitietoja käsittelytoimenpiteistä. GDPR:n periaatteiden mukaan tietoja minimoidaan ja tarpeetonta tietoa poistetaan sekä osassa toimintoja hyödynnetään anonymisointia (tietojen nimettömäksi saattamista).

Asiakkaan henkilötietoja säilytetään rekisterinpitäjän prosessien mukaisella aikataululla. TAMK käyttää tiedonohjaussuunnitelmaa (TOS) säilytysajoille.

Tarpeeton tieto voidaan poistaa myös välittömästi, mutta varmuuskopiointisyklin myötä tiedot poistuvat viimeistään kokonaan. Asiakassuhteen päätyttyä ja asiakkaan toiveesta kaikki tiedot poistetaan myös varmuuskopiointijärjestelmistä. Tietojen poisto on tietoturvallista sekä myös varmuuskopiointijärjestelmät ovat linjassa GDPR:n vaatimuksien kanssa.

3.2.4 Kolmannet osapuolet ja tietojen siirrot

Vain valtuutetut tahot pääsevät käsiksi henkilötietoihin Rego-järjestelmässä. Näihin kuuluvat esimerkiksi rekisterinpitäjän työntekijät, järjestelmän ylläpitäjät sekä mahdolliset ulkoistetut palveluntarjoajat, joilla on tarve käsitellä tietoja työtehtäviensä vuoksi. Asiakkaan henkilötietoja käsittelee rekisterinpitäjän valtuuttamat työntekijät erilaisissa rooleissa niitä vastaavilla valtuuksilla. Rekisterinpitäjä pystyy itse valitsemaan sen, kenellä on pääsy henkilötietoihin ja käyttöoikeuksia on mahdollista muokata. Qreform tarkastelee näitä tietoja vain ylläpitotarkoituksessa.

Rekisterinpitäjä tekee kirjalliset sopimukset kolmansien osapuolien kanssa (esimerkiksi pilvipalveluntarjoaja, ulkoistettu IT-tukipalvelu tai muut Qreformin alihankkijat), joissa määritellään tarkasti vastuut, velvollisuudet ja tietoturvavaatimukset. Sopimuksissa korostetaan, että kolmannet osapuolet käsittelevät henkilötietoja ainoastaan sovittujen tarkoitusten mukaisesti ja noudattaen GDPR:n vaatimuksia.

Mikäli henkilötietoja siirretään EU:n ulkopuolelle, siirrot toteutetaan GDPR:n edellyttämien suojaustoimien mukaisesti EU-komission mallisopimuslausekkeilla tai muutoin tietosuoja-asetuksen mukaisilla suojatoimilla. Regon kohdalla tietoja ei kuitenkaan siirretä EU-alueen ulkopuolelle.

3.3 DPIA-tarpeen arviointi Regon osalta

GDPR:n artikla 35 velvoittaa rekisterinpitäjää tekemään tietosuojan vaikutustenarvioinnin (DPIA), jos henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin rekisteröityjen oikeuksille ja vapauksille. Lisäksi DPIA edistää rekisteröityjen oikeuksien ja vapauksien turvaamista, sillä se tuo esille mahdolliset riskit ja uhat tietosuojaan liittyen. Tietosuojan vaikutustenarviointi toimii myös dokumenttina ja todisteena siitä, että organisaatio on noudattanut

GDPR:n vaatimuksia ja huomioinut tietosuoja-asiat vastuullisesti. DPIA toimii tärkeänä osana sekä riskienhallinnassa että organisaation vastuullisuuden osoittamisessa.

Rego-järjestelmässä riskiä nostattavia tekijöitä ovat esimerkiksi työtapaturma- ja whistleblow-ilmoitukset, jotka voivat sisältää arkaluonteisia tietoja. Järjestelmä myös seuraa henkilöstön toimintaa sekä työympäristön tapahtumia systemaattisesti, joka voidaan laskea laajamittaiseksi seurannaksi organisaation sisällä. Koska tietoja käsitellään suhteellisen laajasti ja määrä lasketaan kohtalaisen suureksi sekä käsiteltävänä on henkilötietoja, jotka voivat altistua tietoturvaloukkauksille, tulee vaikutustenarviointi Regon osalta toteuttaa ennen järjestelmän käyttöönottoa.

TAMK:in aiempi DPIA on tehty erityisesti huomioon ottaen Regon Whistleblowing –osion. Tämä työ laaditaan kokonaisvaltaisesti Rego-järjestelmästä ja työn tarkoituksena on arvioida, ovatko olemassa olevat tiedot ajan tasalla ja riittäviä, sekä tehdä tarvittaessa päivityksiä tai ehdotuksia jatkoa varten. Jos tämän arvioinnin perusteella huomataan merkittäviä muutoksia, jotka voivat vaikuttaa rekisteröityjen oikeuksiin tai tietosuojavaatimusten noudattamiseen, tietoja päivitetään vastaavasti TAMK:in tietosuojavastaavan toimesta. Tavoitteena on varmistaa, että Rego-järjestelmän DPIA vastaa nykytilannetta ja toimii tehokkaana työkaluna tietosuoja-asetuksen vaatimusten toteuttamisessa.

4 REGO-JÄRJESTELMÄN VAIKUTUSTENARVIOINTI

4.1 Arviointiprosessin suunnittelu/toteutus

Opinnäytetyön yhteydessä toteutettiin taulukkomuotoinen vaikutustenarviointi Tietosuojavaltuutetun toimiston vuoden 2021 ohjeistuksen pohjalta. Tämän opinnäytetyön rinnalle laadittu excel-taulukko ei ole nähtävissä, sillä se on tehty vain TAMK:in sisäiseen käyttöön. Kirjallinen osio toimii taulukkoa pohjustavana sekä syventävänä osiona, joka tarjoaa laajempaa kontekstia, perusteluja ja taustatietoa DPIA-prosessin ymmärtämiseksi.
Vaikutustenarviota laadittaessa työkaluina käytettiin thinking-portfoliota, tietosuojavastaavan haastatteluja, toimittajan ja rekisterinpitäjän toimittamia tietoja, korkeakoulukonsernin tietoturvapolitiikkaa, tiedonohjaussuunnitelmaa, pääkäyttäjää, intraa, EU:n tietosuoja-asetusta (GDPR) sekä tietosuojalakia (1050/2018).

Arviointi käynnistyi määrittelemällä tarkasti arvioinnin kohde, eli mitkä käsittelytoimet ja järjestelmät kuuluivat mukaan arviointiin. Vaikutustenarviointi laadittiin excel-taulukkoon, jossa arviointi jäsenneltiin eri osioihin. Arviointiprosessin alussa käytiin läpi Regon yleinen kuvaus. Sen jälkeen arvioitiin vaikutustenarvioinnin tarpeellisuus ja käsittelyn oikeasuhteisuus. Seuraavaksi tarkasteltiin käsiteltäviä henkilötietoja, käsittelijöitä sekä rekisteröityjen oikeuksia. Tässä kohdassa huomioitiin myös arvioitavat oikeusperusteet sekä muut osapuolet.

Yksi keskeinen osa prosessia oli riskien arviointi, jossa tunnistettiin ja analysoitiin mahdollisia uhkia rekisteröityjen oikeuksille ja vapauksille. Arvioinnissa riskit jaettiin juridisiin, teknisiin ja organisatorisiin riskeihin. Taulukon viimeiselle välilehdelle kirjattiin lopuksi ehdotukset jatkotoimenpiteistä havaittujen riskien hallitsemiseksi tai poistamiseksi. Tunnistettuihin riskeihin suunniteltiin lieventäviä toimenpiteitä, kuten henkilöstön koulutuksia ja säännöllisiä järjestelmätarkastuksia.

4.2 Tietosuojasääntelyn vaatimusten toteutuminen

Miten voidaan varmistaa, että henkilötietojen käsittely täyttää kaikki tietosuojasääntelyn vaatimukset? Tämä kysymys on keskeinen kaikille organisaatioille, jotka käsittelevät henkilötietoja. Tässä kappaleessa käsitellään vaatimusten täyttämisen edellytyksiä ja arvioidaan sääntelyn toteutumista käytännössä.

Rego-järjestelmän henkilötietojen käsittelyperusteena on lakisääteisten velvoitteiden toteutuminen ja joissakin tilanteissa henkilötietojen käsittely perustuu myös rekisterinpitäjän oikeutettuun etuun, eli esimerkiksi järjestelmän toiminnan ja turvallisuuden varmistamiseen. Suostumuksella voidaan käsitellä myös arkaluonteisia tai muita tietoja, joita rekisteröity itse ilmoittaa. Kerättävinä ja käsiteltävinä henkilötietoina ovat kuitenkin lähtökohtaisesti vain välttämättömät henkilötiedot palvelun toteuttamiseksi tarkoitusperusteellisesti. Koska henkilötietojen käsittely perustuu pääosin lakisääteiseen velvoitteeseen, ei vastustamisoikeus ole voimassa. Rekisterinpitäjän oikeutettu etu perusteena antaa rekisteröidylle kuitenkin oikeuden vastustaa henkilötietojensa käsittelyä henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella, jolloin rekisterinpitäjän tulee arvioida uudelleen henkilötietojen käsittelyyn oikeuttavat perusteet ja keskeytettävä käsittely, ellei kyseessä ole pakottavaa oikeutettua perustetta tai ellei käsittely ole tarpeen oikeusvaateen laatimiseksi tai puolustamiseksi.

Rekisteröidylle informoidaan henkilötietojen käsittelystä palvelun käyttöehdoissa, joissa kuvataan tarkemmin se, mihin kerättyjä tietoja on sallittua käyttää. Rekisteröidyillä on pääsy omiin tietoihinsa ja ne tiedot, jotka eivät ole saatavilla, toimitetaan sähköpostitse pyydettäessä. Virheellisistä tiedoista on mahdollista tehdä oikaisupyyntö, joka toteutetaan määräaikojen puitteessa. Henkilötietoja säilytetään rekisterinpitäjän prosessien mukaisella aikataululla, poissulkien tarpeeton tieto, joka voidaan poistaa asiakkaan toimesta välittömästi. Automaattisen varmuuskopiointisyklin myötä tiedot kuitenkin poistuvat

viimeistään tietyn ajan, tässä tapauksessa 10 vuoden, kuluttua. Poistoprosessi on tietoturvan mukainen.
Organisatorista ja hallinnollista tietoturvaa suojataan myös käyttöoikeuksia rajaamalla, järjestelmäkirjauksilla, tietoturvakäytäntöjä- ja toimintasuunnitelmia noudattamalla sekä ylläpitämällä ja tietoja poistamalla. Henkilötietoja suojataan myös käyttämällä tuni-tunnuksia rekisteröidyn tunnistamiseksi sekä kaksivaiheisen tunnistautumisen avulla.

4.3 Riskien tunnistaminen ja analyysi

Riskien tunnistaminen aloitettiin analysoimalla excel-taulukkoon henkilötietojen keräämiseen ja käsittelyyn liittyviä toimenpiteitä ja tarkastelemalla rekisteröityjen oikeuksien toteutumista sekä muita mahdollisia vaikutuksia liittyen rekisteröityjen oikeuksiin ja vapauksiin. Tarkastelun kohteena olivat perusteellisesti kaikki henkilötietojen elinkaareen liittyvät kohdat, eli kerääminen, tallentaminen, yhdistäminen, käyttö ja muokkaaminen, luovutus ja saataville asettaminen, siirtäminen, säilyttäminen sekä hävittäminen. Näiden kohtien kanssa yhteen peilattiin tietosuojaperiaatteita, eli lainmukaisuutta ja kohtuullisuutta, läpinäkyvyyttä, käyttötarkoitussidonnaisuutta, minimointia ja säilytysaikojen rajoittamista, täsmällisyyttä, eheyttä, luottamuksellisuutta sekä käytettävyyttä.

Uhkien vakavuutta sekä todennäköisyyttä arvioitiin numeerisella taulukolla, jossa niin vakavuutta kuin todennäköisyyttä kuvaamaan valittiin oma numeronsa asteikolla 1-4. Luku 1 kuvasi vähäistä vakavuutta/epätodennäköistä uhkaa ja luku 4 puolestaan oli vakavuudessa kriittisen merkki, todennäköisyydessä lähes varman merkki. Valitut luvut kerrottiin keskenään kaavalla todennäköisyys x vakavuus, jonka jälkeen saatiin kuvaava riskiluku. Riskiarvot luokitellaan usein niin, että arvot 1–5 kuvaavat matalaa riskiä, 6–9 keskitason riskiä, ja arvot yli 10 korkeaa riskiä, jotka vaativat välittömiä toimia.

Mahdolliset uhat liittyivät esimerkiksi luottamuksellisuuden loukkaukseen, tietojen saatavuuden menetykseen sekä eheyden vaarantumiseen. Riskit voitiin jakaa esimerkiksi teknisiin riskeihin, organisatorisiin riskeihin sekä oikeudellisiin riskeihin.

4.3.1 Tekniset uhat

Tekniset uhat ovat riskejä, jotka liittyvät teknologiaan, järjestelmiin tai ohjelmistoihin ja jotka voivat vaarantaa arvioitavan järjestelmän tai toiminnon, tässä tapauksessa Regon, tietoturvan, luotettavuuden tai toimivuuden. Teknisiä uhkia ovat esimerkiksi järjestelmän kaatuminen, tiedon katoaminen, saataville asettaminen tai muu tiedon väärinkäyttäminen, joka voi johtaa tietovuotoihin tai automaattisen prosessin epäonnistuminen. Voidaan havainnoida, että Regon tapauksessa teknisten uhkien hallinta oli merkittävässä osassa vaikutustenarviointia. Erityisesti huomioitiin ohjelmiston omia mahdollisia uhkia, jotka liittyivät esimerkiksi tietojen saavutettavuuteen, automaattisesti tehtäviin järjestelmäkirjauksiin ja tietojen poistoprosessiin sekä tietojen säilytykseen tai tietovuodon mahdollisuuteen. Näitä arvioitiin kuitenkin kevyesti, sillä järjestelmä on suojattu tehokkaasti ja toimintaa seurataan jatkuvasti monella tasolla, jolloin mahdollisiin epäkohtiin puuttuminen välittömästi on näin ollen helpompaa minimoiden lopullista riskiä.

4.3.2 Organisatoriset uhat

Organisatorisilla uhilla tarkoitetaan tässä kohdassa niitä riskejä, mitkä aiheutuvat organisaation toimintatavoista viitaten sillä erityisesti ihmisten, tiedon ja prosessien hallintaan. Organisatoriset uhat ovat monesti näkymättömämpiä kuin tekniset, mutta yhtä kriittisiä, joka voitiin huomata vaikutustenarviointia tehdessä. On tärkeää, että organisaatiolla on saatavilla olevat asianmukaiset tiedot sekä selkeät toimintatavat ja vastuut.

Organisatorisina uhkina tarkasteltiin erityisesti tietojen käsittelyyn liittyvää prosessia, jolloin huomattiin, että toimintatapojen määritteleminen selkeästi esimerkiksi tietojen dokumentointiin, luovutukseen sekä säilytysaikaan liittyen esiintyivät alussa korkeina riskeinä. Huomioitiin myös mahdollinen hitaus viestinnässä, jolloin esimerkiksi henkilötietojen päivityspyyntö voisi jäädä

huomiotta, joka aiheuttaisi mahdollisen riskin turhien tai väärien tietojen säilyttämisestä. Lopussa uhat asettuivat kaikki numeroasteikolla epätodennäköiseen arvoon.

4.3.3 Oikeudelliset uhat

Oikeudelliset uhat ovat riskejä, jotka liittyvät suoraan lakiin, määräyksiin, sopimuksiin tai esimerkiksi viranomaisvaatimuksiin. Jos toiminta ei ole sovussa voimassa olevan lain kanssa, se voi johtaa erilaisiin seuraamuksiin, kuten sakkoihin, korvauksiin tai oikeudenkäynteihin. Tässä tapauksessa huomioidaan erityisellä tarkkuudella EU:n tietosuoja-asetus sekä tietosuojalaki.

Oikeudellisia riskejä havaittiin muutamia, jotka liittyivät lähtökohtaisesti vain välttämättömien henkilötietojen keräämiseen tarkoitusperusteellisesti, tietojen dokumentointiin sekä sopimuksiin. Myös nämä riskit arvioitiin epätodennäköisinä suojatoimenpiteiden jälkeen.

4.4 Suojaustoimet ja toimenpide-ehdotukset

Riskien tunnistaminen, niiden arviointi ja sopivien suojaustoimien suunnittelu ovat keskeisiä lähtökohtia, joiden varaan koko vaikutustenarvioinnin luotettavuus ja käytännön merkityksellisyys perustuvat. Tekniset, organisatoriset ja oikeudelliset riskit ovat selkeästi kytköksissä toisiinsa sekä vaikuttavat toistensa toteutumiseen. Tästä syystä on hyvä lähestyä riskejä yhtenäisenä kokonaisuutena, jossa tekniset, organisatoriset ja oikeudelliset näkökulmat täydentävät toisiaan ja mahdollistavat laajemman arvion mahdollisista uhkista.

Ensisijainen suojatoimenpide teknisten riskien kohdalla on järjestelmien toiminnan jatkuva seuraaminen, mahdollisiin epäkohtiin puuttuminen välittömästi, ohjelmien ylläpito ja vahvan suojauksen ylläpito sekä kehittäminen.
Ensisijaisia suojatoimenpiteitä organisatoristen riskien pienentämiseksi on tietosuoja-asetuksen noudattaminen henkilötietojen käsittelyyn liittyen, eli huolehtien siitä, että vain välttämättömät tiedot kerätään ja tietokentät näille tarkistetaan, jotta ne pysyvät varmasti tarkoituksenmukaisina. Muiden tietojen

kohdalla huolehditaan siitä, että tietojen käsittelylle on suostumus. Myös henkilötietojen luovuttamiseen, säilytysaikoihin, oikaisupyyntöjen käsittelyyn ja henkilötietojen poistamiseen on tärkeä laatia asianmukaiset omat toimenpiteet, joita noudattaa. Henkilöstön kouluttaminen on myös tärkeässä osassa mitä tulee ohjelmiston käyttöön ja tiedon käsittelyyn, ja tähän voidaan liittää mukaan myös käyttöoikeuksien jatkuva hallinnointi, joka vähentää omalta osaltaan riskiä henkilötietojen väärinkäyttöön liittyen.

Vaikka oikeudelliset riskit tulevat hyvin esiin myös aiemmissa suojatoimissa, voidaan erikseen vielä korostaa sitä, että organisaation on tärkeää toteuttaa henkilötietojen käsittelyprosessi GDPR:n ja tietosuojalain mukaisesti sekä tarvittaessa myös päivittää vaikutustenarviointia.

5 POHDINTA JA YHTEENVETO

Vaikka tietosuojan vaikutustenarviointi voidaan nähdä lakisääteisenä velvoitteena, toisin sanoen eräänlaisena pakkona, tulisi sitä pyrkiä tarkastelemaan myös organisaation toimintaa rakentavana sekä tukevana osana. Hyvin tehty DPIA auttaa riskien tunnistamisen sekä niiden minimoimisen lisäksi luomaan vahvaa pohjaa, jonka päälle yrityksen on helpompi lähteä rakentamaan kestäviä ja lainmukaisia toimintatapoja. Se mahdollistaa myös vahvan pohjan luottamuksen rakentamiseen esimerkiksi rekisteröityjen, oman henkilöstön ja viranomaisten kanssa. Työkaluna DPIA on hyvin laajamittainen, jonka avulla voidaan pyrkiä tekemään asioita paremmin – se tulisi siis nähdä monen eri asian mahdollistajana, eikä pakkona tai rajoituksena yritykselle.
Tämän työn avulla voidaan havainnoida, miten tietosuojan vaikutustenarviointi mahdollistaa riskejä tunnistamalla löytämään yrityksen heikkoja kohtia ja korjaamaan niitä usealla osa-alueella, vaikka vaikutustenarviointi virallisesti tehdäänkin järjestelmäkohtaisesti. Yrityksen näkökulmasta katsoen voidaan siis todeta, että DPIA ei ole vain hallinnollinen asiakirja, vaan ennemminkin jatkuvasti elävä työkalu organisaation itsetutkiskeluun.

Juridisesta näkökulmasta DPIA toimii riskienhallinnan työkaluna, jonka avulla organisaatio voi suunnitella henkilötietojen käsittelyä siten, että se on avoimesti dokumentoitua, tarpeeseen perustuvaa ja suhteellista. Vaikutustenarvioinnin kautta organisaatio voi osoittaa, että se noudattaa keskeisiä tietosuojaperiaatteita, kuten tietojen minimointia, asianmukaista tietoturvaa sekä rekisteröityjen oikeuksien kunnioittamista. Juridisesti se ei ole vain suositus, vaan myös lakisääteinen velvollisuus joissain tilanteissa, joissa henkilötietojen käsittely todennäköisesti aiheuttaa korkeaa riskiä rekisteröidyn oikeuksille ja vapauksille. Sen lisäksi, että suojataan rekisteröityjen oikeuksia, DPIA voi toimia myös välineenä yrityksen suojaamiseksi. Mikäli vaikutustenarviointi on tehty huolellisesti ja toimet dokumentoitu asianmukaisesti, se voi toimia lieventävänä seikkana viranomaistarkastuksissa tai oikeudellisissa prosesseissa.

Eettisesti tarkasteltuna kaikki lainmukainen toiminta ei ole automaattisesti perusteltua tai oikein yksilön oikeuksien ja kokemusten näkökulmasta. Vaikutustenarviointi auttaa varmistamaan, että henkilötietojen käsittelyä

tarkastellaan kokonaisvaltaisesti ja yksilöiden oikeuksia kunnioittaen, eikä vain juridisesta näkökulmasta. Kyseessä on siis työkalu, joka tehokkaasti suojelee myös rekisteröityjen oikeuksia, kuten yksityisyyttä ja itsemääräämisoikeuksia. DPIA tuo selkeästi nähtäväksi ne mahdolliset uhat ja haitat, mitä voi henkilölle aiheutua, ja näin ollen konkretisoi sen, että henkilötietojen käsittely on enemmän kuin vain teknistä tai juridista toimintaa – kyse on ennen kaikkea ihmisoikeuksien ja yksilön arvon kunnioittamisesta tämän avulla.

Regon kohdalla voidaan todeta, että DPIA on merkityksellisessä roolissa, sillä käsiteltävänä on sekä eettisiä, että oikeudellisia kysymyksiä. Esimerkiksi Regon Whistleblowing–osa mahdollistaa ilmoitusten tekemisen anonyyminä, joka tukee henkilön sananvapautta ja henkilökohtaista turvallisuutta, mutta se ei pelkästään riitä, ellei pystytä myös varmistumaan siitä, millaisia riskejä henkilötietojen käsittelyyn liittyy niin ilmoittajan kuin ilmoituksen kohteen osalta. Tietosuojan vaikutustenarvioinnin avulla pystytään hallita mahdollisia riskejä ennakoivasti ja tätä kautta varmistua myös siitä, että henkilötietojen käsittelyä on suojattu riittävästi.
Henkilöstön näkökulmasta DPIA tukee myös työntekijöiden oikeusturvaa, sillä se tarjoaa mahdollisuuden tarkastella kriittisesti esimerkiksi työntekijöiden seurantaa sekä niitä tapoja, joilla henkilötietoja kerätään ja käsitellään eri tilanteissa.

Yhteenvetona voidaan todeta luvun 1.2 kysymysten avulla, että DPIA-prosessin toteutus Rego-järjestelmän kohdalla on toteutettu systemaattisesti noudattaen tietosuojalainsäädännön vaatimuksia sekä organisaation sisäisiä ohjeistuksia. Voidaan myös todeta, että Rego-järjestelmän kohdalla on huolehdittu siitä, että rekisteröityjen oikeudet, kuten tietojen keräämisen rajoittaminen vain tarpeelliseen ja pääsyn salliminen henkilötietoihin, toteutuvat asianmukaisesti. Organisaation kehittämisen työkaluna DPIA on edistänyt jatkuvaa parantamista ja riskienhallintaa. Kokonaisuudessaan DPIA on todettu siis erinomaiseksi työkaluksi, joka tukee sekä lainmukaisten velvoitteiden täyttämistä että eettisten arvojen ja periaatteiden huomioimista organisaation toiminnassa.

Tulevaisuudessa voidaan ajatella, että DPIA:n merkitys tulee vielä kasvamaan entisestään. Tekoälyn ja automaattisen päätöksenteon yleistyessä myös

yritysten henkilötietojen käsittely on muutospisteessä ja vaatii entistä tarkempaa ennakoivaa riskienhallintaa. Tekoälyä ei tule kuitenkaan nähdä negatiivisena tekijänä, joka tekee asioista monimutkaisempia, vaan esimerkiksi Regon kohdalla tekoälyn hyödyntäminen voisi tulevaisuudessa tarkoittaa esimerkiksi whistleblowing –ilmoitusten automaattista jaottelua niiden vakavuuden perusteella. Tämä mahdollistaisi nopeamman reagoinnin vakaviin väärinkäytöksiin, mutta korostaisi puolestaan DPIA:n asemaa. Tekoälyä voitaisiin myös käyttää toteuttamaan automaattista riskien luokittelua, jossa kaikki säilytettävä data olisi kategorioitu esimerkiksi tietojen arkaluonteisuuden perusteella, joka mahdollistaisi resurssien keskittämisen kriittisimpiin tietoihin.
Yhteenvetona voidaan todeta, että tulevaisuudessa DPIA hyödyntää yhä enemmän kehittynyttä automaatiota ja analytiikkaa, joka auttaa tuomaan tietosuojan osaksi organisaation strategista päätöksentekoa ja vastuullista toimintaa.

Tämän opinnäytetyöprosessin aikana sain erinomaisen käsityksen siitä, mitä tietosuojan vaikutustenarviointi tarkoittaa käytännön tasolla ja miksi sen tekeminen on organisaation tietosuojatyössä keskeisessä roolissa. Prosessin aikana ymmärsin, miten DPIA toimii paitsi riskienhallinnan työkaluna, mutta myös organisaation vastuullisuuden osoittajana. Käytännön osuudessa taulukkomuotoisen DPIA:n laatiminen vaati huolellisuutta. Jokainen taulukon osa-alue edellytti tarkkaa harkintaa siitä, mitä henkilötietoja käsitellään, mihin tarkoitukseen niitä käytetään, kenellä on pääsy tietoihin ja millä tavoin ne suojataan tehokkaasti. Riskien arviointiosio opetti minulle sen, kuinka tärkeää on perustella jokainen arvioitu riski ja toimenpide selkeästi, jotta arviointi tukee aidosti tietosuojan toteutumista. Oppimisen yhteenvetona voin todeta, että tämä kokonaisuus ja erityisesti DPIA:n käytännön toteutus vahvisti merkittävästi tietosuojan osaamistani sekä ymmärrystä siitä, miten tehdään ja miksi tehdään.

LÄHTEET

Andreasson, A. & Ylipartanen, A. 2022. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus (GDPR). E-kirja. 2. Helsinki: Tietosanoma. Viitattu 10.7.2025. Vaatii käyttöoikeuden. https://www.ellibslibrary.com/reader/9789518854817

Euroopan komissio. n.d. Mikä on rekisterinpitäjä tai tietojen käsittelijä? Verkkosivu. Viitattu 11.7.2025. Saatavissa: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_fi

European Comission. n.d. Data Protection in the EU. Verkkosivu. Viitattu 11.7.2025. Saatavissa: https://commission.europa.eu/law/law-topic/data-protection_en

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679.Virallinen lehti L 119, 4.5.2016. Verkkosivu. Viitattu 17.7.2025. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679

Evans, A. 2022. Enterprise Cybersecurity in Digital Business. E-kirja. 1. painos. London: Routledge. Viitattu 10.7.2025. Vaatii käyttöoikeuden. https://www.oreilly.com/library/view/enterprise-cybersecurity-in/9781000459371/

Kharpal, A. 2023. Meta fined record $1.3 billion over EU user data transfers to the U.S. CNBC. Verkkosivu. Viitattu 11.7.2025. Saatavissa: https://www.cnbc.com/2023/05/22/meta-fined-record-1point3-billion-over-eu-user-data-transfers-to-the-us-.html

Qreform. 2025. Rego Whistleblow. Verkkosivu. Viitattu 17.7.2025. Saatavissa: https://www.qreform.com/rego-whistleblow/

Shah, S. 2023. Meta Was Just Fined a Record-Breaking $1.3 Billion by E.U. Time. Verkkosivu. Viitattu 11.7.2025. Saatavissa: https://time.com/6281713/meta-facebook-fine-eu/

Tieteen termipankki. 2025. Anonymisointi. Verkkosivu. Viitattu 21.7.2025. Saatavissa: https://tieteentermipankki.fi/wiki/Avoin_tiede:anonymisointi

Tietosuojavaltuutetun toimisto. n.d. Ennakkokuuleminen. Verkkosivu. Viitattu 21.7.2025. Saatavissa: https://tietosuoja.fi/ennakkokuuleminen

Tietosuojavaltuutetun toimisto. n.d. Erityisten henkilötietoryhmien käsittely. Verkkosivu. Viitattu 21.7.2025. Saatavissa: https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely

Tietosuojavaltuutetun toimisto. n.d. Henkilötietojen käsittelijät. Verkkosivu. Viitattu 21.7.2025. Saatavissa: https://tietosuoja.fi/henkilotietojen-kasittelijat

Tietosuojavaltuutetun toimisto. n.d. Henkilötietojen käsittely. Verkkosivu. Viitattu 21.7.2025. Saatavissa: https://tietosuoja.fi/henkilotietojen-kasittely

Tietosuojavaltuutetun toimisto. n.d. Henkilötietojen pseudonymisointi ja anonymisoidut tiedot. Verkkosivu. Viitattu 21.7.2025. Saatavissa: https://tietosuoja.fi/pseudonymisointi-anonymisointi

Tietosuojavaltuutetun toimisto. n.d. Tietosuojatyön painopisteitä. Verkkosivu. Viitattu 21.7.2025. Saatavissa: https://tietosuoja.fi/tietosuojatyon-painopisteita

Tietosuojavaltuutetun toimisto. n.d. Tietoturvaloukkaukset. Verkkosivu. Viitattu 21.7.2025. Saatavissa: https://tietosuoja.fi/tietoturvaloukkaukset

Tietosuojavaltuutetun toimisto. 2020. Tietosuojavaltuutetun toimiston seuraamuskollegio määräsi kolme seuraamusmaksua tietosuojarikkomuksista. Verkkosivu. Viitattu 11.7.2025. Saatavissa: https://tietosuoja.fi/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista

Tietosuojavaltuutetun toimisto. n.d. Vaikutustenarviointi. Verkkosivu. Viitattu 10.7.2025. Saatavissa: https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto. n.d. Oikeus vastustaa tietojen käsittelyä. Verkkosivu. Viitattu 21.7.2025. Saatavissa: https://tietosuoja.fi/oikeus-vastustaa-kasittelya