Pelillistämisen keinot tietosuojaosaamisen kehittämisessä. Esimerkkinä Humanistinen ammattikorkeakoulu Oy.

Christa Sairio

2025 Laurea

Laurea-ammattikorkeakoulu

Pelillistämisen keinot tietosuojaosaamisen edistämisessä. Esimerkkinä Humanistinen ammattikorkeakoulu Oy

Christa Sairio

Tulevaisuuden innovatiiviset digitaaliset järjestelmät

Opinnäytetyö

Toukokuu, 2025

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tulevaisuuden innovatiiviset digitaaliset palvelut

Tradenomi (YAMK)

Christa Sairio

Pelillistämisen keinot tietosuojaosaamisen edistämisessä. Esimerkkinä Humanistinen ammattikorkeakoulu Oy

Vuosi 2025 Sivumäärä 92

Yleinen tietosuoja-asetus eli GDPR (General Data Protection Regulation) tuli voimaan toukokuussa 2018. Se asettaa yhtenäiset velvoitteet henkilötietojen turvalliselle käsittelylle koko EU-alueella. Tietosuoja on keskeinen osa nykyajan organisaatiokulttuuria. Työntekijöiden osaamista on ylläpidettävä ja päivitettävä säännöllisesti, jotta tietosuojauhkia voidaan ennaltaehkäistä ja tunnistaa.

Tämän opinnäytetyön tarkoituksena oli ymmärtää, kuinka pelillistäminen voi edistää tietosuojaosaamisen kehittymistä. Tavoitteena oli suunnitella ja toteuttaa tietosuojapeli, joka parantaa työntekijöiden kykyä tunnistaa ja reagoida arjen tietosuojatilanteisiin. Opinnäytetyön tietoperusta muodostuu EU-tasoiseen tietosuoja-asetukseen, Suomen kansalliseen tietosuojalakiin ja pelillistämiseen työelämässä. Opinnäytetyön tutkimuksellinen lähestymistapa on konstruktiivinen tutkimus.

Opinnäytetyön toimeksiantaja on Humanistinen ammattikorkeakoulu Oy. Tietosuojaosaamisen kehittämisen tueksi luotiin pelillinen ympäristö interaktiiviselle Thinglink-alustalle, jossa pelaaja voi harjoitella osaamistaan kohdennettujen tietosuojaskenaarioiden avulla. Peliä testasi seitsemän organisaation työntekijää, joiden työtehtäviin kuuluu päivittäinen henkilötietojen käsittely. Pelillisen materiaalin vaikutusta työntekijöiden tietosuojaosaamiseen selvitettiin kyselyillä, jossa osallistujat arvioivat tietosuojaosaamistaan ennen peliä ja sen jälkeen.

Tulokset osoittivat pelillistämisen lisäävän työntekijöiden tietosuojaosaamista ja motivaatiota kehittää omaa tietosuojaosaamistaan. Tietosuojaosaamisen edistäminen pelillistämisen avulla on yksi keino täyttää lain vaatimaa osoitusvelvollisuutta.

Organisaation antaman palautteen mukaan pelillistämisen kokemus ehkä jopa tylsäksi koettuun aiheeseen oli innostava. Lisäksi organisaation mukaan osallistujat pitivät todella tärkeänä, että pelillinen oppiminen tarjoaa konkreettisia esimerkkejä ja tilaisuuden testata tietojaan käytännössä. Tämä auttaa ymmärtämään ja sisäistämään asioita paremmin kuin pelkkä tekstin lukeminen.

Pelillistäminen on hyvä menetelmä tietosuojaosaamisen kehittämisessä, mutta sen onnistuminen edellyttää huolellista suunnittelua ja kohderyhmän tarpeiden huomioimista. Pelillistämisen hyödyntäminen tarjoaa potentiaalia myös laajempaan osaamisen kehittämiseen organisaatioissa. Tämänkaltaista pelaamisen konseptia voidaan hyödyntää monella toimialalla. Jatkokehittämisenä suositellaan pelin laajentamista muihin kohderyhmiin ja eri organisaatiokonteksteihin, tietosuojaportaalin määrittämistä ja narratiivien lisäämistä koulutusmateriaaliin.

Asiasanat: GDPR, tietosuoja, tietosuojaosaaminen, pelillistäminen, interaktiivinen oppiminen

Laurea University of Applied Sciences **Abstract**

Innovative Digital Services of the Future

Master of Business Administration

Christa Sairio

Gamification Methods for Advancing Data Protection Competence. Example of Humak University of Applied Science

Year 2025 Pages 92

The General Data Protection Regulation (GDPR) came into force in May 2018. It establishes uniform obligations for the secure processing of personal data throughout the EU area. Data protection is a central part of modern organizational culture. Employees' skills must be maintained and updated regularly to prevent and identify data protection threats.

The purpose of this thesis was to understand how gamification can promote the development of data protection knowledge. The aim was to design and implement a data protection game that improves employees' ability to identify and respond to everyday data protection situations. The knowledge base of the thesis consists of the EU-level data protection regulation, Finland's national data protection law, and gamification in working life. The research approach of the thesis is constructive research.

The thesis was commissioned by Humak University of Applied Sciences. To support the development of data protection competence, a gamified environment was created on the interactive Thinglink platform, where players can practice their skills through targeted data protection scenarios. The game was tested by seven employees of the organization, whose daily tasks involve the handling of personal data. The impact of the gamified material on employees' data protection competence was examined through surveys in which participants evaluated their competence before and after playing the game.

The results showed that gamification increases employees' data protection knowledge and motivation to develop their own data protection skills. Promoting data protection knowledge through gamification is one way to fulfill the accountability required by law.

According to feedback from the organization, the gamification experience for a topic that might even be considered boring was inspiring. Additionally, according to the organization, participants found it important that gamified learning provides concrete examples and an opportunity to test their knowledge in practice. This helps to understand and internalize things better than just reading text.

Gamification is a good method for developing data protection knowledge, but its success requires careful planning and consideration of the target group's needs. Utilizing gamification also offers potential for broader skills development in organizations. This kind of gaming concept can be utilized in many industries. As further development, it is recommended to expand the game to other target groups and different organizational contexts, define a data protection portal, and add narratives to the training material.

Keywords: GDPR, data protection, data protection competence, gamification, interactive learning

Sisällys

1 Johdanto

Tietosuoja on digitalisoituneessa maailmassa keskeinen ja globaali teema. Se on noussut viime vuosina haasteeksi organisaatioille. Henkilötietoja kerätään ja käsitellään valtavia määriä, ja ne liikkuvat pääosin digitaalisesti. Teknologian nopea kehitys ja kasvavat tietoturvauhat, kuten kyberhyökkäykset, tietomurrot ja identiteettivarkaudet ovat vahvistaneet henkilötietojen suojan merkitystä kaikilla toimialoilla. Organisaatiot ympäri maailmaa pyrkivät kehittämään järjestelmiä ja toimintamalleja henkilötietojen käsittelyyn.

Euroopan unionissa tietosuojan merkitys korostui erityisesti, kun EU:n yleinen tietosuoja-asetus (GDPR) astui voimaan. Se asettaa yhtäläiset vaatimukset tietosuojan käsittelylle kaikissa EU-maissa. Asetus antaa yksilöille kattavat oikeudet hallita omia henkilötietojaan ja asettaa organisaatioille velvollisuuksia tietosuojan hallinnassa. GDPR ei ainoastaan vahvistanut yksilöiden oikeuksia, vaan se myös velvoittaa organisaatioita osoittamaan lainsäädännön noudattamisen.

Suomessa EU:n tietosuoja-asetusta täydentää kansallinen tietosuojalaki. Laki sisältää säännöksiä, jotka täsmentävät tietosuoja-asetuksen sisältöä. Kansallista tietosuojalakia sovelletaan EU-alueella tapahtuvaan henkilötietojen käsittelyyn, jos organisaation toimipaikka sijaitsee Suomessa. (Tietosuojalaki 2018) Henkilötietojen käsittely on monen organisaation ydinprosessi, ja lain voimaantulon myötä organisaatiot ovat joutuneet uudelleen miettimään henkilötietojen keräämisen perusteita.

Organisaatioille tietosuoja ei ole pelkästään lakisääteinen velvoite, vaan kilpailuetu, joka vahvistaa asiakkaiden luottamusta ja tukee riskienhallintaa. Viime vuosina maailmalla ja myös Suomessa on tapahtunut useita merkittäviä tietoturvaloukkauksia, joissa henkilötietoja on päätynyt vääriin käsiin inhimillisten virheiden, identiteettivarkauksien, tietojenkalastelun, haittaohjelmien tms. takia. (Kyberturvallisuuskeskus 2020). Tietomurrot ja luottamuksen menetys ovat uhkia, jotka koskettavat kaiken kokoisia organisaatioita kaikilla toimialoilla.

Työntekijän näkökulmasta tietosuoja voi vaikuttaa tylsältä ja abstraktilta aiheelta, vaikka työntekijät ovat keskeisessä roolissa tietosuojan toteutumisessa. Tietosuojalainsäädäntö velvoittaa organisaatiota huolehtimaan työntekijöiden riittävästä osaamisesta. Tietosuojaosaaminen on arvokas etu työmarkkinoilla, mutta samalla myös työntekijän henkilökohtainen etu. Tämä tekee tietosuojaosaamisen kehittämisestä olennaista.

Tietosuojaosaamisen merkitys on kasvanut tietosuoja- ja tietoturvauhkien lisääntyessä. Uhkien torjunta edellyttää työntekijöiltä osaamista sekä kykyä tunnistaa ja hallita riskejä. Organisaatioiden liiketoiminnan jatkuvuuden varmistamiseksi niillä on oltava osaava henkilökunta. Henkilötietojen sähköinen käsittely nopeuttaa toimintoja, mutta samalla se lisää riskiä

tietosuojaloukkauksille ja tietoturvaongelmille. Data on tietotalouden ydin, ja siihen liittyvät riskit kasvavat jatkuvasti. Andreasson, Riikonen & Ylipartanen (2019, 13) korostavat tiedon arvoa ja kuvaavat sitä kasvavaksi ja merkittäväksi tuotannontekijäksi.

Vakiintuneet koulutusmenetelmät, kuten luennot ja verkkokurssit, eivät aina riitä motivoimaan työntekijöitä tietosuojaosaamisen kehittämiseen. Pelillistäminen tarjoaa uuden lähestymistavan, joka tekee oppimisesta interaktiivista ja käytännönläheistä. Työntekijät voivat simuloida todellisia tietosuojatilanteita, jolloin passiivisen tiedon vastaanottaminen muuttuu aktiiviseksi oppimiseksi. Työntekijöiden taitojen ja kykyjen jatkuva kehittäminen on välttämätöntä, jotta organisaatio pysyy kilpailukykyisenä.

Ilmiö liittyy erityisesti siihen, miten työntekijöiden osaamista voidaan kehittää niin, että he tunnistavat ja hallitsevat tietosuojauhkiin liittyviä riskejä arjen työtehtävissä. Koska työtehtävät sisältävät runsaasti tietosuojaan liittyviä tilanteita, tämän kehittämistyön aihevalinta oli luonteva.

Opinnäytetyön kieliasun ja tekstin sujuvoittamisessa on osittain käytetty Microsoft Copilot- ja ChatGPT 3.5 ja 4.0 mini -tekoälyohjelmia.

1.1 Opinnäytetyön tarkoitus ja tavoite

Tässä opinnäytetyössä sovelletaan konstruktiivisen tutkimuksen lähestymistapaa. Opinnäytetyön tarkoitus on ymmärtää pelillistetyn oppimisen tarjoamia mahdollisuuksia tietosuojaosaamisen kehittämisessä. Oppimisen pelillistäminen tarkoittaa peleissä käytettyjen elementtien hyödyntämistä pelaajan motivointiin. Aihetta voidaan kuvata tietosuojaosaamisen edistämisenä pelillistämisen avulla, jossa tavoitteena on vahvistaa työntekijöiden tietosuojaosaamista, sillä pelillistämisen hyödyntäminen oppimisen tukena voi lisätä tietosuojaosaamisen käytännönläheisyyttä.

Opinnäytetyön tavoitteena on suunnitella ja toteuttaa tietosuojapeli, joka parantaa työntekijöiden kykyä tunnistaa ja reagoida tietosuojauhkiin arjessa. Peli on suunniteltu käsittelemään samoja tietosuojan teemoja, joita kartoitetaan ennen pelin alkamista toteutettavassa kyselyssä. Kyselyssä selvitetään työntekijöiden lähtötaso tietosuojaan liittyvissä asioissa, ja pelin päätyttyä toteutetaan toinen kysely, jolla arvioidaan oppimistuloksia. Pelin vaikutuksia arvioidaan vertaamalla ennen ja jälkeen -kyselyjen tuloksia. Näin voidaan tarkastella, miten peli ja pelillistäminen vaikuttaa tietosuojaosaamisen kehittymiseen ja kuinka pelin rakenne, ja osallistujien motivaatio ovat vaikuttaneet oppimistuloksiin.

Opinnäytetyössä rajoitutaan tarkastelemaan vain Humanistisen ammattikorkeakoulu Oy:n työntekijöitä ja heidän osaamistaan tietosuojasta. Opinnäytetyössä ei käsitellä tekoälyn tietosuojaa, tiedonhallinta- eikä julkisuuslain vaikutuksia tietosuojaan.

1.2 Toimeksiantajan esittely

Humanistinen ammattikorkeakoulu Oy (Humak) on valtakunnallinen ammattikorkeakoulu, joka sai vakinaisen toimiluvan 2002. Se on erikoistunut järjestö- ja nuorisotyöhön, seikkailukasvatukseen, työyhteisöjen kehittämiseen, kulttuurituotantoon, luovan toimialan yrittäjyyteen ja tulkkausalaan. Humakilla on alueyksiköitä kuudella paikkakunnalla: Helsinki, Kauniainen, Tampere, Turku, Jyväskylä ja Kuopio. (Humak tilinpäätös 2023.) Loppuvuodesta 2024 organisaation palveluksessa työskentelee yhteensä noin 160 henkilöä.

Humak on vahvuusalojensa johtava toimija Suomessa ja Euroopassa keskittyen koulutukseen, tutkimus-, kehittämishankkeisiin ja innovaatiotoimintaan (TKI) sekä julkaisu- ja liiketoimintaan. Humak toimii valtakunnallisena ja alueellisena kehittäjäkumppanina erityisesti yhteisöjen kehittämisen, kulttuurituotannon ja kielellisen saavutettavuuden aloilla. Humak panostaa vahvasti TKI-toimintaan, jonka puitteissa toteutetaan vuosittain lukuisia erillisrahoitteisia hankkeita. TKI on myös tiiviisti yhdistetty koulutustoimintaan, joten opiskelijoiden osaaminen on mukana monissa hankkeissa. (Humak 2024.)

Tutkinto-opiskelijoita Humakissa on noin 2600 ja opiskelu on mahdollista toteuttaa päivä-, monimuoto- tai verkko-opintoina. Tutkinto-opiskelijoiden lisäksi on tuhansia avoimen ammattikorkeakoulun opiskelijoita, jossa tarjolla on yksittäisiä kursseja tai tutkintoon johtavia polkuopintoja. Palautteiden perusteella valmistuneet opiskelijat ovat tyytyväisiä saamaansa tutkintoon ja viisi vuotta valmistumisen jälkeen tehtävän uraseurantakyselyn mukaan valmistuneet opiskelijat pystyvät hyödyntämään opiskeluaikana hankittua osaamista työelämässä. (Humak 2024; Ammattikorkeakoulujen uraseurantakysely 2024.)

Humakin strategia keskittyy ydinosaamisen vahvistamiseen, jota pidetään keskeisenä tekijänä, vaikka toimintaympäristöt tai rahoitusmallit muuttuisivat. Osaamiskärkiä, kuten avointa ammattikorkeakoulua ja TKI-toimintaa on kehitetty ja vahvistettu ja strategian toimeenpanoa tukevat erilaiset kehittämisohjelmat. Vuoden 2023 tilastojen mukaan toiminnan painopisteitä on onnistuttu siirtämään jatkuvan oppimisen, ylempien ammattikorkeakoulututkintojen ja TKI-toiminnan vahvistamiseen ja tämä tukee strategian tavoitteita. (Humak tilinpäätös 2023.)

Humak haluaa edistää työntekijöiden osaamisen kehittämistä eri aloilla ja tietosuoja on yksi ajankohtainen teema. Organisaatiolle halutaan löytää konkreettinen ratkaisu, jonka avulla voidaan parantaa työntekijöiden käytännön tietosuojaosaamista. Tavoitteena on vahvistaa organisaation riskienhallintakykyä ja edistää tietosuojan toteutumista arjessa.

2 Kohti organisaatioiden parempaa tietosuojaosaamista

Tässä kappaleessa tarkastellaan Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2016), Suomen kansallista

tietosuojalainsäädäntöä 1050/2018 (Tietosuojalaki 2018) sekä pelillistämistä ja sen teoreettisia lähtökohtia. Nämä muodostavat tämän opinnäytetyön keskeisen tietoperustan. Lainsäädännön vaikutuksia käsitellään organisaation työntekijöiden tietosuojaosaamisen edistämisen näkökulmasta.

Tietosuojaosaamisen kehittämiseen voidaan hyödyntää erilaisia menetelmiä, joista yksi on pelillistäminen. Oppimisen pelillistäminen tarkoittaa pelielementtien hyödyntämistä työntekijän motivoinnissa ja osaamisen kehittämisessä. Sen avulla monimutkaisia lakipykäliä voidaan esittää ymmärrettävämmin ja tarjota työntekijälle omaan työhön liittyviä konkreettisia esimerkkejä. Pelillistäminen voi tarjota uudenlaisen lähestymistavan tietosuojatiedon omaksumiseen ja vahvistaa organisaation tietosuojakulttuuria. Opinnäytetyössä tarkastellaan, miten pelillistämisen periaatteita voidaan hyödyntää tietosuojaosaamisen kehittämisessä.

Tietosuojalainsäädäntö edellyttää organisaatiolta vahvaa ja ajantasaista tietosuojaosaamista. Tietosuoja keskittyy henkilötietojen käsittelyn turvallisuuteen ja lainmukaisuuteen, ja monille organisaatioille se on olennainen osa päivittäisiä työtehtäviä. Tietosuojaosaaminen tukee myös organisaation riskienhallintaa antamalla työntekijöille valmiuksia riskien tunnistamiseen ja hallintaan. Lainsäädännön vaatimukset luovat perustan tietosuojaosaamisen tärkeydelle, ja sen ymmärtäminen on edellytys osaamisen kehittämiselle.

2.1 EU:n yleinen tietosuoja-asetus

EU:n yleinen tietosuoja-asetus GDPR (General Data Protection Regulation) astui voimaan vuonna 2016, ja sitä alettiin soveltamaan 2018. Asetusta pidetään yleisesti henkilötietojen sääntelyn ”kultaisena standardina”. Yleinen tietosuoja-asetus asettaa yhtenäiset säännöt henkilötietojen suojelulle koko EU-alueella.

Tietosuoja tarkoittaa henkilötietojen oikeaoppista käsittelyä ja se on jatkuva prosessi, johon vaikuttaa laaja lainsäädäntö. Tietosuojasäännökset määrittelevät, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Käytännössä tietosuojalainsäädäntö koskee kaikkia organisaatioita, jotka keräävät ja käsittelevät henkilötietoja. Yleisen tietosuoja-asetuksen keskeisenä tavoitteena on suojella luonnollisten henkilöiden perusoikeuksia ja -vapauksia sekä erityisesti heidän oikeuksiaan henkilötietojen suojaan. Tämä sisältää oikeuden saada tietoa, oikeuden tietojen poistamiseen ja oikeuden tutustua omiin tietoihin. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, (yleinen tietosuoja-asetus).)

Henkilötietojen määrittely on tärkeää, sillä ne kattavat kaikki tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti. Suora henkilötieto tarkoittaa tietoa, jonka perusteella henkilö voidaan tunnistaa välittömästi ilman lisätietoja. Välillinen henkilötieto ei yksinään mahdollista henkilön tunnistamista, mutta yhdistettynä muihin tietoihin se voi johtaa tunnistamiseen.

Henkilötietoja ovat esimerkiksi nimi, syntymäaika, puhelinnumero ja kotiosoite. Myös välilliset tiedot, kuten auton rekisterinumero tai lemmikin eläinlääkäritiedot voivat paljastaa henkilöstä enemmän kuin ajattelisi. Pelkästään lemmikin terveystiedot eivät ole henkilötietoja. Jos ne voidaan yhdistää omistajan nimeen, osoitteeseen tai muuhun tunnistetietoon, niistä tulee henkilötietoja.

Näiden tietojen käsittelyyn liittyy tietosuoja-asetuksen periaatteet, kuten sisäänrakennettu ja oletusarvoinen tietosuoja. Sisäänrakennettu tietosuoja varmistaa, että yksityisyys on huomioitu jo järjestelmien ja prosessien suunnitteluvaiheessa. Oletusarvoinen tietosuoja edellyttää, että henkilötietoja käsitellään oletusarvoisesti korkealla yksityisyydensuojalla (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 2016)

Tietosuoja-asetuksen voimaantulon jälkeen vuonna 2018 eurooppalaiset yritykset ovat joutuneet rajoittamaan tietojen tallennusta ja käsittelyä. GDPR on vaikuttanut merkittävästi EU:ssa toimiviin henkilötietoja kerääviin yrityksiin, sillä sen noudattaminen on lisännyt datan kustannuksia noin 20 prosenttia. Erityisesti IT-alalla vaikutus on ollut jopa 24 prosenttia, kun teollisuudessa ja palvelualoilla kustannusten kasvu on ollut noin 18 prosenttia. Vaikka GDPR on vähentänyt datan keräämistä ja käsittelyä, informaation tuottamisen kustannukset ovat siitä huolimatta nousseet noin neljä prosenttia. (Claburn 2024.)

Oikeusministeriö raportoi vuonna 2024 toista kertaa EU-komissiolle EU:n yleisen tietosuoja-asetuksen soveltamiskokemuksista Suomessa. Raportti perustuu 66 palautteeseen julkiselta ja yksityiseltä sektorilta, ja siinä analysoidaan yleisen tietosuoja-asetuksen hyötyjä ja haasteita. Raportissa käsitellään myös EU:n yleisen tietosuoja-asetuksen ja muun lainsäädännön yhteensovittamista. Hyötyinä nousee esille lisääntynyt tietoisuus tietosuojasta, henkilötietojen vahvistuminen organisaatioissa sekä yhtenäisen lainsäädännön etu. Ongelmiksi on koettu asetuksen vaikeaselkoisuus, tulkinnanvaraisuus sekä sen soveltamisesta aiheutunut hallinnollinen taakka. Lisäksi osa organisaatioista koki, ettei viranomaisohjeistus ole riittävän selkeää ongelman ratkaisemiseen. (Kantonen & Pohjalainen 2024.)

Tietosuoja-asetuksen voimaantulo on lisännyt yksityishenkilöiden ja organisaatioiden tietoisuutta tietosuojasta. Samalla se on kasvattanut kysyntää tietosuojaratkaisuille, kuten ohjelmistoille ja asiantuntijapalveluille. Tämä näkyy mm. Internet-haulla, jossa tietosuojaan liittyvillä hakusanoilla saadaan suuri määrä aiheeseen liittyviä hakutuloksia ja palveluntarjoajia. Tietosuoja on jo terminä tuttu ja siitä puhutaan toisinaan myös kriittisesti. Yleisesti koetaan, että tietosuoja voi tehdä henkilötietoja sisältävän tutkimuksen toteuttamisesta haastavaa.

2.2 Suomen kansallinen tietosuojalaki

Vuoden 2019 alusta voimaan tullut kansallinen tietosuojalaki täydentää toukokuussa 2018 voimaan tullutta EU:n yleistä tietosuoja-asetusta. Yleinen tietosuoja-asetus kumosi Suomen aiemman henkilötietolain 523/1999. Yksi keskeinen ero niiden välillä on se, että

tietosuojalailla säädetään tietosuoja-asetuksessa tarkoitetusta kansallisesta valvontaviranomaisesta, joka Suomessa on tietosuojavaltuutettu (Tietosuojavaltuutetun toimisto 2024a.) Tietosuojalaki varmistaa, että henkilötietojen käsittely tapahtuu lainmukaisesti ja että tietosuoja on Suomen olosuhteissa riittävällä tasolla (Kuntaliitto 2019).

Suomen julkiselle sektorille lisähaasteita aiheuttaa tietosuoja- ja julkisuuslain yhteensovittaminen. Yksi keskeinen ongelma on velvollisuus vastata julkisuuslain mukaisiin tietopyyntöihin. Lausunnonantajien mukaan nämä haasteet johtuvat oikeuksien vastakkaisista tavoitteista ja lakien yhteensovittaminen vie aikaa ja resursseja. (Kantonen ym. 2024.)

Kansallisessa tietosuojalaissa käsitellään myös Suomen tietosuojavaltuutetun asemaa ja tehtäviä, tietosuojarikkomusten sanktioita sekä erityisiä tietojenkäsittelytilanteita. Suomen tietosuojavaltuutettuna on toiminut Anu Talus marraskuusta 2020 alkaen. Lisäksi hänet valittiin toukokuussa 2023 Euroopan tietosuojaneuvoston (EDPB) puheenjohtajaksi, ja hän edustaa Suomea kyseisessä neuvostossa. Hänen edeltäjänsä, eläkkeelle jääneen Reijo Aarnion uran tunnuslauseet olivat ”Tietosuoja on iloinen asia” ja ”Tietosuoja on menestystekijä”. Talus on ilmoittanut jatkavansa samoilla linjoilla. (Pärssinen 2023.)

Tietosuojalaki vahvistaa tietosuojavaltuutetun toimivaltaa, joka antaa valtuudet puuttua mahdollisiin tietosuojarikkomuksiin. Tämä sisältää myös sakkojen ja muiden sanktioiden määräämisen organisaatioille. Tietosuojavaltuutetulla on keskeinen rooli lain valvonnassa ja täytäntöönpanossa Suomessa. (Oikeusministeriö 2018.)

2.3 Tietosuojan toteutus käytännössä

Lainsäädäntö suojaa yksityisyyttä ja korostaa sen tärkeyttä. Pelkkä lainsäädäntö ei kuitenkaan riitä, vaan organisaatioiden ja yksilöiden on osallistuttava turvallisemman maailman rakentamiseen. Tämä edellyttää tietosuojan edistämistä paitsi sääntöjen noudattamisen kautta myös vastuullisella toiminnalla, jatkuvalla koulutuksella ja tietosuojatietoisuuden lisäämisellä.

Organisaatioilla on oltava selkeät tietosuojakäytännöt, ja niiden on varmistettava teknisten ja hallinnollisten suojatoimien riittävyys. Lisäksi on tärkeää luoda avoin tietosuojakulttuuri, jossa henkilötietojen käsittely on läpinäkyvää ja eettistä. Kun organisaatiot ja yksilöt toimivat yhdessä, henkilötietojen käsittely voi olla sekä turvallista että tehokasta, edistäen luottamusta ja yksityisyyden suojaa digitaalisessa maailmassa.

2.3.1 Rekisterinpitäjä

Rekisterinpitäjä on keskeinen toimija henkilötietojen käsittelyssä. Rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot sekä vastaa henkilötietojen lainmukaisesta käsittelystä. (Korpisaari, Pitkänen & Warma-Lehtinen 2018.)

Korpisaaren ym. (2018) mukaan rekisterinpitäjä on suomenkielisessä käännöksissä epäonnistunut nimitys, sillä henkilötietojen ei tarvitse olla rekisterissä. Rekisterinpitäjä ei siis ole pelkästään taho, joka ylläpitää varsinaista rekisteriä, vaan mikä tahansa toimija, joka käsittelee henkilötietoja digitaalisesti ja päättää niiden käsittelystä ja keinoista. Organisaation työntekijät käsittelevät henkilötietoja rekisterinpitäjän tehtävien toteuttamiseksi (Euroopan komissio 2025).

Rekisterinpitäjän velvollisuuksiin kuuluu tietosuojaperiaatteiden noudattaminen kaikissa henkilötiedon käsittelyvaiheissa ja pystyttävä osoittamaan niiden noudattaminen. Kaikki toimenpiteet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuvaan riskiin. Rekisterinpitäjän on arvioitava nämä riskit ja niiden perusteella toteuttaa tarvittavat suojatoimet. (EDPB 2025a.)

2.3.2 Rekisteröity

Rekisteröity on yksilö, jonka henkilötietoja oppilaitos tai muu rekisterinpitäjä käsittelee palkanmaksun, asiakastietojen, opiskelijarekisterin tms. yhteydessä. Käytännössä rekisteröity voi olla kuka tahansa asiakas, opiskelija, työntekijä tai verkkosivuston vierailija. Korpisaaren ym. (2018) mukaan myös rekisteröity on suomenkielisessä käännöksessä epäonnistunut nimitys, sillä se on harhaanjohtava. Tietosuoja-asetuksen säädökset koskevat kaikkia ihmisiä, joiden henkilötietoja käsitellään, vaikka niitä ei ole tallennettu rekisteriin.

EU:n yleisen tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus saada selkeää ja ymmärrettävää tietoa siitä, mitä henkilötietoja kerätään ja mihin tarkoitukseen niitä käytetään. Henkilötietojen käsittelyn on perustuttava tietosuoja-asetuksen määritteleмään oikeusperusteeseen. Oikeuksien soveltaminen määräytyy osittain sen mukaan, millä oikeusperusteella henkilötietoja käsitellään. (EDPB 2025b.)

Rekisteröidyllä on mahdollisuus vaikuttaa omien tietojensa käsittelyyn sekä tarvittaessa rajoittaa tai estää niiden käyttöä. Rekisteröidyllä on aina oikeus saada tietoa henkilötietojensa käsittelystä, tutustua omiin tietoihinsa sekä oikaista virheelliset tai puutteelliset tiedot. Nämä oikeudet ovat voimassa riippumatta siitä, millä oikeusperusteella tietoja käsitellään. Lisäksi rekisteröity voi pyytää henkilötietojensa poistamista, jos niitä ei enää tarvita alkuperäiseen tarkoitukseen. Hän voi myös vaatia tietojen käsittelyn rajoittamista, jolloin tietoja saa edelleen säilyttää, mutta niitä ei saa muutoin käsitellä. (EDPB 2025b; Tietosuojavaltuutetun toimisto 2024b)

Rekisteröidyllä on oikeus siirtää henkilötietonsa järjestelmästä toiseen yleisesti käytetystä ja koneellisesti luettavassa muodossa. Lisäksi rekisteröity voi vastustaa henkilötietojensa käsittelyä, jos käsittely perustuu rekisterinpitäjän oikeutettuun etuun tai yleisen edun mukaiseen tehtävään. (EDPB 2025b; Tietosuojavaltuutetun toimisto 2024b.)

Rekisteröidyllä on oikeus vaatia, että häntä koskevat päätökset eivät perustu pelkästään automaattiseen käsittelyyn, vaan niihin osallistuu myös ihminen. Tämä koskee esimerkiksi työsuorituksiin tai taloudelliseen tilanteeseen liittyviä päätöksiä. Niillä voi olla vaikutusta rekisteröidyn asemaan tai oikeuksiin. (EDPB 2025b; Tietosuojavaltuutetun toimisto 2024b.)

Rekisterinpitäjällä on velvollisuus vastata rekisteröidyn oikeuksia koskeviin pyyntöihin lähtökohtaisesti kuukauden kuluessa. Rekisteröidylle on annettava selkeää tietoa oikeuksista ja tarjottava helppokäyttöisiä toimia niiden toteuttamiseen. Rekisterinpitäjän tulee dokumentoida pyynnöt ja niihin annetut vastaukset. Kaikki rekisteröidyn oikeudet eivät kuitenkaan aina ole voimassa, ja tietojen poistamisesta voidaan kieltäytyä lakisääteisten velvoitteiden perusteella. (EDPB 2025a.)

2.3.3 Tietosuojavastaava

Tietosuoja-asetuksen artiklat 37–39 määrittelevät ehdot tietosuojavastaavan nimittämisen, aseman ja tehtävät. Tietosuoja-asetus edellyttää tietosuojavastaavan nimeämistä tapauksissa, jos on viranomainen tai julkishallinnon toimija, käsittelee suuria määriä arkaluonteisia henkilötietoja tai seuraa ihmisiä laajamittaisesti, säännöllisesti ja järjestelmällisesti. Lisäksi organisaatio voi nimetä tietosuojavastaavan ilman lain vaatimaa perustetta. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679b 2016)

Tietosuojavastaava edistää organisaation tietosuojaosaamista, toimii organisaation tietosuojan asiantuntijana sekä työntekijöille että asiakkaille. Hänen tehtäviinsä kuuluu sääntöjen noudattamisen valvonta, yhteydenpito valvontaviranomaisiin ja rekisteröityihin sekä tietosuoja-asioissa neuvominen. Tietosuojavastaavaa sitoo salassapitovelvollisuus, ja sen rikkominen on rangaistavaa. (Tietosuojavaltuutetun toimisto 2024c.)

Tietosuojavastaavan on oltava riippumaton työntekijä ilman eturistiriitoja tehtäviensä kanssa. Hän ei voi esimerkiksi olla johdon edustaja tai henkilö, joka päättää henkilötietojen käsittelyn keinoista ja tarkoituksesta. Eturistiriitoja voi syntyä, jos tietosuojavastaavana toimii henkilö, jolla on muualla organisaatiossa päätäntävaltaa henkilötietojen käsittelyyn liittyen. (Tietosuojavaltuutetun toimisto 2024c.)

Tietosuojavastaavalle ei myöskään ole olemassa erillisiä pätevyysvaatimuksia, mutta käytännössä täytyy olla johdon tuki sekä aito asiantuntemus tietosuojaan ja tietoturvaan liittyvistä kokonaisuuksista (Tietosuojavaltuutetun toimisto 2024d). Oikeustieteellisestä koulutuksesta on hyötyä, mutta se ei tietosuoja-asetuksen mukaan ole välttämätön. Myös Tietoviikon artikkelin asiantuntijoiden mukaan juridiikan tunteminen on tärkeää, vaikka se ei yksinään riitä. Tietosuojavastaavan on lisäksi ymmärrettävä miten järjestelmät ja teknologia toimivat omassa organisaatiossa (Ahokas 2024.)

Tietosuojavastaavan tehtävä vaatii myös kykyä seurata jatkuvasti tietosuojaan liittyviä lainsäädännöllisiä ja teknologisia muutoksia ja ennakoida niiden vaikutuksia organisaation toimintaan. Hänen on pystyttävä tunnistamaan mahdollisia uhkia ja varautumaan niihin etukäteen. (Andreasson ym. 2019, 52.)

Tietokirjailija Järvisen (2017) tulkinnan mukaan tietosuojavastaava ei todellisuudessa vastaa mistään, sillä vastuu on aina yrityksen johdolla. Yritykset ovat joutuneet nimeämään ja kouluttamaan tehtävään tuhansia henkilöitä. Hän myös pohtii uusien työpaikkojen määrää, jos samoja resursseja suunnattaisiin yritysten liiketoiminnan kehittämiseen ja EU-yritykset päättäisivät nimittää saman määrän innovaatiovastaavia? Toisaalta tietosuoja voi olla myös innovaatioiden ajuri, jolloin organisaatiot kehittävät uusia tietosuojaystävällisiä teknologioita. Ilman asianmukaista tietosuojaa organisaatiot voivat kohdata haasteita, jotka rajoittavat niiden innovointikykyä.

Asianajaja Warma-Lehtinen toteaa Tietoviikon artikkelissa, että monissa organisaatioissa tietosuojavastaavan rooli ymmärretään väärin. Kaikki tietosuojaan liittyvät asiat päätyvät usein tietosuojavastaavan tehtävälistalle, vaikka hänen vastuunsa on tarkastaa organisaation tietosuojakäytänteiden olevan sääntelyn mukaisia. Lopulliset päätökset tietosuojatoimista tekee kuitenkin organisaation johto. Toisin kuin titteli saattaa antaa ymmärtää, tietosuojavastaava ei ole vastuussa organisaation tietosuojasta. (Ahokas 2024.)

Tietosuojavastaavan rooli on keskeinen, mutta rekisterinpitäjä on viime kädessä vastuussa henkilötietojen käsittelyn lainmukaisuudesta. Tietosuojavastaava toimii neuvojana ja valvojana, mutta hän ei päätä tietojen käsittelyn keinoista tai lainmukaisuudesta. Hänellä on kuitenkin valta ja velvollisuus puuttua epäkohtiin ja varmistaa, että organisaation tietosuojakäytännöt täyttävät vaatimukset. (Yleinen tietosuoja-asetus 2016; Voutilainen 2022; Pönkä 2022; Eronen 2022.)

Andreassonin (2023) mukaan tietosuojavastaavan tehtävä on monissa organisaatioissa erittäin huonosti resursoitu, mikä heijastuu suoraan toiminnan laatuun. Suomessa tietosuojavastaavien kirjo on liian laaja ja joissain tapauksissa esimerkiksi kunnanjohtaja voi olla nimetty tietosuojavastaavaksi, vaikka tämä ei ole tarkoituksenmukaista. Andreasson ym. (2019, 199) myös toteavat, että havaintojen mukaan päätoimisia tietosuojavastaavia on harvoissa organisaatioissa, ja tehtävää hoidetaan usein muun työn ohessa. Tämä vaikeuttaa asiantuntijuuden kehittymistä ja lisäksi osaamaton tietosuojavastaava on organisaatiolle merkittävä tietosuojariski.

Apulaistietosuojavaltuutettu Pihamaan mukaan kyselyt osoittavat, että tietosuojavastaavilla ei ole riittävästi aikaa tehtäviinsä, vaikka GDPR on määritellyt heidän vastuunsa selkeästi (Kanta 2021). Myös Pönkän (2022) mukaan resurssien puute on yksi merkittävimmistä ongelmista ja tietosuojavastaavilla ei ole riittävästi aikaa, rahaa tai tekijöitä hoitaakseen kaikkia

tehtäviä asianmukaisesti. Tämä voi johtaa siihen, että tietosuoja-asetuksen vaatimuksia ei noudateta täysin ja riskianalyysit ja vaikutustenarvioinnit jäävät tekemättä.

Toinen merkittävä haaste on johdon tuen puute. Tietosuojaa saatetaan pitää vain pakollisena velvoitteena, eikä sen merkitystä ymmärretä organisaation johdossa. Lisäksi tietosuojavastaavan on voitava toimia itsenäisesti ja objektiivisesti, jotta hän voi varmistaa tietosuojasäännösten noudattamisen. Tehtävän menestyksekäs hoitaminen vaatii riittävät resurssit, johdon tuen ja mahdollisuuden toimia riippumattomasti. (Pönkä 2022.)

Euroopan tietosuojaneuvosto (EDPB) on julkaissut raportin, jossa analysoitiin EU-maiden tietosuojavastaavien nimittämistä ja asemaa. Suomessa kyselyyn vastasi 50 eri alojen organisaatiota toukokuussa 2023. Raportissa nousivat esille kolme keskeistä teemaa, joita ovat resurssien puute, tietosuojavastaavien riippumattomuus ja tehtävät sekä ongelmat raportoinnissa. EDPB:n suosittelee organisaatioille, että tietosuojavastaaville varataan riittävät resurssit, aika ja mahdollisuudet tehtävän hoitamiseen. (EDPB 2024). EDPB julkaisema raportti tukee suomalaisten asiantuntijoiden näkemyksiä resurssien, ajan, rahan ja tuen puutteesta.

Tietosuojavastaavalla on avainrooli henkilötietojen vastuullisesta ja lain mukaisesta käsittelystä organisaatiossa. Tietosuojavastaava toimii organisaation henkilötietojen käsittelytehtävien asiantuntijana, jolloin hänen on huomioitava tietosuojalaki eri asioiden yhteydessä. Monissa yrityksissä on erillinen tietosuojaryhmä, joka tukee tietosuojavastaavaa eri toiminnoissa. Tietosuojavastaava tulisi nähdä henkilötietojen käsittelytehtävien mahdollistajana, ei rajoittajana, vaikka hänet saatetaan kokea esteenä muutoin toimivalle suunnitelmalle tai uudelle idealle.

Tietosuojavastaava joutuu navigoimaan uhkien maastossa, koska alalla on usein tilanteita, joissa säännökset ja vaatimukset voivat olla monitulkintaisia tai ristiriitaisia. Tämä sisältää mm. riskien arviointia, tietosuojaa koskevien politiikkojen ja menettelytapojen kehittämistä sekä dokumentaation ylläpitoa.

2.3.4 Osoitusvelvollisuus

Tietosuoja-asetus edellyttää, että henkilötietoja keräävät ja käsittelevät organisaatiot voivat osoittaa noudattavansa asetuksen säännöksiä. Tätä kutsutaan osoitusvelvollisuudeksi. Organisaation on myös pystyttävä näyttämään, että se on tunnistanut tietosuojariskit ja toteuttanut tarvittavat suojatoimet henkilötietojen suojaamiseksi. Lisäksi organisaation on dokumentoitava tietosuojatoimenpiteensä, jotta voidaan osoittaa asetuksen mukainen riskienhallinta.

Tietosuoja-asetus sisältää vaatimuksia osoitusvelvollisuudesta ja näiden vaatimusten noudattaminen on arvioitava tapauskohtaisesti. On tärkeää, että organisaatiot ottavat osoitusvelvollisuuden huomioon jo suunnitteluvaiheessa, kun ne määrittelevät, miten ne keräävät ja käsittelevät henkilötietoja. Henkilötietojen siirto kolmansiin maihin. kuten Yhdysvaltoihin,

aiheuttaa edelleen oikeudellista epävarmuutta, mikä tekee osoitusvelvollisuuden täyttämisestä entistä haastavampaa (Kantonen ym. 2024).

”Dokumentoi kaikki tai sitä ei tapahtunut!” Tämä on tietosuoja-asiantuntijoiden yleisesti käytössä oleva tunnuslause, jota tietosuojavastaavan tulee noudattaa. Ilman asianmukaista dokumentointia tietosuojan toteutumista on vaikea todentaa. Se voi aiheuttaa vaikeuksia tietosuojaan liittyvässä osoitusvelvollisuudessa. Yhtenä tietosuojavastaavan tehtävänä on dokumentaation laatimisen, saatavuuden ja säilyttämisen valvonta.

Tietosuojavaltuutetun toimisto (2024e) on listannut keskeisiä toimenpiteitä, joita osoitusvelvollisuuden täyttäminen edellyttää. Näitä ovat tietosuojavastaavan nimittäminen, tietosuojaa koskevan vaikutustenarvioinnin laatiminen, ennakkokuuleminen ja velvollisuus laatia seloste käsittelytoimista. Lisäksi organisaatioiden tulisi dokumentoida, miten päätökset on tehty velvoitteiden noudattamisen tai noudattamatta jättämisen suhteen.

Osoitusvelvollisuuden laajuus riippuu organisaation koosta, käsiteltävien henkilötietojen määrästä ja tyypistä. Rekisterinpitäjän täytyy ottaa osoitusvelvollisuus huomioon jo henkilötietojen käsittelyn suunnitteluvaiheessa. Osoitusvelvollisuuden toteuttamisessa voidaan käyttää tukena sertifikaattien ja käytännesääntöjen käyttöön ottamista. (Tietosuojavaltuutetun toimisto 2024e.) Dokumentaation ja toimenpiteiden riittävyyttä on arvioitava säännöllisesti.

Tietosuoja-asetuksen hallinnollisella taakalla tarkoitetaan esimerkiksi osoitusvelvollisuuden dokumentointia ja säilytysaikojen noudattamista. Haaste koettelee erityisesti pieniä ja keskisuuria organisaatioita resurssien, rahan ja osaamispulan takia (Kantonen ym. 2024).

2.3.5 Vaikutustenarviointi

Tietosuoja-asetuksen artikla 35 mukaan rekisterinpitäjän on tehtävä tietosuojan etukäteinen vaikutustenarviointi (DPIA, Data Protection Impact Assesment), jos suunniteltu henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille. Vaikutustenarvioinnin avulla tunnistetaan, arvioidaan ja hallitaan henkilötietojen käsittelyyn liittyviä riskejä sekä varmistetaan, että henkilötietojen käsittely on oikeasuhtaista ja onko jäljelle jäänyt riski hyväksyttävä. Vaikutustenarviointi tulee tehdä ennen henkilötietojen käsittelyn aloittamista ja sitä päivitetään tarvittaessa. Lisäksi päivittämisen tarvetta tulee arvioida säännöllisin väliajoin. (Tietosuojavaltuutetun toimisto 2024f.)

Vaikutustenarviointi on erityisen tärkeä tilanteissa, joissa henkilötietojen käsittelyssä käytetään uutta teknologiaa, käsitellään laajamittaisesti erityisiä henkilötietoryhmiä, kuten terveystietoja tai rikostuomioita, arvioidaan henkilöiden ominaisuuksia automaattisesti tai valvotaan julkisia alueita laajasti ja järjestelmällisesti. Mikäli edellä mainituista kaksi kriteeriä täyttyy, tulee rekisterinpitäjän tehdä vaikutustenarviointi. (Tietosuojavaltuutetun toimisto 2024f.)

Jokainen organisaatio vastaa itse oman toimintansa tietosuoja-arvioinnista. Tietosuojavaltuutetun toimiston ohjeistus toimii yleisenä ohjeena ja sitä on sovellettava organisaation oman toiminnan luonteen mukaisesti. Suomessa on saatavilla myös palveluja, jotka tukevat organisaatioiden tietosuojavaatimusten täyttämistä. Näihin palveluihin kuuluu esimerkiksi sovellusten ja verkkopalvelujen tietosuojaselvityksiä ja työkaluja, jotka helpottavat ja tukevat vaikutustenarviointien tekemistä.

On tärkeää, että vaikutustenarviointi on aidosti riskien arviointia, joka auttaa organisaatiota löytämään ratkaisuja riskien hallintaan. Vaikka tietosuojavaltuutetun toimisto tarjoaa ohjeet ja veloituksettoman työkalun arvioinnin tekemiseen, käytännön haasteita voi aiheuttaa asiantuntemuksen ja resurssien puute. Organisaatio voi halutessaan julkaista vaikutustenarvioinnin, mutta tällöin on huomioitava mahdolliset turvallisuusriskit ja liikesalaisuudet. (European Comission 2017).

Andreasson ym. (2019, 67) korostavat, että tietosuojaa koskevan vaikutustenarvioinnin on oltava jatkuva prosessi eikä vain yksittäinen toimenpide.

2.3.6 Yksityisyyden hallinta

Internetin online-palveluita käyttävät lähes kaikki 16-89-vuotiaat (Tilastokeskus 2025). Käyttäjien oikeus hallita tietojaan ja yritysten vastuu suojata niitä muodostavat digitaalisen yksityisyyden perustan. Verkkoidentiteetin hallinta ja yksityisyyden suoja ovat verkossa keskeisiä, ja moni käyttäjä tiedostaa niiden merkityksen.

Barth ja de Jong (2017) tutkivat kirjallisuuskatsauksen avulla ilmiötä, jota kutsutaan nimellä privacy paradox (yksityisyysparadoksi). Se tarkoittaa ristiriitaa käyttäjien yksityisyysasenteiden ja todellisen käyttäytymisen välillä. Huolimatta yksityisyyteen liittyvistä riskeistä, käyttäjät jatkavat usein alustojen ja palveluiden käyttöä ja jakavat tietojaan, vaikka se saattaa vaarantaa heidän yksityisyytensä.

Saman ilmiön havaitsivat Barth ja de Jong yhdessä Jungerin, Hartelin ja Roppeltin (2019, 55) kanssa tutkiessaan eri ikäisten yliopisto-opiskelijoiden tietosuojakäyttäytymistä mobiilisovellusten lataamisessa ja käytössä. Teknisesti taitavien opiskelijoiden kokeellisessa tutkimuksessa havaittiin, että tietosuoja-asiat eivät olleet merkittävä tekijä sovelluksen valinnassa, vaikka osallistujat olivat tietoisia riskeistä. Heille sovelluksen toiminnallisuus ja hinta olivat tärkeämpiä kriteerejä kuin yksityisyyden suoja. Tutkimuksen mukaan käyttäjät siis ilmoittivat olevansa huolissaan yksityisyydestään, mutta eivät käytännössä toimi sen mukaisesti, vaan lataavat riskialttiita sovelluksia ja paljastavat epäröimättä yksityisiä tietojaan. (Barth ym. 2019, 57.)

Myös Li, Luo, Zhang ja Xu (2017) totesivat tutkimuksessaan, että vaikka käyttäjät raportoivat olevansa huolissaan yksityisyydestään, heidän toimintansa Internetissä poikkeaa usein näistä huolenaiheista.

Paspatis ym. (2024) tutkivat perinteisten oppimismenetelmien vaikutusta tietosuojaosaamisen kehittämiseen. Heidän tutkimuksensa mukaan luennot ja kirjallisuus ovat yleisimpiä menetelmiä, joita käytetään tietosuojaan liittyvässä oppimisessa. Tulokset osoittavat, että perinteiset oppimismenetelmät kannustavat passiiviseen oppimiseen, jossa opiskelijat ovat tiedon vastaanottajia sen sijaan, että osallistuisivat aktiivisesti oppimisprosessiin. Lisäksi tällainen lähestymistapa ei ota huomioon opiskelijoiden yksilöllisiä eroja, mikä voi heikentää sitoutumista, kriittistä ajattelua ja ongelmanratkaisukykyä. Lisäksi perinteisessä menetelmässä keskitytään usein teoreettisiin käsitteisiin, jotka ovat usein irrallaan todellisuuden tapahtumista, ja tämä voi estää opiskelijoiden kyvyn soveltaa saatuja tietoja arjen tapahtumiin. (Paspatis ym. 2024.)

Privacy Lab on kokeellisen oppimisen ympäristö, jota Paspatis ym. (2023, 405) analysoivat tutkimuksessaan. Siinä tarkasteltiin teknologiayrityksen kokemuksellisen oppimisen vaikutuksia ihmisten tietosuojakäyttäytymisen tietotekniikan yhteydessä. Oppimisympäristössä hyödynnettiin käytännön työpajoja, tietoturvaloukkausten simulaatioita ja vuorovaikutteisia keskusteluja ja työntekijät osallistuivat aktiivisesti reaalimaailman skenaarioihin. He harjoittelivat tietosuojariskien tunnistamista tuotekehityksessä, tietosuojatoimenpiteiden analysointia ja päätöstentekoa. Tutkimuksen mukaan kokemuksellinen oppiminen voi olla tehokas menetelmä tietosuojaosaamisen ja -käyttäytymisen kehittämiseksi. (Paspatis ym. 2023, 398).

2.3.7 Minimointi, pseudonymisointi ja anonymisointi

Henkilötietojen minimointi, pseudonymisointi ja anonymisointi ovat tietosuojaa parantavia menetelmiä. Niiden tavoitteena on vähentää henkilötietojen tarpeetonta käsittelyä ja suojata rekisteröityjen yksityisyyttä.

Pseudonymisointi on tehokas keino käsitellä henkilötietoja siten, että henkilöä ei voi tunnistaa suoraan tiedoista, mutta hänet voidaan tunnistaa tietoja yhdistelemällä. Mikäli tietoja ei pseudonymisoida, käsittelylle on aina oltava perusteellinen syy. (Tietosuojavaltuutetun toimisto 2024g.) Tietosuoja-asetuksen mukaan pseudonymisoidut tiedot ovat edelleen henkilötietoja ja niiden käsittelyyn sovelletaan tietosuojalakia (EDPB 2025.).

Apulaistietosuojavaltuutetun mukaan pseudonymisointi voi vähentää rekisteröityihin kohdistuvia riskejä. Se oli peruste tietosuojavaltuutetun toimiston päätökselle, jossa yliopiston opiskelijanumeroihin liitettyjen tenttitulosten julkaisu yliopiston intranetissä on sallittua ilman opiskelijoiden suostumusta, mikäli tietojen suojaamiseksi toteutetaan asianmukaiset tekniset ja organisatoriset toimenpiteet. Päätös perustuu tietosuoja-asetuksen ja julkisuuslain

vaatimuksiin, ja opiskelijalla on mahdollisuus kieltää tietojensa julkaiseminen. (Tietosuojavaltuutettu 2021.)

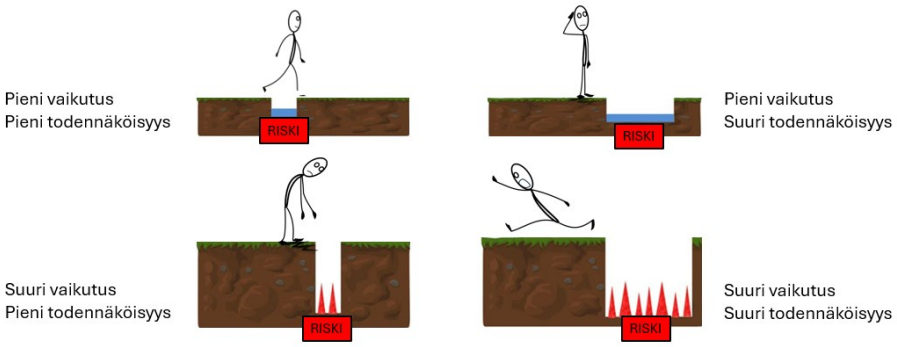
Anonymisointi on prosessi, jossa henkilötiedot on muutettu niin, että tietoja ei voi palauttaa tunnistettavaan muotoon. Pelkkä yksilöintitietojen poistaminen ei välttämättä riitä, jos henkilö on tunnistettavissa jonkin muun välillisen tiedon tunnisteesta, esimerkiksi harvinainen sairaus. Anonymisoinnin arvioinnissa otetaan huomioon rahalliset resurssit, teknologia ja aika. Toisaalta anonymisoidut tiedot jäävät tietosuojasääntelyn ulkopuolelle, sillä niistä ei voida tunnistaa yksilöä edes tietoja yhdistelemällä. (Tietosuojavaltuutetun toimisto 2024g.)

Oikeusministeriön lausunnossa on tuotu esille, että Suomen tietosuojalainsäädäntöä tulkitaan tarkemmin kuin muissa EU-maissa keskimäärin ja osa Suomen lausunnonantajista piti pseudonymisoinnin ja anonymisoinnin kansallisia tulkintoja liian tiukkana. Esimerkiksi tutkimustoiminnassa on ilmennyt pseudonyymin ja anonyymin tulkintoihin liittyviä ongelmia, joka osaltaan on vaikeuttanut tutkimustoimintaa. Anonyymin määritelmä on liian tiukka ja Euroopassa tehtävä tutkimustoiminta vaikeutuu, jolloin aineistojen kansainvälinen vertailu voi estyä. (Kantonen ym. 2024.)

2.3.8 Tietosuojariskien hallinta

Tietosuojalla suojataan henkilötietojen käsittelyä, yksityisyyttä ja varmistetaan henkilötietojen käsittelyn lainmukaisuus, oikeudenmukaisuus ja läpinäkyvyys. Kuten Andreasson ym. (2019, 12) toteavat, tietosuoja-asetus perustuu riskipohjaiseen lähestymistapaan ja riskin kasvaessa käsittely edellyttää organisaatiolta vahvempia suojaustoimia henkilötietojen käsittelyyn. Lisäksi Andreasson ym. (2019, 12) mainitsevat kaikkien hyötyvän, kun henkilötietojen käsittely on tasapainossa.

Tietosuojariskin määritelmä perustuu siihen, että riski muodostuu tapahtumasta, sen todennäköisyydestä ja seurauksista. Riskien arvioinnissa voidaan käyttää erilaisia menetelmiä (Korpisaari ym. 2018.) Tietosuojavaltuutetun toimisto tarjoaa veloituksettoman Excel-työkalun riskien arvioimiseen, jossa todennäköisyys ja vahingon suuruus arvioidaan numeerisella laskennalla. Työkalussa on huomioitu Suomen lainsäädäntö ja ohjeistuksessa on esimerkkejä riskien tunnistamiseksi. Vaikutustenarvioinnin ydinkysymykset keskittyvät siihen, mitä, miksi ja miten organisaatio aikoo käsitellä henkilötietoja ja tunnistaa käsittelyn vaikutukset rekisteröityihin. Tärkeää on siis pohtia, mikä voi mennä pieleen, kuinka todennäköistä on, että jokin menee pieleen ja miten pieleen menemisen todennäköisyyttä voidaan vähentää.



Kuvio 1: Riskin visualisointi (mukaillen alan yleistä riskin visualisointia)

Julkisella sektorilla tiedonhallintalaki varmistaa viranomaisten käsittelevän tietoaineistoja yhdenmukaisesti, laadukkaasti ja tietoturvallisesti. Se vähentää henkilötietojen käsittelyyn liittyviä tietosuojariskejä ja tukee julkisuusperiaatteen toteuttamista. (Laki julkisen hallinnon tiedonhallinnasta 906/2019.)

Tietosuojariskejä, kuten tietovuotoja, luvattomia pääsyjä ja tietojen väärinkäyttöä, voidaan hallita asianmukaisilla suojatoimilla. Tietosuojavastaava joutuu navigoimaan uhkien maastossa, koska alalla on usein tilanteita, joissa säännökset ja vaatimukset voivat olla monitulkintaisia tai ristiriitaisia. Organisaation tietosuojavastaavan tehtävänä on tunnistaa tietosuojauhkia ja kehittää strategioita niiden hallitsemiseksi yhdessä organisaation kanssa. Lisäksi muuttuva lainsäädäntö ja teknologinen kehitys vaativat osaamisen ylläpitoa ja kehittämistä.

Digitaalisessa ympäristössä henkilötietoja käsitellään ja siirretään päivittäin organisaatioiden välillä jokapäiväisessä toiminnassa. Tämä lisää riskejä henkilötietojen virheelliselle käsittelylle. Korpisaaren ym. (2018) mukaan monille myös sosiaaliset verkostot ovat keskeinen osa identiteettiä. Palvelut mahdollistavat vaihtelevasti omien tietojen hallinnan. Digitalisaatio ja uudet teknologiat ovat tuoneet mukanaan tietosuojariskejä, joita käyttäjät eivät aina tiedosta.

2.3.9 Tietoturvariskien hallinta

Tietoturvan avulla toteutetaan tietosuojaa. Tietoturva keskittyy teknisiin ja organisatorisiin toimiin, jolla varmistetaan tiedon eheys, luottamuksellisuus ja saatavuus. Yleinen tietosuoja-asetus yhdistää tietoturvan ja tietosuojan vahvasti toisiinsa. Jokaisella EU-kansalaisella on perusoikeus henkilötietojen suojaan. Sen varmistaminen edellyttää vahvaa tietoturvaa.

Organisaation tietoturvakäytännöt suojaavat tietoja, yksityisyyttä ja mainetta sekä varmistavat toiminnan jatkuvuuden (Kyberturvallisuuskeskus 2020). Keskeisiä osa-alueita, kuten tietojen salaaminen sekä tallennettuna että siirron aikana on tärkeä tekijä. Pääsynhallinnan avulla varmistetaan, että vain valtuutetut henkilöt pääsevät käsiksi tietoihin ja vahva autentikointi sekä hyväksyntä takaavat, että käyttäjät ovat todella niitä, keitä he väittävät olevansa.

Vahva tunnistautuminen, kuten monivaiheinen tunnistautuminen, on nykyään jo minimivaatimus tilien kaappaamisen ja henkilötietojen luvattoman käytön estämiseksi. Lisäksi järjestelmät ja ohjelmistot pidetään ajan tasalla tietoturvapäivityksillä, huolehditaan varmuuskopioinnista ja palautusharjoituksista, sekä ylläpidetään ja valvotaan lokitietoja ja varmistetaan riskienhallinnan prosessien toimivuus.

Tietoturvakäytännöt eivät rajoitu pelkästään teknisiin toimenpiteisiin, vaan ne ulottuvat myös organisaatiokulttuuriin ja työntekijöiden osaamiseen. Työntekijöiden kouluttaminen on olennaista, jotta he osaavat tunnistaa tietoturvauhkia ja toimia oikeaoppisesti riskien minimoimiseksi. Säännölliset koulutukset ja selkeät ohjeet varmistavat, että kaikki organisaation jäsenet ymmärtävät oman roolinsa tietoturvan ja tietosuojan ylläpitämisessä, mikä puolestaan torjuu verkkorikollisuutta, tukee lainsäädännön noudattamista ja rakentaa luottamusta yhteistyökumppaneihin ja asiakkaisiin. Tietoturvakäytäntöjen ja tietosuojan yhteensovittaminen takaa, että organisaation tiedot käsitellään turvallisesti ja lainmukaisesti, ja varmistaa, että tietojen luottamuksellisuus, eheys ja saatavuus säilyvät, suojaten samalla henkilötietoja ja varmistaen niiden saatavuuden ja muuttumattomuuden tarvittaessa. (Kyberturvallisuuskeskus 2020; Kyberturvallisuuskeskus 2024a)

Poliisin ja Kyberturvallisuuskeskuksen verkkosivuilla tietomurto määritellään oikeudettomaksi tunkeutumiseksi tietojärjestelmään. Verkkosivulla luetellaan myös yleisimpiä tietomurtojen tapoja ja annetaan ohjeita tietomurtojen ehkäisemiseen ja vahinkojen minimoimiseen. (Poliisi 2024; Kyberturvallisuuskeskus 2024b). Organisaatioilla tulisi olla selkeät menettelytavat tietomurtojen tai muiden tietoturvaloukkausten varalle, jotta ne voivat minimoida vahingot ja ilmoittaa asiasta asianmukaisesti viranomaisille ja rekisteröidyille.

Tietoturvaloukkauksilla voi olla vakavia seurauksia organisaatioille, mukaan lukien taloudelliset menetykset, mainehaitat ja oikeudelliset seuraamukset. Asiakkaiden ja yhteistyökumppaneiden luottamus voi heiketä merkittävästi, jos heidän henkilötietonsa joutuvat vääriin käsiin. Tämä korostaa osaamisen ja tehokkaiden tietoturvakäytäntöjen merkitystä. Yritykset, jotka eivät kykene suojaamaan tietojaan asianmukaisesti, saattavat menettää kilpailukykynsä ja asemansa markkinoilla ja pahimmassa tapauksessa ajautua konkurssiin.

Vaikka tietoturvaloukkaus ei aina kohdistu henkilötietoihin ja se on laajempi käsite kuin tietomurto, se kattaa kaikki tilanteet, joiden seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, paljastuu luvatta tai päätyy sellaisten henkilöiden käsiin, joilla ei ole oikeutta käsitellä niitä (Tietosuojavaltuutetun toimisto 2024h). F-Securen (2024) mukaan tietovuoto on yksi esimerkki tietoturvaloukkauksesta, joka voi tapahtua tahallisesti tietomurron seurauksena tai vahingossa esimerkiksi huolimattomuuden takia. Kaikki tietomurrot ovat tietoturvaloukkauksia, mutta kaikki tietoturvaloukkaukset eivät ole tietomurtoja. Käsitteitä saatetaan käyttää toistensa synonyymeina, vaikka niillä on hieman eri merkitys.

F-Secure (2024) tarjoaa käyttäjille veloituksetta verkkotyökalun, joka auttaa tarkastamaan, onko henkilökohtaisia tietoja joutunut tunnetuissa tietomurroissa vääriin käsiin. Antamalla palveluun oman sähköpostiosoitteen, työkalu skannaa tietomurtojen tietokantoja ja ilmoittaa, jos tietoja on paljastunut näissä murtotapauksissa. Käyttäjä saa sähköpostiin yhteenvedon mahdollisista tietovuodoista ja ohjeita, miten voi suojautua ja minimoida riskit.

2.4 Pelillistäminen

Pelien yleismaailmallinen luonne ja digitaalisten alustojen nopea kehitys asettavat haasteita pelillistämisen tutkimukselle. Koska pelit ja pelillistäminen vaikuttavat monilla eri aloilla, niiden kattavaa teoreettista selitystä on vaikea muodostaa. Krath, Schürmann ja von Korflesch (2021) tekivät systemaattisen kirjallisuuskatsauksen, jossa he tunnistivat 118 erilaista teoriaa, joita on käytetty pelillistämisen ilmiön ymmärtämiseen.

Krath ym. (2021) mukaan tutkimusten perusteella pelillistämisen psykologiset mekanismit ja teoreettinen ymmärrys ovat edelleen hajanaisia. Itsemääräämisteoria on kuitenkin ylivoimaisesti eniten käytetty teoria pelillistämiseen liittyvissä tutkimuksissa. Tämä osoittaa, että pelillistämisen toimivuudelle ei ole olemassa yhtä kaiken kattavaa teoriaa, vaan sen vaikutuksia tarkastellaan useista eri näkökulmista. Pelillistämisen teoriaa tarkastellaan tässä kappaleessa siitä näkökulmasta, miten se voi tukea tietosuojalainsäädännön ymmärtämistä ja soveltamista käytännössä.

2.4.1 Pelillistämisen historia

Suomella on pitkä ja rikas pelaamisen historia, jonka juuret ulottuvat tuhansien vuosien taakse. Arkeologisissa kaivauksissa on löydetty jopa 8 000 vuotta vanhoja pelin osia, mikä kertoo siitä, että pelaaminen on ollut osa ihmisten elämää jo varhaisista ajoista lähtien. Nykyään Suomi tunnetaan vahvana pelialan osaajana ja edelläkävijänä peliteollisuuden, -kulttuurien ja -tutkimuksen saralla. Vaikka Suomen peliteollisuus on saavuttanut kansainvälistä menestystä ja tuonut esiin uudenlaisia liiketoimintamalleja, se ei ole lunastanut odotuksia taloutta pelastavana uutena "Nokiana" (Friman, Arjoranta, Kinnunen, Heljakka & Stenros 2022, 10–26.)

Pelaaminen on kiehtonut ihmisiä vuosisatojen ajan, ja erilaiset pelilliset elementit ovat olleet mukana arjessa jo ennen kuin niille kehitettiin nykyaikaisia nimityksiä. Erityisesti uhkapelaamisella on pitkä historia, ja sitä on harjoitettu niin ajanvietteenä kuin taloudellisena keinona. Menneinä vuosisatoina majataloissa ja anniskelupaikoissa pelattiin uhkapelejä noppien ja korttien avulla. Pelissä panoksina saattoivat olla raha, vaatteet, hevoset tai jopa kokonaiset kuningaskunnat (Suomen Museot 2024.)

Hyötypelien (Serious games) historia juontaa juurensa kauas menneisyyteen. Niiden pääasiallinen tarkoitus ei ole viihdyttäminen, vaan taitojen opettaminen ja kehittäminen. Alun perin hyötypelejä käytettiin sotilaallisessa koulutuksessa, ja myöhemmin niitä alettiin hyödyntää

myös koulutuksen ja liiketoiminnan tarpeisiin. (Deterding, Dixon, Khaled & Nacke 2011, 10.) Kylmän sodan aikainen Neuvostoliitto tarjoaa esimerkin pelillistetystä järjestelmästä, jossa työntekijöitä ja tehtaita kannustettiin kilpailemaan pistejärjestelmällä tuottavuuden lisäämiseksi. Tämä kokeilu kuitenkin epäonnistui, koska järjestelmä oli irrotettu taloudellisesta todellisuudesta, eikä se lopulta parantanut tuotantotehokkuutta. (Silic & Lowry 2020.)

Hyötypelien käsitettä on myös kyseenalaistettu. Klabbers (2009) kritisoi termiä, koska se viittaa siihen, että hyötypeleillä olisi vastakohta. Eli pelejä, joilla ei ole mitään hyötyä tai järkeä. Hän ei ole löytänyt kirjallisuudesta vastaavaa käsitettä, joka määrittelisi tämän oletetun "hölynpölypelien" kategorian. Hänen mukaansa hyötypelin käsitteellinen vastakkainasettelu voi olla harhaanjohtava, sillä kaikilla peleillä voi olla arvoa jossakin kontekstissa.

Sotapelien käyttö koulutusvälineenä ei ole uusi ilmiö. Klabbers (2009) mainitsee, että jo vuonna 1810 Preussin armeija alkoi käyttää sotapelejä upseerikoulutuksessa simuloimalla historiallisia taisteluita. Suomessa puolustusvoimat hyödyntävät edelleen pelillistämistä ja hyötypelejä osana koulutusmenetelmiään (Maanpuolustuskorkeakoulu 2021; Puolustusvoimat 2020).

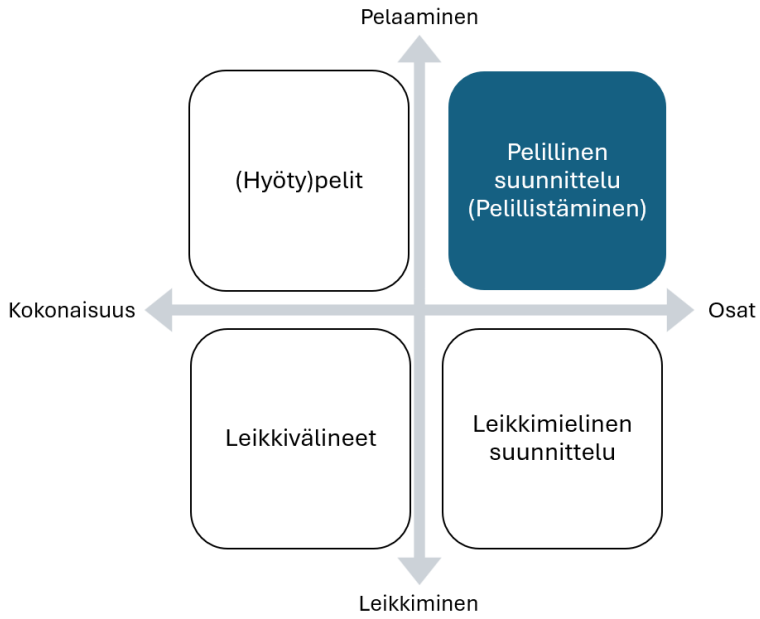
Pelien merkitys kulttuurissa ja yhteiskunnassa on laajempi kuin pelkkä viihde. Mäyrä (Friman ym. 2022, 35) korostaa, että pelit ovat olleet osa ihmiskulttuuria kaikkialla maailmassa kautta aikojen. Pelitutkimus on kehittynyt omaleimaiseksi tieteenalaksi, joka tarkastelee pelaamista moninaisena ilmiönä. Pelien vaikutukset eivät rajoitu vain yksilötason kokemuksiin, vaan ne ulottuvat laajasti yhteiskuntaan, koulutukseen ja talouteen. Pelillistämisen historia on osoitus siitä, kuinka pelien elementtejä on hyödynnetty vuosisatojen ajan eri tarkoituksiin, ja se antaa viitteitä siitä, miten niiden käyttö voi kehittyä tulevaisuudessa.

2.4.2 Pelillistämisen määritelmä

Deterding ym. (2011, 10) määrittelevät pelillistämisen tarkoittavan pelisuunnitteluelementtien, kuten pisteiden, tasojen ja haasteiden, hyödyntämistä muissa kuin peleihin liittyvissä yhteyksissä. Pelillistämisen tavoitteena on lisätä käyttäjien motivaatiota, sitoutumista ja kokemuksellisuutta esimerkiksi työelämässä, koulutuksessa ja markkinoinnissa. Se ei kuitenkaan tarkoita kokonaisen pelin rakentamista, vaan pelielementtien yhdistämistä olemassa olevaan prosessiin. Deterding ym. myös erottavat pelillistämisen pelillisestä suunnittelusta (gameful design), joka käsittelee pelillisen kokemuksen muotoilua kokonaisvaltaisemmin.

Pelillistämisen käsite liittyy läheisesti peleihin ja hyötypeleihin, mutta se eroaa niistä tavoitteidensa ja toteutustapojensa osalta. Vaikka pelien tarkasta määritelmästä ei ole yksimielisyyttä, niitä pidetään usein vapaaehtoisena toimintana, joka tapahtuu erillään todellisesta elämästä ja luo kuvitteellisen maailman. Tämä maailma voi olla todellisuuteen sidoksissa tai täysin irrallinen siitä, ja se vangitsee pelaajan huomion kokonaan (Landers, Auer, Helms, Marin & Armstrong 2019).

Deterding ym. (2011, 13) sijoittavat pelillistämisen osaksi laajempaa pelien ja pelillisen kulttuurin kokonaisuutta, jossa hyödynnetään pelien suunnittelutapoja tavoilla, jotka eivät liity perinteiseen pelaamiseen. Eri ilmiöt voidaan jakaa neljään luokkaan sen perusteella, missä määrin ne perustuvat sääntöihin ja tavoitteelliseen toimintaan (pelit) tai vapaamuotoisuuteen (leikki).



Kuvio 2:Pelillistämisen sijoittuminen (mukaillen Deterding ym. 2011, 13)

Pelillistäminen asettuu luokkaan, jossa hyödynnetään pelien elementtejä ilman, että luodaan kokonaista peliä. Näihin elementteihin voi kuulua esimerkiksi tasoja, pisteitä ja haasteita, jotka tukevat oppimista ja sitoutumista.

Pelillisyys ei ole yksiselitteinen käsite, vaan sillä on useita näkökulmia. Hamari ja Huotari (2012) tarkastelevat pelillistämistä palvelumarkkinoinnin näkökulmasta ja korostavat sen kokemuksellisuutta järjestelmällisen lähestymistavan sijaan. Heidän mukaansa pelillistämisen tavoitteet ja keinot muistuttavat markkinoinnin strategioita, joissa käyttäjän kokemus ja sitoutuminen ovat keskeisiä tekijöitä.

Pelillistämistermin alkuperä on osittain epäselvä. Deterding ym. (2011) viittaavat siihen, että käsite syntyi digitaalisen median teollisuudessa ja ensimmäinen dokumentoitu käyttö tapahtui vuonna 2008. Toisaalta Thomas, Baral, Crocco ja Mohanan (2023) mainitsevat joidenkin tutkijoiden uskovan, että Nick Pelling loi termin jo vuonna 2002.

Pelillistäminen ei ole saanut pelkästään positiivista vastaanottoa, vaan sitä on myös kritisoitu. Deterding ym. (2011, 9) huomauttavat, että termi on kohdannut vastustusta erityisesti peliteollisuudessa, koska sitä on tulkittu väärin ja toteutettu yksinkertaistetusti. Tämä on synnyttänyt vaihtoehtoisia lähestymistapoja, kuten McGonigalin (2011) esittämät "Alternate Reality

Games", joissa pelillisiä elementtejä yhdistetään tosielämän konteksteihin onnellisuuden ja menestyksen edistämiseksi.

Kritiikkiä on esittänyt myös pelitutkija Bogost (2011), joka on nimittänyt pelillistämistä "bullshitiksi" ja ehdottanut sen korvaamista termillä "exploitationware" (hyväksikäyttöohjelma). Hänen mukaansa pelillistämistä käytetään usein manipulatiivisesti motivoimaan ihmisiä toimimaan tavoilla, jotka eivät muutoin heitä kiinnostaisi. Tästä huolimatta hän ei kiellä sen potentiaalia, vaan näkee sen keinona tehdä rutiininomaisista ja tylsistä tehtävistä mielekkäämpiä.

Pelillistämisen vaikutukset eivät rajoitu vain yksittäisten pelielementtien lisäämiseen. Landers (2019, 137) korostaa, että todellinen pelillistäminen on paljon muutakin kuin pisteiden ja tasojen käyttöä. Se on suunnitteluprosessi, jossa yhdistetään pelien suunnitteluperiaatteita ja psykologista tutkimusta, jotta voidaan luoda järjestelmiä, jotka motivoivat käyttäjiä johdonmukaisesti, yleistettävästi ja eettisesti kestävällä tavalla.

Vaikka pelillistämisellä voidaan saavuttaa merkittäviä hyötyjä, sen suunnittelun laatu ratkaisee onnistumisen. On tärkeää ymmärtää, miten pelielementit vaikuttavat käyttäytymiseen ja millä tavoin ne voidaan integroida mielekkäästi eri konteksteihin.

2.4.3 Pelillistäminen työelämässä

Pelillistämisen suosio on kasvanut erityisesti työelämässä, jossa organisaatiot etsivät keinoja sitouttaa työntekijöitä ja lisätä heidän motivaatiotaan. Peliteollisuuden kehitys on herättänyt kiinnostusta pelillisten elementtien soveltamiseen myös muilla aloilla, ja organisaatiot eri puolilla maailmaa hyödyntävät pelillistämistä työntekijöiden, asiakkaiden ja opiskelijoiden sitouttamisessa (Dreimane 2021).

Armstrong ja Landers (2018) määrittelevät pelillistämisen prosessiksi, jossa lisätään pelielementtejä olemassa oleviin prosesseihin vaikuttaakseen ihmisten käyttäytymiseen ja saavutuksiin. Järvensivu (2017) tarkastelee hyötypelien soveltamista suomalaisessa työelämässä ja huomauttaa, että pelillistämisellä voi olla positiivisia vaikutuksia työntekijöiden kouluttamiseen ja työhyvinvoinnin edistämiseen. Hän kuitenkin painottaa, että vaikutukset riippuvat työn luonteesta ja organisaatiokulttuurista, mikä korostaa tarvetta räätälöidä pelillistettyjä ratkaisuja kunkin organisaation tarpeisiin.

Pelillistämisen soveltaminen työelämässä ei ole uusi ilmiö. Klabbersin (2009) mukaan pelejä käytettiin jo varhain johtajien kouluttamiseen yritystoiminnan kilpailutilanteisiin. Tällaisissa tilanteissa liiketoimintaa tarkasteltiin strategiapelin tavoin, jossa menestyminen edellyttää harkittuja päätöksiä ja resurssien hallintaa. Landers, Auer, Collmus ja Armstrong (2018, 1–2) viittaavat myös Klabbersiin, joka suhtautuu kriittisesti pelillisyyden käsitteeseen ja tulkitsee sen johtamismenetelmäksi, jonka tavoitteena on parantaa työpaikkojen suorituskykyä

käyttäytymistieteellisten keinojen avulla. Klabbers kyseenalaistaa pelillistämisen tieteellisyyden väittäen, että se on ensisijaisesti liike-elämän työkalu eikä tieteenala. Tähän näkemykseen on esitetty vastaväitteitä, ja Landers ym. (2018, 17) pyrkivät kumoamaan Klabbersin väitteet korostamalla pelillisyyden filosofista perustaa sekä sen asemaa pelitieteen kentällä.

Kaikki pelillistämishankkeet eivät kuitenkaan ole onnistuneet. Tämä on konkreettisesti nähtävissä Gabriellen (2018) kuvaamassa tapauksessa Disneyland Resortin pesulatyöntekijöistä Kaliforniassa. Disney otti käyttöön reaaliaikaisen seurantajärjestelmän, joka arvioi työntekijöiden tehokkuutta värikoodatuilla tulostauluilla. Tämä johti kovan kilpailun syntymiseen, mikä aiheutti työntekijöille uupumusta ja lisäsi työtapaturmien määrää. Myös Järvensivu (2017) mainitsee tapauksen, jossa tehtaan työntekijöiden monitaitoisuutta pyrittiin kehittämään pelillistämällä, mutta hanke epäonnistui, koska se ei huomioinut työntekijöiden tapaa organisoida työtehtävänsä mielekkäämmin.

Landers (2019) varoittaa, että pelillistämisen väärinkäyttö voi johtaa tilanteisiin, joissa lisätään ainoastaan pinnallisia pelielementtejä, kuten pisteitä ja palkintoja, ilman syvällistä ymmärrystä niiden vaikutuksista. Hamari, Koivisto ja Sarsa (2014) korostavat, että pelillistämisen teho perustuu siihen, miten se vaikuttaa käyttäytymiseen ja motivaatioon. Armstrong ym. (2018) puolestaan painottavat, että pelillistämisen tulee tukea sisäistä motivaatiota, eikä sen tulisi perustua pelkästään ulkoisiin palkintoihin, kuten pisteisiin ja tasoihin.

Pelillistämisen vaikuttavuus työelämässä riippuu siitä, miten se on suunniteltu. Armstrong ym. (2018, 4) toteavat, että jos tavoitteena on lisätä työntekijöiden sisäistä motivaatiota oppia, pelkkä pisteiden tai merkkien lisääminen ei riitä. Sen sijaan tarvitaan elementtejä, jotka tukevat pitkäjänteistä motivaatiota, kuten selkeät palautteet, saavutusten tunnistaminen ja mahdollisuudet kehittyä tehtävien kautta. Tällöin pelillistäminen ei jää pelkäksi ulkoiseksi palkitsemiseksi, vaan tukee oppimista ja johtaa haluttuun käyttäytymisen muutokseen.

Almeidan, Kalinowskin, Uchôan ja Feijón (2023) tutkimus tuo esiin pelillistämisen mahdolliset haittavaikutukset ja muistuttaa, että sen onnistuminen ei ole itsestään selvää. Heidän mukaansa esimerkiksi kilpailulliset elementit voivat aiheuttaa liiallista painetta ja heikentää työtyytyväisyyttä. Esimerkiksi organisaatio, joka ottaa käyttöön pistejärjestelmän työntekijöiden koulutusmoduuleissa, voi huomata, että työntekijät alkavat suorittaa moduuleja mahdollisimman nopeasti pisteiden keräämiseksi, mutta eivät sisäistä oppimateriaalia, mikä lopulta heikentää koulutuksen päätavoitetta.

Armstrong ym. (2018, 1) nostavat esiin toisen haasteen, joka liittyy pelillistämisen laajaan mutta epätarkkaan käyttöön. Heidän mukaansa termiä käytetään usein yleisesti kaikesta pelilliseen viittaavasta työpaikalla. Tämä voi johtaa siihen, että pelillistämistä sovelletaan virheellisesti, ja pelkkien pelillisten elementtien lisääminen ilman taustalla olevien psykologisten vaikutusten ymmärtämistä voi heikentää tuloksia. Siksi on olennaista, että pelillistämistä

käytettäessä huomioidaan kohderyhmän tarpeet ja valitaan sellaiset pelimekaniikat, jotka tukevat tavoiteltua käyttäytymistä ja motivaatiota.

Pelillistämisen soveltaminen työelämässä on siis monisyinen ilmiö, jonka onnistuminen edellyttää huolellista suunnittelua. Sen hyödyntämisessä ei ole kyse pelkästään pelielementtien lisäämisestä, vaan kokonaisvaltaisesta suunnitteluprosessista, jossa ymmärretään, miten pelillisyys vaikuttaa käyttäytymiseen ja motivaatioon. Jos pelillistämistä hyödynnetään strategisesti ja organisaation tarpeisiin sopivalla tavalla, se voi olla tehokas keino työelämän kehittämisessä.

2.4.4 Pelillistäminen tietosuojaosaamisen kehittämisessä

Tietosuojalainsäädäntö velvoittaa organisaatiot varmistamaan, että niiden työntekijät osaavat käsitellä henkilötietoja asianmukaisesti. Kuten Andreasson ym. (2019, 12) toteavat, tietosuoja-asetuksen keskeinen periaate on riskiperusteinen lähestymistapa, mikä tarkoittaa, että organisaatioiden on mukautettava tietosuojakäytäntönsä käsiteltävien henkilötietojen luonteen ja riskien mukaisesti. Lainsäädäntö edellyttää myös osoitusvelvollisuuden toteuttamista eli dokumentointia siitä, kuinka henkilötietojen käsittelyyn liittyviä riskejä hallitaan.

Perinteiset koulutusmenetelmät, kuten kirjalliset ohjeet ja luennot, eivät aina onnistu herättämään työntekijöiden kiinnostusta tietosuojaan. Teoreettinen materiaali voi olla abstraktia ja vaikeaselkoista, jolloin se jää etäiseksi eikä yhdisty työntekijöiden päivittäisiin työtehtäviin. Vakiintuneet koulutusmenetelmät, kuten verkkokurssit ja kirjalliset oppaat, voivat olla hyödyllisiä, mutta ne eivät välttämättä motivoi työntekijöitä syventämään osaamistaan. Tämän kehittämistyön tietoperusta tukee näkemystä, jonka mukaan interaktiiviset koulutusmenetelmät voivat parantaa organisaation valmiuksia vastata tietosuojan haasteisiin.

Pelillistäminen tarjoaa mahdollisuuden lisätä motivaatiota ja sitoutumista tietosuojakoulutuksessa hyödyntämällä pelielementtejä, kuten pisteitä ja palkintoja. Se mahdollistaa myös tietosuojatilanteiden harjoittelun turvallisessa ympäristössä, mikä voi auttaa työntekijöitä soveltamaan tietosuojasäännöksiä käytännössä. Pelillistetty oppiminen voi myös helpottaa tiedon omaksumista ja tehdä oppimisesta mielekkäämpää. Koska pelillistämisen vaikutukset näkyvät usein pitkällä aikavälillä, sen tuottavuutta on vaikea mitata suoraan. Se voi kuitenkin osaltaan edistää organisaation tietoturvakulttuuria ja luoda turvallisemman työympäristön, joka tukee myös taloudellista tehokkuutta.

Tietosuojalainsäädännön ja pelillistämisen teorioiden näkökulmat täydentävät toisiaan. Tietosuoja-asetus edellyttää organisaatioilta tietosuojakäytännön ja osaamisen jatkuvaa kehittämistä, mutta se ei määrittele tarkkoja keinoja, joilla koulutus tulisi toteuttaa. Pelillistäminen voi tarjota käytännön menetelmiä tietosuojaan liittyvien velvoitteiden sisäistämiseen. Näistä syistä pelillistäminen valittiin tämän kehittämistyön toteuttamisen menetelmäksi, sillä se tarjoaa käytännönläheisen tavan oppia ja soveltaa monimutkaista ja usein abstraktia tietoa.

Työntekijöiden kiinnostusta voidaan lisätä tarjoamalla tietoiskutyyppisiä koulutuksia, jotka perustuvat todellisiin esimerkkeihin ja tapahtumiin. Konkreettiset tapaukset havainnollistavat tietosuojan merkitystä ja tekevät aiheesta helpommin ymmärrettävän. Kansainvälisellä tasolla tällaisia tapauksia voidaan löytää esimerkiksi IAPP:n (International Association of Privacy Professionals) verkkosivuilta, joissa seurataan globaalisti tapahtuvia tietosuojaloukkauksia, kyberhyökkäyksiä ja organisaatioiden saamia tietosuojasakkoja. Suomessa tietoa löytyy parhaiten median kautta. Liiallinen keskittyminen tietosuojarikkeisiin ja sanktioihin voi kuitenkin aiheuttaa henkilökunnassa pelkoa ja epävarmuutta, mikä voi johtaa siihen, että tietosuojaa vältellään liiallisella varovaisuudella eikä henkilötietoja uskalleta käsitellä edes silloin, kun se on tarpeellista.

Pelillistämisen vaikutuksia tietosuojaosaamisen kehittymisessä on tutkittu eri näkökulmista. Armstrong ym. (2018, 2–3) havaitsivat teknologiaturvallisuuden koulutuksessa, että narratiivin ja tarinallisten elementtien käyttö teki koulutusmateriaaleista kiinnostavampia ja sai parempaa palautetta kuin perinteiset koulutusmenetelmät. Samansuuntaisesti Francia Thronton, Trifas ja Bowden (2014) toteavat, että pelillistäminen voi parantaa tietoturvatietoisuutta ja -koulutusta organisaatioissa, mutta sen onnistuminen edellyttää huolellista suunnittelua.

Hoxhuntin (2023) artikkelissa kuvataan käytännön esimerkki siitä, kuinka pelillistäminen voi lisätä kiinnostusta tietosuojakoulutukseen. AES-energiayhtiössä työntekijöiden osallistuminen koulutuksiin nousi 10 prosentista 70 prosenttiin vain muutamassa kuukaudessa, kun koulutus pelillistettiin. Tämä osoittaa, että pelillistämisellä voidaan lisätä osallistumista ja sitouttaa työntekijöitä tietosuojaan, mikä voi vaikuttaa organisaatiokulttuuriin pysyvästi.

Pelillistämiseen liittyy kuitenkin myös haasteita. Ennen sen käyttöönottoa on tärkeää pohtia, mitä oppimistavoitteita halutaan vahvistaa ja miten varmistetaan, että pelillistetty koulutus tukee oikeanlaista oppimista. Armstrong ym. (2018, 2) huomauttavat, että jos työntekijät kokevat koulutuksen sisällön hyödyttömäksi, koulutusmateriaalin parantaminen voi olla tehokkaampi ratkaisu kuin pelillistäminen. Jos taas koulutukseen liittyy ennakkoluuloja tai negatiivisia asenteita, narratiivinen lähestymistapa voi auttaa sitouttamaan osallistujia.

Pelillistetyn koulutuksen ja koulutuksen sisällön pelillistämisen välillä on myös ero. Armstrong ym. (2018, 3) toteavat, että pelillistetty koulutusmenetelmä voi olla vähemmän tehokas kuin koulutuksen sisällön pelillistäminen. Siksi ennen päätöstä pelillistämisen käytöstä on arvioitava, tarvitseeko koulutuksen sisältö itsessään muutosta, vai voiko pelillisyys toimia tukevana elementtinä oppimisessa.

Lisäksi Armstrong ym. (2018, 2) korostavat, että pelillistäminen ei korvaa perinteisiä opetusmenetelmiä, vaan se toimii niitä täydentävänä elementtinä. Tämä havainto korostaa pelillisen suunnittelun merkitystä ja sitä, että pelillistämisen tulee perustua laajempaan oppimisen kehykseen. Gjertsen, Gjære, Bartnes ja Flores (2017) tukevat tätä näkemystä tutkimuksessaan, jossa selvitettiin, miten pelillistämistä voisi hyödyntää tietoturvakoulutuksessa. Tulosten

mukaan pelillistäminen voi lisätä motivaatiota ja oppimistuloksia, mutta jos koulutus koetaan pakotetuksi tai vaikeaksi yhdistää työtehtäviin, työntekijät eivät välttämättä sitoudu siihen. Tämä korostaa Armstrongin ym. (2018, 2) esittämää huolta siitä, että pelillistäminen voi epäonnistua, jos osallistujat eivät koe sitä hyödylliseksi.

Pelillistäminen voi siis olla tehokas tapa kehittää tietosuojaosaamista, mutta sen onnistuminen edellyttää tarkkaa suunnittelua ja kohderyhmän tarpeiden ymmärtämistä. Se ei ole itsessään ratkaisu tietosuojakoulutuksen haasteisiin, mutta oikein sovellettuna se voi tehdä oppimisesta mielekkäämpää, käytännönläheisempää ja vaikuttavampaa.

2.4.5 Pelillistämisen yhteenveto

Pelillistäminen on monipuolinen ilmiö, joka soveltuu laajasti eri aloille, kuten työelämään ja koulutukseen. Sen avulla voidaan lisätä motivaatiota, parantaa oppimistuloksia ja sitouttaa työntekijöitä. Kuitenkin sen vaikuttavuus ei ole itsestäänselvyys, vaan se riippuu ennen kaikkea siitä, kuinka huolellisesti ja tavoitteellisesti pelillisiä elementtejä hyödynnetään.

Tietosuojaosaamisen kehittämisessä pelillistämisellä on potentiaalia tehdä koulutuksesta kiinnostavampaa ja käytännönläheisempää. Edellä mainitut tutkimukset osoittavat, että pelillistäminen voi lisätä osallistujien motivaatiota ja auttaa omaksumaan tietosuojaperiaatteita tehokkaammin kuin perinteiset menetelmät. Hamari ym. (2014) kuitenkin korostavat, että pelillistämisen vaikutukset eivät ole automaattisia, vaan ne riippuvat siitä, kuinka hyvin pelielementit valitaan ja kuinka ne tukevat oppimistavoitteita.

Vaikka pelillistäminen voi tarjota monia etuja, on tärkeää tunnistaa myös siihen liittyvät haasteet. Friman ym. (2022) suhtautuvat pelillistämiseen varauksella ja huomauttavat, että sen tuottavuushyödyt eivät ole yksiselitteisiä. Lisäksi huonosti suunniteltu pelillistäminen voi johtaa negatiivisiin kokemuksiin, kuten liialliseen kilpailuun tai ulkoisten palkintojen korostumiseen sisäisen motivaation kustannuksella. Tämä asettaa paineita pelillistämisen suunnittelulle, sillä väärin toteutettuna se voi pahimmillaan heikentää oppimista ja motivaatiota.

Pelillistäminen ei myöskään sovi kaikille. Tässä kehittämistyössä pelillistämiseen ei ole varattu budjettia, minkä vuoksi voi joutua tyytymään kuvitteellisiin etenemismenetelmiin. Tämä voi johtaa osallistujien kokemukseen siitä, että heidän aikansa kuluu turhaan. Kaikki eivät myöskään koe kilpailuasetelmia motivoiviksi, ja esimerkiksi tasohyppelyt tai pistejärjestelmät voivat tuntua keinotekoisilta ja tarpeettomilta. Siksi on tärkeää tunnistaa erilaisia tapoja motivoida osallistujia ja tarjota vaihtoehtoisia mekanismeja.

Kritiikistä huolimatta tutkimukset osoittavat, että oikein suunniteltuna pelillistäminen voi tehdä oppimisesta motivoivampaa ja sitouttavampaa. Pelkkä pelillisten elementtien lisääminen ei kuitenkaan riitä, vaan niiden on oltava tarkoituksenmukaisia ja kohderyhmälle sopivia.

Deterding ym. (2011, 12) painottavat, että onnistunut pelillistäminen edellyttää tasapainoa eri elementtien välillä ja niiden huolellista sovittamista oppimistavoitteisiin.

Näiden tutkimusten ja havaintojen perusteella pelillistäminen voi olla tehokas tapa lisätä tietosuojatietoisuutta ja kehittää osaamista organisaatiossa. Se tekee oppimisesta vuorovaikutteisempaa ja mukaansatempaavampaa, mikä puolestaan parantaa sitoutumista ja tietosuojakäytäntöjen noudattamista. Samalla on kuitenkin varmistettava, että pelillistäminen on suunniteltu huolellisesti ja se tukee organisaation todellisia oppimistavoitteita.

Organisaation tietosuojavastaavan tehtävänä on varmistaa henkilötietojen käsittelyn lainmukaisuus, valvoa niiden käsittelyä ja ohjeiden noudattamista, sekä neuvoa ja toimia asiantuntijana tietosuojaan liittyen. Lainsäädäntö ei tarjoa menetelmiä opetuksen toteuttamiselle, joten malli ja menetelmä on avoin kaikille organisaatioille. On tärkeää pitää työntekijöiden perustietämystä tietosuojan osalta ajan tasalla, sillä kokonaisuus on niin laaja ja työntekijöiden, jotka eivät työn puolesta ole tekemisissä tietosuoja-asioiden kanssa, ei jaksa kiinnostua siitä syvemmällä tasolla.

Lopulta pelillistäminen on vain yksi työkalu muiden joukossa. Sen tehokkuus riippuu siitä, kuinka hyvin se on sovitettu kohderyhmän tarpeisiin ja kuinka tarkoituksenmukaisia pelilliset mekanismit ovat. Tietosuojaopetuksessa sen avulla voidaan tehdä oppimisesta interaktiivisempaa ja helpommin omaksuttavaa, mutta onnistuminen edellyttää tarkkaa suunnittelua ja osallistujien tarpeiden huomioimista.

Pelillistäminen voi olla tehokas keino tietosuojaosaamisen kehittymisessä. Tutkimukset osoittavat, että se voi parantaa oppimistuloksia ja lisätä motivaatiota. Deterdingin ym. (2011, 12) mukaan pelielementit on kuitenkin valittava huolella, jotta ne palvelevat koulutuksen tavoitteita. Hamari ym. (2014) vahvistavat tätä näkemystä ja tuovat esiin, että pelillistäminen voi edistää oppimista juuri siksi, että se lisää sitoutumista ja motivaatiota. Armstrong ym. (2018, 6) lisäävät, että pelillistämisen tulee olla käytännönläheistä ja tukea oppijan sisäistä motivaatiota.

2.5 Tietoperustan yhteenveto

Tietosuojalainsäädäntö asettaa organisaatioille vastuuta ja edellyttää konkreettisia toimia työntekijöiden tietosuojatietoisuuden edistämiseksi. Organisaatiolla ja työntekijöillä on oltava riittävä osaaminen henkilötietojen käsittelyyn. Se korostaa henkilötietojen suojan merkitystä sekä työnantajan, työntekijän ja yksilön näkökulmasta. Vaatimusten täyttäminen ei ole pelkästään juridinen velvollisuus, vaan osa myös organisaation toimintakulttuuria. Tietosuojalainsäädäntö ei myöskään määritä, miten näitä vaatimuksia tulisi käytännössä toteuttaa.

Tietosuoja-asetuksen keskeinen periaate on riskiperusteinen lähestymistapa. Organisaation on siis mukautettava tietosuojaperiaatteensa käsiteltävien henkilötietojen perusteella.

Lainsäädäntö myös velvoittaa osoittamaan lainsäädännön noudattamisen ja organisaation on myös dokumentoitava henkilötietojen käsittelyyn liittyviä riskejä.

Perinteiset koulutusmenetelmät, kuten kirjalliset ohjeet ja luennot eivät aina riitä kiinnostamaan tai edistämään työntekijöiden tietosuojaosaamista. Teoreettinen materiaali voi olla abstraktia ja vaikeaselkoista, joka ei yhdisty päivittäiseen työhön.

Pelillistämisessä voidaan hyödyntää erilaisia pelin elementtejä, kuten pisteitä tai palkintoja ja ne voivat lisätä motivaatiota ja sitoutumista. Lisäksi pelillistäminen tarjoaa mahdollisuuden kokeilla tietosuojaan liittyviä tilanteita turvallisessa ympäristössä. Pelillistäminen voi vastata haasteeseen tarjoamalla käytännönläheisen oppimiskokonaisuuden, jonka avulla voidaan tukea tietosuojan soveltamista arjessa. Pelillistetyt ratkaisut voivat lisäksi helpottaa tiedon omaksumista. Kehittämistyössä pelillistämisen vaikutus on epäsuora eikä tuottavuutta voida mitata millään mittarilla, vaan sen vaikutus nähdään pitkällä aikavälillä luomalla kaikille turvallisempi työympäristö, jolloin se tukee myös taloudellista tehokkuutta.

Yleisellä tasolla koulutuksen tarvetta arvioitaessa tulee tunnistaa puutteet koulutuksen osalta. Sen jälkeen voidaan arvioida pelillistämisen mahdollisuuksia ongelmien ratkomiseen. (Armstrong ym. 2018, 3.)

Lemmetty (2024, 261, 268) kirjoittaa kriittisen näkökulman osaamisen kehittämisestä ja on nostanut esille tärkeitä havaintoja oppimisen vastuusta työelämässä. Hän pohtii erityisesti sitä, onko vastuu oppimisesta siirtynyt liikaa yksilöille ja koulutusjärjestelmille. Teknologian kehittyminen ja työelämän tehostuminen ovat luoneet uusia osaamisvaatimuksia ja lisäävät työntekijöiden kuormitusta. Lemmetyn (2024, 271) mukaan monikaan ei selviä moniasiantuntijuuden tai muun multitaskaamisen haasteista, vaan tähän tarvitaan jokaisen osapuolen yhteisvastuuta. Tietosuojaosaaminen on olennainen osa jatkuvaa oppimista, sillä teknologian kehityksen vaatimukset edellyttävät kaikilta valmiutta sopeutua työelämän haasteisiin.

Voisiko työnantaja tukea työntekijän oppimista, jottei oppiminen jää työntekijän vastuulle? Tämä on tärkeää etenkin silloin, kun työntekijän omat tiedonhankintakyvyt ja resurssit eivät riitä muuttuvan tietosuojalainsäädännön ymmärtämiseen ja soveltamiseen. Salon (2012) artikkelissa hoivapalvelun työntekijöiden koulutustarpeita tutkittiin teoreettisesti Scissonsin arvioivan mallin mukaan. Tässä mallissa koulutustarpeen ohjaaviksi ulottuvuuksiksi määritellään ammatillinen osaaminen, asiaankuuluvuus ja motivaatio. Ammatillinen osaaminen viittaa työntekijöiden nykyisiin tietoihin ja taitoihin, asiaankuuluvuus viittaa siihen, miten tärkeänä he kokevat eri taidot ja tiedot omassa työssään. Motivaatio viittaa työntekijöiden halukkuuteen oppia ja kehittää omia taitoja. Yhdistämällä ammatillinen osaaminen ja asiaan kuuluvuus, voidaan tunnistaa tärkeitä alueita, joissa työntekijät kokevat olevansa epäpäteviä.

Kun pohditaan koulutuksen arvioinnin prosessia ja pelillistämisen mahdollisuuksia tietosuojan osaamisen kehittämisessä, on tärkeää miettiä, vastaako koulutuksen kehittämiseen käytetty

aika ja resurssit todellista tarvetta. Armstrongin ym. (2018, 5) esittämä vaihe tarjoaa kehyksen koulutustarpeiden tunnistamiselle ja arvioinnille, mutta herättävät myös kysymyksen: onko organisaatiossa tarvetta kehittää tietosuojan osaamista pelillistämisen avulla, sillä tutkittua tietoa tästä ei ole olemassa.

Näin ollen, ennen kuin päätetään lähteä kehittämään tietosuojan osaamista pelillistämisen keinoin, tulisi tehdä koulutuksen tarvearviointi ja miettiä eri vaihtoehtojen hyötyjä organisaation tavoitteisiin. Lisäksi voi pohtia, onko pelillistäminen oikea lähestymistapa näiden puutteiden ratkaisemiseksi. Vaikka se voi tarjota motivoivan tavan oppia, se ei välttämättä ole paras tapa vastata koulutustarpeeseen.

Tietosuojaosaaminen hyödyttää organisaatiota, työntekijöitä ja asiakkaita. Organisaatio saa tehokkuutta, kustannussäästöjä, paremman riskienhallinnan ja vahvemman maineen luotettavana toimijana. Työntekijöille se parantaa asiakastietojen käsittelyä, oikeusturvaa ja työviihtyvyyttä. Asiakkaille se takaa laadukkaamman palvelun ja luottamuksen tietojen lainmukaiseen käsittelyyn. Tietosuojaan sijoittaminen on investointi, joka maksaa itsensä takaisin tuottavuuden, tehokkuuden ja kustannussäästöjen kautta. (Andreasson ym. 2019, 50–51.)

Tietosuojalainsäädännön ja pelillistämisen teorioiden näkökulmat täydentävät toisiaan. Tietosuoja asettaa vaatimukset organisaatioille ja korostaa riittävää osaamista. Pelillistämisen teoriat antavat käytännön menetelmiä tietosuojaan liittyvien velvoitteiden sisäistämiseen. Näiden tekijöiden perusteella pelillistäminen valittiin kehittämistyön toteuttamisen menetelmäksi. Se tarjoaa mahdollisuuden oppia käytännönläheisesti, mikä on tärkeää abstraktin ja vaikeaselkoisen sisällön oppimisessa.

3 Kehittämisasetelma

Kehittämistyön tavoitteena on suunnitella ja toteuttaa tietosuojapeli, joka parantaa työntekijöiden kykyä tunnistaa ja reagoida arjen tietosuojatilanteisiin. Kehittämistyö toteutetaan konstruktiivisen lähestymistavan mukaan. Tässä luvussa esitellään kehittämistyön eteneminen, kuvataan kehittämistyön menetelmät ja aineiston analysointi.

Kehittämistyön toimeksiantajana on Humanistinen ammattikorkeakoulu Oy (Humak). Toimeksiantajan työntekijät koostuvat monialaisista ammattilaisista, joista jokainen on tekemisissä henkilötietojen kanssa jollain tasolla. Organisaation tietosuojan toteutumisesta vastaa nimetty tietosuojavastaava. Hän koordinoi ja valvoo henkilötietojen käsittelyyn liittyviä käytäntöjä. Tietosuojavastaava myös konsultoi työntekijöitä tietosuojahaasteissa. Tärkeänä osana on myös seurata tietosuojasta käytävää keskustelua eri medialähteissä ja jatkuvasti arvioida sen merkitystä organisaation näkökulmasta. Organisaatiossa toimii myös erilaisia ryhmiä, joiden yhteistyöllä varmistetaan kokonaisturvallisuuden toimivuus. Organisaation tietosuojavastaava on käytännössä todennut tarpeet tietosuojatietoisuuden kehittämiselle.

Tietosuoja on ollut aiheena ajankohtainen jo vuosia. Tietosuojasta on saatavalla kirjallista materiaalia runsaasti, mutta täsmätiedon etsintä on aikaa vievää ja vastausten saaminen on epävarmaa. Kehittämistyön lähtökohtana oli kiinnostus tietosuojaan sekä tarve kehittää ja vahvistaa organisaation tietosuojaosaamista muulla kuin kirjallisella materiaalilla. Lainsäädäntö edellyttää organisaatioita käsittelemään henkilötietoja turvallisesti ja lainmukaisesti, mutta työntekijät voivat jäädä epätietoisiksi velvoitteistaan.

Pelillistäminen tarjoaa käytännönläheisen menetelmän osaamisen kehittämiseen. Pelillistetty oppiminen voi auttaa konkretisoimaan käytännön tietosuojatilanteita. Kehittämistyön tarkoituksena on ymmärtää pelillistetyn oppimisen tarjoamia mahdollisuuksia tietosuojaosaamisen kehittämisessä.

Kehitetyllä pelillä pyritään motivoimaan työntekijöitä kehittämään tietosuojaosaamistaan innostavalla tavalla. Pelillisyys tukee arjen tietosuojatilanteiden tunnistamista ja niihin reagoimista.

3.1 Konstruktiivinen tutkimus

Konstruktiivinen tutkimus on metodologia, joka keskittyy käytännön ongelmien ratkaisemiseen kehittämällä uusia innovatiivisia ratkaisuja eli konstruktioita. Se on menetelmän keskeinen käsite, joka voi tarkoittaa mitä tahansa luotua ideaa, mallia tai järjestelmää. Konstruktio voi ilmetä esimerkiksi uutena organisaatiorakenteena, suunnitelmana tai kaupallisena tuotteena. Menetelmällä on rajaton määrä toteutusmahdollisuuksia. Tutkimus alkaa merkityksellisen ja teoreettisesti kiinnostavan ongelman tunnistamisella. Tämän jälkeen tekijä perehtyy aiheeseen sekä käytännön että teorian näkökulmasta, jonka pohjalta kehittää innovatiivisen ratkaisun. (Lukka 2014.)

Lukan (2000) mukaan konstruktiivisessa tutkimuksessa keskeistä on todellisten, käytännössä merkityksellisten ongelmien ratkaiseminen. Näin tutkimus ei keskity pelkkään teoreettisiin pohdintoihin. Konstruktio tulee suunnitella kohdeorganisaation kannalta konkreettisen ongelman ratkaisemiseen. Ei riitä, että ratkaisu kehitetään teoreettisesti, vaan sitä pitää testata ja soveltaa käytäntöön.

Lukka (2014) mainitsee, että konstruktiivinen lähestymistapa motivoi käytännön toimijat osallistumaan tutkimukseen, koska sen tavoitteena on ratkaista todellisia ongelmia. Lisäksi konstruktiivisessa tutkimusotteessa korostetaan tutkijan ja käytännön toimijoiden välistä yhteistyötä ja vuorovaikutusta. Näin ollen molemmat osapuolet oppivat ja antavat aikaa prosessin läpiviemiseen.

Konstruktiivinen tutkimus on hyvä keino vähentää etäisyyttä teorian ja käytännön välillä. Vaikka konstruktiivinen lähestymistapa on käytännönläheinen, se on siitä huolimatta tiiviisti

sidoksissa teoriaan. Se sopii hyvin tilanteisiin, joissa halutaan yhdistää käytännön ongelmaratkaisu ja teoria.

Virtanen (2006, 46) toteaa konstruktiivisen lähestymistavan sopivan hyvin kehittämistyön lähestymistavaksi, sillä siinä yhdistyvät organisaation kehittäminen ja tieteellisen tiedon tuottaminen. Konstruktiivisessa tutkimuksessa tuotetaan yksi pätevä ratkaisu organisaation ongelmaan. Lisäksi hän kirjoittaa, että onnistunut konstruktio on yleistettävissä ja siirrettävissä eteenpäin muihin organisaatioihin.

Rajan veto konstruktiivisen tutkimuksen ja ongelmanratkaisun välillä voi olla haastavaa. Konstruktiivinen tutkimus ei ole pelkkää ongelmanratkaisua tai konsultointia, vaan sen tavoitteena on kehittää tieteellisesti perusteltuja ratkaisuja ja samalla arvioida niitä kriittisesti. (Kasanen, Lukka & Siitonen 1993, 252.)

Kaikki edellä mainitut lähteet korostavat konstruktiivisen lähestymistavan käytännönläheisyyttä, teorian merkitystä, aktiivista yhteistyötä kohdeorganisaation kanssa ja innovatiivisten ratkaisujen luomista ja arviointia.

3.2 Kehittämistyön eteneminen

Kehittämistyön lähtökohtana on tunnistettu käytännön haaste ja tavoitteena on löytää toimiva ratkaisu siihen. Konstruktiivinen lähestymistapa mahdollistaa ratkaisun testaamisen aidossa ympäristössä, jolloin ratkaisumalli voidaan sovittaa työelämän tarpeisiin. Kehittämistyössä otetaan huomioon organisaation toimintakulttuuri sekä käyttäjien tarpeet, jotta ratkaisu olisi käytännössä toimiva ja hyödyllinen.

Konstruktiivisessa tutkimuksessa keskeistä on konkreettisten ongelmien ratkaiseminen ja uuden toimintamallin kehittäminen. Konstruktiivisen lähestymistavan keskeiset piirteet (Lukka 2000) on esitetty taulukossa 1, jossa lisättynä kehittämistyön käytännön esimerkki aiheesta.

Taulukko 1: Konstruktiivisen lähestymistavan keskeiset piirteet (Lukka 2000, 2).

Konstruktiivinen tutkimus	Selite	Huomioitavaa	Esimerkki
Keskittyminen todellisiin ongelmiin ja hankitaan esiymmärrys.	Pyritään ratkaisemaan käytännön merkityksellinen ongelma.	Ratkaisun tulee olla organisaation kannalta käytännössä toteutettavissa.	Havaittiin puutteellinen tietosuojaosaaminen, joten toteutettiin tietosuojaosaamisen kartoitus.

Innovatiivisen ratkaisun tuottaminen	Uuden ja hyödyllisen ratkaisun kehittäminen.	Uusi menetelmä, prosessi tai tuote, joka tuo ratkaisun. Yritysyhteistyö.	Tietosuojatietoisuuden lisäämiseksi kehitettiin uusi pelillistetty oppimismalli, jonka avulla voi harjoitella erilaisia tietosuojatilanteita.
Ratkaisun toteuttaminen ja testaaminen	Kehitetyn ratkaisun käytännön testaus.	Iteratiivinen prosessi, jossa toimivuutta kehitetään jatkuvan palautteen perusteella. Yritysyhteistyö.	Testaus testiryhmällä ja sen jälkeen kohderyhmällä.
Osallistuminen ja yhteistyö	Aktiivinen yritysyhteistyö.	Yhteistyö organisaation kanssa, jotta ratkaisumallista saadaan hyödyllinen.	Pelin skenaarioiden määrittely yhteistyössä organisaation kanssa.
Aiempi teoria	Aiempaa teoreettista tietoa hyödynnetään ratkaisun kehittämisessä.	Aiempi tutkimus antaa perustan ratkaisun kehittämiselle.	Pelillisen ympäristön suunnittelussa hyödynnettiin aiempia tutkimuksia pelillistämisen vaikutuksista.
Empiiristen löydösten ja teorian yhteys	Yhteys ei ole ennalta määrätty	Yhteys muuttuu etenemisen myötä	Pelillistetyn ympäristön kysymykset olivat liian vaikeita. Niitä selkiytettiin ja muutettiin helpommiksi.

Vaikka konstruktiivinen menetelmä tarjoaa merkittäviä etuja, siihen liittyy myös tiettyjä riskejä. Tutkimuksen aikana voi ilmetä arkaluonteisia tietoja, joita kohdeorganisaatio ei halua julkaista. Tämän riskin minimoimiseksi on suositeltavaa sopia julkaisukäytännöistä jo ennen yhteistyön aloittamista. Toinen yleinen haaste on kohdeorganisaation sitoutumisen heikkeneminen tutkimuksen aikana. Tämä voi johtua siitä, ettei ongelma osoittaudukaan organisaation

näkökulmasta niin kriittiseksi kuin alun perin ajateltiin. Organisaatio ei ehkä ole valmis myöskään panostamaan riittävästi toteutukseen. Riskin hallitsemiseksi on tärkeää analysoida ongelman käytännön merkitys ennen kehitysprosessin aloittamista. (Lukka 2003, 97.)

3.2.1 Kehittämistyön ongelma

Lukka (2003, 86) korostaa tutkimusaiheen valinnan olevan yksi tärkeimmistä vaiheista tutkimuksessa, eikä konstruktiivinen tutkimus ole poikkeus. Tutkimusaiheen tulee olla sekä käytännössä merkityksellinen että teoreettisesti perusteltu. Hän myös mainitsee ihanteellisen tutkimuksen olevan sellainen, jossa käytännön ongelma on ristiriitainen tai aiemmin puutteellisesti analysoitu.

Ristiriitaa voi aiheuttaa esimerkiksi Barth ym. (2019, 55) mainitsema seikka, jossa opiskelijat olivat huolissaan omasta yksityisyydestään, mutta siitä huolimatta jakoivat epäröimättä yksityisiä tietoja sosiaalisessa mediassa. Lukan (2014) mukaan ongelman käytännön merkitys tulee arvioida huolellisesti ja kriittisesti kohdeorganisaation kanssa ennen kehittämistyön aloittamista.

Tietosuojakäytäntöjen saaminen osaksi organisaatioiden käytäntöjä voi olla haasteellista. Koulutusmateriaalit, kuten kirjalliset aineistot, keskittyvät usein teoreettisiin ja lainsäädännöllisiin näkökulmiin. Ne eivät välttämättä vastaa työntekijöiden käytännön tarpeisiin. Tämän seurauksena työntekijät saattavat jäädä epätietoiseksi omista tietosuojavelvoitteistaan. Ongelma on tiedostettu jo aiemmin, mutta tässä vaiheessa tunnistettiin kehittämistyön osalta mielenkiintoinen haaste.

Organisaation vakiintuneita koulutusmenetelmiä ovat luennot, verkkokurssit, videot, kirjalliset ohjeet ja oppaat. Vahvuutena on menetelmien tehokkuus, selkeys ja onnistutaan tavoittamaan myös suuria määriä ihmisiä saavutettavalla materiaalilla. Monet koulutustilaisuudet ovat nykyään myös jollain tavalla interaktiivisia ja niissä pyritään osallistamaan kuulijoita mukaan tekemiseen ja ideointiin. Tämä näkyy esimerkiksi ryhmätyöskentelyn, työpajojen ja kyselyiden muodossa. Tietosuojaosaamisen kehittämisessä ei tällä hetkellä ole käytössä interaktiivisuutta tai pelillistämisen keinoja, kuten pisteitä, tasoja tai osaamisen merkkejä, jotka voisivat kannustaa työntekijöitä edistymään.

Organisaation intranetissä on runsaasti tietosuojan kirjallista materiaalia, kuten osoitusvelvollisuuden toteuttaminen, tietosuojakäsikirja, tietosuojaselosteet, tietosuojan huoneentaulu, ym. yleinen kirjallinen koulutusmateriaali. Materiaalia on siis paljon tarjolla, mutta ei kiinnitetä huomiota siihen, onko materiaali luettu ja ymmärretty. Uusilta työntekijöiltä saatetaan odottaa tietosuojaosaamista ilman, että heille tarjotaan edellytyksiä sen hankkimiseen.

Epävirallisen kyselyn mukaan kirjalliset ohjeet ja säännöt ovat koettu yksitoikkoiseksi, vaikeaselkoisiksi, mutta kuitenkin itsestään selviksi. Vaikeaselkoisuuden osalta ajateltiin, ettei

sisältö koske itseä omissa työtehtävissä eikä se ole mielenkiintoinen, vaan se kuuluu toiselle osastolle ja sen takia siitä ei tarvitse kiinnostua. Tietosuoja-asioiden saatetaan luulla kuuluvan pelkästään organisaation IT-osastolle, vaikka tietosuojalainsäädännön noudattaminen on kuitenkin jokaisen työntekijän vastuulla.

Verkon välityksellä henkilökunnalle on myös pidetty tietosuojakoulutuksia, mutta tilastojen mukaan tallenteita ei ole katsottu jälkikäteen. Ovatko perinteiset tietosuojaohjeistukset ja tietosuojakoulutukset usein tehottomia ja unohtuvat nopeasti?

Organisaatiossa jokaisen työntekijän on vuosittain suoritettava itseopiskeluna verkkokurssi, jonka avulla työntekijä voi päivittää osaamistaan tietosuojan ja tietoturvan osalta. Verkkokurssilla aiheita käsitellään yleisellä tasolla ja sisältö päivitetään kerran vuodessa vastaamaan nykyisiä arjen uhkatilanteita. Verkkokurssin voi suorittaa itselle sopivana aikana. Kysymyskategoriat ovat yleisiä tietosuojaan ja tietoturvaan liittyviä aiheita ja kysymykset ovat hyvin muotoiltuja ja käytännönläheisiä. Verkkokurssin kesto on noin 2 tuntia jos lukee aiheeseen liittyvän kirjallisen materiaalin ja katsoo videot. Kirjallinen materiaali on selkeä ja sisältää vain olennaisen, mutta materiaalissa tai videoissa ei ole interaktiivisuutta tai palkitsevia elementtejä, joka innostaisi lukemaan tai katsomaan materiaalia.

Pelillisyyttä on aikaisemmin pyritty hyödyntämään mm. Taisto-harjoituksen ja Digiturvallinen elämä -mobiilipelin avulla. Molemmat ovat Digi- ja väestötietoviraston julkaisuja ja ne tarjoavat kaksi erilaista lähestymistapaa tietosuojan ja tietoturvan oppimiseen. Molemmat pyrkivät parantamaan organisaatioiden ja yksilöiden valmiuksia käsitellä näitä aiheita, mutta niiden toimintamallissa on merkittävä ero. (Digi- ja väestötietovirasto 2024a; Digi- ja väestötietovirasto 2024b.)

Marraskuussa 2024 Aalto-yliopisto ja Liikenne- ja viestintäministeriö lanseerasivat Cyber City Tycoon -mobiilipelin, jonka tavoitteena on kehittää EU-kansalaisten kyberturvaosaamista. Peli hyödyntää pelillistämisen keinoja ja perustuu todellisiin kyberrikollisuuden ilmiöihin. Pelissä käyttäjän tavoitteena on kasvattaa rikosimperiumia keräämällä rahavaroja erilaisten minipelien avulla. Rahavarojen kerääminen on edellytys pelissä etenemiselle. Se tekee siitä viihteellisen, mutta samalla oppimista tukevan lähestymistavan. (Aalto-yliopisto 2024.) Tämä mobiilipeli voisi toimia varteenotettavana houkuttimena kyberturvaosaamisen ymmärtämiseen ja kasvattamiseen. Pelaamisen yhteydessä käyttäjä saa vinkkejä siitä, miten omaa suojautumista kyberuhkia vastaan voi parantaa.

Keskustelut työnantajan edustajan kanssa käytiin läpi tietosuojan haasteista ja haluttiin aihetta tarkastella uudesta näkökulmasta. Sen sijaan, että tietosuojakoulutus perustuisi perinteisiin materiaaleihin, nähtiin tarpeelliseksi kehittää ratkaisu, joka tekee tietosuojasta konkreettisemman ja lähestyttävämmän aihealueen.

Kehittämistyössä pyritään vastaamaan tähän haasteeseen kehittämällä pelillinen oppimisratkaisu, joka tuo tietosuojan osaksi työntekijän käytännön työtehtäviä.

3.2.2 Esiymmärrys aiheesta

Konstruktiivisessa tutkimuksessa esiymmärrys toimii lähtökohtana, mutta sitä tarkennetaan ja täydennetään empiirisen työn ja käytännön kokemusten perusteella. Teorian ja käytännön vuoropuhelu on keskeistä ja tutkijan ennakkotieto suuntaa prosessia. Esiymmärryksen hankkiminen ei rajoitu pelkästään organisaatiosta saadun tiedon keräämiseen. Sen avulla varmistetaan kehittämistyössä luodun ratkaisun olevan toimiva ja käytännöllinen. (Lukka 2000, 8; Lukka 2014.)

Lukan (2014; 2000, 5) mukaan kehittämistyön esiymmärryksen saamiseksi keskeinen vaihe on aiheeseen liittyvä teoriapohjainen kirjallisuuskatsaus. Tämä vaihe luo perustan koko kehittämistyölle ja varmistaa, että ratkaisu pohjautuu aiempaan tutkimukseen ja teorioihin. Kehittämistyön alkuvaiheessa on tärkeää seurata, miten asiat organisaatiossa toimivat ennen ratkaisuehdotuksen tekemistä. Mikäli esiymmärrys jää puutteelliseksi, voidaan kehittää jotain, mikä ei oikeasti ratkaisen ongelmaa tai vastaa käytännön tarpeita.

Esiymmärryksen avulla voidaan hahmottaa organisaation nykytilaa ennen varsinaista kehittämistyötä sekä tunnistaa näkyviä ja piileviä haasteita (Lukka 2014). Piileviä tietosuojahaasteita voivat olla esimerkiksi työntekijöiden tiedostamattomat toimintatavat, jotka perustuvat vanhentuneisiin käytäntöihin ja ”näin on aina tehty” -ajatteluun. Lisäksi haasteita voivat aiheuttaa piittaamattomuus, tietämättömyys, vanhentunut tietosuojapolitiikka tai tilanteet, joita työntekijä ei tunnista ongelmaksi.

Ojasalon, Moilasen ja Ritalahden (2018, 40, 122) mukaan kysely on hyödyllinen tiedonkeruumenetelmä, kun aiheesta on jo olemassa runsaasti tietoa, mutta ymmärrystä halutaan syventää. Se sopii hyvin lähtötilanteen selvittämiseen ja kehittämistyön lopuksi arvioimaan saavutettuja tuloksia. Kyselyn onnistuminen edellyttää huolellista suunnittelua, ja lähtökohtana on tiedostaa, millaista tietoa halutaan kerätä ja miten saadut tiedot analysoidaan. Kysymysten tulee olla selkeitä, helposti ymmärrettäviä ja perustua teoriaan. Lisäksi on tärkeää pohtia, kenelle kysely lähetetään ja kuinka hyvin otos edustaa koko kohderyhmää. Ojasalo ym. (2018, 130) myös lisäävät, että kyselyn suunnittelun on perustuttava kehittämistyön tavoitteisiin, jotka on määriteltävä selkeästi ennen kyselyn toteuttamista

Ojasalo ym. (2018, 121–122) mainitsevat kyselyn olevan nopea ja luotettava tiedonkeruumenetelmä, mutta sen heikkoutena on saadun tiedon pinnallisuus. Vehkalahti (2014, 43) korostaa, että otoksen on edustettava perusjoukkoa mahdollisimman tarkasti.

Kirjallisuuskatsaus

Kirjallisuuskatsauksen avulla muodostettiin käsitys tietosuojatietoisuuden tutkimuksesta ja pelillistämisen soveltamisesta oppimisympäristöissä. Lukka (2014) painottaa, että esiymmärrys syntyy sekä organisaatiosta saadusta tiedosta että aiemmista tutkimuksista ja teorioista. Pelillisyydestä löytyi runsaasti teoriaa ja empiirisiä tutkimuksia, jotka perustuvat esimerkiksi kyselyihin, haastatteluihin ja havainnointiin. Monet tietosuojatutkimukset keskittyivät erityisesti tietosuojakäytäntöjen jalkauttamiseen organisaatioissa. Tästä syystä pelillisyyden lähestymistapaa oli tarpeen rajata tarkemmin. Kehittämistyössä keskityttiin tietosuojaosaamisen käytännönläheiseen kehittämiseen realististen työelämäskenaarioiden avulla.

Lähtötasoa kartoittava kysely

Esiymmärryksen saamiseksi toteutettiin ennen peliä -kysely (kyselylomake liitteessä 1), jonka tavoitteena oli kartoittaa organisaation asiantuntijoiden tietosuojaosaamisen tasoa. Vaikka kvantitatiivinen aineisto ei ole konstruktiivisen tutkimuksen keskeinen menetelmä (Virtanen 2006, 47), tässä tapauksessa se tarjosi arvokasta tietoa lähtötilanteesta. Kyselyn tulokset esitetään tarkemmin luvussa 3.3, aineiston analysointi.

Kysymykset laadittiin tietosuojalainsäädännön, kehittämistyön tekijän asiantuntemukseen ja organisaatiokohtaisen tiedon pohjalta. Kysely toteutettiin kahdessa vaiheessa. Ennen peliä toteutetulla kyselyllä kartoitettiin osallistujien lähtötason tietosuojatietoisuus, ja pelin jälkeisellä kyselyllä selvitettiin, miten osaaminen oli mahdollisesti muuttunut pelillisen oppimisen seurauksena. Tulosten vertailun avulla voitiin arvioida pelin vaikutuksia tietosuojaosaamisen kehittymiseen.

Kysely toteutettiin organisaation käytössä olevalla Webropol-kyselytyökalulla, ja se suunniteltiin anonyymiksi. Taustatietoja ei kysytty ja kaikki kysymykset olivat vapaaehtoisia. Perusjoukoksi valittiin organisaation yksikkö, joka työskentelee päivittäin tietosuojaan liittyvien asioiden parissa. Kyselyjen ja pelien geneeriset linkit lähetettiin osallistujille sähköpostitse ja sähköpostia käytettiin ainoastaan kehittämistyön viestinnässä. Kyselyn kysymykset jaettiin teemoihin, joita olivat:

- Yleinen tietosuoja
- Henkilötietojen käsittely ja suostumus
- Tietoturvaloukkaukset ja kriisitilanteet
- Opiskelijoiden oikeudet ja tietojen tarkastus
- Henkilötietojen käsittelyperusteena laki
- Arvio vastaajan omasta tietosuojaosaamisesta

Jokaisen teeman alle laadittiin osittain organisaation toimialaan kohdennettuja kysymyksiä. Strukturoitujen kysymysten käyttö vähensi vastausvaihtoehtojen tulkinnanvaraisuutta ja paransi vastausprosenttia. Kyselyn hyödyntäminen ennen konstruktion suunnittelua mahdollisti osallistujien lähtötason tietämyksen kartoittamisen.

Pelin jälkeinen kysely lähetettiin seitsemälle osallistuneelle pelaajalle muutamia päiviä myöhemmin, mutta huolimatta uusintapyynnöistä vastauksia saatiin vain kuusi. Kysymykset olivat identtisiä ennen peliä toteutetun kyselyn kanssa, mikä mahdollisti suoran vertailun pelin vaikutuksista.

Esiymmärryksen lopputuloksena muodostui selkeä kuva kehittämishankkeen lähtötilanteesta, minkä perusteella voitiin siirtyä ratkaisumallin kehittämiseen. Esiymmärryksen hankkiminen luo pohjan kehittämistyön ymmärtämiselle ja innovatiivisen ratkaisumallin konstruoinnille. (Kasanen ym. 1993.) Ennen peliä ja jälkeen pelin -kyselyiden tuloksia hyödynnettiin ratkaisumallin suunnittelussa. Ne auttoivat tunnistamaan keskeisiä kehittämiskohteita, joiden ratkaisemiseen pelillistämisessä keskityttiin.

3.2.3 Ratkaisumallin konstruointi

Lukka (2000, 2) toteaa ratkaisumallin konstruoinnin olevan keskeinen osa tutkimusta. Se on innovatiivinen prosessi, jossa pyritään ratkaisemaan käytännön ongelma luomalla uusia, teoreettisesti perusteltuja ja käytännössä sovellettavia ratkaisuja.

Lukka myös (2014) korostaa teorian merkitystä ja painottaa, että konstruktiot tulee rakentaa olemassa olevan tietämyksen varaan ja tutkimustulokset on reflektoitava takaisin tietoperustaan. Ratkaisumallin kehittäminen ei ole pelkästään valmiiden ratkaisujen soveltamista, vaan tavoitteena on luoda uutta ja hyödyllistä tietoa, joka vastaa käytännön tarpeisiin (Lukka 2014; Lukka 2003, 84, 87). Prosessi etenee iteratiivisesti, eli ratkaisua kehitetään ja testataan vaiheittain, jolloin jokainen kierros syventää ymmärrystä ja mahdollistaa mallin parantamisen.

Konstruktiivinen tutkimus edellyttää kokeilevaa ja arvioivaa lähestymistapaa (Lukka 2003, 87; Lukka 2014). Prosessi perustuu ideointiin, pienimuotoiseen testaamiseen ja jatkuvaan kehittämiseen, kunnes lopputulos on toimiva. Jos ratkaisumallia ei synny, kehitystyötä ei ole syytä jatkaa. Käytännössä tämä tarkoittaa ratkaisujen iteratiivista muokkaamista ja arviointia niiden toimivuuden varmistamiseksi.

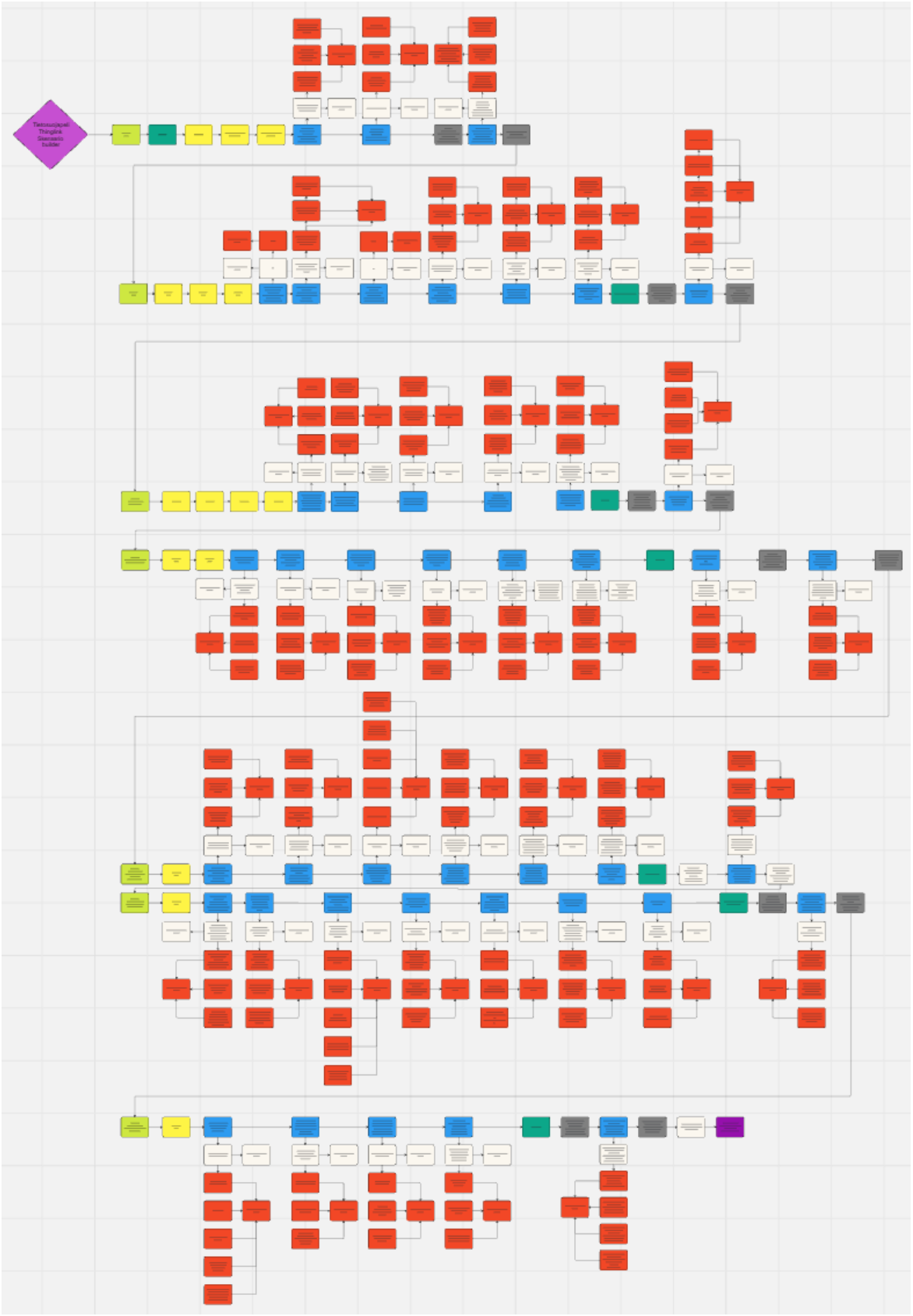
Kehittämistyössä pelillistäminen oli lähtökohtaisesti keskeisessä roolissa, koska tutkimusten mukaan se lisää oppimisen motivaatiota. Ratkaisumallin suunnittelu keskittyi pelillistämisen käytännön toteutukseen, eikä muita vaihtoehtoisia lähestymistapoja tarkasteltu. Tavoitteena oli luoda interaktiivinen ja visuaalisesti kiinnostava ympäristö, joka tukee osallistujien kykyä ymmärtää ja soveltaa tietosuojakäytäntöjä. Pelin avulla voidaan myös tunnistaa mahdollisia haasteita tietosuojaosaamisen kehittämisessä, kuten työntekijöiden passiivisuus tai tietosuojan kokeminen monimutkaiseksi ja vaikeasti sovellettavaksi.

Kehittämisprosessi aloitettiin toimintasuunnitelman ja aikataulun laatimisella. Alkuvaiheessa käytössä oli Excelin Gantt-kaavio, mutta myöhemmin tehtävien hallinta ja aikataulutus

siirrettiin visuaalisemmalle Miro-yhteistyöalustalle. Tämä tarjosi paremman hahmotettavuuden kokonaisuudelle ja helpotti suunnittelua.

Osana kehittämisprosessia suoritettiin digitaalisten pelialustojen vertailua eli benchmarkkausta. Ojasalon ym. (2018, 43–44) mukaan benchmarking on menetelmä, jossa omaa toimintaa kehitetään vertaamalla sitä muihin organisaatioihin ja parhaisiin käytäntöihin. Maksullisia vaihtoehtoja oli tarjolla runsaasti, ja osa palveluntarjoajista tarjosi 30 päivän maksuttomia kokeilujaksoja. Tämä aika ei kuitenkaan olisi riittänyt perusteelliseen testaukseen, ja koska budjettia ei ollut käytettävissä, toteutus oli suunniteltava täysin ilman rahallisia resursseja.

Pelin käsikirjoitus luotiin Miro-alustalle, joka tarjosi rajattoman digitaalisen työtilan sisällön suunnitteluun ja mallintamiseen. Miro mahdollisti visuaalisen suunnittelun, ideoinnin ja tiedostojen integroinnin, mikä helpotti pelin rakenteen hahmottamista. Sinne määritettiin pelin yksityiskohtainen vuokaavio, joka kuvasi etenemisjärjestyksen, huoneet, siirtymät, kysymykset, oikeat ja virheelliset vastaukset sekä käytetyt pelisovellukset. Vuokaavio toimi keskeisenä ohjaavana työkaluna, joka varmisti pelin loogisen etenemisen. Sitä päivitettiin jatkuvasti kehitysprosessin edetessä ja muutoksia tehtäessä.



Kuvio 3: Miron vuokaavio pelistä

Vuokaavion värien selitys:

Taulukko 2: Vuokaavion värien selitys

Pelin aloitus ja lopetus	
Siirtyminen uuteen huoneeseen	
Tietosuojaan liittyvä peli	
Tietoisku ja mahdollisuus siirtyä intran sisältöön	
Motivoivat välipalautteet pelin jatkamisesta	
Kysymys	
Oikea vastaus ja selite oikealle vastaukselle	
Virheellinen vastaus ja selite virheelliselle vastaukselle	

Pelialustaksi valikoitui Thinglink, joka mahdollistaa käyttäjäystävällisen ja interaktiivisen mediasisällön toteuttamisen. Sen käyttö on monelle työntekijälle jo ennestään tuttua ja vaikka näin ei olisikaan, se on helppokäyttöinen ilman erillistä ohjeistusta. Lisäksi Thinglink toimii moitteettomasti mobiililaitteella, ja sen sisältö skaalautuu hyvin eri näyttökokoihin. Menetelmävalinnassa keskeisenä tekijänä olivat organisaation käytössä jo valmiina olevat Thinglink ja Webropol, jotka ovat vakiintuneet työkalut organisaatiossa.

Ennen pelin teknistä toteutusta tutkittiin Thinglinkin ominaisuuksia ja perehdyttiin webinaareihin, joissa käsiteltiin esimerkiksi skenaarioiden rakentaja -ominaisuutta. Tämä ominaisuus oli yksi vaihtoehdoista pelin toteutukseen. Lisäksi Thinglinkin asiantuntijan (Pennanen 2024) kanssa järjestettiin tapaaminen, jossa hänen antamia neuvoja hyödynnettiin pelin etenemisen suunnittelussa.

Testausvaiheen jälkeen päädyttiin hyödyntämään Thinglinkin skenaarioiden rakentajaa. Sen avulla voidaan luoda polkuja, joissa pelaaja etenee valintojen perusteella. Pelin rakenne muotoutui lopulta yksinkertaiseksi skenaarioksi, jossa eteneminen tapahtuu oikeilla valinnoilla. Virheellisestä valinnasta ei seuraa mitään, mutta pelaaja saa selitteen, miksi valittu vaihtoehto oli virheellinen.

Pelin tavoitteet pohjautuvat organisaation käytännön tarpeisiin. Huoneiden tehtävät koostuvat tietosuojaan liittyvistä interaktiivisista haasteista. Osallistuja saa oikean tai virheellisen

valinnan jälkeen välittömästi kannustavan palautteen. Peli rakennettiin vaiheittain, edeten huone kerrallaan.

Taulukko 3: Pelin huoneiden tavoitteet

Huone	Tavoite	Huoneen sisältö	Painike intraan
Ulkotilojen turvallisuus	Tunnistaa ulkotiloihin liittyviä riskejä	Käytännönläheisten tilanteiden lisääminen peliin.	Kriisi- ja hätätilanteet
Tietosuoja ja turvallisuus yleisessä tilassa	Tunnistaa tietosuojan ja turvallisuuden merkitys yleisessä tilassa	Käytännönläheisten tilanteiden lisääminen peliin.	Turvallisuusohjeet, tietosuojan muistilista
Henkilötietojen suojaaminen	Tunnistaa henkilötietojen suojaaminen niiden käsittelyssä	Käytännönläheisten tilanteiden lisääminen peliin.	Tietosuojakäsikirja, tietosuojapolitiikka
Henkilötietojen minimointi ja käsittely	Tunnistaa tietojen minimointi ja käsittelyn lainmukaisuus	Käytännönläheisten tilanteiden lisääminen peliin.	Tietoturvaperiaatteet
Rekisteröidyn oikeudet ja tietojen käsittelyn lainmukaisuus.	Tunnistaa rekisteröidyn oikeudet ja tietojen käsittelyn lainmukaisuus.	Käytännönläheisten tilanteiden lisääminen peliin.	Salasanapolitiikka
Empiiristen löydösten ja teorian yhteys	Yhteys ei ole ennalta määrätty	Käytännönläheisten tilanteiden lisääminen peliin.	Tietosuojakäsikirja

Kyselyssä ja pelin suunnittelussa käytettiin samoja ja samankaltaisia teemoja, mutta niiden esittämistapa, kysymyksen muotoilu ja selitteet vaihtelivat. Molemmissa ympäristössä kysymykset esitettiin kysymys-vastaus-muodossa, mutta pelissä oli lisäksi mukana konkreettisia tilanteita. Kyselyssä kysyttiin: Miksi oppilaitoksen täytyy noudattaa tietojen minimoinnin

periaatetta opiskelijatietoja kerätessään? Pelissä samaan aiheeseen viittaava kysymys oli muotoiltu: Mikä vaihtoehdoista liittyy tietojen minimointiin ja käsittelyn tarkoitukseen? Virheelliset vastausvaihtoehdot erosivat toisistaan ja oikea vastaus oli samankaltainen molemmissa ympäristöissä. Kaikki Thinglink-alustalla pelin etenemisessä vastaan tulevat tehtävät, haasteet ja polutukset merkittiin myös Miroon, jotta näiden järjestys ja suunnittelu olisi paremmin halittavissa.

Pelin työnimenä oli Tietosuojaninja ja pelaaja toimi GDPR-agenttina. Jokaisessa huoneessa esitettiin yksi GDPR-agentin tunnistama konkreettinen tietosuojauhka. Tilanteita olivat esimerkiksi lojumaan jääneet henkilötietoja sisältävät paperit tai vartioimaton, avoinna oleva tietokone. GDPR-agentti korjasi tilanteen ja jätti palautteen oikeasta toimintatavasta.

3.2.4 Ratkaisumallin toimivuuden testaaminen

Testausvaiheessa arvioidaan ratkaisun käytännön toimivuutta ja hyödyllisyyttä todellisessa toimintaympäristössä. Konstruktiivisessa tutkimuksessa korostuu käytännönläheisyys, iteratiivisuus ja ongelmanratkaisu. Tavoitteena ei ole ainoastaan luoda teoreettisesti merkittävä ratkaisu, vaan myös käytännössä toimiva ja hyödyllinen lopputulos. (Kasanen ym. 1993.)

Havainnointi oli osallistuvaa ja tapahtui vuorovaikutuksessa osallistujien kanssa. Havainnointi on keskeinen menetelmä, jolla tutkija perehtyy kohdeorganisaatioon (Virtanen 2006, 47). Vaikka Ojasalo ym. (2021, 116) mainitsevat, että havainnoija voi häiritä tilannetta läsnäollaan, niin pelaajat kuitenkin keskittyivät pelaamiseen positiivisella asenteella.

Ojasalo ym. (2021, 116) mainitsevat, että havainnointitekniikka voi olla myös strukturoimatonta, jolloin sen tavoitteena on kerätä mahdollisimman paljon tietoa ilman ennalta määriteltyjä luokitteluja. Tämä lähestymistapa soveltui hyvin pelin testaamiseen, sillä tavoitteena oli tunnistaa pelaajien spontaanit reaktiot ja ymmärtää heidän kokemuksiaan ilman valmiita arviointikehyksiä.

Toteutus testausryhmän osalta

Ennen ja jälkeen -kyselyt toteutettiin Webropol-kyselytyökalulla. Ojasalon ym. (2018, 132) mukaan kyselylomakkeen onnistunut suunnittelu edellyttää selkeitä kysymyksiä, tarkkoja ohjeita vastaajille sekä harkittua avointen ja suljettujen kysymysten käyttöä. He korostavat myös, että testaus ja huolellisesti laadittu saatekirje parantavat vastausprosenttia.

Ensimmäisessä vaiheessa testausryhmän avulla testattiin sekä peli että siihen liittyvät kyselyt. Pelin testaus toteutettiin kolmessa pelitilanteessa, joista osa tapahtui kasvokkain ja osa etäyhteydellä. Testitilanteissa havainnoitiin pelin etenemistä vastausnopeutta sekä osallistujien reaktioita tehtäviin. Pelin ajanotto ja testausvaihe paljastivat tarpeen muokata kysymyksiä, sillä 75 prosenttia testaajista koki ne liian vaikeiksi. Monet kysymykset sisälsivät tietosuojatermejä, joiden merkitys ei ollut osallistujille ennestään tuttu. Tämä hidasti vastaamista ja

vaikeutti pelin etenemistä, erityisesti niillä testaajilla, jotka eivät työssään käsitelleet tietosuojaan liittyviä asioita.

Pelin testauksen keskeinen tavoite oli selvittää, kuinka hyvin pelin sisältö auttaa hahmottamaan tietosuojaan liittyviä keskeisiä periaatteita ja tunnistamaan työssä vastaantulevia tilanteita, joissa tietosuojatoimenpiteet ovat olennaisia. Arviointikohteina olivat sisällön ymmärrettävyys ja sen tehokkuus tietosuojaosaamisen vahvistamisessa. Pelin käytettävyyttä ei testattu erikseen, mutta sen sujuvuudesta ja käyttöliittymästä saadut palautteet antoivat lisätietoa sisällön omaksuttavuudesta.

Lisäksi havaittiin, että kyselyn täyttäminen ja pelin pelaaminen samanaikaisesti koettiin liian raskaaksi. Tämän vuoksi päädyttiin siihen, että ennen peliä -kyselyn voi järjestää kohderyhmälle hyvissä ajoin ennen Thinglink-pelin pelaamista, jotta osallistujilla olisi paremmat valmiudet keskittyä peliin.

Testaajilta saatu palaute ei sisältänyt konkreettisia kehitysehdotuksia pelin tehtävien sisältöön, mutta yleinen käsitys tietosuojasta koettiin haastavaksi, vaikeaksi ja vieraaksi. Monet tietosuojatermit, kuten rekisteröity, rekisterinpitäjä ja läpinäkyvyys, eivät olleet tuttuja, ja moni vastauksista perustui arvauksiin. Yksi neljästä testaajasta tunsi tietosuoja-aiheen entuudestaan ja pystyi vastaamaan kysymyksiin tietoisena merkityksestä. Testauksien pohjalta tehtiin korjauksia pelin huonekohtaisiin tehtäviin, erityisesti pelin niihin kysymyksiin, joiden muotoilu aiheutti väärinymmärryksiä.

Testausryhmälle toteutetut ennen ja jälkeen -kyselyt osoittivat vain vähäistä parannusta vastaajien osaamisen muutoksessa. Tämä oli odotettavaa, koska vain yhdellä osallistujalla oli ennestään kokemusta tietosuojasta. Kyselyssä vastaukset esitettiin eri tavalla kuin pelissä, mikä saattoi vaikuttaa oikean vaihtoehdon valintaan. Testauksen jälkeen tehtiin hienosäätöä kysymysten osalta, koska osa testaajista ymmärsi kysymyksen eri tavalla kuin mitä oli tarkoitettu.

Toteutus kohderyhmän osalta

Testausryhmän jälkeen kysely lähetettiin kohderyhmän kahdeksalle edustajalle, joista seitsemän vastasi ennen peliä ja kuusi pelin jälkeen. Ennen ja jälkeen -kyselyt kohderyhmä teki oman aikataulunsa mukaan. Ennen peliä kyselyyn vastasi seitsemän henkilöä ja pelin jälkeen kuusi henkilöä. Vastausprosentti ennen peliä oli 87 % ja pelin jälkeen 75 %. Kysymykset pidettiin samoina molemmissa kyselyissä, jotta tulokset olisivat vertailukelpoisia ja vältettäisiin tulkinnallisia vääristymiä. Hypoteesina oli, että jokaisella osallistujalla tietosuojaosaaminen on vähintään tyydyttävällä tasolla, sillä työtehtävät edellyttävät osittaista tietosuojan hallintaa.

Kohderyhmän pelin havainnointi toteutettiin kolmessa pelitilanteessa etäyhteyden kautta videokameroiden avulla. Havainnoinnin tavoitteena oli tarkastella pelaajien reaktioita ja

tunteita sekä ymmärtää, miten peli vaikutti oppimisprosessiin. Testaajilta ja kohderyhmältä pyydettiin käyttämään ääneen ajattelun -menetelmää, eli ilmaisemaan pelin aikana, milloin he kokivat innostusta tai turhautumista. Tämä auttoi havainnoijaa tunnistamaan, mihin kohtiin peliä reaktiot kohdistuivat. Havainnot täydentyivät kirjallisilla muistiinpanoilla, joissa merkittiin osallistujien kommentteja pelin rakenteesta, tehtävien selkeydestä sekä mahdollisista kehitysehdotuksista.

Pelin aikaiset positiiviset reaktiot ilmenivät onnistumisen kokemuksina, nyökkäilyinä, mietteliäinä ilmeinä ja sanallisina kommentteina, joissa huomioitiin tietyn tehtävän mielekkyys. Negatiiviset reaktiot puolestaan näkyivät turhautumisena, epäröintinä ja huokailuina. Näitä tunteita seurattiin erityisesti silloin, kun osallistujat kohtasivat hankalia kysymyksiä tai epävarmuutta herättäviä tietosuojateemoja.

Ennen peliä ja jälkeen pelin -kyselyt

Ennen peliä -kysely sisälsi yhteensä 34 kysymystä, joista 33 oli monivalintakysymystä ja yksi arvioitiin Likertin asteikolla. Likertin asteikkoa käytetään järjestysasteikkona esimerkiksi mielipiteiden arvioiden mittaamiseen (Vilkka 2007). Pelin jälkeiseen kyselyyn lisättiin yksi lisäkysymys, joten yhteensä oli 35 kysymystä, joista kaksi arvioitiin Likertin asteikolla. Kaikissa monivalintakysymyksissä oli vain yksi oikea vastausvaihtoehto.

Kyselyt täytettiin vastaajien omalla ajalla. Kyselyiden anonymiteetti varmistettiin siten, ettei vastaajien taustatietoja, kuten ikää, sukupuolta tai työkokemusta, kerätty. Tämä mahdollisti, että osallistujat pystyivät vastaamaan rehellisesti ilman pelkoa henkilökohtaisesta tunnistamisesta. Se myös tarkoitti, ettei osaamisen kehittymistä voitu seurata yksilötasolla.

Kehittämistyön eteneminen

Kehittämistyön etenemistä havainnollistaa taulukko 4, jossa iteratiivinen kehittämistyö esitetään lineaarisesti etenevänä prosessina. Prosessin aikana peliä muokattiin useita kertoja saadun palautteen perusteella. Viimeisimpien muutosten jälkeen pelaajia ei kuitenkaan ollut enää saatavilla, joten niiden vaikutusta toimivuuteen ei päästy testaamaan käytännössä. Kehittämistyön lopullinen tuotos ja tulokset esiteltiin toimeksiantajalle, ja saatu palaute auttoi arvioimaan kehittämistyön onnistumista.

Taulukko 4: Kehittämistyön etenemisen prosessi

Vaihe	Tavoite
Kehittämistyön suunnittelu ja vaiheistus	Määrittää etenemissuunnitelma

Tietoperusta	Lainsäädäntöön ja pelillistämisen tutkimukseen perustuva kehittämistyön tietoperusta
Pelin suunnittelu	Määrittää tietosuoja-aiheinen pelillistetty menetelmä
Kyselyn suunnittelu ja toteutus	Tarkoituksenmukaiset kysymykset ennen ja jälkeen pelin
Pelin toteutus	Pelin toteutus pelattavaan muotoon
Ennen peliä -kyselyn toteutus testaajilla	Aineiston keruu ja muutostarpeiden toteutus
Pelin toteutus testaajilla	Havainnointi ja muutostarpeiden toteutus
Pelin toteutus testaajilla	Havainnointi ja muutostarpeiden toteutus
Pelin toteutus testaajilla	Havainnointi ja muutostarpeiden toteutus
Jälkeen pelin -kyselyn toteutus testaajilla	Aineiston keruu ja muutostarpeiden toteutus
Ennen peliä -kyselyn toteutus kohderyhmällä	Aineiston keruu
Pelin toteutus kohderyhmällä	Havainnointi ja muutostarpeiden toteutus
Pelin toteutus kohderyhmällä	Havainnointi ja muutostarpeiden toteutus
Pelin toteutus kohderyhmällä	Havainnointi ja muutostarpeiden toteutus
Jälkeen pelin -kyselyn toteutus kohderyhmällä	Aineiston keruu
Kyselytulokset	Ennen ja jälkeen -kyselyiden analysointi
Tulokset	Tulosten analysointi
Esittely toimeksiantajalle	Palaute

3.2.5 Ratkaisumallin teoreettinen pohja ja innovatiivisuus

Kehittämistyön tulokset vahvistavat aiempaa tutkimustietoa pelillistämisen vaikutuksista. Pelillistämisen on todettu lisäävän motivaatiota ja sitoutumista oppimisprosessiin, mutta sen onnistunut toteutus edellyttää huolellista suunnittelua. Hamari ym. (2014) ja Armstrong ym. (2018, 2) osoittavat, että pelillistämisen avulla voidaan tehostaa oppimista ja parantaa osallistujien sitoutumista koulutukseen. Armstrong ym. (2018, 2) kuitenkin korostavat, että pelillistämisen vaikutukset eivät ole automaattisia, vaan niiden on tuettava oppimistavoitteita. Ilman selkeää pedagogista suunnittelua pelillistäminen voi jäädä pinnalliseksi tai jopa heikentää oppimiskokemusta.

Perinteiset koulutusmateriaalit, kuten tekstiin, ääneen ja kuviin perustuvat ohjeistukset, tarjoavat tärkeää taustatietoa. Ne jäävät usein passiivisiksi ja yleisluonteisiksi materiaaleiksi. Materiaaliin voi aina palata, mutta sen ei välttämättä koeta tukevan käytännön työskentelyä. Pelillinen lähestymistapa tuo koulutukseen uuden ulottuvuuden, jossa oppiminen tapahtuu aktiivisesti päätöksiä tekemällä ja saaden välitöntä palautetta. Lisäksi pelin skenaarioita voidaan muokata vastaamaan organisaatioiden ja työympäristöjen muuttuviin tarpeisiin, mikä tekee siitä joustavan ja pitkäkestoisen oppimisratkaisun. Perinteisten koulutusmateriaalien rinnalla peli muodostaa kokonaisvaltaisen ja toimivan oppimiskokonaisuuden.

Tietosuojapelin uutuusarvo syntyy pelillisen oppimisen ja tietosuojakoulutuksen yhdistämisestä uudella tavalla. Tämä lähestymistapa ei ole aiemmin ollut käytössä Humakissa, mikä tekee ratkaisusta uudistuksen tietosuojakoulutuksen toteuttamisessa. Pelin avulla tietosuojaan liittyvää oppimista voidaan lähestyä käytännönläheisesti. Ratkaisu tuo tietosuojakoulutukseen käytännönläheisyyttä ja kannustaa osallistujaa aktiiviseen osallistumiseen.

Pelin joustavuus mahdollistaa sen mukauttamisen eri kohderyhmille ja organisaatioille. Pelillinen ympäristö tarjoaa turvallisen tavan harjoitella tilanteita ilman todellisia seuraamuksia. Lainsäädännön asettamia vaatimuksia voidaan simuloida käytännönläheisesti, jolloin osallistujat pääsevät soveltamaan tietosuojaosaamistaan konkreettisissa skenaarioissa. Uutuusarvo perustuu ratkaisun sovellettavuuteen erilaisissa organisaatioympäristöissä.

3.2.6 Ratkaisun soveltuvuusalueen laajuuden tarkastelu

Kehittämistyön tuloksien laajempaa hyödynnettävyyttä arvioidaan tarkemmin luvussa 5, Johtopäätökset ja pohdinta. Lisäksi pohditaan kehitetyn pelin skaalautuvuutta ja hyödynnettävyyttä varsinaista kehittämiskontekstia laajemmin.

3.3 Aineiston analysointi

Aineiston analysointi on osa konstruktiivisen tutkimuksen prosessia. Sen avulla pyritään ymmärtämään ongelmaa syvällisemmin ja kehittämään ratkaisuja aiemman teoreettisen tiedon

pohjalta. Tulosten tarkastelussa vertaillaan empiiristä aineistoa ja aiempaa tutkimusta, minkä perusteella voidaan tehdä johtopäätöksiä ratkaisun toimivuudesta (Lukka 2014).

Tässä kappaleessa kuvataan kerätyn aineiston analysointi. Aineisto koostuu ennen peliä ja jälkeen pelin -kyselyiden vastauksista sekä pelaamisen aikaisesta havainnoinnista. Analyysissä käsitellään valikoituja tuloksia ennen ja jälkeen pelin toteutetuista kyselyistä. Kyselyiden osalta tarkasteluun on otettu ne kysymykset, joiden kohdalla havaittiin osaamisen kehittymistä. Lisäksi tarkastellaan niitä kysymyksiä, joissa vastausten oikeellisuus pelin jälkeisessä kyselyssä muuttui virheelliseksi. Näitä muutamia virheellisiä vastauksia ei kuitenkaan tulkita osaamisen heikkenemiseksi ja niiden merkitys tulosten arvioinnissa on vähäisempi.

Havainnoinnin avulla oli mahdollista seurata pelaajien reaktioita, ongelmanratkaisua ja päätöksentekoa. Tulosten analysoinnissa keskitytään tarkastelemaan, miten tietosuojaosaaminen kehittyi pelillistetyn menetelmän vaikutuksesta. Kyselytulokset antoivat kuvan organisaation yhden yksikön tietosuojaosaamisen tasosta.

Analyysissä hyödynnettiin osittain triangulaatiota, jossa yhdistetään useita tutkimusmenetelmiä tulosten luotettavuuden lisäämiseksi (Ojasalo ym. 2018, 105). Kyselytulosten analyysi perustui vastausten muutoksiin sekä pelin aikaiseen havainnointiin. Vastaajamäärä väheni pelin jälkeen yhdellä henkilöllä, mikä saattoi vaikuttaa prosenttiosuuksiin. Pienessä otoksessa yksittäisillä vastauksilla on suurempi painoarvo. Vaikutuksen suuruus määräytyy sen perusteella, kuinka paljon puuttuvan vastaajan vastaukset olisivat poikenneet muiden vastauksista.

Webropolin oletusraporteissa käytetään saavutettavuusvaatimukset täyttäviä värejä, mutta yhdistetyissä raporteissa vastausvaihtoehdot haluttiin erottaa visuaalisesti selkeämmin. Raporttien värivalinnat täyttävät vähintään WCAG-saavutettavuusohjeiston AA-tason vaatimukset.

Liitteessä 1 (taulukkomuodossa) esitetään ennen ja jälkeen -kyselyiden kaikki kysymykset ja oikeat vastaukset. Analyysissä Webropolin kyselytulokset esitetään osittain visuaalisina palkkikaavioina, joissa näkyvät ennen ja jälkeen -kyselyiden yhdistetyt tulokset. Kaavioista käy ilmi, missä kysymyksissä on havaittavissa takapakkia tai kehitystä. Niissä näkyvät kaikki annetut vastausvaihtoehdot sekä osallistujien valitsemat vastaukset. Ennen peliä iso osa vastaajista vastasi kysymyksiin oikein, mikä osoittaa lähtökohtaisesti hyvää tietosuojaosaamisen tasoa. Mikäli peli ei olisi vaikuttanut osaamiseen millään tavalla, tulosten olisi odotettu pysyvän samana myös jälkikyselyssä

Kyselytuloksia tarkasteltiin vertailemalla vastauksien muutoksia ennen ja jälkeen pelin. Likert-asteikolla mitatut kysymykset eivät olleet mukana prosentuaalisessa vertailussa, vaan niitä käsitellään erikseen. Prosentuaalinen vertailu antoi konkreettista dataa oppimisen muutoksesta.

3.3.1 Pelin vaikuttavuuden arviointi

Kyselytulosten perusteella osallistujien vastauksissa tapahtui sekä positiivisia että negatiivisia muutoksia. Osassa kysymyksistä oikeiden vastausten osuus kasvoi selvästi, ja positiivista kehitystä löytyi jokaisesta teemasta. Osa kysymyksistä tuotti kuitenkin saman jakauman ennen ja jälkeen pelin. Erityisen mielenkiintoinen havainto tehtiin kolmessa kysymyksessä, joissa osallistujat vastasivat oikein ennen peliä, mutta virheellisesti pelin jälkeen.

Pelin jälkeisessä kyselyssä annettiin 11 oikeaa vastausta enemmän kuin ennen peliä. Vaikka oikein vastattujen kysymysten määrä kasvoi, pelin jälkeisessä kyselyssä vastaajia oli vähemmän, mikä vaikuttaa tulosten vertailuun. Puuttuva vastaaja olisi voinut antaa joko heikon tai vahvan arvion osaamisestaan, mikä olisi voinut vaikuttaa tuloksiin. Prosentuaalinen muutos kuitenkin osoittaa, että oikein vastanneiden osuus kasvoi, vaikka absoluuttinen oikeiden vastausten määrä pysyi samana.

Kysymykset, joihin vastattiin 100 % oikein sekä ennen että jälkeen pelin, liittyivät pääosin rekisterinpitäjän vastuisiin ja lain noudattamiseen. Tämä viittaa siihen, että kyseiset aiheet olivat vastaajille ennestään tuttuja ja osaaminen oli jo valmiiksi riittävällä tasolla. On myös mahdollista, että kysymykset ja vastausvaihtoehdot eivät mitanneet tietosuojaosaamista riittävän syvällisesti. Haasteellisempien vastausvaihtoehtojen lisääminen voisi kannustaa tarkempaan harkintaan ja syvempään oppimiseen. Vaikka tulos on positiivinen, se osoittaa, ettei pelillistämisellä ollut vaikutusta, koska muutosta ei tapahtunut. Kaikkiin näihin kysymyksiin löytyi kuitenkin vastaus myös pelin aikana.

Osa kysymyksistä säilytti oikeiden ja virheellisten vastausten määrän samana ennen ja jälkeen pelin. Tämä voi viitata siihen, ettei pelillistäminen käsitellyt kysymysten aiheita riittävän selkeästi tai pelissä esitettyjen tietojen omaksuminen jäi pinnalliseksi. Vaikka oikeat ja virheelliset vastausvaihtoehdot olivat pelin aikana helposti saatavilla, osallistujien keskittyminen saattoi kohdistua enemmän pelin suorittamiseen kuin oppimiseen. Erityisesti kysymyksissä, joissa virheellinen vastaus muuttui toiseksi virheelliseksi vastaukseksi, voi olla kyse uuden väärinkäsityksen syntymisestä.

3.3.2 Osaamisen kehittyminen pelin avulla

Kyselytulokset osoittivat, että suurimmassa osassa kysymyksiä oikeiden vastausten määrä kasvoi pelin jälkeen. Yhden vastaajan puuttuminen saattaa osaltaan selittää virheellisten vastausten vähenemistä ja oikeiden vastausten prosentuaalista kasvua. Pelin jälkeinen tulos viittaa kuitenkin siihen, että vastaajat olivat varmemmalla pohjalla vastatessaan, ja monessa kysymyksessä virheellisiä vastauksia ei enää esiintynyt lainkaan.

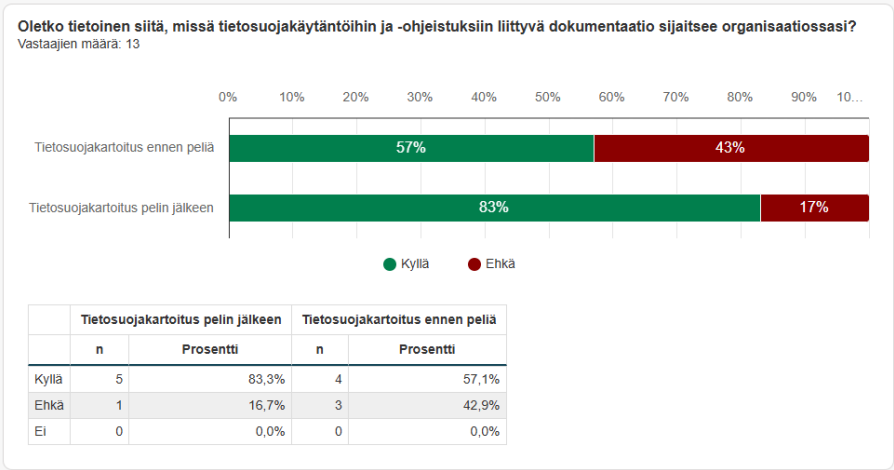
Taulukossa 5 on niiden kysymysten prosentuaalinen määrä kokonaisuudesta, joissa oikeiden vastausten määrä kasvoi pelin jälkeen. Taulukossa ei ole niitä kysymyksiä, joissa kysytään vastaajan omaa mielipidettä Likertin asteikolla.

Taulukko 5: Oikein vastattujen kysymysten prosentuaalinen ero ennen ja jälkeen pelin

Kysymys	Oikein ennen peliä % (N=7)	Oikein pelin jälkeen % (N=6)
Miten tietosuoja-asetus edistää yksilöiden oikeuksia?	71 %	83 %
Mikä on henkilötiedon käsittelijä?	29 %	50 %
Millä edellytyksillä yritys voi käsitellä henkilötietoja ilman rekisteröidyn suostumusta?	86 %	100 %
Kuinka pitkään opiskelijatietoja voidaan säilyttää opintojen päättymisen jälkeen?	86 %	100 %
Voidaanko opiskelijatietoja käyttää tutkimustarkoituksiin ilman opiskelijan suostumusta?	57 %	67 %
Milloin tietoturvaloukkaus on raportoitava rekisteröidyille tai valvontaviranomaisille?	14 %	33 %
Milloin henkilötietojen käsittelyä voidaan jatkaa ilman suostumusta?	86 %	100 %
Mitä tapahtuu, jos henkilö peruuttaa aiemmin antamansa suostumuksen tietojensa käsittelyyn?	86 %	100 %
Mitä tarkoittaa käsittelyn läpinäkyvyys?	86 %	100 %
Jos laki vaatii oppilaitosta säilyttämään opiskelijan tiedot tietyn ajan,	72 %	83 %

mitä tulee tehdä, kun säilytysaika päättyy?		

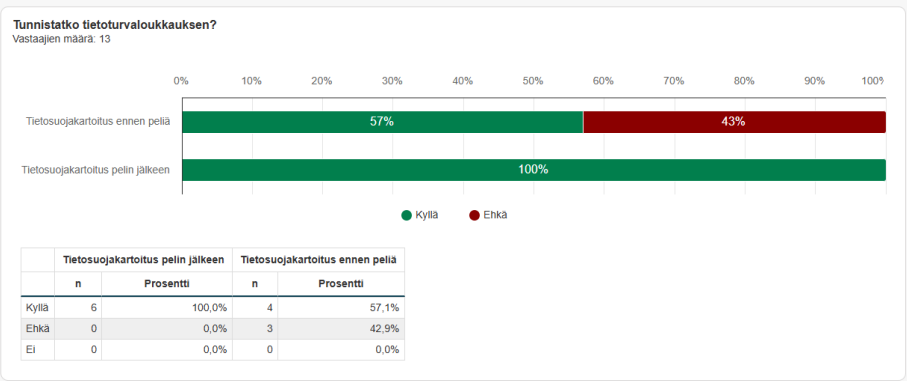
Kyselyssä pelaajilta kysyttiin omaa arviota organisaation tietosuojadokumentaation olemassaolon ja sijainnin tietoisuudesta. Sen tietoisuus parani merkittävästi. Lisäksi dokumentaation merkitys on tullut pelaajille selkeämmäksi.



	Tietosuojakartoitus pelin jälkeen		Tietosuojakartoitus ennen peliä	
	n	Prosentti	n	Prosentti
Kyllä	5	83,3%	4	57,1%
Ehkä	1	16,7%	3	42,9%
Ei	0	0,0%	0	0,0%

Kuvio 4: Dokumentaation sijainti organisaatiossa

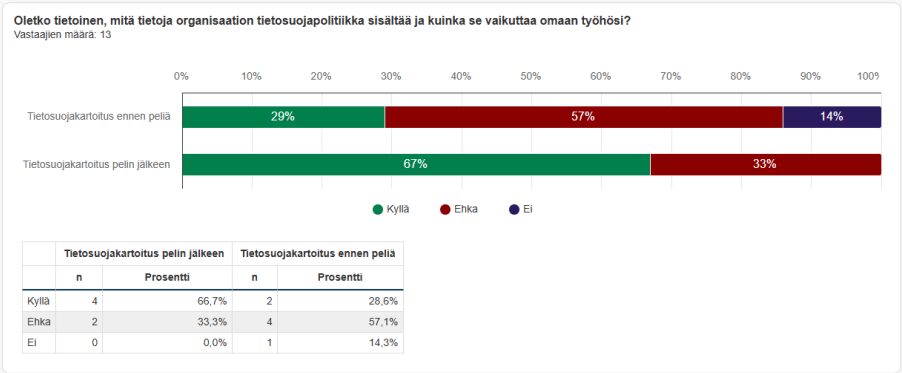
Tietoturvaloukkausten tunnistaminen vahvistui huomattavasti pelin jälkeen. Pelissä olevat käytännön skenaariot auttoivat osallistujia hahmottamaan tietoturvauhkia aiempaa paremmin.



	Tietosuojakartoitus pelin jälkeen		Tietosuojakartoitus ennen peliä	
	n	Prosentti	n	Prosentti
Kyllä	6	100,0%	4	57,1%
Ehkä	0	0,0%	3	42,9%
Ei	0	0,0%	0	0,0%

Kuvio 5: Tietoturvaloukkauksen tunnistaminen

Tietosuojapolitiikan ymmärtäminen on tärkeä osa henkilötietojen käsittelyä. Tulokset osoittivat, että sen merkitys osallistujien työssä vahvistui pelillistämisen myötä.



	Tietosuojakartoitus pelin jälkeen		Tietosuojakartoitus ennen peliä	
	n	Prosentti	n	Prosentti
Kyllä	4	66,7%	2	28,6%
Ehka	2	33,3%	4	57,1%
Ei	0	0,0%	1	14,3%

Kuvio 6: Tietoisuus tietosuojapolitiikan sisällöstä

Kuitenkin on mahdollista, että termi ”tietosuojapolitiikka” itsessään vähentää kiinnostusta dokumenttiin perehtymiseen, sillä nimi voi kuulostaa byrokraattiselta tai vaikeaselkoiselta. Organisaatio voisi harkita dokumentin nimeämistä uudelleen, jotta se tuntuisi helpommin lähestyttävältä.

Pelillistäminen antoi vastaajille mahdollisuuden harjoitella tietosuojan toteuttamista käytännön tilanteissa kuvitteellisessa ympäristössä. Tulokset osoittavat, että vastaajien varmuus kasvoi (taulukko 6) ja oppimista tapahtui niin lähtötasoltaan epävarmojen kuin varmempienkin osallistujien keskuudessa. Erityisesti aiemmin epävarmat vastaajat kokivat osaamisensa vahvistuneen pelin myötä. Ennen peliä kukaan ei antanut korkeinta arvosanaa, mutta pelin jälkeen ainakin yksi vastaajista arvioi varmuutensa korkeimmalle tasolle. Tämä osoittaa, että peli ei ainoastaan vahvistanut, vaan myös syvensi osallistujien tietosuojaosaamista.

Taulukko 6: Varmuus tietosuojan toteuttamisesta omassa työssä

Kuinka varmaksi tunnet itsesi GDPR mukaisen tietosuojan toteuttamisen omassa työssäsi? Arviointi asteikolla 1-10. N=6		
Varmuustaso	Ennen peliä	Jälkeen pelin
Täysin epävarma	0 %	0 %
Epävarma	0 %	0 %
Osittain varma	71 %	0 %
Melko varma	29 %	83 %
Täysin varma	0 %	17 %

Pelaajien oma arvio tietosuojan toteuttamisesta omassa työssä osoitti selkeää positiivista kehitystä. Tämä viittaa siihen, että pelillinen harjoittelu antoi paremman käsityksen tietosuojan ymmärtämisestä omassa työssä. Lisäksi peli lisäsi pelaajien luottamusta omiin taitoihin. Jälkeen pelin arviossa ei ollut enää osittain varmoja vastauksia ja pelaaminen hyödytti erityisesti lähtötasoltaan epävarmempia vastaajia. Pelin jälkeen he kokivat osaamisensa vahvistuneen.

Lopuksi osallistujilta pyydettiin oma arvio pelillistämisen vaikutuksesta tietosuojaosaamiseen asteikolla 1–10. Tämä antaa kokonaiskuvan siitä, miten vastaajat itse kokivat pelin hyödyt ja sen vaikutuksen oppimiseen.

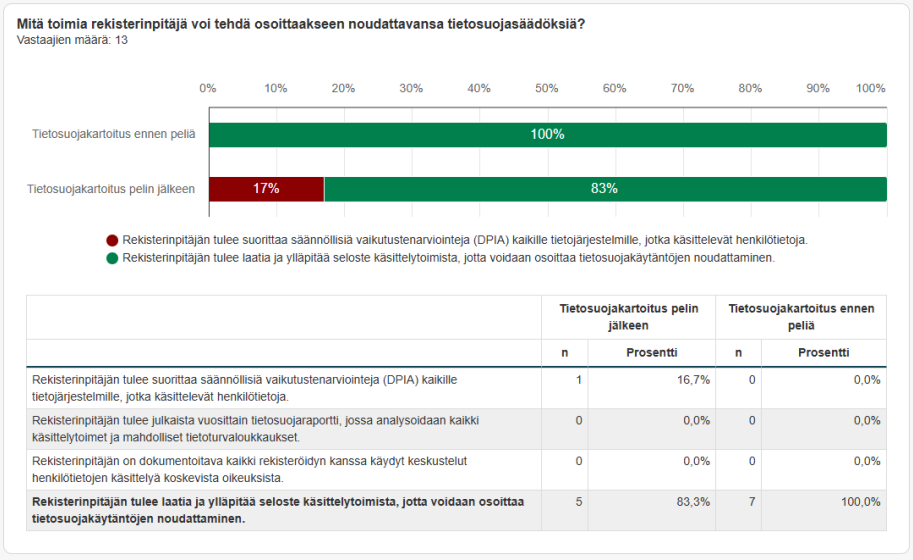
Taulukko 7: Pelaajien oma arvio pelillistämisen vaikutuksesta

Oliko pelaamisella vaikutusta tietosuojaosaamisen kehittymisessä? N=6	
Arviointiasteikko 1–10	Jälkeen pelin
1-6	0 %
7	17 %
8	33 %
9	17 %
10	33 %

Se, ettei kukaan arvioinut vaikutusta vähäiseksi, tukee käsitystä pelillistämiseen tarjonneen hyödyllistä tietoa. Kaikki arvosanat sijoittuvat asteikon yläpäähän 7-10. Pelin vaikutus koettiin pääosin vahvana. Tulokset osoittavat, että osallistujat olivat melko yksimielisiä pelillistämisen hyödyistä. Kahden vastaajan antama korkein arvosana osoittaa, että he kokivat pelin vahvistaneen heidän omaa osaamistaan erityisen paljon. Jopa heikoiten osaamisensa arvioinut vastaaja koki pelillä olleen myönteinen vaikutus tietosuojaosaamiseensa. Tämä viittaa siihen, että pelaamisella on ollut hyötyä lähtötasosta riippumatta.

3.3.3 Muut huomiot

Kolmessa kysymyksessä vastaajat vastasivat oikein ennen peliä, mutta virheellisesti pelin jälkeen.



	Tietosuojakartoitus pelin jälkeen		Tietosuojakartoitus ennen peliä	
	n	Prosentti	n	Prosentti
Rekisterinpitäjän tulee suorittaa säännöllisiä vaikutustenarviointeja (DPIA) kaikille tietojärjestelmille, jotka käsittelevät henkilötietoja.	1	16,7%	0	0,0%
Rekisterinpitäjän tulee julkaista vuosittain tietosuojaraportti, jossa analysoidaan kaikki käsittelytoimet ja mahdolliset tietoturvaloukkaukset.	0	0,0%	0	0,0%
Rekisterinpitäjän on dokumentoitava kaikki rekisteröidyn kanssa käydyt keskustelut henkilötietojen käsittelyä koskevista oikeuksista.	0	0,0%	0	0,0%
Rekisterinpitäjän tulee laatia ja ylläpitää seloste käsittelytoimista, jotta voidaan osoittaa tietosuojakäytäntöjen noudattaminen.	5	83,3%	7	100,0%

Kuvio 7: Ennen peliä oikein, pelin jälkeen virheellisesti vastattu

Tämä herättää kysymyksen siitä, aiheuttiko pelillinen oppiminen epävarmuutta tai väärinkäsityksiä. Mahdollisia syitä voivat olla pelissä käytetty sanamuoto, joka muutti vastausten tulkintaa, tai se, ettei peli onnistunut vahvistamaan oikeita tietoja riittävästi. Lisäksi, jos pelillistämisen aikana saatu tieto ei liittynyt pelaajien aiempaan osaamiseen tai työssä kohdattuihin tilanteisiin, oppiminen saattoi jäädä lyhytaikaiseksi.

Pelillistämisen ja pelin jälkeisen kyselyn välinen aikaväli oli noin viikko, mikä voi osaltaan selittää vastausten heikentymisen. Pelin aikana opittu tieto ei välttämättä siirtynyt pitkäkestoiseen muistiin ilman kertausta. Tämä korostaa tarvetta yhdistää pelillistetty oppiminen muihin menetelmiin, kuten kertaukseen tai syventäviin harjoituksiin, jotta opittu tieto saadaan pysyvämmäksi.

Ilman jatkoa, toistoa ja käytännön soveltamista opitut asiat voivat helposti unohtua. Vaikka yhden vastauksen muuttuminen oikeasta virheelliseksi saattaa vaikuttaa vähäiseltä, pienessä otoskoossa sillä voi olla yllättävän suuri vaikutus kokonaisuuteen. Tulokset voivat viitata pelin aikaiseen kuormitukseen. Pelin aikana saatu runsas tietomäärä saattoi olla liikaa omaksuttavaksi kerralla. Lisäksi uudet näkökulmat saattoivat sekoittaa vastaajien olemassa olevia käsityksiä, mikä voi vaikuttaa vastauksiin.

On myös mahdollista, että pelin aikana saatu uusi tieto ei jäänyt pitkäkestoiseen muistiin, vaan unohtui ennen pelin jälkeistä kyselyä. Vastaajat eivät ehkä enää olleet täysin varmoja oikeista vastauksista tai ennen peliä annetut vastaukset olivat osittain arvauksia. Satunnaiset virheelliset vastaukset ovat myös mahdollinen selitys tuloksille.

3.3.4 Pelin avulla tapahtuneen osaamisen kehittymisen arviointi

Kyselytuloksista voidaan todeta, että monien kysymysten osalta tulokset pysyivät muuttumattomina, vaikka odotuksena oli, että pelillistäminen toisi esiin osaamisen muutoksia. Tämä voi viitata siihen, ettei pelillistäminen lisännyt vastaajien osaamista merkittävästi tai ettei pelin sisältö käsitellyt aihepiirejä riittävän kattavasti. Toisaalta joidenkin kysymysten osalta oikeat vastaukset muuttuivat virheellisiksi pelin jälkeen. Tämä voi tarkoittaa, että pelin aikana syntyi uusia pohdintoja tai väärinymmärryksiä.

Vastaajamäärän väheneminen pelin jälkeisessä kyselyssä voi vaikuttaa tulosten tarkasteluun. Pienessä otannassa yksittäisten vastausten merkitys korostuu, ja jokaisen vastaukset voivat vaikuttaa kokonaiskuvaan merkittävästi. Lopullisen vaikutuksen suuruus riippuu siitä, kuinka paljon puuttuvien vastaajien vastaukset olisivat poikenneet muiden vastauksista. Vaikka tulokset eivät ole yksiselitteisiä, ne antavat viitteitä siitä, millä tavoin pelillistäminen voi vaikuttaa tietosuojaosaamiseen.

Työterveyslaitoksen tutkija Kalakoski (2019) toteaa, että Hermann Ebbinghausin 1800-luvun loppupuolella kehittämä unohtamisen teoria osoittaa, että opittu tieto unohtuu nopeasti

ilman tiedon käyttöä tai kertausta. Kalakosken mukaan uuden osaamisen säilyttäminen edellyttää sen soveltamista käytännössä ja työpaikkakoulutuksetkin tulisi ajoittaa niin, että opittua voidaan hyödyntää heti. Unohtamista voidaan hänen mukaansa ehkäistä varaamalla aikaa käytännön harjoitteluun. Oppimisen perusperiaatteet, kuten jatkuva harjoittelu ja asioiden omaksuminen pienissä osissa, ovat Kalakosken mukaan säilyneet tehokkaina menetelminä ajan myötä. (Kalakoski 2019)

Kuten Armstrong ym. (2018) toteavat, pelillistämisen rinnalle tarvitaan elementtejä, jotka tukevat pitkäjänteistä motivaatiota. Tämä tukee Kalakosken (2019) mainintaa, että oppiminen edellyttää toistuvaa harjoittelua eikä yksittäinen pelillinen kokemus riitä muuttamaan oppimistuloksia merkittävästi. Yksittäinen pelillinen kokemus voi tukea oppimista, mutta ei välttämättä riitä muuttamaan oppimistuloksia pysyvästi.

Kyselytulokset osoittavat, että pelillistäminen voi olla hyödyllinen menetelmä tietosuojaosaamisen kehittämisessä. Jotta se tukisi oppimista mahdollisimman tasapainoisesti ja vähentäisi väärinymmärrysten riskiä, pelin kysymyksiä ja sisältöä on kehitettävä edelleen. Aineiston analyysin perusteella kysymysten haastavuus olisi voinut olla suurempi, ja vastausvaihtoehtojen tulisi olla lähempänä toisiaan, jotta vastaajat joutuisivat pohtimaan valintojaan tarkemmin.

4 Tulokset

Tässä luvussa esitellään kehittämistyön tulokset, jotka liittyvät tietosuojapelin pelaamiseen. Luvussa kuvataan pelin sisältöä, palautteen pohjalta tehdyt muutokset ja osallistujien kokemukset pelistä. Pelin sisällön suunnittelussa ja toteutuksessa huomioitiin kohderyhmän tarpeet ja aiemmat tutkimukset pelillistämisen vaikutuksista oppimiseen. Tavoitteiden saavuttamiseksi pelillisiä elementtejä hyödynnettiin päätöksenteossa, pisteytyksessä ja palautteessa.

4.1 Pelillinen ratkaisu tietosuojaosaamisen kehittämiseen

Peli on lähtökohtaisesti yksilöpeli, mutta mitään estettä yhdessä suorittamiselle ei ole. Osallistujat voivat pelata itsenäisesti tai ryhmässä keskustellen, mikä tukee myös tiedon jakamista ja yhteistyötä. Peliin ei toteutusvaiheessa vaadita kirjautumista organisaation tunnuksilla, vaan se on pelattavissa suoran linkin kautta. Tämä madaltaa osallistumiskynnystä ja mahdollistaa pelin käytön joustavasti eri tilanteissa.

Pelin näkyvyys määräytyy jakoasetusten perusteella. Peli voi olla kaikille avoin, jolloin kuka tahansa voi käyttää sitä ilman kirjautumista. Peliä voidaan jakaa QR-koodin tai suoran linkin avulla. Lisäksi peli voidaan rajata vain organisaation käyttäjille, jolloin sen käyttö edellyttää kirjautumista.

Pelin toteutuksessa käytettiin Thinglink-alustaa, johon luotiin realistisia ja kohdennettuja tietosuojatilanteita. Pelissä hyödynnettiin pelillisiä elementtejä, kuten päätöksentekotilanteita, pisteytystä ja palautetta. Pelissä on seitsemän huonetta, jotka etenevät määrätyssä järjestyksessä. Jokaisella huoneella on tietty tietosuojaan liittyvä teema, ja osallistujien on ratkaistava huonekohtaisia tehtäviä ja tietosuojakysymyksiä saadakseen pisteitä ja edetäkseen pelissä. Pisteet kertyivät ainoastaan huoneiden välisistä kysymyksistä. Oikea valinta on edellytys etenemiselle, mikä kannustaa pelaajia pohtimaan vastausta.

Huoneiden visuaalinen ilme on rakennettu hyödyntämällä Thinglinkin 360° kuvakirjastoa, josta valittiin oppilaitosympäristöön liittyviä kuvia (Higher Education). Kaikkien Thinglinkin kuvien käyttöön on palveluntarjoajan lupa. Kuvakokoelmasta valittiin useita samaan ympäristöön sijoittuvia kuvia, jotka mahdollistivat yhtenäisen ja johdonmukaisen visuaalisen ilmeen pelin eri huoneissa. Visuaalisten elementtien valinnassa painotettiin selkeää oppilaitosympäristöä.

Saavutettavuuden varmistamiseksi pelissä kaikki tekstimuotoiset sisällöt ovat luettavissa myös ääneen, mutta tässä vaiheessa ainoastaan suomen kielellä. Tämä tekee pelistä saavutettavamman erilaisille käyttäjäryhmille ja mahdollistaa sen käytön myös tilanteissa, joissa lukeminen ei ole ensisijainen tapa omaksua tietoa.

Pelin elementit ovat:

- 7 huonetta
- 44 kysymystä, joissa oikean lisäksi virheellisiä vastausvaihtoehtoja 3–5 per kysymys
- 15 tietoiskua, joista 12:sta on painike intraan
- 7 kerättävää sanaa
- 8 peliä

Huoneissa on teemaan liittyviä tehtäviä, jotka tulee suorittaa ennalta määrätyssä järjestyksessä. Ensimmäinen tehtävä on aina lyhyt tietoisku, joista pelaaja voi painikkeella siirtyä organisaation intraan lukemaan lisätietoja.

Pelaajalle esitetään rooliin kohdennettuja tietosuojalainsäädäntöön perustuvia kysymyksiä. Kysymysten vastausvaihtoehdot vaihtelivat neljän ja kuuden välillä. Kaikissa kysymyksissä on vain yksi oikea vastausvaihtoehto. Virheellisestä valinnasta pelaaja sai palautteen ja kannustuksen yrittää uudelleen. Oikeasta valinnasta pelaaja sai positiivisen palautteen sekä selityksen valinnasta. Pelin kaikki huoneet noudattivat samaa kaavaa. Toteutetussa mallissa on osaamistasosta riippumatta sama sisältö.

Jokaisessa huoneessa on pelielementti, kuten tietosuojaan liittyvä muistipeli, ristikko, palapeli tms. Nämä pelit on toteutettu ulkoisen palvelun kautta ja upotettu alustaan pelielementteinä. Kaikkien ulkoisten pelien kuvien käyttöön on palveluntarjoajan lupa. Peleissä

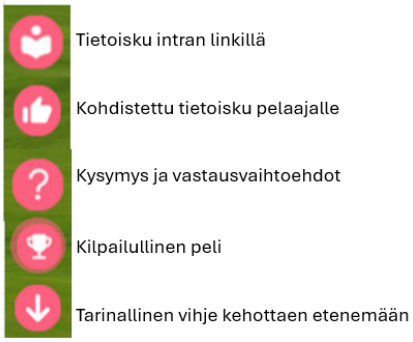
näytetään käytetty ja käytettävissä oleva aika. Osassa peleistä pystyi kilpailemaan aikaa tai elämiä vastaan. Tehtävän suorituksen jälkeen pelaajaa onniteltiin ylistävillä sanoilla ja fanfaareilla. Mahdollinen sijoitus ja tulostaulu näytetään nimettömänä.

Tehtävien välillä pelaajaa ohjataan eteenpäin tarinallisilla vihjeillä, joiden tarkoituksena on luoda mysteerin ja jännittävyyden tunnetta. Näiden avulla haluttiin antaa pelaajalle tunne, että hän on osa tarinaa ja hänen päätöksillään on merkitystä.

Pelin suorittamisella ei ole aikarajoitusta, ja kesto kokonaisuudessaan on noin 45 minuuttia. Jos käyttäjä kirjautuu ulos alustalta tai sulkee selaimen, siinä tapauksessa peli on aloitettava alusta.

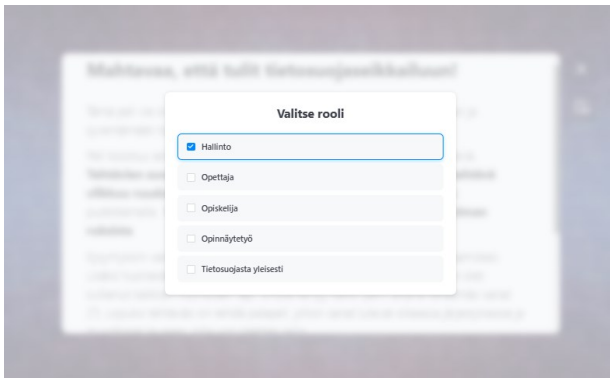
4.1.1 Pelin aloitus ja eteneminen

Pelaaminen alkaa lyhyellä kirjallisella ohjeistuksella, jossa lihavoituna pelaajan muistettavat kohdat. Huoneen tehtävät on merkitty tageilla, jotka toimivat visuaalisina ohjaimina ja kertoivat tehtävän sisällön. Tag tarkoittaa interaktiivista sisältöpistettä, jota painamalla tulee jonkinlaista mediaa, tekstiä tai tehtävää. Ohjeistuksessa myös tagien sisällön merkitys.



Kuvio 8: Tagien selitteet

Ohjeistuksen jälkeen pelaaja valitsee roolin. Valinnan perusteella pelaajalle esitetään rooliin kohdennettuja kysymyksiä. Tässä vaiheessa pelin suorittaminen vain yhdellä roolilla on mahdollista. Valittaessa joku muu rooli, pelaaja saa kehotteen valita hallinnon rooli.



Kuvio 9: Roolin valinta

Rooleina valittavissa:

- Hallinto
- Opetushenkilöstö
- Opiskelija
- Opinnäytetyö
- Tietosuoja yleisesti

Roolivalinnan jälkeen pelaaja siirtyy ensimmäiseen huoneeseen.

Huoneeseen tultaessa tilan kuva pyörii hitaasti ja automaattisesti 360° vaakasuunnassa, jos pelaaja ei tee mitään. Ensimmäisen klikkauksen jälkeen pyöriminen keskeytyy ja sen jälkeen pelaaja pystyy vaihtamaan katselukulmaa hiiren vedä ja pudota -toiminolla. Se mahdollistaa ympäristön tarkastelun kaikista kuvakulmista ja oikean tagin löytämisen.

Huoneen ensimmäinen tag vilkkuu näytöllä ja pelaaja pystyy ainoastaan valitsemaan sen.

Kuvio 10: Pelin aloitusnäkymä (henkilöhahmo luotu Dall-E3 kuvageneraattorilla)

Ohjeistuksessa on mainittu liikkumisen tavoista ja pelaajan täytyy muistaa liikkua huoneessa hyödyntäen hiiren vedä ja pudota -toimintoa. Pelaajan täytyy suorittaa tehtävät tietyssä järjestyksessä ennen kuin hän voi edetä seuraavaan vaiheeseen.

Kun pelaaja tulee huoneeseen, ensimmäisen tehtävän tag vilkkuu punaisena ja tekemättömät tehtävät näkyvät lukkosymboleina. Kun tehtävä on suoritettu, tag jää punaiseksi tagia tarkoittavalla sisällöllä. Suoritettuun tehtävään on mahdollista palata myöhemmin. Jos seuraava suoritettava tehtävä ei näy näytöllä, tagia näytetään vilkuttamalla sitä joko näytön oikeassa tai vasemmassa reunassa.

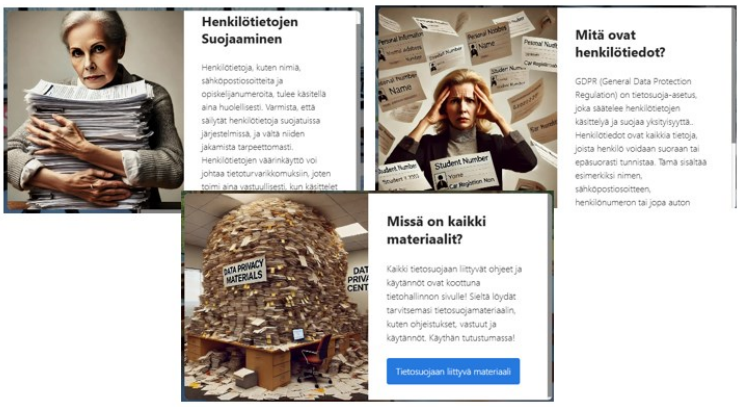
Kuvio 11: Pelin ensimmäinen huone

Pelin ensimmäisen huoneen ensimmäisessä tehtävässä pelaajalla on mahdollisuus pyöräyttää itselleen hauska aiheeseen liittyvä pelinimi. Tämä toimii kevyenä aloituksena ja madaltaa kynnystä osallistumiseen. Pelinimellä ei ole vaikutusta suoritukseen.

Kuvio 12: Pelinimen arvonta

4.1.2 Tietoiskut

Huoneen tehtävinä on tietoiskut, joissa lyhyesti kerrotaan huoneen teemasta. Kaikissa huoneissa on vähintään yksi tietoisku. Tietoiskujen tarkoituksena on antaa pelaajalle taustatietoa aiheesta ennen muiden tehtävien suorittamista. Tietoiskun lyhyt ja ytimekäs esitystapa antaa pelaajalle ymmärrettävyyttä päätöksentekoa vaativissa tehtävissä. Osassa tietoiskuissa on painike organisaation intraan. Kuviossa 13 on kuvakaappauksia huoneissa olevista tietoiskuista.



Kuvio 13: Huoneiden tietoiskuja (kuvat luotu DALL-E 3 kuvageneraattorilla)

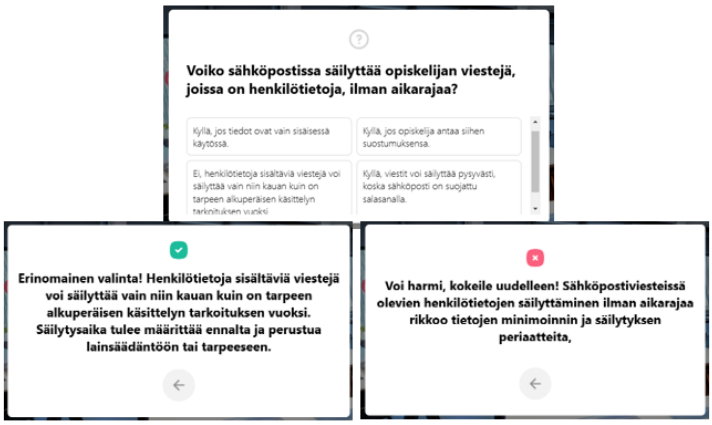
Huoneiden tietoiskut haluttiin saada käyttäjäystävälliseksi ja visuaalisesti selkeäksi. Tietoiskuissa on tekoälyllä (Microsoft Copilot, Dall-E 3 kuvageneraattori) luotu aiheeseen liittyvä kuva, henkilöhahmo tai pelkästään kasvot, jonka ulkomuodolla haluttiin visualisoida aihetta niin, että se kuvastaa eri ikäisiä ja eri kansallisuuksia neutraalilla tavalla. Armstrongin ym. (2018) mukaan avatarien käyttö voi parantaa oppimiskokemusta ja edistää tiedon omaksumista, niiden käyttö pelialustalla ei kuitenkaan ollut mahdollista.

Tietoiskujen jälkeen pelaajalle kohdennetaan huomio (kuvio 14), jossa hän pelaajana huomaa tietosuojaan vaikuttavan puutoksen ja ohjeistuksen, miten se korjataan.

Kuvio 14: Huoneen pelaajalle kohdennettu tietoisku linkillä organisaation intraan

4.1.3 Kysymys-/vastausparit

Tietoiskujen jälkeen pelaajan tulee vastata kysymyksiin pakollisessa järjestyksessä. Kysymykset ovat kohdennettuja kysymyksiä liittyen huoneen teeman aiheisiin. Huonekohtaisia kysymyksiä on 3–8. Kaikki kysymykset esitetään monivalintatehtävinä ja vastausvaihtoehtona on 4–6 vastausta, joista vain yksi on oikea vaihtoehto. Huonekohtaisista kysymyksistä ei kerääntynyt pisteitä.



Kuvio 15: Kysymys ja valinnan mukainen vastausvaihtoehto

Sekä oikeille että väärille vastauksille annetaan tarkempi selite, joka auttoi osallistujaa ymmärtämään miksi valinta on oikea tai virheellinen.

4.1.4 Huonekohtaiset pelit

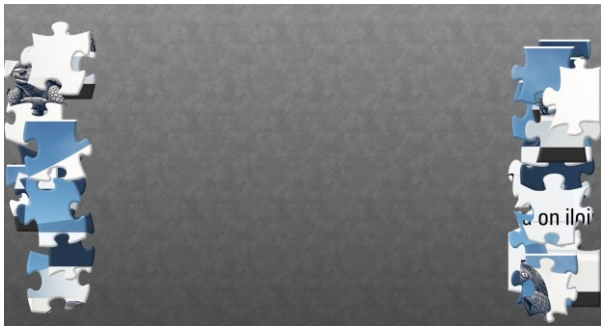
Huonekohtaisilla pelielementeillä halutaan tarjota vaihtelevia ja innostavia tehtäviä. Tehtävien suorittaminen vaatii pelaajilta kuitenkin osaamista, muistamista ja tietojen soveltamista. Kaikki pelielementit on upotettu osaksi pelialustaa ulkoisen palvelun kautta.

Tietosuojan muistipelissä pelaajan tulee löytää toisiinsa liittyviä korttipareja. Oranssille kortille tulee löytää musta vastinpari oikealla sisällöllä. Parit sisältävät tietosuojakäytäntöihin liittyviä oikeuksia ja velvollisuuksia ja niiden kuvauksia. Virheellisessä valinnassa korttipari pysyi luettavana kahdeksan sekuntia, kunnes korttipari kääntyy nurinpäin. Sen jälkeen pelaaja pystyy klikkaamaan uuden korttiparin.

Kuvio 16: Tietosuojan muistipeli

Korttipareja on neljä ja aiheet liittyivät huoneen teemaan. Pelissä hyödynnetään perinteistä muistipelitekniikkaa, jossa pelaaja yhdistää toisiinsa liittyviä tietoja. Muistipelissä ei ollut aikarajoitusta.

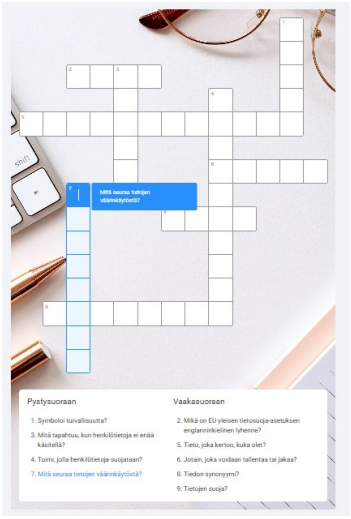
Tietosuojan palapelissä pelaajan tehtävänä on koota 32-palainen palapeli. Palapelit ovat helposti lähestyttäviä elementtejä, ja lopputuloksena muodostuu positiivinen tunnuslause tietosuojasta.



Kuvio 17: Tietosuojapalapeli

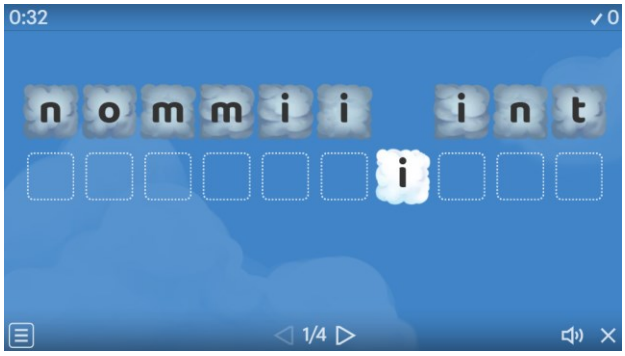
Keventävänä elementtinä palapelin lopputulos auttaa pelaajaa suhtautumaan tietosuojaan vakavasti, mutta samalla myös myönteisellä tavalla.

Tietosuojan ristisanatehtävässä pelaajan tehtävänä on löytää oikeat sanat annetuille vihjeille. Tehtävä on perinteinen sanaruudukko, jossa pelaaja täyttää vastauksia sekä vaaka- että pystysuunnassa. Vastauksen virheelliset kirjaimet korostuivat eri värillä. Ristisanatehtävässä oli mahdollista saada kehuja ja palautetta vasta kun oli sen onnistuneesti suorittanut.



Kuvio 18: Tietosuojan ristisanatehtävä

Tietosuojan kirjaimet sanoiksi -tehtävä on sanapeli, jossa pelaaja sijoittaa yksittäisiä kirjaimia oikeisiin ruutuihin muodostaakseen tietosuojateemaisia sanoja. Jos kirjain sijoitetaan väärään ruutuun, pelaaja saa välittömän palautteen punaisella ruksilla. Kun kirjain sijoitetaan oikein, ruutuun tulee vihreä hyväksyntämerkintä, ja kirjain jää paikalleen.

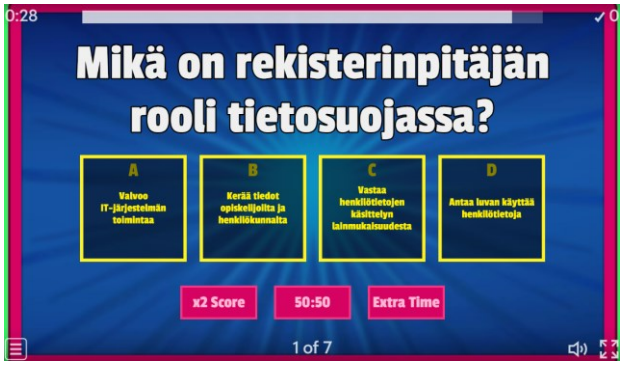


Kuvio 19: Tietosuojan kirjaimet sanoiksi -tehtävä

Tietosuojan piilosana -tehtävä on aikaan rajattu sanapeli, jossa pelaajan tehtävänä on löytää tietosuojaan liittyviä sanoja annettujen vihjeiden perusteella. Tehtävässä sanat on piilotettu kirjainruudukkoon joko vaaka-, pysty- tai vinoriveihin. Jokaisella virheellisellä merkinnällä menettää yhden elämän. Kun kaikki elämät on käytetty tai aika loppuu, peli päättyy. Halutessaan pelin voi aloittaa alusta, jolloin sanat kirjainruudukossa sijoitetaan eri paikkoihin.

Kuvio 20: Tietosuojan piilosana -tehtävä

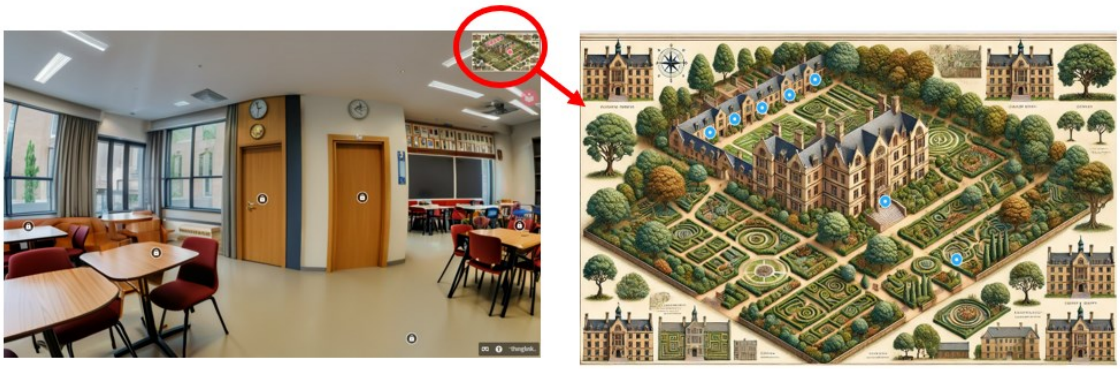
Tietosuojan TV-visa on monivalintapohjainen tietokilpailu, joka haastaa nopeaan harkintaan ja päätöksentekoon. Kilpailu etenee kysymys kerrallaan, ja pelaajalla on rajattu aika vastata kuhunkin kysymykseen. Pelaajalla on käytössään oljenkorret, ja yksi oljenkorsista on aikalisä, joka antaa lisäsekunteja vastaamiseen. Toisen oljenkorren avulla voi poistaa kaksi varmasti väärää vastausta. Kolmannen avulla voi kaksin- tai kolminkertaistaa seuraavan kierroksen pisteet oikealla vastauksella.



Kuvio 21: Tietosuojan TV-visa

Pelaaja kerryttää pisteitä huoneiden välissä olevista kysymyksistä. Virheellisestä vastauksesta annetaan selitys, miksi se on virheellinen, ja selityksessä kerrotaan toisin sanoin, mikä on oikea vastaus. Oikeasta vastauksesta saa kerättävän yksittäisen sanan sekä kehotteen jatkaa eteenpäin.

Huoneiden oikeassa yläkulmassa näkyy koko pelin pohjapiirros, josta klikkaamalla saa esiin kampusympäristön yläilmakuvan. Pohjapiirros on klikattavissa joka huoneessa.

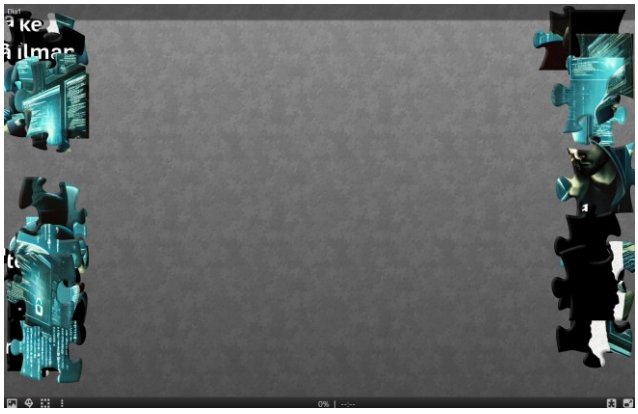


Kuvio 22: Lähikuva yhdestä huoneesta ja koko pelialustalta

Kartan siniset pisteet merkitsevät pelin seitsemää huonetta. Niitä klikkaamalla pelaajalla on mahdollisuus siirtyä huoneesta toiseen ilman pakotettua etenemisjärjestystä. Kartta oli näkyvissä ja aktivoitavissa jokaisessa huoneessa.

4.1.5 Pelin lopetus

Viimeisen huoneen jälkeen osallistujien tuli koota palapeli pelin aikana kerätyistä sanoista.



Kuvio 23: Tietosuojapalapeli

Palapelin jälkeen pelaajaa onnitellaan suorituksesta ja hän pääsee näkemään oman pistesaldonsa ja huoneiden väliset kysymykset ja vastaukset.

Kuvio 24: Pelin lopetus

Alun perin tarkoituksena oli kerätä pelaajilta nimetöntä palautetta pelin päätyttyä. Pelivaiheessa palautelomakkeen linkki jäi kuitenkin lisäämättä päätössivulle, minkä seurauksena kohderyhmän kirjallinen palaute itse pelistä jäi saamatta.

4.2 Pelillistämisen soveltuvuus tietosuojaosaamisen kehittymiseen

Ensimmäisen pelikierroksen palautteessa nousi esiin käytettävyyteen liittyviä haasteita, jotka vaikuttivat pelin sujuvuuteen. Yksi merkittävimmistä haasteista oli navigoinnin epäselvyys. Pelaajien oli aluksi vaikea hahmottaa, miten huonekohtainen tehtävä suljetaan ja milloin ruudun alareunassa näkyvää nuolta tuli painaa seuraavaan huoneeseen siirtymiseksi. Vaikka nuolipainike ei ollut aktiivinen ennen tehtävän suorittamista, sen näkyminen aiheutti hämmennystä. Pelaajat eivät heti oivaltaneet, että tehtävä suljetaan oikean yläkulman ruksista. Tämän vuoksi ohjeistusta selkeytettiin korostamalla tehtäväkohtaista sulkemista lihavoituna tekstinä.

Tietoiskujen kuvituksessa käytettiin tekoälyn tuottamia ihmishahmoja. Ensimmäisissä versioissa hahmot olivat pääasiassa länsimaisia, vaaleaihoisia, kauniita ja nuoria, mikä vahvisti stereotyyppisiä mielikuvia. Eräs pelaaja huomautti, että kuvituksen tulisi paremmin heijastaa monimuotoisuutta ja tasa-arvoa. Tämän palautteen pohjalta hahmoja muokattiin monipuolisemmiksi, jotta ne edustaisivat paremmin reaalimaailman ihmistyyppejä.

Ristisanatehtävä koettiin mukavaksi, mutta ensimmäisellä pelikierroksella sanat olivat liian pitkiä ja haastavia, mikä johti turhautumiseen. Pelaajat kokivat, etteivät pystyneet keksimään oikeita vastauksia. Tehtävää helpotettiin lyhentämällä sanoja ja vähentämällä ristisanojen määrää. Muutoksista huolimatta seuraavilla pelikierroksilla sanat olivat edelleen liian vaikeita. Kolmannella pelikierroksella osa pelaajista jätti tehtävän kesken, koska vastausten keksiminen tuntui mahdottomalta. Jatkokehityksessä tulisi pohtia sopivampaa vaikeustasoa, esimerkiksi lisävihjeiden avulla.

Muistipelissä korttiparit pysyivät ensimmäisellä kierroksella auki vain neljä sekuntia, mikä oli liian lyhyt aika tiedon sisäistämiseen. Sen sijaan pelaajien huomio keskittyi korttien sijainnin muistamiseen. Korttien näkyvyyttä pidennettiin kahdeksaan sekuntiin, mikä auttoi pelaajia

keskittymään paremmin sisältöön. Myös korttiparien määrä koettiin liian suureksi, joten se puolitettiin kahdeksasta neljään.

Pelin lopussa pelaajien tuli muodostaa pelin aikana kerätyistä sanoista lause, joka päätti pelin. Pelin aikana lause osoittautui liian vaikeaksi, sillä sanoista pystyi muodostamaan useita eri versioita. Thinglink-alustalla hyväksyttävänä vastauksena oli kuitenkin vain yksi tarkasti määritelty lause. Useiden erilaisten lauseiden kokeilu aiheutti turhautumista ja kävi myös niin, että oikeaa lausevaihtoehtoa ei löytynyt. Ratkaisuna viimeinen vaihe muutettiin palapeliksi, jossa pelaajien tuli koota lause pelin aikana kerätyistä sanoista.

Osassa kysymyksistä ja vastausvaihtoehdoista oli sanamuotoja, jotka aiheuttivat väärinymmärryksiä. Lisäksi muutaman kysymyksen osalta tuli pyyntö selventää jo kysymyksessä tietyn termin tarkoitus. Niitä tarkennettiin, jotta pelaajat ymmärtäisivät tehtävänannot yksiselitteisesti.

Pelin vaikutuksia arvioidaan vertaamalla ennen ja jälkeen -kyselyiden tuloksia. Näin voidaan tarkastella, miten peli ja pelillistäminen vaikuttaa tietosuojaosaamisen kehittymiseen ja kuinka pelin rakenne, ja osallistujien motivaatio ovat vaikuttaneet oppimistuloksiin.

Tulosten perusteella voidaan todeta, että mittarien arvojen nousu tukee ajatusta siitä, että pelillistäminen on edistänyt tietosuojatietoisuuden kehittymistä. Peli ei kuitenkaan ollut yhtä hyödyllinen kaikille osallistujille. Se näytti hyödyttävän enemmän niitä, joiden lähtötaso oli heikompi. Sen sijaan ne, joilla oli vahvempi lähtötaso, eivät välttämättä kokeneet merkittävää kehitystä, koska hallitsivat suuren osan käsiteltävistä aiheista jo ennen peliä.

Pelaajat kokivat, että peli oli virkistävä tapa oppia, koska se tarjosi vaihtoehdon perinteiselle tekstin lukemiselle ja luentojen seuraamiselle. Pelaaminen teki aiheesta kiinnostavamman ja tarjosi mukavan tavan tietosuojaosaamisen kehittymiselle. Palkitsevuus, kilpailulliset elementit ja tehtävien oikeat valinnat motivoivat pelaajia, vaikka he eivät pitäneet itseään kilpailuhenkisinä.

Pelaajien mielestä yhdessä pelaaminen teki tilanteesta sosiaalisempaa ja mielekkäämpää. Vaikka peli ei ollut suunniteltu varsinaiseksi ryhmäpeliksi, pelaajat huomasivat saavansa lisämotivaatiota ja vertaistukea kollegoiden läsnäolosta. Yhdessä pelaaminen antoi mahdollisuuden keskustella tehtävien ratkaisuista.

> ”Musta tuntuu, että samoja tietosuojajuttuja käsitellään eri muodossa, ja se oli aika kivaa”.
>
> ”Osissa kysymyksistä sai oikein miettiä oikeaa vastausta”.
>
> ”Esimerkit olivat hyviä”.

Palapelit saivat kiitosta ja niitä ehdotettiin lisättäväksi peliin. Osallistujat kommentoivat:

> ”Palapeli oli tosi kiva”, ”palapelissä ei voi muuta kuin onnistua”, ”palapeli oli helpottava”.

Äänimaailman osalta mielipiteet jakautuivat. Osa piti ääniä häiritsevinä, mutta fanfaarien kuuluminen onnistumisen yhteydessä koettiin kuitenkin palkitsevaksi. Pelaajat arvioivat teknisen käytettävyyden hyväksi, eikä pelaaminen vaatinut erityisiä digitaalisia taitoja. Osallistujat totesivat, että

> ”Ulkoasu ja toiminnallisuus olivat odotuksia paremmat”.

> ”Visuaalisuus oli kiva lisä”.

4.3 Pelillistetyn oppimisen tarjoamat mahdollisuudet tietosuojaosaamisen kehittämisessä

Kokonaisuudessaan pelaajien antaman palautteen perusteella pelillistäminen on toimiva menetelmä tietosuojaosaamisen opiskeluun. Pelillistäminen tarjosi kiinnostavan ja motivoivan tavan oppia tietosuojaa. Se ei ainoastaan tehnyt aiheesta kiinnostavaa, vaan auttoi myös testaamaan omia tietoja ja saamaan välitöntä palautetta. Pelaajat voivat kokeilla kysymyksiin eri vastausvaihtoehtoja ja nähdä niiden vaikutukset ilman todellisia seurauksia.

5 Johtopäätökset

Tässä luvussa esitetään kehittämistyön keskeiset johtopäätökset, arvioidaan kehittämistyön toteutusta ja tuloksia sekä tarkastellaan kehittämistyössä ilmenneitä onnistumisia ja haasteita. Lisäksi pohditaan kehittämistyön eettisyyttä ja luotettavuutta sekä esitetään ehdotuksia jatkokehittämisen mahdollisuuksista.

Tämän opinnäytetyön aihevalinnan taustalla on kasvava tarve tietosuojaosaamisen kehittämiseen työelämässä. Euroopan unionin yleinen tietosuoja-asetus (GDPR) ja kansallinen tietosuojalaki edellyttävät organisaatioilta tietosuojakäytäntöjen noudattamista ja henkilötietojen asianmukaista käsittelyä. Lakisääteisten vaatimusten lisäksi tietosuojaosaaminen on yhä keskeisempi tekijä organisaatioiden riskien- ja maineenhallinnassa sekä liiketoiminnan jatkuvuuden varmistamisessa.

Aihevalinnan taustalla on myös henkilökohtainen kiinnostus tietosuojaan ja sen merkityksen kasvuun työelämässä. Tietosuojan hallintaan liittyvät kysymykset ovat tulleet yhä keskeisemmiksi monilla toimialoilla. Organisaatioiden haasteena on varmistaa, että henkilöstö tunnistaa tietosuojariskit ja osaa toimia säädösten mukaisesti. Tähän liittyen kehittämistyön tavoitteena oli selvittää, kuinka pelillistäminen voi edistää tietosuojaosaamisen kehittämistä ja mitkä tekijät vaikuttavat sen onnistumiseen organisaatioympäristössä.

Kehittämistyön tulokset osoittavat, että pelillistämisen etuna on sen interaktiivisuus ja mahdollisuus harjoitella päätöksentekoa todellisuutta simuloivissa skenaarioissa. Tämä tukee ajatusta siitä, että käytännönläheiset skenaariot voivat auttaa sisäistämään tietosuojakäytännöt tehokkaammin kuin pelkästään teoreettinen opetus. Positiivinen ja vuorovaikutteinen ilmapiiri lisäsi osallistujien aktiivisuutta, mikä voi osaltaan tukea tiedon omaksumista ja sen soveltamista työelämässä.

Vaikka pelillistämisellä havaittiin olevan myönteisiä vaikutuksia oppimiseen, menetelmän tehokkuuteen liittyy myös haasteita. Yksi keskeinen kysymys on opitun tiedon pitkäaikainen säilyminen. Koska kehittämistyössä tarkasteltiin tuloksia pienellä viiveellä pelin jälkeen, ei ole varmuutta siitä, kuinka hyvin osallistujat muistavat ja soveltavat oppimaansa pitkällä aikavälillä. Lisäksi pelillistäminen saattaa vaikuttaa eri tavoin eri oppimistyylejä edustaviin henkilöihin. Se voi asettaa haasteita koulutuksen suunnittelulle ja toteutukselle.

Pelillistämisen tehokkuus riippuu suuresti sen toteutustavasta ja organisaatiokontekstista. Kuten Armstrong ym. (2018, 2) mainitsevat, tutkimustulosten perusteella pelillistäminen on hyödyllinen silloin, kun se yhdistetään organisaation muuhun koulutuskokonaisuuteen eikä jää irralliseksi harjoitukseksi. Jotta menetelmästä saataisiin mahdollisimman suuri hyöty, sen tulisi tukea työntekijöiden jatkuvaa oppimista ja olla osa laajempaa tietosuojakulttuurin kehittämistä.

Pelillistämisen onnistuminen vaatii myös organisaation sitoutumista. Jos organisaatio kannustaa kokeilukulttuuriin ja oppimiseen, pelillistämisen hyödyt voivat olla merkittäviä. Toisaalta, jos koulutus nähdään pakollisena suorituksena ilman selkeää yhteyttä päivittäiseen työhön, sen vaikuttavuus voi jäädä vähäiseksi (Gjertsen ym. 2017). Tämä korostaa tarvetta suunnitella koulutus niin, että se vastaa työntekijöiden todellisiin tarpeisiin ja tukee arkipäivän työtehtäviä.

Kehittämistyö osoittaa, että pelillistäminen on lupaava menetelmä tietosuojaosaamisen kehittämisessä. Se tarjoaa motivoivan, käytännönläheisen ja osallistavan tavan oppia tietosuojakäytäntöjä. Tulokset myös osoittavat, että pelillistäminen voi lisätä sitoutumista koulutukseen ja se luo turvallisen ympäristön tietosuojatilanteiden harjoittelulle.

Pelillistäminen ei kuitenkaan ole ratkaisu kaikkiin tietosuojaosaamisen kehittämisen haasteisiin. Sen tehokkuus riippuu toteutuksesta, organisaation koulutuskulttuurista ja siitä, miten menetelmää sovelletaan osana jatkuvaa koulutusta. Jotta pelillistämisestä saataisiin täysi hyöty, sen tulisi olla osa laajempaa strategiaa, jossa huomioidaan organisaation tarpeet, työntekijöiden erilaiset oppimistyylit ja tietosuojaosaamisen pitkäjänteinen kehittäminen.

5.1 Kehittämistyön ja tulosten arviointi

Kehittämistyö toteutettiin konstruktiivisena opinnäytetyönä, ja sen tavoitteena oli ymmärtää pelillistetyn oppimisen vaikutuksia tietosuojaosaamisen edistämiseen. Keskeisenä kehittämistoimenpiteenä suunniteltiin ja toteutettiin interaktiivinen tietosuojapeli, jonka vaikuttavuutta arvioitiin ennen ja jälkeen -asetelmaan perustuvilla kyselyillä. Tulosten perusteella tarkasteltiin työntekijöiden kykyä tunnistaa ja reagoida tietosuojauhkiin päivittäisessä työssään.

Salon (2012) mukaan koulutuksen tarvearviointi tulisi tehdä ennen koulutuksen toteuttamista. Tässä kehittämistyössä ei tehty erillistä tarvearviointia, sillä tietosuojaosaamisen kehittämisen tarve oli jo tunnistettu. Ennen ja jälkeen -kyselyt toimivat epäsuorina tarvearviointeina, sillä ennen peliä toteutettu kysely kartoitti osallistujien lähtötason, ja jälkikysely mittasi pelillistämisen vaikutuksia. Tämä lähestymistapa mahdollisti koulutusmenetelmän vaikuttavuuden arvioinnin ilman erillistä ennakkovaiheen tarvekartoitusta.

Kyselyaineiston analysointi oli selkeämpää strukturoidun kysymysrakenteen ansiosta. Strukturoitujen kysymysten valinta perustui siihen, että näin saatiin todennäköisemmin vertailukelpoisia vastauksia tietosuojaan liittyvistä näkökohdista.

Kohderyhmä koostui organisaation työntekijöistä, jotka käsittelevät henkilötietoja päivittäin eri rooleissa, mutta toimivat samojen aihealueiden parissa. Pelin sisältö suunniteltiin kohdentumaan juuri tämän ryhmän tarpeisiin, jotta sen vaikuttavuus olisi mahdollisimman suuri. Peliin luotiin skenaarioita, jotka vastaavat kohderyhmän tyypillisiä tietosuojahaasteita. Sekä skenaarioita, joista julkisen palvelun tarjoajana on hyvä olla tietoinen.

Kehittämistyön lähestymistapa oli konstruktiivinen, ja strukturoidusta kyselyaineistosta huolimatta aineisto analysoitiin laadullisin menetelmin. Pelillistämisen vaikutuksia arvioitiin ensisijaisesti kyselytulosten perusteella, ja toissijaisena arviointimenetelmänä hyödynnettiin pelaamisen aikaista laadullista havainnointia. Tämä mahdollisti osallistujien reaktioiden ja oppimisprosessin havainnoinnin, ja se täydensi kyselytutkimuksen tuloksia.

Kehittämistyön tulokset vahvistivat, että pelillistäminen voi tukea tietosuojaosaamisen kehittymistä, mutta sen vaikuttavuus edellyttää huolellista suunnittelua. Kuten Hamari ym. (2014) toteavat, pelillistämisen vaikutukset ovat tehokkaimpia, kun sovellusympäristö ja käyttäjien yksilölliset tarpeet huomioidaan. Tämä havainto korostaa tarvetta kohdentaa pelin sisältö tarkasti käyttäjäryhmän tarpeiden mukaan.

Kyselytulosten perusteella peli onnistui lisäämään tietoisuutta organisaation tietosuojadokumentaation olemassaolosta ja sijainnista. Lisäksi pelin käsittelemät tietosuojateemat lisäsivät osallistujien varmuutta oman tietosuojaosaamisensa suhteen. Yksi vastaaja jäi kuitenkin epävarmaksi, mikä saattaa johtua dokumentaation löydettävyydestä. Tällä hetkellä

tietosuojadokumentaatio ei ole optimaalisessa sijainnissa, ja sen siirtäminen helpommin saavutettavaan paikkaan on suunnitteilla. Tämä viittaa siihen, että organisaation sisäinen viestintä dokumentaation sijainnista ja käytöstä voisi vaatia selkeyttämistä.

Lainema ym. (2021, 51) korostavat, että pelillistämisen onnistuminen edellyttää huolellista suunnittelua ja pedagogista ohjausta. Deterding ym. (2011) puolestaan toteavat, että pelillistäminen voi parantaa oppimismotivaatiota ja sitouttaa osallistujia tehokkaammin kuin perinteiset koulutusmenetelmät, kuten kirjalliset materiaalit tai verkkokurssit. Armstrongin ym. (2018) mukaan pelillistäminen toimii parhaiten täydentävänä menetelmänä, ei korvaavana ratkaisuna. He myös toteavat, että on tärkeää valita kohderyhmän tarpeita tukevat pelielementit.

Tämä kehittämistyö tukee aiempia havaintoja, sillä osallistujat kokivat pelillistetyn oppimisen mielekkäämmäksi ja hyödyllisemmäksi erityisesti silloin, kun sisältö oli osallistujille suunnattua. Pelillistämisen hyödyntäminen ei ainoastaan kehitä tietosuojaosaamista, vaan voi edistää organisaation tietosuojakulttuuria. Gjertsenin ym. (2017) tutkimus korostaa osallistujien sitoutumisen merkitystä, mikä näkyy tämän työn tuloksissa.

Osallistujat kokivat pelin hyödylliseksi ja antoivat sille myönteistä palautetta. Tulosten perusteella voidaan todeta, että pelillistäminen voi toimia tehokkaana menetelmänä tietosuojaosaamisen kehittämisessä myös tulevaisuudessa. Tämä kehittämistyö vahvistaa aiempien tutkimusten havaintoja pelillistämisen hyödyistä oppimismotivaation lisäämisessä ja tietosuojaosaamisen kehittämisessä. Vaikka itsevarmuus tietosuojan toteuttamisessa kasvoi pelillistämisen myötä, se ei yksinään riitä varmistamaan syvällistä oppimista. Kuten Hamari ym. (2014) korostavat, pelielementtien valinnan tulee tukea oppimistavoitteita. Pelillistämistä voi hyödyntää osana laajempaa kokonaisuutta.

5.2 Pohdinta

Tämän opinnäytetyön keskeinen arvo muodostuu sen tarjoamasta käytännön hyödystä organisaatiolle ja työntekijöille. Työssä kehitettiin pelillistetty oppimismenetelmä, jonka tavoitteena oli lisätä työntekijöiden tietosuojaosaamista osallistavalla ja motivoivalla tavalla. Tulokset osoittivat, että pelillistäminen voi olla tehokas tapa edistää tietosuojaosaamista ja sitouttaa osallistujia aiheen käsittelyyn.

Koska tavoitteena oli löytää osallistava ja motivoiva tapa kehittää tietosuojaosaamista, kehittämistyössä päätettiin hyödyntää pelillistämistä, vaikka ei ollut pedagogista tai pelitutkimuksen liittyvää osaamista. Valintaan vaikutti se, että pelillistämisen arvioitiin tekevän oppimisesta osallistavampaa ja motivoivampaa. Lisäksi se kannustaisi osallistujia pohtimaan omia valintojaan tietosuojaan liittyvissä tilanteissa.

Opinnäytetyö tarjosi myös tekijälle uusia näkökulmia ja oppimiskokemuksia. Tietosuojaan liittyvä tietämys vahvistui erityisesti lainsäädännön soveltamisen osalta. Keskeinen onnistuminen oli tietosuojapelin suunnittelu ja toteutus. Peli ei ainoastaan motivoinut osallistujia, vaan myös tarjosi heille konkreettisia oivalluksia tietosuojasta. Osallistujien palaute ja heidän kykynsä soveltaa oppimaansa käytännössä vahvistivat, että peli täytti sille asetetut tavoitteet.

Kehittämistyössä ilmeni kuitenkin myös haasteita. Kehittämistyön edetessä tietoisuus pelillistämisestä lisääntyi merkittävästi, vaikka se oli vain pintaraapaisu. Pelimaailman laajuuden hahmottaminen ja pelillistämisen teorioihin perehtyminen osoittautuivat vaativiksi. Ennakkoon pelillisyys nähtiin vain yksinkertaisena menetelmänä. Kävi nopeasti selväksi, ettei kyse ole pelkästään peleistä ja niiden elementeistä. Kirjallisuuteen perehtyminen osoitti sen olevan monimutkainen ja laaja-alainen kokonaisuus, jossa yhdistyvät pedagogiikka, psykologia, käyttäytymistieteet ja teknologia. Pelillistämiseen liittyviä teorioita on Krathn ym. (2021) mukaan peräti 118, mikä teki oman kirjallisuuskatsauksen laatimisesta työlästä. Olennaisten näkökulmien valinta ja aiheen rajaaminen vaativat tarkkaa harkintaa, jotta kehittämistyössä voitiin keskittyä keskeisimpiin näkökulmiin.

Kysymysten suunnittelussa oli huomioitava kohderyhmän vaihteleva tietosuojan osaamistaso. Mukana oli sekä pitkään alalla toimineita asiantuntijoita että työntekijöitä, joilla oli vain muutaman vuoden kokemus tietosuojasta. Kysymysten tuli olla riittävän selkeitä vähemmän kokeneille, mutta samalla tarpeeksi haastavia kokeneemmille asiantuntijoille. Lisäksi tasapainon löytäminen pelillistämisen viihteellisyyden ja opittavan sisällön välillä oli haastavaa. Pelin tuli olla kiinnostava ja motivoiva, mutta sen viihteellisyys ei saanut vähentää koulutuksellista arvoa. Liian leikkimielinen peli voisi viedä huomiota oppimistavoitteista ja johtaa siihen, että pelaajat keskittyvät enemmän pelistrategiaan kuin tietosuojaosaamisen kehittämiseen.

Etäyhteydellä toteutettu peli loi omat haasteensa havainnoinnille. Vaikka osallistujien videokamerat olivat päällä, pelaamista ei tallennettu, ja havainnot tuli kirjata välittömästi. Tämä saattoi vaikuttaa havaintojen kattavuuteen. Toisaalta reaaliaikainen videoyhteys mahdollisti ilmeiden ja eleiden havainnoinnin erittäin hyvin.

Perinteisesti tietosuojakoulutus on nojannut kirjallisiin materiaaleihin ja luentopohjaisiin koulutuksiin. Tämä kehittämistyö osoitti, että vaihtoehtoiset koulutusmenetelmät voivat lisätä työntekijöiden sitoutumista ja parantaa oppimistuloksia.

Spithovenin ja Drenthin (2024) mukaan organisaatioilla on tarpeen parantaa työntekijöiden kykyä tunnistaa ja reagoida tietoturvaan ja tietosuojaan liittyviin riskeihin. Heidän tutkimuksensa mukaan työntekijöiden käyttäytymiseen vaikuttavat monet tekijät, kuten asenteet, osaaminen ja työnantajan antama tuki. Sptithovenin ym. (2024) sekä Bélanger, Maier ja Maierin (2022) tutkimukset korostavat koulutuksen keskeistä roolia, mutta painottavat, että sen on oltava motivoivaa ja käytännönläheistä. Tutkimukset tukevat myös sitä näkökulmaa, että perinteiset luentopohjaiset koulutukset voivat olla tehottomia työntekijöiden käyttäytymisen

muutokseen. Lisäksi Spithoven ym. (2024) painottavat, että organisaatiokohtaisten riskien ymmärtäminen on avainasemassa koulutuksen suunnittelussa.

Tämän kehittämistyön tulokset tukevat tätä näkemystä. Vaikka pelillistämisen hyödyt olivat selkeitä, työn yleistettävyys on rajallinen pienen otoskoon ja organisaatiokohtaisen lähestymistavan vuoksi. Tulokset osoittavat kuitenkin, että pelillistäminen voi olla tehokas menetelmä tietosuojaosaamisen kehittämisessä, erityisesti silloin, kun se räätälöidään organisaation tarpeisiin.

Organisaation palautteen mukaan osallistujat kokivat pelissä etenemisen ja saavutusten saamisen palkitsevaksi. Tämä lisäsi oppimismotivaatiota verrattuna tilanteisiin, joissa tietosuojaa käsitellään vain lukemalla tai luentoja kuuntelemalla. Kilpailuvietti ja aikapaine toivat lisähaastetta, ja yhdessä pelaaminen teki kokemuksesta mielekkäämmän. Pelissä ei keskitytty pelkästään omiin virheisiin, vaan myös kanssapelaajien toimintaa havainnoitiin ja arvioitiin. Vuorovaikutteisuus toisten kanssa teki pelaamisesta mukavaa.

Palautteen mukaan peli koettiin myös teknisesti helppokäyttöiseksi, eikä sen läpikäyminen vaatinut erityisiä teknisiä taitoja. Organisaation mukaan sisällön konkreettiset esimerkit olivat erityisen tärkeitä, sillä niiden avulla asioiden sisäistäminen onnistui paremmin kuin pelkästään kirjallisen materiaalin pohjalta. Osallistujat pitivät peliä mukavana tapana oppia ja kokivat sen tuovan vaihtelua perinteisiin koulutusmenetelmiin. Organisaation edustaja vertasi peliä urheiluvalmennukseen, jossa yksitoikkoisia harjoituksia tehdään houkuttelevammiksi kilpailun ja pelillisten elementtien avulla. Hän kuvasi peliä myös niin, että siinä ”huijattiin innostumaan” muuten tylsältä tuntuvasta aiheesta. Organisaation antaman palautteen mukaan pelillistämisen lisääminen muuten tylsäksi koettuun aiheeseen oli innostava kokemus.

Ratkaisun sovellettavuuden arviointi eri konteksteissa on keskeinen osa konstruktiivisen tutkimuksen onnistumista. Tutkijan tulee pystyä irrottautumaan empiirisestä työstä ja tarkastella kriittisesti sekä prosessin tuloksia että niiden toteutusehtoja (Lukka 2000, 7). Konstruktiiviselle tutkimusotteelle on ominaista, että kehitetyn ratkaisun yleistettävyys ja siirrettävyys myös muihin organisaatioihin on mahdollista (Virtanen 2006, 48). Lukan (2000, 2) mukaan puolueettoman arvioinnin takaamiseksi on tärkeää analysoida ratkaisun vahvuuksien lisäksi sen rajoitteet ja mahdolliset kehitystarpeet.

Pelin joustavuus mahdollistaa sen mukauttamisen erilaisten organisaatioiden tarpeisiin. Organisaatiokohtaiset erot, kuten toimintakulttuuri, resurssien saatavuus ja pelin pelaamiseen varattu aika, voivat vaikuttaa toteutukseen. Pelillistämisen onnistunut soveltaminen edellyttää suunnittelua, riittäviä resursseja sekä kohderyhmän tarpeiden tuntemista. On myös huomioitava, että organisaatioiden lähtötilanteet tietosuojan suhteen voivat vaihdella merkittävästi, mikä vaikuttaa pelin sisällön räätälöintiin ja sen soveltuvuuteen eri yhteyksissä.

Aikaisemmat tutkimukset ovat osoittaneet (Armstrong & Landers 2018, 4; Francia ym. 2014; Gjertsen ym. 2017; Hamari ym. 2014), että pelilliset elementit oikein suunniteltuna ja kohdennettuna voivat lisätä sitoutumista ja motivaatiota. Tietosuoja voi olla aiheena laaja ja monimutkainen, mutta pelillistämisen avulla siihen saadaan konkretiaa ja käytännönläheisyyttä. Tämän kehittämistyön tulokset tukevat aikaisempia tutkimuksia, eikä tuloksissa tullut esiin uutta eivätkä tulokset olleet ristiriidassa aikaisempien tutkimusten kanssa.

5.3 Eettisyys ja luotettavuus

Tutkimuseettinen neuvottelukunta on opetus- ja kulttuuriministeriön asettama asiantuntijaelin, jonka tehtävänä on käsitellä tieteelliseen tutkimukseen liittyviä eettisiä kysymyksiä ja edistää tutkimusetiikkaa Suomessa (TENK 2024). Tietosuoja itsessään edistää eettisten periaatteiden noudattamista ja luotettavaa toimintaa. Tämä opinnäytetyö liittyy vahvasti eettisyyteen, ja kehitetyn pelin tavoitteena on edistää tietojen eettistä hallinnointia ja käsittelyä organisaatioissa.

Tässä opinnäytetyössä on noudatettu Arenen (Ammattikorkeakoulujen opinnäytetöiden eettiset suositukset 2024) eettisiä suosituksia sekä Tutkimuseettisen neuvottelukunnan (TENK 2024) hyvän tieteellisen käytännön periaatteita. Kehittämistyö ei edellyttänyt TENK:n määrittämää eettistä ennakkoarviointia.

Kyselyiden ja pelaamisen osalta kehittämistyöstä keskusteltiin ennakkoon kohderyhmän esihenkilön kanssa. Hän antoi suostumuksensa ja osallistui myös itse. Osallistujia informointiin sähköpostitse lähetetyllä informointilomakkeella, jossa kerrottiin opinnäytetyön tavoitteesta, ennen ja jälkeen -kyselyistä ja pelistä.

Organisaation kanssa käytiin läpi kehittämistyön toteutukseen liittyvät yksityiskohdat ja sovittiin opinnäytetyön toteutuksesta. Aineistonhallintasuunnitelmassa on kuvattu kehittämistyön eteneminen, kerättävä aineisto, aineiston dokumentointi, laadun varmistaminen, informointien ja suostumusten toteuttaminen ja aineiston hävittäminen heti, kun se ohjeistuksen mukaan on mahdollista.

Kehittämistyön menetelmät ja tulokset on kuvattu ja analysoitu huolellisesti ja niistä on raportoitu avoimesti ja rehellisesti. Kehittämistyön menetelmäosuudessa osallistujilta kerättiin ainoastaan välttämätön henkilötieto (sähköpostiosoite) kehittämistyön etenemisen suhteen. Pelitilaisuuksia ei tallennettu, eikä osallistujien henkilötietoa ollut tallennettuna kirjallisissa muistiinpanoissa. Kaikki osallistujat osallistuivat vapaaehtoisesti ja heitä kohdeltiin tasavertaisesti ja kunnioittavasti. Muiden tuottamaa tutkimusta tai tietoa ei ole vääristelty, ja lähteisiin on viitattu ja ne on merkitty asianmukaisesti.

Eettisyys ja luotettavuus ovat keskeisiä periaatteita kehittämisasetelmassa. Opinnäytetyön tekijä toimii itsenäisesti rekisterinpitäjänä ja on vastuussa henkilötietojen käsittelyn

tarkoituksesta ja käsittelyn keinoista. Kaikki aineisto on kerätty ja käsitelty aineistonhallintasuunnitelman mukaisesti, luottamuksellisesti ja ainoastaan suostumuksen antaneiden osallistujien osalta.

Tulosten luotettavuus varmistetaan käyttämällä laadullisia menetelmiä, jolla halutaan saada monipuolisempi näkökulma. Aineisto analysoitiin ilman ennakkoluuloja tai henkilökohtaisia näkemyksiä. Analyysin lähtökohtana oli kerätty tieto, ja johtopäätökset perustuvat aineistoon eikä omiin oletuksiin. Pelillistämisen onnistumista arvioidaan selkeillä ja läpinäkyvillä kriteereillä.

Mielenkiintoisena näkökulmana voidaan todeta, että Tutkimuseettisen neuvottelukunnan, Turusen (2024), mukaan GDPR on vienyt huomiota pois eettiseltä pohdinnalta. Näiden yhdistely tutkimuksissa on aiheuttanut väärinymmärryksiä, jossa pääosan on vienyt tietosuoja. Yhteinen tavoite on kuitenkin ihmisen suojelu, vaikka eettinen pohdinta ei ole lakisääteistä.

Työelämässä pelillistämiseen liittyy eettisiä ja sosiaalisia riskejä, erityisesti työntekijöiden hyvinvoinnin ja yksityisyyden näkökulmasta. Ongelmia syntyy, jos tietoja kerätään ilman suostumusta tai avoimuutta. Erityisen riskialtista on henkilökohtaisen tiedon, kuten mielialan tai käyttäytymisen analysointi. Työntekijöillä tulisi olla oikeus nähdä, mitä tietoja heistä tallennetaan ja että tiedon käyttö on läpinäkyvää ja rajattua. Eettisesti kestävässä pelillistämisessä yksityisyys, vapaaehtoisuus ja tietojen oikeudenmukainen käsittely ovat keskeisiä. Pelillistäminen ei saa muodostua valvontajärjestelmäksi, joka lisää työntekijöiden stressiä tai rajoittaa heidän henkilökohtaista vapauttaan työympäristössä. (Shahri, Hosseini, Phalp, Taylor & Ali 2024)

Tässä kehittämistyössä pelillistämisen tarkoituksena oli oppimisen tukeminen. Tavoitteena ei ollut työntekijöiden vertailu tai arviointi. Peli suunniteltiin niin, että se auttoi pohtimaan tietosuojaan liittyviä valintoja turvallisessa ympäristössä ilman kilpailua tai paineita pärjätä muita paremmin. Näin varmistettiin, että pelillistäminen toteutettiin eettisesti ja oppimista sekä työntekijöiden hyvinvointia tukevalla tavalla.

5.4 Jatkokehittäminen

Tämän kehittämistyön perusteella pelillistäminen voi toimia tehokkaana menetelmänä tietosuojaosaamisen kehittämisessä. Tuloksena syntynyt interaktiivinen tietosuojapeli tarjoaa monia mahdollisuuksia jatkokehittämiselle, jotta siitä saataisiin entistä kattavampi ja monipuolisempi.

Yksi kehityssuunta on pelin sisällön laajentaminen roolipohjaiseksi eri vaikeusasteilla. Tämä mahdollistaisi organisaation eri toimijoiden, kuten hallinnon, TKI:n, opetushenkilöstön ja opiskelijoiden, tarpeiden huomioimisen. Nykyisellä pelialustalla ei kuitenkaan ole mahdollista arpoa kysymyksiä kysymyspankista eri rooleille ja vaikeusasteille, mutta tämä voisi olla

kehittämisen kohteena. Lisäksi käyttäjäpalautteen kerääminen ja hyödyntäminen auttaisi parantamaan pelin sisältöä ja käytettävyyttä.

Z-sukupolvi on kasvanut digitaalisessa maailmassa. He voisivat toimia tietosuojalähettiläinä, jotka jakavat tietoa parhaista tietosuojakäytännöistä ja toimivat mentoreina muille. Heidän osaamisensa voisi tuoda uusia näkökulmia ja innovaatioita pelielementtien kehittämiseen. Vaikka edellisillä sukupolvilla on enemmän elämän- ja työelämäkokemusta, eri sukupolvien näkökulmien ja teknologisen osaamisen yhdistäminen voisi auttaa tietosuojan koulutusta.

Mielenkiintoinen jatkokehittämisen kohde voisi olla tietosuojaportaali, joka integroituisi organisaation oppimisympäristöön, kuten Moodleen tai Canvasiin. Portaali voisi tarjota ajankohtaista tietoa tietosuojasta ja tietoturvasta sekä mahdollisuuden suorittaa peli oppimisympäristön kautta. Kirjautuminen varmistaisi, että vain valtuutetut käyttäjät pääsevät aineistoon käsiksi. Portaali voisi tarjota vaihtoehtoisen oppimismenetelmän niille, jotka eivät koe pelaamista itselleen luontevaksi tavaksi oppia. Oppimisprosessia voisi tukea erilaisilla palkitsemisen muodoilla, kuten tunnustuksilla tai todistuksilla. Lisäksi voitaisiin selvittää, voisivatko opiskelijat ansaita opintopisteitä tietosuojaportaalin suorittamisesta ja miten tietosuojan ja tietoturvan oppimisella olisi pitkäaikaisvaikutuksia.

Kiinnostava näkökulma olisi myös tutkia, voisiko massiivinen avoin verkkokurssi (MOOC) toimia pelillistetyn tietosuojakoulutuksen alustana. Tällainen kurssi voisi tavoittaa laajemman yleisön ja mahdollistaa tietosuojaosaamisen kehittämisen myös organisaatioiden ulkopuolella.

Narratiivin lisääminen koulutusmateriaaliin voisi myös olla kehittämisen arvoinen alue. Armstrong ym.(2018, 3) osoittavat tutkimuksessaan, että teknologiakoulutuksen materiaalin narratiivisuus lisäsi osallistujien tyytyväisyyttä ja paransi oppimiskokemusta. Voisiko sama periaate toimia myös tietosuojakoulutuksessa? Tarinalliset elementit voisivat tehdä oppimisesta elämyksellisempää ja auttaa osallistujia hahmottamaan tietosuojan käytännön merkityksen paremmin.

Lisäksi voitaisiin tutkia, miten tosielämässä tapahtuneita tietosuojarikkeitä ja -haasteita voitaisiin hyödyntää koulutusmateriaalissa. Peliin voisi lisätä skenaarioita, jotka perustuvat oikeasti tapahtuneisiin tietosuojarikkeisiin. Pelaajille voitaisiin tarjota vaihtoehtoja tilanteen ratkaisemiseksi. Esimerkiksi Postin tapaus, jossa asiakkaille luotiin automaattisesti OmaPosti-laatikko ilman käyttäjän suostumusta, johti tietosuojavaltuutetun toimiston määräämään merkittävään seuraamusmaksuun (Kangas 2024). Omakohtaisena kokemuksena voi sanoa postilaatikon sisältöineen olleen aikamoinen yllätys.

Pelillistämisen sovellettavuutta voitaisiin myös laajentaa organisaatiokohtaisesti. Skenaarioita voitaisiin mukauttaa eri organisaatioiden tarpeisiin, jolloin sisältö vastaisi paremmin kunkin työympäristön tietosuojahaasteita. Saman alan organisaatioilla on usein samankaltaisia

tietosuojaan liittyviä ongelmia, ja pelin avulla niitä voitaisiin käsitellä käytännönläheisesti roolipohjaisten skenaarioiden kautta.

Tässä kehittämistyössä ei pystytty mittaamaan oppimisen pitkäaikaisvaikutuksia. Jatkossa voisi olla hyödyllistä kehittää arviointityökaluja, joilla voidaan seurata oppimisen kehittymistä pidemmällä aikavälillä. Lisäksi tietosuojakoulutuksen vaikuttavuutta voitaisiin vertailla perinteisiin oppimismenetelmiin, kuten verkkokursseihin tai luentopohjaiseen koulutukseen, ja selvittää, tuottaako pelillistäminen pysyvämpiä oppimistuloksia, jos sitä käytetään säännöllisesti osana koulutusta.

Edesmenneen Benjamin Franklinin (University of Cambridge 2012) sanoin:

> “An ounce of prevention is worth a pound of cure.”

Lähteet

Painetut

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava. Printon, Tallinna: Tietosanoma Oy.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2018. Kehittämistyön menetelmät Uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro.

Sähköiset

Aalto-yliopisto. 2024. Cyber Citizen -hanke kehittää eurooppalaisten kyberturvataitoja pelillistämisen avulla. Viitattu 13.3.2025. https://www.aalto.fi/fi/uutiset/cyber-citizenhanke-kehittaa-eurooppalaisten-kyberturvataitoja-pelillistamisen-avulla.

Ahokas, K. 2024a. Tietosuojavastaava ei vastaa tietosuojasta. Tivi. Viitattu 5.9.2024. https://www.tivi.fi/uutiset/tietosuojavastaava-ei-vastaa-tietosuojasta-monet-ovat-ymmartaneet-roolin-vaarin/c5ba5c80-a544-44ad-a596-436de798e3d7.

Ahokas, K. 2024b. Tällaista on tietosuojavastaavan työ. Tivi. Viitattu 26.6.2024. https://www.tivi.fi/uutiset/tallaista-on-tietosuojavastaavan-tyo-pitaa-ymmartaa-lakia-lokeja-ja-teknologiaa/338fa280-00bc-4058-bce5-541038656f65.

Almeida, C., Kalinowski, M., Uchôa, A., & Feijó, B. 2023. Negative effects of gamification in education software: Systematic mapping and practitioner perceptions. Information and Software Technology. Viitattu 1.4.2023. Elsevier. https://www.sciencedirect.com/science/article/pii/S0950584922002518. DOI: 10.1016/j.infsof.2022.107142.

Ammattikorkeakoulujen opinnäytetöiden eettiset suositukset. 2024. Ammattikorkeakoulujen rehtorineuvosto Arene ry. Viitattu 1.1.2025. https://arene.fi/wp-content/uploads/Raportit/2018/arene_ammattikorkeakoulujen-opinnaytetoiden-eettiset-suositukset.pdf?_t=1526903222.

Ammattikorkeakoulujen uraseurantakysely. 2024. Viitattu 27.12.2024. https://vipunen.fi/fi-fi/_layouts/15/xlviewer.aspx?id=/fifi/Raportit/Ammattikorkeakoulutus%20-%20uraseuranta%20-%20rahoitusmalli%20-%20amk.xlsb.

Armstrong, M. & Landers, R. 2018. Gamification of employee training and development: Gamification of employee training. International Journal of Training and Development. Viitattu 11.11.2024. https://onlinelibrary.wiley.com/doi/abs/10.1111/ijtd.12124. DOI: 10.1111/ijtd.12124.

Barth, S. & de Jong, M. 2017. The privacy paradox– Investigating discrepancies between expressed privacy concerns and actual online behavior– A systematic literature review. https://pdf.sciencedirectassets.com/271579/1-s2.0-S0736585317X0004X/1-s2.0-S0736585317302022/main.pdf?X-Amz-Security-To

Barth, S., de Jong, M., Junger, M., Hartel, P. & Roppelt, J.C. 2019. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Viitattu 5.10.2024. https://www.sciencedirect.com/science/article/pii/S0736585317307724. DOI: 10.1016/j.tele.2019.03.003.

Bélanger, F., Maier, J. & Maier, M. 2022. A longitudinal study on improving employee information protective knowledge and behaviors. Computers & Security. Viitattu 22.11.24. https://www.sciencedirect.com/science/article/pii/S0736585317307724.

Bogost, I. 2011. Bogost.com. Gamification is Bullshit. Viitattu 11.10.2024. https://bogost.com/writing/blog/gamification_is_bullshit/.

Claburn, T. 2024. Europe's GDPR has led to less data storage and processing. Viitattu 29.2.24. https://www.theregister.com/2024/02/21/gdpr_data_processing_costs/.

Deterding, S., Dixon, D., Khaled, R. & Nacke, L. 2011. From game design elements to gamefulness: defining gamification. Viitattu 7.4.2024. https://www.researchgate.net/publication/230854710_From_Game_Design_Elements_to_Gamefulness_Defining_Gamification.

Digi- ja väestötietovirasto. 2024a. Taisto-harjoitus on mahdollisuus testata ja kehittää organisaationne digiturvaa. Viitattu 1.1.2024. https://dvv.fi/taisto.

Digi- ja väestötietovirasto. 2024b. Digiturvallinen elämä -koulutuskokonaisuus. Viitattu 1.1.2024. https://dvv.fi/digiturvallinen-elama.

Dreimane, S. 2021. Gamification before its definition – An overview of its historical development. Viitattu 25.11.24. https://library.iated.org/view/DREIMANE2021GAM.

EDPB. 2025a. Viitattu 9.3.2025. https://www.edpb.europa.eu/sme-data-protection-guide/data-controller-data-processor_fi.

EDPB. 2025b. Viitattu 26.2.2025. https://www.edpb.europa.eu/sme-data-protection-guide/respect-individuals-rights_fi

EDPB. 2025c. Viitattu 21.2.2025. https://www.edpb.europa.eu/sme-data-protection-guide/faq-frequently-asked-questions/answer/what-difference-between_fi.

EDPB. 2024. Viitattu 17.1.2024. https://www.edpb.europa.eu/our-work-tools/our-documents/other/coordinated-enforcement-action-designation-and-position-data_en.

Euroopan komissio. 2025. Viitattu 9.3.2025. https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_fi.

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Viitattu 19.8.2024. https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04/fin.

European Comission. 2017. Guidelines on Data Protection Impact Assessment. Viitattu 22.8.2024. https://ec.europa.eu/newsroom/article29/items/611236/.

Francia, G., Thornton, D., Trifas, M. & Bowden, T. 2014. Gamification of Information Security Awareness Training. Viitattu 27.3.24. https://www.sciencedirect.com/science/article/pii/B9780124114746000050>. DOI: 10.1016/B978-0–12-411474-6.00005-0.

Friman, U., Arjoranta J., Kinnunen J., Heljakka K. & Stenros J. 2022. Pelit kulttuurina. Tampere: Vastapaino. Viitattu 1.12.24. https://koneensaatio.fi/wp-content/uploads/2023/04/pelit_kulttuurina_arvostelu.pdf#page=35.

F-Secure. 2024a. Mikä on tietomurto? Viitattu 29.8.2024. https://www.f-secure.com/fi/articles/what-is-a-data-breach.

F-Secure. 2024b. Tarkista, ovatko henkilö-tietosi vuotaneet pimeään verkkoon? Viitattu 29.8.2024. https://www.f-secure.com/fi/identity-theft-checker.

Gabrielle, V. 2018. The dark side of gamifying work. Fast Company. Viitattu 3.11.24. https://www.fastcompany.com/90260703/the-dark-side-of-gamifying-work.

Gjertsen, E., Gjære, E., Bartnes, M. & Rocha, W. 2017. Gamification of Information Security Awareness and Training. ResearchGate. Viitattu 7.4.24. DOI: 10.5220/0006128500590070. https://www.researchgate.net/profile/Maria-Bartnes/publication/314523152_Gamification_of_Information_Security_Awareness_and_Training/links/5ba3773ba6fdccd3cb652a88/Gamification-of-Information-Security-Awareness-and-Training.pdf

Hamari, J. & Huotari, K. 2012. Defining Gamification - A Service Marketing Perspective. ResearchGate. Viitattu 7.4.2024. https://www.researchgate.net/publication/259841647_Defining_Gamification_-_A_Service_Marketing_Perspective. DOI: 10.1145/2393132.2393137.

Hamari, J., Koivisto, J. & Sarsa, H. 2014. Viitattu 3-11-24. Does Gamification Work? -- A Literature Review of Empirical Studies on Gamification. Hawaii International Conference on System Sciences. http://ieeexplore.ieee.org/document/6758978/>. DOI: 10.1109/HICSS.2014.377.

Hoxhunt. 2023. 10 Steps to Award-Winning Cybersecurity Training. Viitattu 26.3.2024. https://www.hoxhunt.com/blog/10-steps-to-award-winning-cybersecurity-training-the-aes-cso50-playbook.

Humak. 2024. Humanistinen ammattikorkeakoulu. Viitattu 27.12.2024. https://www.humak.fi/tutkimus-ja-kehityspalvelut.

Humak tilinpäätös. 2023. Toimintakertomus ja tilinpäätös 1.1.-31.12.2023. Viitattu 27.12.2024. https://www.humak.fi/wp-content/uploads/2024/06/Humak-tilinpaatos-2023-julkinen.pdf

Järvensivu, A. 2017. Pelillistäminen ja digitaaliset pelit työelämän kehittämismenetelminä. Aikuiskasvatus. 37(4). Viitattu 25.3.2024. https://journal.fi/aikuiskasvatus/article/view/88440.

Järvinen, P. 2017. Tietosuojavastaavat – toimivat yhteyshenkilöinä mutta eivät todellisuudessa vastaa mistään. Tivi. Viitattu 14.4.2024. https://www.tivi.fi/blogit/tietosuojavastaavat-toimivat-yhteyshenkiloina-mutta-eivat-todellisuudessa-vastaa-mistaan/3a08bbc3-f5d5-3ba3-b7a0-38e2fddc4b47.

Kalakoski, V. 2019. Tietoasiantuntija. Tietojohtaminen Ry. Viitattu 11.12.2024. https://www.tietojohtaminen.com/tietoasiantuntija-2-32019.

Kangas, L. 2024. Yle Uutiset. Viitattu 2.1.2025. https://yle.fi/a/74-20124822.

Kanta. 2021. Tietosuojatyö tehostuu organisaatioissa. Viitattu 16.8.2024. https://www.kanta.fi/ammattilaiset/artikkeli/-/asset_publisher/E0GUmalM4d8l/content/tietosuojaty%C3%B6-tehostuu-organisaatioissa

Kantonen, S. & Pohjalainen, A. 2024. EU:n yleisen tietosuoja-asetuksen soveltamiskokemuksia Suomessa. Valtioneuvosto. Viitattu 29.12.2024. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165679/OM_2024_18_ML.pdf?sequence=1&isAllowed=y.

Kasanen, E., Lukka, K. & Siitonen, A.1993. The Constructive Approach in Management Accounting Research. Viitattu 25.1.2025. https://mycourses.aalto.fi/pluginfile.php/183797/mod_resource/content/1/Kasanen%20et%20al%201993.pdf%3e.

Klabbers, J. 2009. The magic circle: Principles of gaming & simulation. ResearchGate. Viitattu 26.11.2024. https://www.researchgate.net/publication/273947293_The_magic_circle_Principles_of_gaming_simulation.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi tietosuojalainsäädäntö. Alma Talent Oy. Viitattu 9.3.2025. http://nelli.laurea.fi/login?url=https://verkkokirjahylly.almatalent.fi/teos/19ju431708

Krath, J., Schürmann, L. & von Korflesch, H. F. O. 2021. Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. Computers in Human Behavior. Viitattu 3.12.2024. https://www.sciencedirect.com/science/article/pii/S0747563221002867.

Kuntaliitto 2019. Tietosuojalaki. Viitattu 16.8.2024. https://www.kuntaliitto.fi/laki/julkisuus-ja-tietosuoja/tietosuoja-asetus/tietosuojalaki.

Kyberturvallisuuskeskus. 2020. Näin pidät huolta tietoturvasta kotona ja työpaikalla. Viitattu 27.8.2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla.

Kyberturvallisuuskeskus. 2024a. Tietoturvasääntely. Viitattu 28.8.2024. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturvasaantely.

Kyberturvallisuuskeskus. 2024b. Tietomurrot. Viitattu 28.8.2024. https://www.kyberturvallisuuskeskus.fi/fi/tietomurrot.

Lainema, K. & Lainema, T. 2021. Valmiuksia tulevaisuuden työelämään simulaatiopeli-oppimisen kautta. Pelitutkimuksen vuosikirja. Viitattu 10.10.2024. https://pelitutkimus.journal.fi/article/view/108008.

Laki julkisen hallinnon tiedonhallinnasta 906/2019. 2019. Viitattu 5.3.2024. https://www.finlex.fi/fi/laki/alkup/2019/20190906.

Landers, R., Auer, E.M., Collmus, A.B., Armstrong, M. 2018. Gamification Science, Its History and Future: Definitions and a Research Agenda. Simulation & Gaming. Viitattu 25.11.2024. https://doi.org/10.1177/1046878118774385.

Landers, R., Auer, E., Helms, A., Marin, S., Armstrong, M. 2019. Gamification of Adult Learning: Gamifying Employee Training and Development. Viitattu 1.4.2024. https://doi.org/10.1017/9781108649636.012.

Landers, R. 2019. Gamification Misunderstood: How Badly Executed and Rhetorical Gamification Obscures Its Transformative Potential. Journal of Management Inquiry. Viitattu 3.11.2024. https://doi.org/10.1177/1056492618790913.

Lemmetty, S. 2024. Kuka vastaa ja kuka maksaa, kun oppimisvaatimukset työelämässä kasvavat? Työelämän tutkimus. Viitattu 6.12.2024. https://doi.org/10.37455/tt.146052.

Li, H., Luo, X., Zhang, J., Xu, H. 2017. Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. Information & Management. Viitattu 24.11.2024. 1012–1022. https://doi.org/10.1016/j.im.2017.02.005.

Lukka, K. 2000. The key issues of applying the constructive approach to field research. ResearchGate. Viitattu 5.2.2025. https://www.researchgate.net/publication/281549256_The_key_issues_of_applying_the_constructive_approach_to_field_research.

Lukka, K. 2003. The Constructive Research Approach. ResearchGate. Viitattu 13.1.2025. https://www.researchgate.net/publication/247817908_The_Constructive_Research_Approach.

Lukka, K. 2014. Metodix. Viitattu 25.1.2025. https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/.

Maanpuolustuskorkeakoulu. 2021. Sotapelaamisen avulla luodaan keskustelua ja vuorovaikutusta taktiikan opetuksessa. Viitattu 26.11.2024. https://maanpuolustuskorkeakoulu.fi/-/sotapelaamisen-avulla-luodaan-keskustelua-ja-vuorovaikutusta-taktiikan-opetuksessa.

McGonigal, J. 2011. Reality Is Broken. The Penguin Press. Viitattu 26.11.2024. https://educacaofisicaaefcps.wordpress.com/wp-content/uploads/2018/07/reality_is_broken.pdf.

Oikeusministeriö. 2018. Viitattu 18.8.2024. https://oikeusministerio.fi/-/uusi-tietosuojalaki-voimaan-vuoden-2019-alusta.

Paspatis, I., Tsohou, A., 2023. How to Influence Privacy Behavior Using Cognitive Theory and Respective Determinant Factors. Journal of Cybersecurity and Privacy. Viitattu 12.2.2024. https://doi.org/10.3390/jcp3030020.

Paspatis, I., Tsohou, A., 2024. Experiential Transformation in Privacy Behavior: A New Framework for Privacy Behavior Enhancement. Journal of Cybersecurity and Privacy. Viitattu 7.2.2024. https://doi.org/10.3390/jcp4010005.

Poliisi. 2024. Tietomurrot. Viitattu 28.8.2024. https://poliisi.fi/tietomurrot.

Puolustusvoimat. 2020. Viitattu 26.11.2024. https://puolustusvoimat.fi/-/tutkimuskatsaus-hyotypeleista.

Pärssinen, K., 2023. Tietosuoja nousi tapetille koko maailmassa. Tivi. Viitattu 20.3.2024. https://www.tivi.fi/uutiset/tietosuoja-nousi-tapetille-koko-maailmassa-kiinakin-on-valmistelemassa-omaa-lainsaadantoa/c2bae663-61a2-48a5-b3a3-9e812f397fd0.

Salo, V., 2012. Työntekijöiden kokeman koulutustarpeen arvioiminen. Ammattikasvatuksen aikakauskirja. Viitattu 1.4.2024. https://journal.fi/akakk/article/view/114448.

Shahri, Hosseini, Phalp, Taylor & Raian 2024. Towards a Code of Ethics for Gamification at Enterprise. ResearchGate. Viitattu 20.2.2025. https://www.researchgate.net/publication/275968573_Towards_a_Code_of_Ethics_for_Gamification_at_Enterprise>. DOI: 10.1007/978-3-662-45501-2_17.

Silic, M., Lowry, P.B. 2020. Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. Journal of Management Information Systems. Viitattu 25.11.2024. https://doi.org/10.1080/07421222.2019.1705512.

Spithoven, R., Drenth, A. 2024. Who will take the bait? Using an embedded, experimental study to chart organization-specific phishing risk profiles and the effect of a voluntary micro-learning among employees of a Dutch municipality. Journal of Cybersecurity. Viitattu 22.12.2024. https://doi.org/10.1093/cybsec/tyae010.

Suomen Museot. 2024. Keskiaikainen uhkapelaaminen: millaista se oli. Viitattu 25.11.2024. https://suomenmuseotonline.fi/keskiaikainen-uhkapelaaminen-millaista-se-oli/.

Thomas, N.J., Baral, R., Crocco, O.S., Mohanan, S. 2023. A framework for gamification in the metaverse era: How designers envision gameful experience. Technological Forecasting and Social Change. Viitattu 25.11.2024. https://doi.org/10.1016/j.techfore.2023.122544.

Tilastokeskus. 2024. Väestön tieto- ja viestintätekniikan käyttö sukupuolen ja ikäluokan mukaan, 2013-2024. Viitattu 16.12.2024. https://pxdata.stat.fi/PxWeb/pxweb/fi/StatFin/StatFin__sutivi/statfin_sutivi_pxt_13ud.px/.

Turunen, R. 2024. Tutkijan ABC-kirja alkaa tutkimusetiikasta. Tutkimuseettinen neuvottelukunta. Viitattu 31.12.2024. https://tenk.fi/fi/ajankohtaista/risto-turunen-tutkijan-abc-kirja-alkaa-tutkimusetiikasta.

TENK. 2024. Hyvä tieteellinen käytäntö (HTK). Viitattu 1.1.2025. https://tenk.fi/fi/hyva-tieteellinen-kaytanto-htk.

Tietosuojalaki. 2018. Viitattu 1.8.2024. https://finlex.fi/fi/laki/alkup/2018/20181050.

Tietosuojavaltuutettu. 2021. Opiskelijanumeroihin yhdistettyjen arvosanojen ja tehtäväkohtaisten pisteiden vieminen yliopiston intranetiin. Viitattu 28.12.2024. https://www.finlex.fi/fi/viranomaiset/tsv/2021/20210823.

Tietosuojavaltuutetun toimisto 2024a. Tietosuojavaltuutetun toimisto valvoo tietosuojaoikeuksiasi. Viitattu 16.8.2024. https://tietosuoja.fi/tietosuojavaltuutetun-toimisto.

Tietosuojavaltuutetun toimisto 2024b. Rekisteröidyn oikeudet. Viitattu 26.2.2025. https://tietosuoja.fi/rekisteroidyn-oikeudet.

Tietosuojavaltuutetun toimisto 2024c. Tietosuojavastaavan nimittäminen. Viitattu 17.3.2024. https://tietosuoja.fi/tietosuojavastaavan-nimittaminen.

Tietosuojavaltuutetun toimisto 2024d. Usein kysyttyä tietosuojavastaavista. Viitattu 23.3.2024. https://tietosuoja.fi/usein-kysyttya-tietosuojavastaavat.

Tietosuojavaltuutetun toimisto 2024e. Osoita noudattavasi tietosuojasäännöksiä. Viitattu 24.1.2024. https://tietosuoja.fi/osoitusvelvollisuus.

Tietosuojavaltuutetun toimisto 2024f. Vaikutustenarviointi. Viitattu 12.2.2024. https://tietosuoja.fi/vaikutustenarviointi.

Tietosuojavaltuutetun toimisto 2024g. Pseudonymisoidut ja anonymisoidut tiedot. Viitattu 16.8.2024. https://tietosuoja.fi/pseudonymisointi-anonymisointi.

Tietosuojavaltuutetun toimisto 2024h. Tietoturvaloukkaukset. Viitattu 29.8.2024. https://tietosuoja.fi/tietoturvaloukkaukset.

Vehkalahti, K. 2014. Kyselytutkimuksen mittarit ja menetelmät. Helsingin yliopisto. Viitattu 4.10.2024. http://hdl.handle.net/10138/305021. DOI: 10.31885/9789515149817.

Vilkka, H. 2007. Tutki ja mittaa Määrällisen tutkimuksen perusteet. Viitattu 31.12.2024. https://trepo.tuni.fi/bitstream/handle/10024/98723/Tutki-ja-mittaa_2007.pdf?sequence=1&isAllowed=y.

Virtanen, A. 2006. Konstruktiivinen tutkimusote Miten koulutus ja elinkeinoelämän odotukset kohtaavat ammattikorkeakoulun opinnäytetöissä. Viitattu 26.1.2025. Ammattikasvatuksen aikakauskirja.

University of Cambridge. 2012. Viitattu 2.1.2025. https://www.cam.ac.uk/research/news/ounce-of-prevention-pound-of-cure.

Yleinen tietosuoja-asetus. 2016. Tietosuojavastaavan nimittäminen. Viitattu 5.4.2023. https://gdpratlas.com/fi/fi-article-37.

Julkaisemattomat

Andreasson, A. 2023. Tietosuojavastaavan tehtävät. Verkkoluento 16.2.2023. Alma Talent. Helsinki.

Eronen, H. 2022. Tietosuojan vaikutukset käytännön työssä. Verkkoluento 10.11.2022. Alma Talent. Helsinki.

Pennanen, H. 2024. Verkkotapaaminen. Thinglink.

Pönkä, H. 2022. Tietosuojavastaavan peruskoulutus. Verkkoluento 1.11.2022. SnellmanEDU. Kuopio.

Voutilainen, Tomi 2022. Tietosuojavastaava ja tiedonhallinta. Verkkoluento. 29.9.2022. Alma Talent. Helsinki.

Kuviot

Taulukot

Liitteet

Liite 1: Ennen ja jälkeen -kyselyiden kysymykset ja vastaukset

Numero	Kysymys	Vastaus
1	Mitä tarkoittaa GDPR?	General Data Protection Regulation
2	Miten tietosuoja-asetus edistää yksilöiden oikeuksia?	Suojaa luonnollisten henkilöiden oikeuksia ja vapauksia henkilötietojen käsittelyssä.
3	Mikä on rekisterinpitäjä?	Organisaatio, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.
4	Mikä on henkilötiedon käsittelijä?	Organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän lukuun ja tämän ohjeiden mukaisesti.
5	Miten rekisterinpitäjän vastuu määritellään?	Rekisterinpitäjän on varmistettava, että henkilötietoja käsitellään lainmukaisesti ja turvallisesti.
6	Mitä tietoja rekisterinpitäjän tulee sisällyttää käsittelytoimien selosteeseen?	Käsittelyn tarkoitus, rekisteröityjen ryhmät, tietojen säilytysajat ja tietojen vastaanottajat.
7	Millä edellytyksillä yritys voi käsitellä henkilötietoja ilman rekisteröidyn suostumusta?	Jos käsittely on tarpeen sopimuksen täytäntöönpanemiseksi tai laillisen velvoitteen noudattamiseksi.
8	Mitä tarkoitetaan tietosuojan vaikutustenarvioinnilla (DPIA)?	Se on prosessi, jolla selvitetään henkilötietojen käsittelyyn liittyvät riskit ennen käsittelyn aloittamista.
9	Mitä osoitusvelvollisuus tarkoittaa käytännössä rekisterinpitäjälle?	Rekisterinpitäjän on pystyttävä todistamaan, että on toteuttanut asianmukaiset toimenpiteet tietosuojan varmistamiseksi.
10	Mitä toimia rekisterinpitäjä voi tehdä osoittaakseen noudattavansa tietosuojasäädöksiä?	Rekisterinpitäjän tulee laatia ja ylläpitää seloste käsittelytoimista, jotta voidaan osoittaa tietosuojakäytäntöjen noudattaminen.
11	Mikä seuraavista ei ole rekisterinpitäjän osoitusvelvollisuuden piirissä?	Rekisterinpitäjän on varmistettava, että tietosuojavastaava valvoo käsittelytoimia, jotta käsittely on tietosuojalainsäädännön mukaista.

12	Miksi oppilaitoksen täytyy noudattaa tietojen minimoinnin periaatetta opiskelijatietoja kerätessään?	Periaatteen avulla oppilaitos varmistaa, että vain tarkoituksen kannalta välttämättömät tiedot kerätään opiskelijoista,
13	Milloin opiskelijoiden henkilötietoja voidaan käyttää ilman heidän suostumustaan?	Kun tiedot ovat välttämättömiä opintojen suorittamisen järjestämiseksi.
14	Kuinka pitkään opiskelijatietoja voidaan säilyttää opintojen päättymisen jälkeen?	Niin kauan kuin on tarpeen lainmukaisten velvoitteiden täyttämiseksi.
15	Voidaanko opiskelijatietoja käyttää tutkimustarkoituksiin ilman opiskelijan suostumusta?	Kyllä, jos opiskelijatiedot anonymisoidaan.
16	Milloin oppilaitos voi rajoittaa opiskelijan tietojen käyttöä, vaikka opiskelija ei ole sitä pyytänyt?	Jos oppilaitos epäilee, että tiedot ovat virheellisiä.
17	Mitä tarkoittaa tietojen pseudonymisointi ja milloin sitä käytetään?	Tietojen muuttaminen niin, ettei niitä voida yhdistää suoraan tiettyyn henkilöön.
18	Milloin tietoturvaloukkaus on raportoitava rekisteröidyille tai valvontaviranomaisille?	Jos tietoturvaloukkaus aiheuttaa todennäköisesti merkittävää riskiä rekisteröidyn oikeuksille ja vapauksille.
19	Miksi henkilöstön kouluttaminen on tärkeää tietoturvaloukkauksien ennaltaehkäisyssä?	Jotta työntekijät osaisivat tunnistaa tietoturvauhat.
20	Missä tilanteissa oppilaitos voi kieltäytyä poistamasta opiskelijan tietoja?	Jos tietojen säilyttäminen on välttämätöntä lakisääteisten velvoitteiden täyttämiseksi.
21	Miten oppilaitos voi varmistaa, että tietopyynnöt käsitellään lain vaatimusten mukaisesti?	Vastaamalla pyyntöön kuukauden kuluessa.
22	Mikä seuraavista on laillinen peruste henkilötietojen käsittelylle?	Henkilötietojen käsittely on tarpeen sopimuksen täytäntöön panemiseksi, johon rekisteröity on osapuolena.
23	Milloin oppilaitos tarvitsee opiskelijan suostumuksen henkilötietojen käsittelyyn?	Kun henkilötietoja käsitellään markkinointitarkoituksiin.
24	Mitä tarkoitetaan henkilötietojen käsittelyn oikeusperusteella?	Ilman oikeusperustetta tietojen käsittely on laitonta.
25	Milloin henkilötietojen käsittelyä voidaan jatkaa ilman suostumusta?	Kun käsittely on välttämätöntä velvoitteen täyttämiseksi.

26	Mitä tapahtuu, jos henkilö peruuttaa aiemmin antamansa suostumuksen tietojensa käsittelyyn?	Rekisterinpitäjän on lopetettava tietojen käsittely, ellei käsittelylle ole muuta laillista perustetta.
27	Mitä tarkoittaa käsittelyn läpinäkyvyys?	Rekisteröidyn on tiedettävä, miten, missä ja miksi hänen tietojaan käsitellään.
28	Mitkä asiat on huomioitava, kun luovutetaan opiskelijan henkilötietoja viranomaisille lain nojalla?	Tietojen luovuttaminen on tehtävä tarkasti lain asettamien vaatimusten mukaisesti.
29	Jos laki vaatii oppilaitosta säilyttämään opiskelijan tiedot tietyn ajan, mitä tulee tehdä, kun säilytysaika päättyy?	Poistaa tiedot tai anonymisoida ne niin, ettei niitä voi enää yhdistää opiskelijaan.
30	Kuinka varmistetaan, että henkilötietojen käsittely lakisääteisen velvoitteen perusteella on läpinäkyvää?	Läpinäkyvyyden varmistamiseksi rekisterinpitäjän tulee antaa rekisteröidyille yhteystiedot, joista he voivat kysyä lisätietoja henkilötietojensa käsittelystä lakisääteisen velvoitteen nojalla.
31	Oletko tietoinen siitä, missä tietosuojakäytäntöihin ja ohjeistuksiin liittyvä dokumentaatio sijaitsee organisaatiossasi?	
32	Tunnistatko tietoturvaloukkauksen?	
33	Oletko tietoinen, mitä tietoja organisaation tietosuojapolitiikka sisältää ja kuinka se vaikuttaa omaan työhösi?	
34	Kuinka varmaksi tunnet itsesi GDPR mukaisen tietosuojan toteuttamisessa omassa työssäsi?	
35	Onko pelaamisella vaikutusta tietosuojaosaamiseesi?	