jamk.fi

GDPR ja WordPress

Tero Paajoki

Opinnäytetyö
Toukokuu 2018
Tekniikan ja liikenteen ala
Insinööri (AMK), mediatekniikan koulutusohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Paajoki, Tero	Opinnäytetyö, AMK	Toukokuu 2018
	Sivumäärä 48	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
GDPR ja WordPress

Tutkinto-ohjelma
Mediatekniikan koulutusohjelma

Työn ohjaaja(t)
Kari Niemi

Toimeksiantaja(t)
Valu Digital Oy

Tiivistelmä

Opinnäytetyö toteutettiin Valu Digital Oy:lle ja sen ensimmäisenä tavoitteena oli koota uuden EU:n tietosuoja-asetuksen (GDPR) keskeisimmät teemat tiiviiksi tietopaketiksi. Toisena tavoitteena oli kehittää WordPress-lisäosa, joka vastaa GDPR:n vaatimuksiin ”Oikeus saada pääsy tietoihin” ja ”Oikeus siirtää tiedot järjestelmästä toiseen” WooCommerce-verkkokauppalisäosaa käytettäessä.

Aluksi lähdettiin selvittämään tietosuojan historiaa, jonka jälkeen siirryttiin selvittämään GDPR:n keskeisimpiä teemoja. Tarkastelun kohteena olivat GDPR:n perusperiaatteet, kattavuus, aikataulu, seuraamukset, rekisteröidyn oikeudet sekä rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet, haasteet ja edut.

Lisäosa rakennettiin standardien mukaisen WordPress Plugin Boilerplate -lisäosapohjan päälle. Jotta lisäosa vastasi GDPR:n vaatimuksiin, suunniteltiin, että se lataa JSON-tiedostona kaikki tietyn käyttäjän tilaus- ja henkilötiedot. Henkilötietojen latauspainike sijoitettiin WordPressin käyttäjänhallintasivulle ja sitä klikkaamalla oikeudet käyttäjänhallintaan omaava käyttäjä voi ladata kaikki sen henkilön tiedot, jonka hallintasivulla painiketta klikataan. Lisäosassa otettiin huomioon tietoturvallisuus kaikissa sen suorittamissa toimenpiteissä.

Sekä GDPR-tietopaketti että lisäosa täyttivät niille asetetut tavoitteet. Tietopaketti toimii mainiosti sisäänheittäjänä GDPR:n maailmaan ja lisäosa vastaa GDPR:n vaatimuksiin, joihin sen oli tarkoituskin vastata. Lisäksi lisäosa vahvistanee sitä käyttävän yrityksen luotettavuutta sekä mahdollistaa kilpailuedun saavuttamisen verkkokauppamarkkinoilla.

Avainsanat (asiasanat)
GDPR, EU:n tietosuoja-asetus, WordPress, WooCommerce, lisäosa, verkkokauppa

Muut tiedot (salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Paajoki, Tero	Bachelor's thesis	May 2018
		Language of publication: Finnish
	Number of pages 48	Permission for web publication: x

Title of publication
GDPR and WordPress

Degree programme
Media Engineering

Supervisor(s)
Niemi, Kari

Assigned by
Valu Digital Oy

Abstract

The thesis was assigned by Valu Digital Oy and the first aim was to bring together the key themes of the new General Data Protection Regulation into a comprehensive information packet. Another goal was to develop a WordPress plugin that is in line with GDPR's "Right of access by the data subject" and "Right to data portability" when using the WooCommerce web store plugin.

The start was to investigate the history of data protection, after which the most important themes of GDPR were went through. The focus was on the fundamental principles, coverage, timetable, penalties, rights of the data subject, and the responsibilities, challenges and benefits of the data controller, and data processor.

The plugin was built in accordance with the standard WordPress Plugin Boilerplate plugin foundation. For the plugin to respond to the requirements of GDPR, it was designed to download all order information and personal data of a specific user as a JSON file. Download button was placed on the WordPress User Edit page and clicking on it, the user with user rights can download all person's user data. The plugin took into account the security of information in all its actions.

Both the GDPR information packet and the plugin fulfilled the goals set for them. The information packet is an excellent entry into the world of GDPR, and the plugin corresponds to the requirements of the GDPR intended to meet. Additionally, the plugin can reasonably be believed to increase the confidence and competitive advantage of the company using it.

Keywords/tags (subjects)
GDPR, EU General Data Protection Regulation, WordPress, WooCommerce, plugin, web store

Miscellaneous (Confidential information)

Sisältö

1 Työn lähtökohdat 5

1.1 Tausta ja toimeksiantaja 5

1.2 Tehtävä ja tavoitteet 5

2 Ennen GDPR:ää - tietosuojan historiaa 6

2.1 Euroopan ihmisoikeussopimus 1950 7

2.2 OECD:n ohjeistus 1980 7

2.3 Henkilörekisterilaki 1988 9

2.4 EU:n tietosuojadirektiivi 1995 ja henkilötietolaki 1999 9

2.5 Erityissääntely 10

2.6 Suomen uusi tietosuojalaki 10

3 GDPR 10

3.1 Yleistä 10

3.2 Termistö 11

3.2.1 Henkilötieto (personal data) 11

3.2.2 Rekisterinpitäjä (data controller) 11

3.2.3 Henkilötietojen käsittelijä (data processor) 12

3.3 Kattavuus 12

3.4 Aikataulu 13

3.5 Valvonta 14

3.5.1 Riippumattomat valvontaviranomaiset 14

3.5.2 Seuraamukset 14

3.6 Rekisteröidyn oikeudet 15

3.6.1 Oikeus tulla unohdetuksi 15

3.6.2 Oikeus tietojen siirtämiseen 16

3.6.3 Oikeus tietojen oikaisemiseen 17

3.6.4 Oikeus käsittelyn rajoittamiseen 17

3.6.5 Oikeus saada pääsy tietoihin 18

3.7 Rekisterinpitäjät ja henkilötietojen käsittelijät 18

3.7.1 Henkilötietojen käsittelyä koskevat periaatteet 18

3.7.2 Tietosuojavastaava 19

3.7.3 Haasteet 20

3.7.4 Hyödyt 21

4 CASE: Lisäosa WooCommercen tilaustietojen ja WordPressin henkilötietojen lataukseen 22

4.1 WordPress 22

4.1.1 WordPress yleisesti 22

4.1.2 WordPress-lisäosa (plugin) 22

4.1.3 Toiminta- (action hook) ja suodatinkoukut (filter hook) 23

4.2 WooCommerce 23

4.3 WordPress Plugin Boilerplate 23

4.4 Lisäosan määrittely 24

4.5 Kehitys- ja testiympäristö 25

4.5.1 Vagrant 25

4.5.2 WooCommerce-verkkokauppa 25

4.6 Lisäosan toteutus 26

4.6.1 Rakenne lisäosalle 26

4.6.2 Painikkeen lisääminen käyttäjänhallintasivulle 27

4.6.3 Ajax-kutsu painiketta klikkaamalla 29

4.6.4 WooCommercen tietyn käyttäjän tilausten haku 30

4.6.5 WordPressin tietyn käyttäjän henkilötietojen haku 32

4.6.6 Sanitointi ja validointi 35

4.6.7 AJAX-kutsun lähteen tarkistus 35

4.6.8 Omien suodatinkoukkujen lisääminen 36

4.6.9 Tyylien lisääminen 36

4.6.10 Käännökset 37

5 Tulokset 38

6 Pohdinta 39

Lähteet 40

Liitteet 44

Liite 1. GDPR termit infografiikkana 44

Liite 2. Esimerkki ladatun JSON-tiedoston sisällöstä 45

Kuviot

Kuvio 1. Aikajana tietosuojan historiasta. 6
Kuvio 2. WordPress Plugin Boilerplaten rakenne. 24
Kuvio 3. Osuuspankin testitunnuksilla pääsee suorittamaan testimaksuja kuvitteelliselta tililtä 26
Kuvio 4. WordPress Plugin Boilerplate Generator 27
Kuvio 5. Käyttäjätietojen latauspainike käyttäjänhallintasivulla 28
Kuvio 6. Toimintakoukkuihin tartuttiin lisäosan Valu_Woouser_Downloader_Loader -luokan omalla funktiolla add_action. 28
Kuvio 7. AJAX-kutsun lähetys ja palautuneen datan lataus. 29
Kuvio 8. WordPressin tietokantataulut, joita WooCommerce käyttää. 31
Kuvio 9. Tilaustietojen hakeminen WooCommercen funktioilla ja moniuloitteisen taulukon luonti. 32
Kuvio 10. WordPressin käyttäjätietojen hakeminen ja mustan listan avainten poisto. 33
Kuvio 11. WordPress-käyttäjän henkilötiedot ovat näkyvillä ja osittain muokattavissa käyttäjänhallintasivulla. 33
Kuvio 12. Lisäosan toiminta vaihe vaiheelta kuvattuna 34
Kuvio 13. $_POST-pyyntö validoitiin ja sanitoitiin sekä token tarkistettiin wp_ajax_get_user_data -koukun kutsumassa get_wp_ajax_user_data -funktiossa .. 35
Kuvio 14. Suodatinkoukut lisättiin apply_filters -funktiolla. 36
Kuvio 15. CSS:llä määritelty ja animoitu loader-ikoni. 37
Kuvio 16. Käännettäväksi halutut tekstit sijoitettiin _e -funktion ensimmäiseksi parametriksi. 37
Kuvio 17. Lisäosan tekstit käännettiin Poeditillä. 38

1 Työn lähtökohdat

1.1 Tausta ja toimeksiantaja

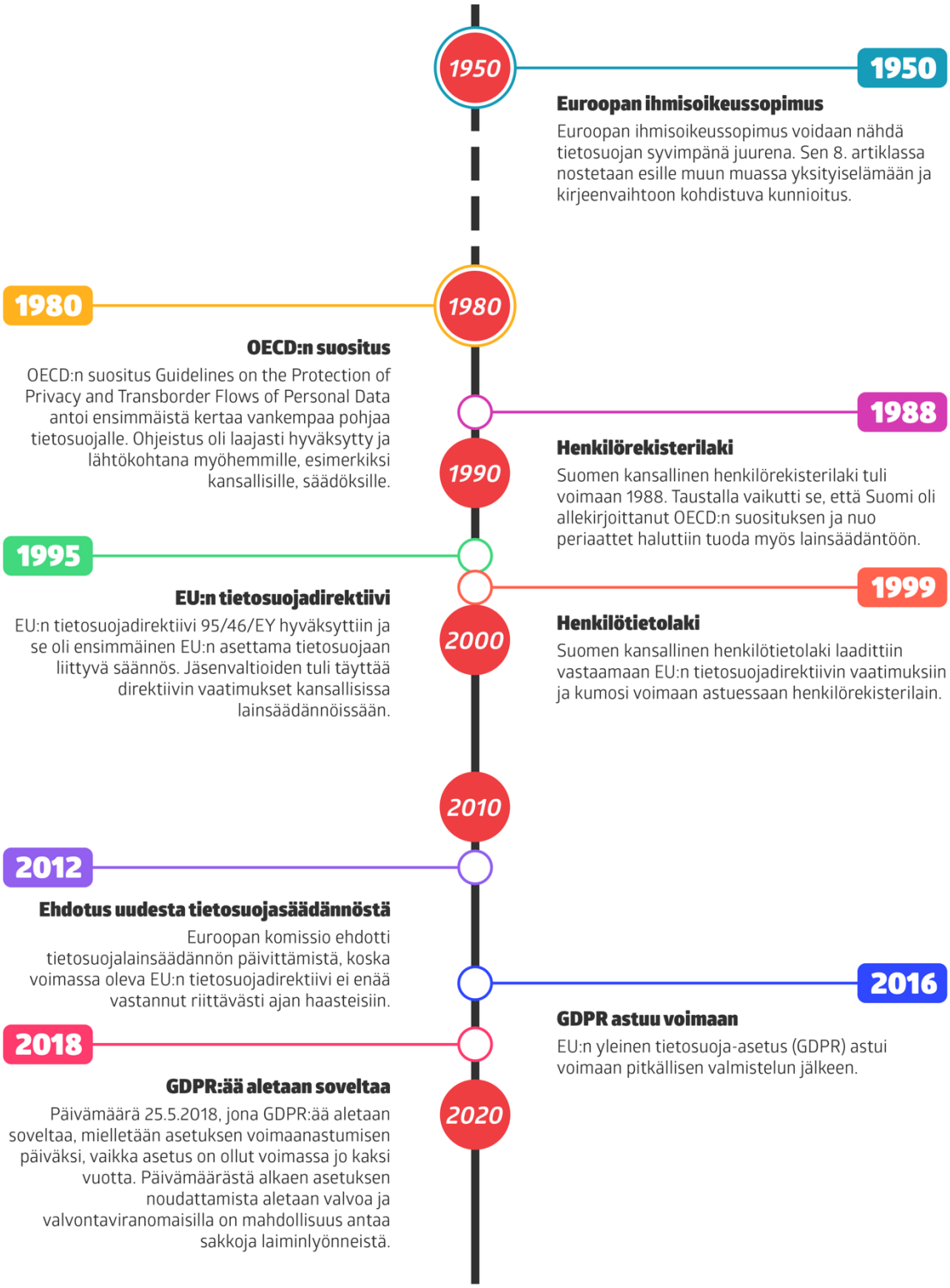
Opinnäytetyö vastasi tarpeeseen kehittää henkilötietojen käsittelyyn liittyviä prosesseja ja toimenpiteitä uuden EU:n tietosuoja-asetuksen (General Data Protection Regulation eli GDPR) vaatimusten mukaisiksi. Läheskään kaikki tietosuoja-asetuksen periaatteet eivät ole periaatteina uusia, mutta yksi keskeisin seikka on se, että uusi asetus määrittelee vaatimuksia ja rangaistuksia ennennäkemättömällä tavalla (EU:n yleinen tietosuoja-asetus - - n.d.). Organisaatioiden näkökulmasta asetus aiheuttaa enimmäkseen päänvaivaa, mutta myös hyötyjä tiedostetaan (Mitä jokaisen kuuluu tietää - - n.d.). Median suhteellisen aktiivisen uutisoinnin johdosta, yhä useammalle luonnolliselle henkilölle alkaa selkiytymään, että “tavallisten ihmisten mahdollisuudet kontrolloida henkilötietojensa käyttöä ovat paranemassa merkittävästi” (Pisto 2018).

Opinnäytetyön toimeksiantaja oli Valu Digital Oy, joka on yli 20-vuotias verkkopalveluiden tuottaja. Yritys toteuttaa verkkopalveluita aina konsepti- ja ilmesuunnittelusta tekniseen toteutukseen saakka. Myös diginäkyvyyden kehittäminen kuuluu keskeisesti Valu Digitalin repertuaariin. Yrityksen päätoimipiste sijaitsee Jyväskylässä, mutta myös Helsingissä on oma pieni etätoimisto. (Yritys n.d.)

1.2 Tehtävä ja tavoitteet

Opinnäytetyön tehtävänä oli käsitellä EU:n tietosuoja-asetus GDPR:n vaikutusta Valu Digitalissa toteutettavaan WordPress-kehitykseen. Tavoitteena oli laajan tietoperustan käsittelyn ja siitä muodostuvan selväkielisen tietopaketin kokoamisen lisäksi kehittää WordPress-lisäosa, joka mahdollistaa verkkokauppalisäosa WooCommercen ja WordPressin tallentaman tiettyyn henkilöön identifioitavissa olevan datan hakemisen ja lataamisen konekielisessä muodossa (JSON). Tehtävä vastaa osaltaan toukokuussa 2018 voimaan tulevan EU:n tietosuoja-asetus GDPR:n vaatimuksiin “Oikeus saada pääsy tietoihin” ja “Oikeus siirtää tiedot järjestelmästä toiseen”.

2 Ennen GDPR:ää - tietosuojan historiaa



Kuvio 1. Aikajana tietosuojan historiasta.

2.1 Euroopan ihmisoikeussopimus 1950

Voidaan sanoa, että GDPR:n syvimmät juuret ovat Roomassa 4. marraskuuta 1950 julkaistussa Euroopan ihmisoikeussopimuksessa (ECHR). Sen 8. artiklassa otsikolla "Oikeus nauttia yksityis- ja perhe-elämän kunnioitusta" sanotaan:

> *1. Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.*
>
> *2. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.*
>
> (Euroopan ihmisoikeussopimus 1998, 8. artikla.)

2.2 OECD:n ohjeistus 1980

Euroopan ihmisoikeussopimuksen artikla on osaltaan OECD:n 1980 antaman ohjeistuksen Guidelines on the Protection of Privacy and Transborder Flows of Personal Data lähtökohtana (OECD Guidelines on the Protection - - 1980). Ohjeistuksesta tuli laajasti kansainvälisesti hyväksytty henkilötietojen käsittelyä koskeva sääntökokoelma (Bałazińska 2016). Ohjeistus sisältää kahdeksan kohtaa:

1) Keräämisen rajoittaminen

Henkilötietoja tulisi kerätä laillisin ja oikeudenmukaisin keinoin. Tarvittaessa asianomaiselle tulisi kertoa tietojen keräämisestä tai siihen pitäisi olla asianomaisen suostumus. (OECD Guidelines on the Protection - - 1980; Bałazińska 2016.)

2) Tietojen tarkoituksellisuus

Henkilötietojen tulisi olla merkityksellisiä keräämisen tarkoitusta ajatellen (OECD Guidelines on the Protection - - 1980; Bałazińska 2016).

3) Tarkoitusten määrittely

Tietojen keräämisen tarkoitukset tulisi määritellä keräämishetkellä (OECD Guidelines on the Protection - - 1980; Bałazińska 2016).

4) Käytön rajaus

Tietoja ei tulisi käyttää muihin tarkoituksiin kuin keräämishetkellä ilmoitettuihin tarkoituksiin. Poikkeuksena:

1. Rekisteröidyn suostumuksella
2. Lain edessä (OECD Guidelines on the Protection - - 1980; Bałazińska 2016.)

5) Turvatoimet

Henkilötiedot tulisi suojata kohtuullisilla turvatoimilla, jotta voitaisiin estää muun muassa luvaton tietojen hävittäminen, käyttö, muokkaaminen, paljastaminen tai ylipäätään tietoihin pääsy (OECD Guidelines on the Protection - - 1980; Bałazińska 2016).

6) Avoimuus

Henkilötietojen sisällön ja käyttötarkoituksen sekä rekisterinpitäjän henkilöllisyyden ja tavanomaisen sijainnin tulisi olla helposti saatavilla (OECD Guidelines on the Protection - - 1980; Bałazińska 2016).

7) Osallisuus tietoihin

Yksilöllä tulisi olla oikeus:

1. Tietää sisältääkö rekisteri omia tietoja
2. Saada tieto kohtuullisessa ajassa, veloituksetta tai edullisesti, kohtuullisella tavalla ja helposti ymmärrettävässä muodossa
3. Saada perustelut, mikäli kohtia 1 ja 2 ei toteuteta
4. Vaatia muutosta virheellisiin tietoihin (OECD Guidelines on the Protection - - 1980; Bałazińska 2016.)

8) Vastuu

Rekisterinpitäjä on vastuussa toimenpiteistä, joita edellä mainittujen periaatteiden noudattaminen vaatii (OECD Guidelines on the Protection - - 1980; Bałazińska 2016).

2.3 Henkilörekisterilaki 1988

Suomi allekirjoitti OECD:n suosituksen, ja muun muassa sen johdattelemana hallitus laati vuonna 1986 esityksen henkilörekisterilaista (HE 49/1986, 20). Henkilörekisterilaki hyväksyttiin 1987 ja tuli voimaan vuoden 1988 alusta (Henkilörekisterilaki 471/1987, 49 §). Laki pohjautui paljolti OECD:n suosituksiin (Henkilörekisterilaki 471/1987).

2.4 EU:n tietosuojadirektiivi 1995 ja henkilötietolaki 1999

Vuonna 1995 hyväksyttiin EU:n tietosuojadirektiivi 95/46/EY ja jäsenvaltioiden tuli tuolloin täyttää kansallisissa lainsäädännöissään direktiivin vaatimukset kolmen vuoden sisällä. Heinäkuussa 1998 Suomen hallitus tekikin esityksen, että vuoden 1987 henkilörekisterilain korvaisi uusi henkilötietolaki.

Tietosuojadirektiivi oli luonnollisesti liikkeellepaneva voima uuden lain esitykselle, mutta esityksessä todettiin myös tarve lain päivittämiselle. Nopean teknologisen ja yhteiskunnallisen kehittymisen tähden lakiin kaivattiin ajanmukaistamista, täsmentämistä ja selkiyttämistä, mutta todettiin kuitenkin myös, että perusteelliselle kokonaisuudistukselle ei ole tarvetta. (HE 96/1998.) OECD:n suositusten ja sitä kautta henkilörekisterilain antama pohja oli perusteiltaan niin hyvä. Uusi henkilötietolaki tuli voimaan 1. kesäkuuta 1999 (HE 96/1998).

EU:n tietosuojadirektiivi 95/46/EY on voimassa 25. toukokuuta 2018 saakka, jolloin se GDPR:n artiklan 94 nojalla kumotaan (Yleinen tietosuoja-asetus 2016/679, 94. artikla).

2.5 Erityissääntely

Tietosuojan sääntely Suomessa pohjautuu tällä hetkellä henkilötietolain lisäksi eri toimialoilla vallitseviin erityislakeihin. Syynä erityissääntelyyn voi olla muun muassa se, että käsiteltävät henkilötiedot ovat hyvin arkaluonteisia. (Ylipartanen & Andreasson 2015.)

2.6 Suomen uusi tietosuojalaki

GDPR:n vaatimukset tulee laittaa täytäntöön kansallisissa lainsäädännöissä ja siksi Suomen hallitus jättikin 1.3.2018 eduskunnalle esityksen uudesta tietosuojalaista. Laki tulee voimaan samana päivänä kuin GDPR:ää aletaan soveltaa 25.5.2018. (EU:n yleisen tietosuoja-asetuksen (GDPR) - - 2018; HE 9/2018.)

3 GDPR

3.1 Yleistä

Prosessi tietosuojalainsäädännön päivittämisestä alkoi tammikuussa 2012 Euroopan komission ehdottaessa asiaa (GDPR Timeline of Events n.d.). Ehdotus lähti tarpeesta, sillä vuonna 1995 asetettu tietosuojadirektiivi oli auttamatta jäänyt jälkeen valtavasta globaalin tietoympäristön olosuhteiden ja verkon palvelujen toimintamallien kehityksestä. Tavoitteena oli turvata henkilötietojen suojaa perusoikeutena ja digitaalitalouden kehitystä, yhtenäistää EU:n alueen käytäntöjä sekä tehostaa rikollisuuden ja terrorismin torjuntaa. (Karhula & Kipinoinen 2017; Mitä jokaisen kuuluu tietää - - n.d.)

Euroopan parlamentti hyväksyi oman versionsa asetuksesta vuonna 2014 ja Euroopan unionin neuvosto kesällä 2015. Syksyn 2015 aikana parlamentti ja neuvosto kävivät asetusta läpi ja pääsivät 15. joulukuuta 2015 sopimukseen sisällöstä ja virallisten hyväksyntöjen jälkeen yleinen tietosuoja-asetus eli GDPR astui voimaan 24. toukokuuta 2016. (GDPR Timeline of Events n.d.)

Koska 2012 käynnistetyn prosessin tavoitteena oli myös rikollisuuden ja terrorismin torjunta, syntyi yleisen tietosuoja-asetuksen lisäksi tietosuojadirektiivi 2016/680, joka koskee nimenomaan rikosasioiden yhteydessä poliisin ja oikeuslaitoksen henkilötietojen käsittelyä. Tietosuojadirektiivi korvaa vuonna 2008 annetun puitepäätöksen. (EU:n tietosuojauudistus ja sen kansallinen täytäntöönpano; Tietosuojadirektiivi (EU) 2016/680.) Tässä opinnäytetyössä tuohon direktiiviin ei kuitenkaan paneuduta tämän enempää.

Karkeasti tiivistäen GDPR täsmentää ja selventää aiempia asetuksia ja vaatimuksia, mutta tuo mukanaan myös uusia velvoitteita ja seuraamuksia (Ylipartanen & Andreasson 2015). Ohjelmistoyritys Isolta on tiivistänyt GDPR:n keskeisimmän sisällön osuvasti yhteen kuvaan (Liite 1) (Happonen 2018).

3.2 Termistö

3.2.1 Henkilötieto (personal data)

Henkilötiedoilla tarkoitetaan tietoja, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Henkilö voi olla tunnistettavissa suoraan tai epäsuorasti erilaisten tunnistetietojen (nimi, henkilötunnus, sijaintitieto, verkkotunnistetieto) tai tunnusomaisten piirteidensä (fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä) vuoksi. Tunnistetusta tai tunnistettavissa olevasta luonnollisesta henkilöstä käytetään termiä rekisteröity ja niin tässä dokumentissakin. (Yleinen tietosuoja-asetus 2016/679, 4. artikla.)

3.2.2 Rekisterinpitäjä (data controller)

Rekisterinpitäjä on taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä voi olla luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin. (Yleinen tietosuoja-asetus 2016/679, 4. artikla.)

3.2.3 Henkilötietojen käsittelijä (data processor)

Henkilötietojen käsittelijä on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun eli käytännön käsittelyn suorittava tai järjestelmän sitä varten luova taho. Henkilötietojen käsittelijä voi olla luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin. (Yleinen tietosuoja-asetus 2016/679, 4. artikla.)

3.3 Kattavuus

GDPR:ää sovelletaan kaikkeen osittain tai täysin automatisoituun henkilötietojen käsittelyyn. Lisäksi soveltamisalaan kuuluu kaikki manuaalinen henkilötietojen käsittely, jonka tuloksena syntyy tai on tarkoitus syntyä rekisterin osa. (Yleinen tietosuoja-asetus 2016/679, 2. artikla.) Esimerkiksi paperiseen arkistoon sovelletaan yhtä lailla henkilötietojen käsittelyä koskevia periaatteita kuin sähköiseenkin arkistoon (Kattilakoski 2017).

GDPR:ää ei sovelleta henkilötietojen käsittelyyn, “jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan” ja “jota suorittavat jäsenvaltiot toteuttaessaan SEU V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa”. SEU on sopimus Euroopan unionin toiminnasta ja V osaston 2 luku siinä koskee rajavalvonta-, turvapaikka- ja maahanmuuttopolitiikkaa. (Yleinen tietosuoja-asetus 2016/679, 2. artikla.)

GDPR ei tietysti koske myöskään henkilökohtaisessa tai kotitalouteensa liittyvässä toiminnassa luonnollisen henkilön suorittamaa henkilötietojen käsittelyä (Yleinen tietosuoja-asetus 2016/679, 2. artikla).

EU:n toimielimet, elimet ja laitokset soveltavat henkilötietojen käsittelyyn asetusta (EY) N:o 45/2001. Tuo ja muut vastaavat säädökset tulee mukauttaa GDPR:n periaatteiden mukaisiksi. Tällä varmistetaan, ettei EU:n sisäisillä hallintojärjestelmillä ole erityisoikeuksia GDPR:n edessä. (Yleinen tietosuoja-asetus 2016/679, 2. artikla.)

GDPR ei rajoita direktiivin 2000/31/EY soveltamista etenkään sen artiklojen 12–15 osalta. Direktiiviä 2000/31/EY kutsutaan direktiiviksi sähköisestä kaupankäynnistä, ja sen artiklat 12–15 koskevat välittäjinä toimivien palveluntarjoajien vastuuta. Asetus

vapauttaa tiedon välittäjänä toimivan palveluntarjoajan vastuusta valvoa liikkuvaa dataa. Palveluntarjoalla on kuitenkin velvollisuus ilmoittaa viranomaisille mahdollisista palvelun vastaanottajan väitetyistä laittomista toimista ja luovuttaa pyynnöstä palvelun vastaanottajaan identifioitavia tietoja viranomaisille. (Yleinen tietosuoja-asetus 2016/679, 2. artikla; Direktiivi 2000/31/EY, 12-15. artiklat.)

Alueellisesti GDPR:ää sovelletaan mikäli rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikka, jossa henkilötietojen käsittelyyn liittyvä toiminta tapahtuu, sijaitsee EU:n sisällä. Sillä ei ole merkitystä, missä käsittely tapahtuu fyysisesti. Mikäli rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikka, jossa henkilötietojen käsittelyyn liittyvä toiminta tapahtuu, sijaitsee EU:n ulkopuolella, sovelletaan GDPR:ää vain, jos unionin alueella olevan rekisteröidyn henkilötietojen käsittely liittyy “tavaroiden tai palvelujen tarjoamiseen näille rekisteröidyille unionissa riippumatta siitä, edellytetäänkö rekisteröidyltä maksua” tai “näiden rekisteröityjen käyttäytymisen seurantaan siltä osin kuin heidän käyttäytymisensä tapahtuu unionissa”. Jos rekisterinpitäjä toimii EU:n ulkopuolella paikassa, jossa sovelletaan jonkin jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla, sovelletaan siellä silloin myös GDPR:ä. (Yleinen tietosuoja-asetus 2016/679, 3. artikla.)

3.4 Aikataulu

GDPR astui voimaan jo 24.5.2016, mutta sitä aletaan soveltamaan kahden vuoden siirtymäajan jälkeen eli 25.5.2018. GDPR:n kansallista soveltamista varten oikeusministeriö asetti täytäntöönpanotyöryhmän (TATTI), joka ehdotti mietinnössään Suomeen uutta tietosuojalakia, joka astuisi voimaan niin ikään 25.5.2018. (Yleinen tietosuoja-asetus 2016/679, 99. artikla; EU:n tietosuojauudistus 2017; EU:n tietosuojauudistus ja sen kansallinen täytäntöönpano 2017; EU:n yleisen tietosuoja-asetuksen - - 2017.)

3.5 Valvonta

3.5.1 Riippumattomat valvontaviranomaiset

Jokaisen jäsenvaltion tulee nimittää yksi tai useampi valvontaviranomainen valvomaan asetuksen soveltamista. Nimittäjänä toimii jäsenvaltion riippumaton elin, esimerkiksi jäsenvaltion hallitus, ja nimittäminen tapahtuu mahdollisimman läpinäkyvällä menettelyllä. Valvontaviranomaisille tulee luoda hyvät edellytykset hoitaa tehtäväänsä mahdollisimman tehokkaasti: välineet, tilat, infrastruktuuri ja henkilöstö. Mikäli jäsenvaltiolla on useampi valvontaviranomainen, tulee jäsenvaltion nimetä yksi edustamaan viranomaisia unionin tietosuojaneuvostossa. Valvontaviranomaisten yhteistyöllä pyritään varmistamaan asetuksen yhdenmukainen soveltaminen kaikissa jäsenvaltioissa. (Yleinen tietosuoja-asetus 2016/679, 51-53. artiklat.)

Asetuksen soveltamisen valvonta- ja täytäntöönpanotyön lisäksi valvontaviranomaisella on merkittävä rooli asetukseen liittyvän tietoisuuden ja ymmärryksen lisäämisessä niin kansallisille toimielimille, rekisterinpitäjille, henkilötietojen käsittelijöille kuin luonnollisille henkilöillekin. Valvontaviranomainen on velvollinen käsittelemään ja tutkimaan kohtuudella rekisteröidyn tai jonkin elimen tekemiä valituksia ja ilmoittamaan tutkinnan etenemisestä ja tuloksista. Rikkomuksista ja toimenpiteistä tulee pitää rekisteriä. Valvontaviranomainen on vastuussa myös muun muassa asetuksen soveltamiseen keskittyvästä tutkimustyöstä. Tehtävälistan viimeinen kohta kiteyttää tehtävän laajuuden: “jokaisen valvontaviranomaisen on alueellaan suoritettava mitä tahansa muita henkilötietojen suojaan liittyviä tehtäviä”. (Yleinen tietosuoja-asetus 2016/679, 57. artikla.)

Tulevaan Suomen kansalliseen tietosuojalakiin on tarkoitus säätää, että riippumattoman valvontaviranomaisen tehtäviä Suomessa tulisi hoitamaan tietosuojavaltuutettu. (Tietopaketti yrityksille - - n.d.)

3.5.2 Seuraamukset

Valvontaviranomainen valvoo, että “sakkojen määrääminen tämän artiklan mukaisesti on kussakin yksittäisessä tapauksessa tehokasta, oikeasuhteista ja varoittavaa”.

Sakon suuruuteen vaikuttavat muun muassa rikkomuksen tahallisuus, luonne, kesto, kohteeksi joutuneiden määrä, vahingon suuruus, aiemmat rikkomukset, pyrkimykset lieventää aiheutuneita vahinkoja, yhteistyökykyisyys valvontaviranomaisen kanssa, ilmitulotapa sekä mahdolliset rekisterinpitäjän rikkomuksella saavutetut taloudelliset edut tai vältetyt tappiot. (Yleinen tietosuoja-asetus 2016/679, 83. artikla.)

Sakkotasoja on kaksi riippuen artikloista, joita on rikottu. Ensimmäisen tason sakko "on enintään 10 000 000 euroa, tai jos kyseessä on yritys, kaksi prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi". Toisen tason sakko "on enintään 20 000 000 euroa, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi". Ensimmäisen tason sakon voi saada muun muassa rekisterinpitäjän velvollisuuksien laiminlyönneistä, esimerkiksi tietosuojavastaavan nimeämättä jättämisestä, ja toisen tason sakon rekisteröidyn oikeuksien laiminlyönneistä, esimerkiksi rekisteröidyn "oikeus tietojen siirtämiseen" laiminlyönnistä. (Yleinen tietosuoja-asetus 2016/679, 83. artikla.)

3.6 Rekisteröidyn oikeudet

3.6.1 Oikeus tulla unohdetuksi

Oikeus tietojen poistamiseen, josta useissa yhteyksissä puhutaan "oikeutena tulla unohdetuksi", tarkoittaa yksinkertaistetusti sitä, että rekisteröidyllä on oikeus pyytää rekisterinpitäjää poistamaan itseään koskevat henkilötiedot rekisterinpitäjän järjestelmästä. Rekisterinpitäjällä on tällöin velvollisuus poistaa tiedot viivyttelemättä, mikäli tietoja ei enää tarvita siihen tarkoitukseen, johon ne alun perin kerättiin, rekisteröity peruuttaa suostumuksensa käsittelyyn, eikä käsittelylle ole muita laillisia perusteita tai tietoja on käsitelty lainvastaisesti. (Yleinen tietosuoja-asetus 2016/679, 17. artikla.)

Mikäli rekisterinpitäjä on julkistanut henkilötiedot ja ne ovat myös muiden rekisterinpitäjien käytössä, tulee kyseisen rekisterinpitäjän pyrkiä omien kohtuullisten resurs-

sien puitteissa pyytämään myös näitä muita rekisterinpitäjiä poistamaan kaikki rekisteröityyn liittyvien henkilötietojen kopiot ja jäljennökset sekä linkit kyseisiin henkilötietoihin (Yleinen tietosuoja-asetus 2016/679, 17. artikla).

Oikeutta tulla unohdetuksi ei sovelleta, jos käsittelyssä on kyse sananvapauden tai tiedonvälitysvapauden käytöstä. Poisto-oikeuden edelle menevät myös tarpeet noudattaa muita lakisääteisiä velvoitteita, suorittaa yleistä etua koskevaa tehtävää, käyttää rekisterinpitäjälle kuuluvaa julkista valtaa, ajaa kansanterveyden yleistä etua sekä tutkia, arkistoida tai tilastoida henkilötietoja tietyin edellytyksin. (Yleinen tietosuoja-asetus 2016/679, 17. artikla.)

3.6.2 Oikeus tietojen siirtämiseen

Rekisteröidyllä on oikeus pyytää ja saada henkilötietonsa "jotka hän on toimittanut rekisterinpitäjälle" ja halutessaan siirtää ne toisen rekisterinpitäjän käyttöön. Muodon tulee olla yleisesti käytetty koneellisesti luettava muoto. Mikäli se vain on teknisesti mahdollista, rekisteröidyllä on oikeus saada siirrettyä tietonsa suoraan rekisterinpitäjältä toiselle. Siirto-oikeus toteutuu, mikäli käsittely perustuu asetuksen mukaiseen suostumukseen tai sopimukseen, ja henkilötietojen käsittely on automaattista. Siirto-oikeus ei koske tilanteita, jolloin henkilötietojen käsittely on osa tehtävää, joka on tarpeellinen yleisen edun tai julkisen vallankäytön kannalta. (Yleinen tietosuoja-asetus 2016/679, 20. artikla.)

EU:n oikeus- ja sisäasioiden neuvosto päätti viime hetkellä muokata komission ehdotusta siten, että sanamuodoksi tuli "jotka hän on toimittanut" (Ihmiskeskeinen tiedonhallinta - - 2017). Sanamuoto herätti aluksi jonkin verran keskustelua siitä, mikä tieto on rekisteröidyn itsensä toimittamaa ja mikä taas ei, sekä kritiikkiä siitä, että useat tahot olivat jättäneet huomioimatta tuon oleellisen sanamuodon. Jari Perko (2016) nosti kritiikissään esimerkiksi julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) raportin EU-tietosuojan kokonaisuudistuksesta, jossa mainitaan, että "rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot" ilman minkäänlaista mainintaa tietojen toimittamisen kriteeristä (EU-tietosuojan kokonaisuudistus 2016). Perko toteaakin sen, että rekisteröity voisi siirtää nimenomaan kaiken häntä koskevan tiedon muualle, olevan yleinen väärä luulo GDPR:än liittyen. (Perko 2016.)

EU:n tietosuojatyöryhmän ohjeistus selventää asiaa perusteellisesti. Työryhmä jaottelee henkilötiedot alkuperänsä mukaan kolmeen ryhmään: ensimmäisenä ”rekisteröidyn aktiivisesti ja tietoisesti toimittamat tiedot”, toisena “havainnoidut tiedot, jotka rekisteröity on toimittanut käyttämällä palvelua tai laitetta” sekä kolmantena päätellyt ja johdetut tiedot. Rekisteröidyn aktiivisesti toimittamat tiedot ovat selkeästi rekisteröidyn toimittamia, mutta myös havainnoidut tiedot voidaan työryhmän mukaan laskea toimitetuiksi tiedoiksi. Esimerkiksi jonkin laitteen keräämät sijaintitiedot ovat tällaista tietoa. Sen sijaan päätellyt ja johdetut tiedot eivät työryhmän mukaan kuulu rekisteröidyn toimittamien tietojen joukkoon, joten niitä ei siirtoa pyydettäessä tarvitse kerätä mukaan. Päätellyillä ja johdetuilla tiedoilla tarkoitetaan luonnollisestikin tietoja, jotka ovat tavalla tai toisella johdettu rekisteröidyn toimittamista tiedoista. Esimerkiksi jos järjestelmä tekee johtopäätöksiä henkilön profiilista analysoimalla rekisteröidyn toimittamia tietoja algoritmin avulla, nuo analyysin tulokset eivät ole tällöin rekisteröidyn toimittamia henkilötietoja ja eivät täten kuulu siirto-oikeuden piiriin. (Oikeutta tietojen siirtämiseen - - 2017, 10-11.)

3.6.3 Oikeus tietojen oikaisemiseen

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää oikaisemaan ja täydentämään henkilötietonsa ilman viivytyksiä. Huomioon täytyy kuitenkin ottaa henkilötietojen käyttötarkoitus. (Yleinen tietosuoja-asetus 2016/679, 16. artikla.)

3.6.4 Oikeus käsittelyn rajoittamiseen

Rekisterinpitäjän tulee pyydettäessä rajoittaa henkilötietojen käsittelyä mikäli henkilötiedot eivät ole paikkansapitäviä, “käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajoittamista”, rekisteröidyllä on oikeudellinen tarve säilyttää tiedot rekisterinpitäjällä vaikka rekisterinpitäjä ei tarvitsisi henkilötietoja enää sen alkuperäisiin tarkoituksiin tai käynnissä on ajanjakso jolloin osapuolet odottavat rekisteröidyn henkilötietojen käsittelyn vastustamisen validiteetin todentamista. Tietojen käsittelyn rajoitukseen voidaan tehdä poikkeus vain rekisteröidyn suostumuksesta, oikeudellisista syistä, muiden henkilöiden oikeuksien suojaamiseksi taikka unionin tai jäsenvaltion yleisen edun vuoksi. (Yleinen tietosuoja-asetus 2016/679, 18. artikla.)

3.6.5 Oikeus saada pääsy tietoihin

Oikeus saada pääsy tietoihin tarkoittaa ensinnäkin sitä, että rekisteröidyllä on oikeus saada tietää, käsitteleekö rekisterinpitäjä rekisteröidyn henkilötietoja vai ei, ja mikäli käsittelee, rekisteröidyllä on oikeus nähdä omat tietonsa. Lisäksi rekisteröidyllä on oikeus tietää henkilötietojen käsittelyn tarkoitukset, mahdolliset tahot joille tietoja luovutetaan erityisesti kolmansissa maissa, tietojen säilytysaika, asetuksen mukaiset tiedot rekisteröidyn oikeuksista, henkilötietojen alkuperä, mikäli on muu kuin rekisteröity itse, mahdollisesta profiloinnista tai vastaavasta käsittelystä sekä kyseisen käsittelyn logiikasta ja seurauksista. (Yleinen tietosuoja-asetus 2016/679, 15. artikla.)

Rekisterinpitäjän tulee toimittaa jäljennös rekisteröidyn henkilötiedoista yleisesti käytetyssä sähköisessä muodossa. Rekisteröidyllä on kuitenkin oikeus pyytää tietoja myös muussa kuin sähköisessä muodossa. (Yleinen tietosuoja-asetus 2016/679, 15. artikla.)

3.7 Rekisterinpitäjät ja henkilötietojen käsittelijät

3.7.1 Henkilötietojen käsittelyä koskevat periaatteet

Rekisterinpitäjillä ja henkilötietojen käsittelijöillä on rekisteröidyn oikeuksiin vastaamisen lisäksi keskeisenä velvoitteena noudattaa yleisiä henkilötietojen käsittelyä koskevia periaatteita, joita on seitsemän:

1) Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Käsittelyn tulee olla rekisteröidyn näkökulmasta läpinäkyvää, lainmukaista, kohtuullista ja asianmukaista (Yleinen tietosuoja-asetus 2016/679, 5. artikla).

2) Käyttötarkoitussidonnaisuus

Henkilötietoja saa käsitellä vain alkuperäisten tarkoitusten mukaisesti (Yleinen tietosuoja-asetus 2016/679, 5. artikla).

3) Tietojen minimointi

Henkilötietoja tulee säilyttää mahdollisimman minimaalinen määrä. Mikäli tiedot eivät ole relevantteja käyttötarkoituksen kannalta, niitä ei tule säilyttää. (Yleinen tietosuoja-asetus 2016/679, 5. artikla.)

4) Täsmällisyys

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee pyrkiä kohtuullisin toimenpitein siihen, että henkilötiedot olisivat mahdollisimman paikkansapitäviä ja riittävän tarkkoja käsittelyn tarkoituksiin nähden (Yleinen tietosuoja-asetus 2016/679, 5. artikla).

5) Säilytyksen rajoittaminen

Henkilötietoja ei saa säilyttää tunnistettavassa muodossa pidempään kuin mitä käsittelyn tarkoituksen kannalta on tarpeen (Yleinen tietosuoja-asetus 2016/679, 5. artikla).

6) Eheys ja luottamuksellisuus

Henkilötietojen käsittelyn on oltava tietoturvallista (Yleinen tietosuoja-asetus 2016/679, 5. artikla).

7) Osoitusvelvollisuus

Rekisterinpitäjän tulee kyetä osoittamaan, että organisaatio on noudattanut edellä esitettyjä periaatteita (Yleinen tietosuoja-asetus 2016/679, 5. artikla).

3.7.2 Tietosuojavastaava

Rekisterinpitäjän tulee nimittää tietosuojavastaava kolmessa eri tapauksessa. Ensinnäkin silloin, jos tietojenkäsittelijä on julkishallinnon toimija, mutta ei kuitenkaan tuomioistuin. Toisekseen silloin, jos rekisterinpitäjän tai henkilötietojen käsittelijän toiminta on luonteeltaan, laajuudeltaan ja tarkoitukseltaan sellaista, että se vaatii rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Ja kolmanneksi silloin, jos käsittelytoimet ovat laajamittaisia ja käsiteltävät henkilötiedot erityisen henkilökohtaisia (esimerkiksi terveystiedot, etninen alkuperä tai uskonnollinen vakaumus) tai ri-

koksia koskevia. Tietosuojavastaavia tulee olla konsernissa vain yksi ja hänen yhteystietonsa tulee olla valvontaviranomaisen tiedossa. (Yleinen tietosuoja-asetus 2016/679, 37. artikla; Tietosuojavastaavat 2017.)

Tietosuojavastaavan on oltava mukana kaikkien konsernin henkilötietojen suojaa koskevien kysymysten käsittelyissä. Vastaavan yksi keskeinen tehtävä on olla tiedonvälittäjänä asetuksen noudattamiseen liittyvissä kysymyksissä koko organisaatiossa. Tiedonvälittämisen ja neuvonnan lisäksi tietosuojavastaava seuraa asetuksen noudattamista organisaatiossa. Tietosuojavastaava on yhteyshenkilö organisaatiosta sekä valvontaviranomaisen että rekisteröityjen suuntaan. (Yleinen tietosuoja-asetus 2016/679, 38-39. artikla; Tietosuojavastaavat 2017.)

3.7.3 Haasteet

Yksi keskeinen GDPR:n mukanaan tuoma ongelma useille yrityksille ja organisaatioille on se, että olemassa oleva tieto on tällä hetkellä hajallaan niin sanotuissa rakenteettomissa tiedoissa: Word-dokumentit, PDF-dokumentit, lokitiedostot, tekstikentät intranetissä, kuvien metatiedot ja paperiarkistot. Rekisterinpitäjälle voi olla todella työlästä kartoittaa GDPR:n soveltamisen alkaessa kaiken tiedon sijaintia ja kartoituksen jälkeen pohtia, kuinka tieto kannattaisi järjestellä niin, että GDPR:n ehdot tulisi täytettyä. Esimerkiksi mikäli rekisteröity pyytää oikeuksiensa mukaan kaikkia omia tietojaan, voi rekisterinpitäjä olla melkoisen haasteen edessä, jos tieto sijaitsee täysin pirstaloituneesti siellä täällä. (Mitä jokaisen kuuluu tietää - - n.d.)

Organisaatioiden järjestäytyminen toimimaan GDPR:n vaatimusten mukaan, on suuri haaste. Se, että henkilöstö jatkossa tietäisi, kuinka tulee toimia ja mihin pyrkiä, jotta toiminta olisi laillista ja turvallista, ei ole helppo askel. Tai se, että prosessit tuottaisivat lainmukaisia henkilötietoja ja pitäisi yllä lainmukaisuutta, ei sekään ole välttämättä helppo askel. Yksi suositus prosessien helpottamiseksi onkin, että data olisi aina, kun mahdollista, anonymisoitua. (Mitä jokaisen kuuluu tietää - - n.d.) Prosessien parantaminen tulee väistämättä vaatimaan organisaatioilta myös järjestelmäinvestointeja (Kerttula 2017).

Haasteet ovat mittavia, ja todennäköisesti kaikki asiat kaikissa organisaatioissa eivät ole ratkaistuna vielä, kun asetusta aletaan soveltaa 25.5.2018. Esimerkiksi kuntasektorilla on esitetty toiveita siitä, että jokaisen ei tarvitsisi keksiä pyörää uudestaan vaan kokemuksia ja toimivia malleja voisi jakaa ja miettiä yhdessä (Lehto 2017). Asetus on lisännyt organisaatioiden motivaatiota toimia yhtenäisesti, koska GDPR todella koskettaa jokaista (Mitä jokaisen kuuluu tietää - - n.d.).

3.7.4 Hyödyt

Henkilötietojen pitäminen hyvässä järjestyksessä, ajanmukaisina ja helposti käsiteltävinä saattaa tuoda jatkossa organisaatioille merkittäviä säästöjä. Myös erilaisten analyysien ja sisäisten tutkimusten tekeminen helpottuu ja ne ovat totuudenmukaisempia. (Mitä jokaisen kuuluu tietää - - n.d.)

Lisäksi asetuksen mallikkaalla noudattamisella on iso merkitys asiakkaiden silmissä ja siksi se luo yrityksille luotettavampaa imagoa ja kilpailuetua. Erityisesti nopeimpien GDPR:n noudattajien uskotaan saavuttavan kilpailuetua. (Hilmansson 2017; Mitä jokaisen kuuluu tietää - - n.d.)

Kaija Puranen (2017) näkee Suomen GDPR:stä suuresti hyötyvänä yhteiskuntana. Monet tekijät luovat Purasen mukaan edellytyksiä sille, että Suomen kansalaisten elämänlaatu voi parantua GDPR:n vaikuttamien toteutusten ja järjestelmien myötä. Tällaisina tekijöinä hän näkee muun muassa läpinäkyvyyden lainsäädännössä, muutoshalukkaat virastot, AI-osaamisen, koneluettavat rajapinnat ja innovatiiviset startupit.

Rekisteröidyn tietojen siirto-oikeuden uskotaan edistävän kilpailua ja uusien digitaalisten palveluiden syntymistä EU:n alueella (Kerttula 2017).

4 CASE: Lisäosa WooCommercen tilaustietojen ja WordPressin henkilötietojen lataukseen

4.1 WordPress

4.1.1 WordPress yleisesti

WordPress on avoimen lähdekoodin julkaisujärjestelmä, jonka Mike Little ja Matt Mulenweg loivat 2003 blogialusta b2/cafelogin pohjalta. Avoimen lähdekoodin julkaisujärjestelmällä tarkoitetaan sivuston sisällön julkaisuun ja ylläpitoon käytettävää järjestelmää, jonka lähdekoodin kopioiminen ja muokkaaminen omiin kaupallisiinkin tarkoitusperiin on sallittua. WordPress on rakennettu PHP:lla ja MySQL:llä. Jo yli 30% maailman kaikista verkkosivustoista käyttää WordPressiä alustanaan. (B2/Cafelog - Where WordPress Started n.d.; Meet WordPress n.d.)

WordPressiä voi käyttää kahdella tavalla: luomalla oman sivuston esimerkiksi wordpress.com kaltaiseen hosting-palveluun tai asentamalla wordpress.org löytyvän kokonaisen asennuksen omalle paikalliselle tai julkiselle palvelimelle. Jälkimmäinen tapa on se, mitä ammattimaisessa WordPress-kehityksessä käytetään. Tällöin käytössä, muokattavissa ja omassa hallinnassa on kaikki WordPressin koodi ja tietokannan sisältö, kun taas wordpress.com:iin luodun sivuston muokkausmahdollisuudet ovat hyvin rajalliset. (Biglione 2016.)

4.1.2 WordPress-lisäosa (plugin)

WordPress-lisäosat ovat kuin pieniä omia ohjelmiaan, joilla voi lisätä toiminnallisuuksia kyseiseen WordPress-sivustoon (What Are WordPress Plugins - - 2017). WordPressin omassa lisäosahakimistossa on tällä hetkellä tarjolla yli 55000 ilmaista lisäosaa (Plugins n.d.). Lisäksi kolmansien osapuolien palveluissa, kuten GitHubissa, on tarjolla tuhansia niin ikään ilmaisia lisäosia ja useat toimijat myös myyvät omia lisäosiaan (What Are WordPress Plugins - - 2017). Uusia lisäosia pystyy kehittämään ja laittamaan tarjolle kuka vain.

4.1.3 Toiminta- (action hook) ja suodatinkoukut (filter hook)

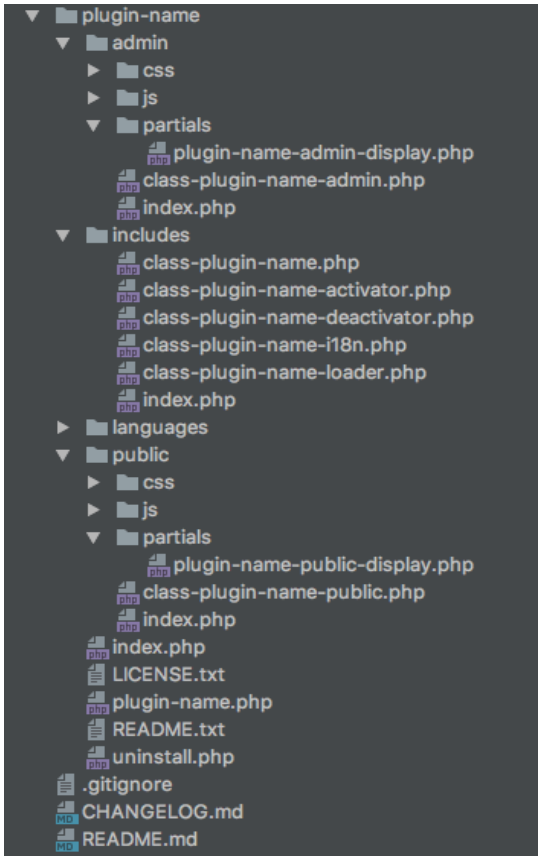
Toiminta- ja suodatinkoukut ovat keskeinen osa WordPress-kehitystä. Koukut antavat kehittäjälle mahdollisuuden tarttua lisäosassaan tai teemassaan funktiolla tiettyyn kohtaan WordPressin ydintä, teemaa tai jotakin lisäosaa, jonne koukku on asetettu. Kehittäjän luomia funktioita siis kutsutaan tiettyinä hetkinä sen mukaan, mihin koukkuun kehittäjä funktionsa asettaa. Toimintakoukut ovat nimensä mukaisesti tarkoitettu suorittamaan jokin haluttu toiminto tietyssä kohdassa koodia. Suodatinkoukuilla sen sijaan on tarkoitus muuttaa jotakin jo olemassa olevaa dataa silloin, kun data kulkee kyseisen koukun läpi. (Plugin API n.d.)

4.2 WooCommerce

WooCommerce on verkkokauppalisäosa WordPressille. Oman arvionsa mukaan WooCommercea käyttää yli 28% kaikista maailman verkkokaupoista ja sitä on ladattu yli 43 miljoonaa kertaa. (Ecommerce Usage Statistics n.d.; The most customizable eCommerce platform - - n.d.) WooCommerce sai alkunsa vuonna 2008 ja on, aivan kuten WordPresskin, Automattic-yrityksen tuote (All around the world - - n.d.).

4.3 WordPress Plugin Boilerplate

Lisäosan ei välttämättä tarvitsisi toimiakseen sisältää kuin yhden tiedoston. Jotta rakenne olisi siisti ja helposti jatkokehitettävä, kannattaa lisäosa kuitenkin rakentaa järjestäytyneemmälle pohjalle. WordPress Plugin Boilerplate on laajasti käytetty rakenne WordPress-lisäosille. Se on WordPressin standardien mukainen (Coding Standards, Documentation Standards), hyvin järjestelty ja olioperustainen pohja laadukkaiden lisäosien kehittämiseen. (WordPress Plugin Boilerplate n.d.; Toolbox of the Smart WordPress - - 2015.) Pohja sisältää admin- ja public-hakemistot, joiden alle on tarkoitus sijoittaa koodia sen mukaan, koskeeko koodi sivuston hallintaa vai julkista puolta. Jos se koskee molempia, voi koodin sijoittaa includes-hakemiston alle. Molemmissa, julkisen ja hallinnan puolella, on omat tyylitiedostot, JavaScript-tiedostot, paikka koukkuihin linkitetyille funktioille sekä partials-hakemisto mahdollisille tulostettaville HTML-palasille.



Kuvio 2. WordPress Plugin Boilerplaten rakenne.

4.4 Lisäosan määrittely

Tavoitteena oli kehittää WordPress-lisäosa, jolla voi ladata WooCommerce-lisäosan tietystä käyttäjästä tallentamat tiedot sekä WordPressin yleiset käyttäjätiedot. Toiminto vastaa GDPR:n vaatimuksiin “oikeus saada pääsy tietoihin” ja “oikeus tietojen siirtämiseen”. Tietojen latauksen voi tehdä rekisterinpitäjä. Loppukäyttäjällä eli asiakkaalla on mahdollisuus pyytää omia tietojaan rekisterinpitäjältä ja rekisterinpitäjällä on mahdollisuus hakea ja toimittaa ne loppukäyttäjälle lisäosaa hyödyntäen.

Käyttäjän tietojen tulee vaatimusten mukaan olla yleisesti käytetyssä koneellisessa muodossa, joten piti tehdä arvio siitä, mikä olisi sopivin koneellinen muoto datan esittämiseksi. Koska tietoja ei haeta vain tarkasteltavaksi, vaan ne tulee olla siirrettävissä, täytyy data ladata jossakin formaatissa. Mahdolliset tiedostomuotovaihtoehdot olivat XML, CSV ja JSON. JSON on nykyään laajasti käytetty ja käytöltään kasvava tiedostoformaatti datalle, joten se oli luonnollinen valinta tätä tarkoitusta varten.

WordPressin hallintapaneeli sisältää käyttäjien hallinnan, josta käyttäjä voi hallita omia ja oikeuksiensa mukaan muiden tietoja. Tarkoitus oli saada tuonne käyttäjänhallintasivulle painike, josta käyttöoikeudet hallintasivulle omaava henkilö voi yhdellä klikkauksella ladata kaikki kyseisen henkilön verkkokaupan tilauksiin liittyvät tiedot sekä yleiset käyttäjätiedot.

4.5 Kehitys- ja testiympäristö

4.5.1 Vagrant

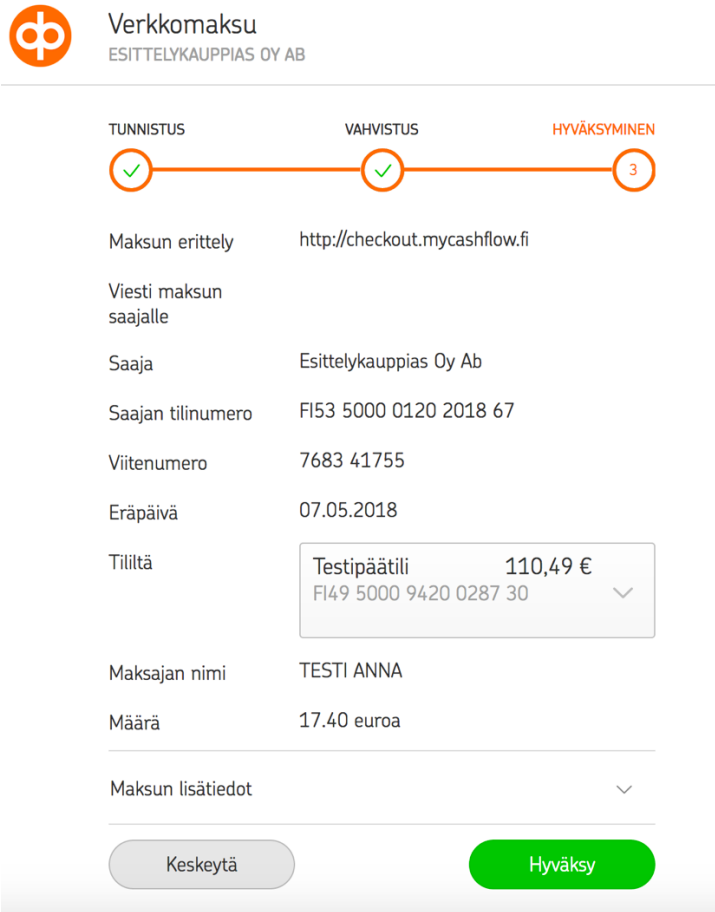
Vagrant on HashiCorpin luoma työkalu virtuaalikoneympäristöjen rakentamiseen yksinkertaisella työnkululla. Vagrant-kehitysympäristöä käytetään hyvin laajasti ammattimaisessa verkkokehityksessä. Työkalu on rakennettu alan standarditeknologioiden päälle ja se käyttää muun muassa Oraclen VirtualBoxia rakentamalla kehitysympäristön sen päälle. Vagrantin etuna on sen helppokäyttöisyys sekä muokkautuvuus käyttäjän tarpeiden mukaan. Vagrant helpottaa myös tiimityöskentelyä, sillä samanlaisen kehitysympäristön luominen muiden tiimiläisten kanssa onnistuu poikkeuksellisen vaivattomasti. HashiCorp mainostaakin, että heitä Vagrantin myötä hyvästit ”toimii minun koneellani” -tyyppisille virhetilanteille. (Introduction to Vagrant n.d.)

Valu Digitalin WordPress-kehitys toteutetaan aina paikallisesti kehittäjien omilla koneilla Vagrant-kehitysympäristöissä.

4.5.2 WooCommerce-verkkokauppa

Lisäosaa kehitettiin paikallisessa Vagrant-kehitysympäristössä jo olemassa olevaa Valu Digitalin rakentamaa verkkokauppatoteutusta hyödyntäen. Tuohon WordPress-pohjaiseen WooCommerce-lisäosalla rakennettuun verkkokauppaan luotiin paikallisesti omat testitunnukset ja testidataa. Testidatan generointi tapahtui tekemällä muutamia tilauksia luodulla testikäyttäjällä. Kyseinen verkkokauppa hyödyntää tilausten maksamisessa Checkoutin lisäosaa, ja jotta testitilaukset sai saatettua loppuun, täytyi myös tilausten maksuprosessit saattaa loppuun saakka. Tähän tarkoituk-

seen Checkoutilla on omat lisäosaan vaadittavat testitunnukset (Merchant ID ja Merchant Secret) ja verkkopankeilla niin ikään testikäyttöön tarkoitettuja tunnuksia (WooCommerce Checkout.fi n.d.; Chapter 3. Test credentials n.d.).



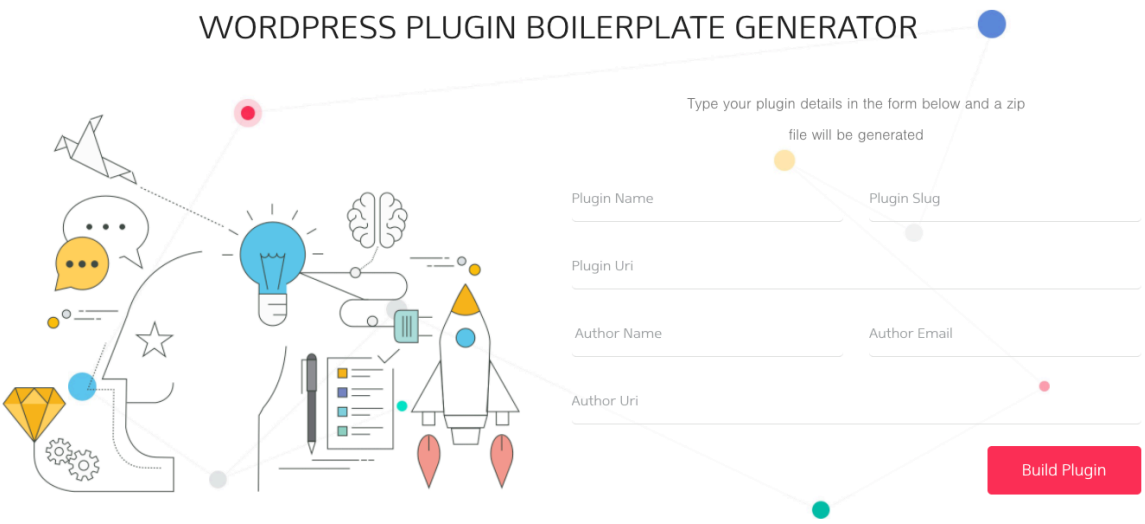
Kuvio 3. Osuuspankin testitunnuksilla pääsee suorittamaan testimaksuja kuvitteelliselta tililtä.

4.6 Lisäosan toteutus

4.6.1 Rakenne lisäosalle

Lisäosa rakennettiin WordPress Plugin Boilerplaten rakenteen mukaiselle pohjalle. Viimeisin versio WordPress Plugin Boilerplatesta löytyy GitHubista ja sen voi ladata sieltä pohjan luontia varten (WordPress Plugin Boilerplate n.d.). Jos pohja ladataan tuolta, kehittäjän tulee, yksilöidäkseen lisäosan, muuttaa reilu määrä tiedostonimiä sekä korvata tekstipätkiä koodista: enimmäkseen kommentteja ja funktioiden nimiä.

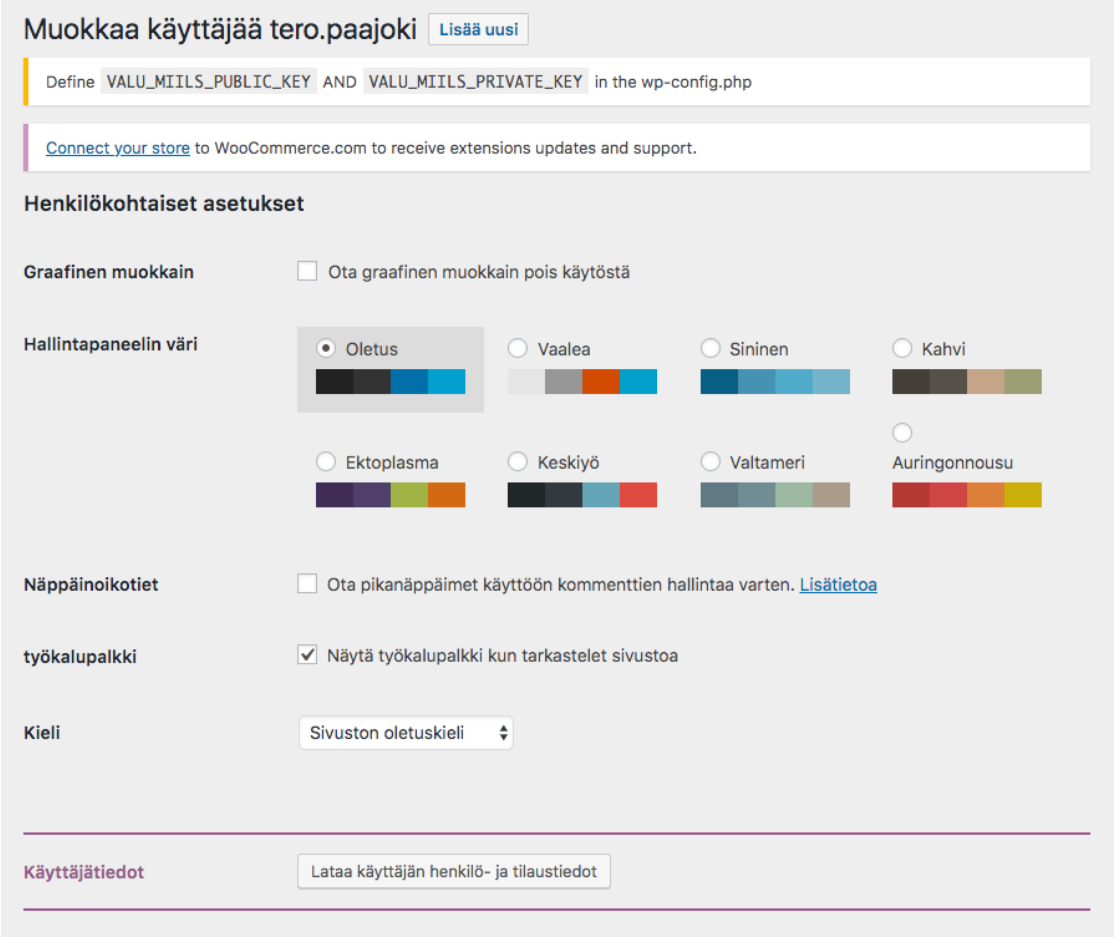
Onneksi WordPress Plugin Boilerplaten kehittäjät ovat tehneet tuon prosessin nopeuttamiseksi selaimessa toimivan WordPress Plugin Boilerplate Generatorin. Lisäosalle generoitiin tuolla työkalulla pohja, jossa oli kaikki lisäosan yksilöivät tekstit valmiiksi paikallaan. (WordPress Plugin Boilerplate Generator n.d.)



Kuvio 4. WordPress Plugin Boilerplate Generator.

4.6.2 Painikkeen lisääminen käyttäjänhallintasivulle

WordPress luo käyttäjänhallintasivun WordPressin ytimessä, ja mikäli tuolle sivulle haluaa tehdä muutoksia ytimeen koskematta, on ainoa vaihtoehto käyttää sivun koodiin asetettuja toimintakoukkuja. Käyttäjänhallintasivulla koukkuja on useampia: eri sijainteja ja osa näkyy vain muiden kuin sen kirjautuneen käyttäjän omalla profiilisivulla. Painike voisi, ja olisi parempikin, olla täysin irrallaan sivulla olevasta suuresta lomake-elementistä <form></form>, mutta koska kaikki koukut sijaitsevat lomakkeen sisällä, täytyi painike sijoittaa lomakkeen sisälle. Parhaimmaksi sijainniksi valikoitui personal_options -toimintakoukku heti alussa henkilökohtaisten asetusten alaosassa. Koukun funktioon lisättiin tarvittava HTML-taulukko sekä sen sisälle itse painike ja ne tulostuivat halutusti käyttäjänhallintasivulle. Funktioon lisättiin myös JavaScript-funktio get_user_data, joten se on mukana käyttäjänhallintasivulla selaimessa.



Kuvio 5. Käyttäjätietojen latauspainike käyttäjänhallintasivulla.

```php
/**
 * Register all of the hooks related to the admin area functionality
 * of the plugin.
 *
 * @since    1.0.0
 * @access   private
 */
private function define_admin_hooks() {

    $plugin_admin = new Valu_Woouser_Downloader_Admin( $this->get_plugin_name(), $this->get_version() );

    $this->loader->add_action( 'admin_enqueue_scripts', $plugin_admin, 'enqueue_styles' );
    $this->loader->add_action( 'admin_enqueue_scripts', $plugin_admin, 'enqueue_scripts' );
    $this->loader->add_action( 'personal_options', $plugin_admin, 'custom_user_profile_fields' );
    $this->loader->add_action( 'wp_ajax_get_user_data', $plugin_admin, 'get_wp_ajax_user_data' );

}
```

Kuvio 6. Toimintakoukkuihin tartuttiin lisäosan Valu_Woouser_Downloader_Loader -luokan omalla funktiolla add_action.

4.6.3 Ajax-kutsu painiketta klikkaamalla

Luotu painike käynnistää tapahtumien ketjun. Koska tarkoitus oli painikkeen klikkaamisen jälkeen pysyä samalla käyttäjänhallintasivulla sitä uudelleen lataamatta, mutta saada kuitenkin dataa sisältävä tiedosto ladattua taustaprosessina, oli AJAX:n hyödyntäminen selvä suunta. AJAX on lyhenne sanoista ”Asynchronous JavaScript and XML” ja se mahdollistaa asynkroniset kutsut palvelimelle. Se tarkoittaa sitä, että palvelimelle voidaan lähettää kutsu ja sieltä voidaan vastaanottaa dataa lataamatta verkkosivua uudestaan.

Painike sisältää onclick-attribuuttina JavaScript-funktiokutsun, joka ajaa get_user_data -funktion. Tuo JavaScript-funktio sisältää AJAX-kutsun, joten painiketta klikattaessa selain jää odottamaan vastausta kutsuun.

```
var data = {
    action: 'get_user_data',
    security: '<?php echo $ajax_nonce; ?>',
    user_email: '<?php echo esc_js( $profileuser->user_email ); ?>',
    user_id: '<?php echo esc_js( $profileuser->ID ); ?>'
};

jQuery.post(ajaxurl, data, function (response) {
    if (response !== null && response !== '') {
        jQuery('<a />', {
            'download': 'userdata_<?php echo esc_js( $profileuser->user_nicename ); ?>.json',
            'href': 'data:application/json,' + encodeURIComponent(response)
        }).appendTo('body').click(function () {
            jQuery(this).remove()
        })[0].click();
    } else {
        console.log('Response was null or empty');
        alert('Response was null or empty.');
    }
    jQuery('.loader').remove();
});
```

Kuvio 7. AJAX-kutsun lähetys ja palautuneen datan lataus.

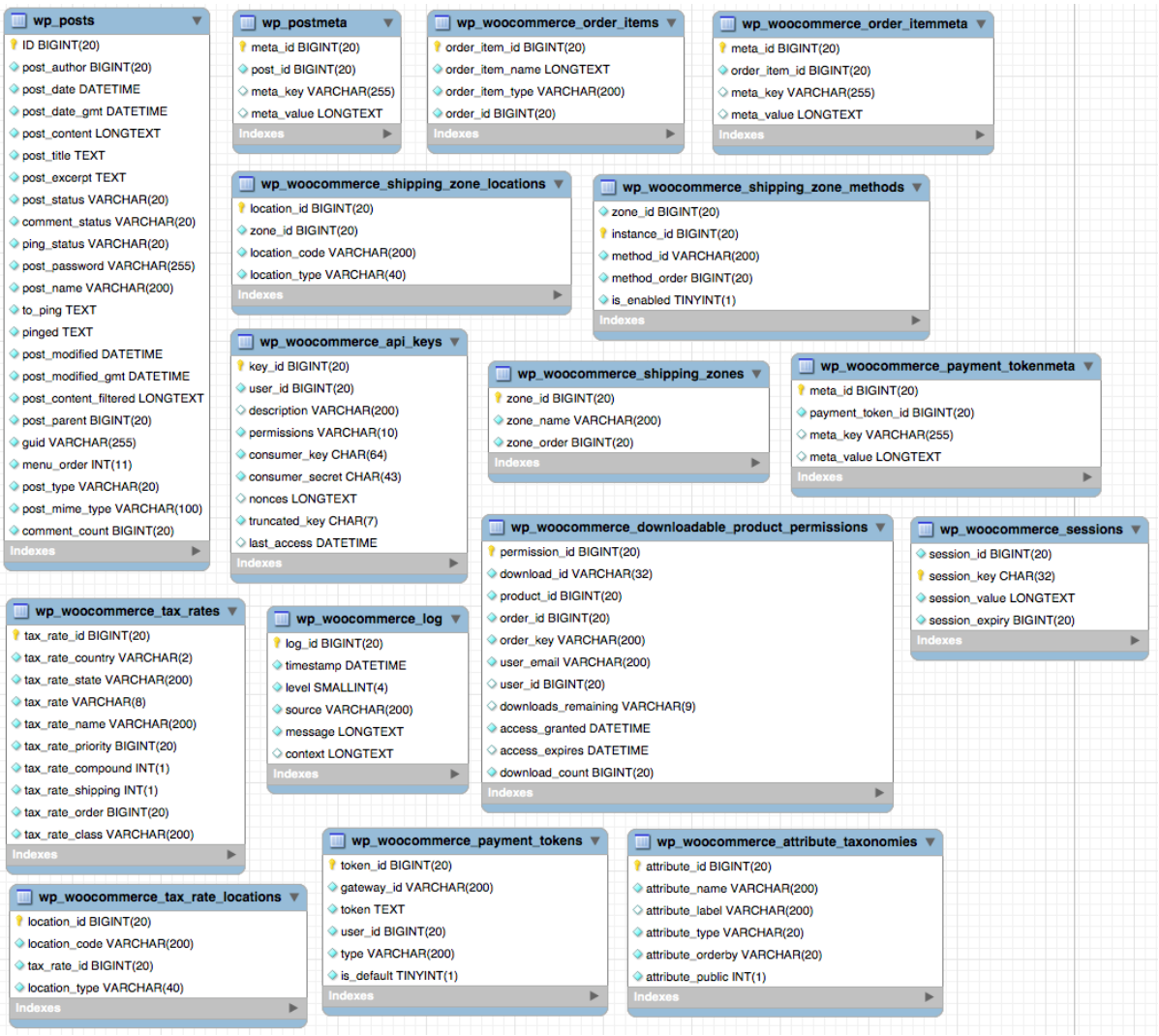
WordPressissä on mahdollista päästä koukulla wp_ajax_*action_name* kiinni lähetettyyn AJAX-kutsuun nimetyn action-avaimen mukaan. Tässä tapauksessa action-avaimeksi asetettiin get_user_data, joten AJAX-kutsuun pääsi käsiksi toimintakoukulla wp_ajax_get_user_data. Jos action-avaimeksi olisi asetettu vaikkapa orders, olisi toimiva toimintakoukku wp_ajax_orders. (AJAX in Plugins n.d.) Voidaan siis sanoa, että painikkeen klikkaus määrittelee WordPressin ytimen wp_ajax_*action_name* -hookin ajallisen sijainnin klikkaushetkeen. Joten tässä tapauksessa lisäosassa tuohon

koukutettu funktio get_wp_ajax_user_data suoritetaan ja kaikki sitä seuraava toiminta suoritetaan taustalla AJAX:in ansioista aina siihen saakka, kunnes selain saa dataa palautuksena.

Kun palautus tulee selaimeen, jQuery rakentaa linkin, joka sisältää download-attribuuttina halutun tiedostonimen sekä href-attribuuttina tiedostomuotomäärityksen sekä saapuneen palautuksen. Tuota linkkiä jQuery sitten itse klikkaa ja sen seurauksena selaimeen saapunut palautus ladataan JSON-tiedostona. Esimerkki ladattavan tiedoston sisällöstä on liitteenä (Liite 2).

4.6.4 WooCommercen tietyn käyttäjän tilausten haku

Datan hakemiselle oli useampia, mutta ei toki toisiinsa nähden yhtä hyviä, ratkaisuja. WordPressin tietokantaan pääsee kätevästi käsiksi hyödyntäen globaalia $wpdb-objektia. Ensimmäinen testaus päästä käsiksi tietokantaan olikin toteutettu juuri tätä objektia hyödyntäen ja omilla SQL-kyselyillä dataa hakien. Ennen sitä piti selvittää tarkkaan tietokannan rakenne, jotta kyselyitä pystyttiin muodostamaan. Periaatteessa lisäosa olisi voitu rakentaa tuon pohjalta, mutta ratkaisu ei olisi ollut järin varma ja kestävä pitkässä juoksussa. WooCommerce ei takaa, että tuollainen suora tietokannasta hakeminen toimisi jatkossakin, kun lisäosaan tulee päivityksiä. Tietokannan rakenne ja datan eri osien sijainnit saattavat muuttua. Siksi täytyi etsiä turvallisempia vaihtoehtoja.



Kuvio 8. WordPressin tietokantataulut, joita WooCommerce käyttää.

WooCommercella on omat funktiot datan hakemista varten ja noiden hyödyntäminen oli tässä tapauksessa ehdottoman järkevää. WooCommerce toteaa itsekin, että esimerkiksi wc_get_orders -funktion käyttö on suositeltava tapa hakea tilauksia järjestelmästä. Sen käyttö on tietoturvallista ja se toimii, vaikka tietokantaan tulisi rakenteellisia muutoksia tulevissa WooCommercen versioissa. He huomauttavat vielä, että muutoksia tietokannan rakenteeseen on jo tullut ja lisää on suunnitteilla, sillä heidän tavoitteenaan on siirtää tilaustietoja entistä enemmän WooCommercen omiin tietokantatauluihin WordPressin vakiotaulujen sijaan. (Wc_get_orders and WC_Order_Query n.d.)

Lisäosan get_wp_ajax_user_data -funktion kutsuma get_user_data_by_identificator -funktio hakee ensin WooCommercen wc_get_orders -funktiolla kyseisen käyttäjän

kaikkien tilausten id:t käyttäen käyttäjän id:tä tunnisteena. Id saadaan $_POST-pyynnöllä, koska AJAX-kutsuun on sisällytettynä parametrina kyseisen käyttäjän id, joka saatiin sinne person_options -koukun custom_user_profile_fields -funktiolle lähettämästä käyttäjädata-parametrista. Tilausten id:iden perusteella sitten haetaan wc_get_order ja get_data -funktioita hyödyntäen tilausten tarkemmat tiedot. Vielä lopuksi haetaan kunkin tilauksen sisältämät tuotteet get_items -funktiolla ja kaikki tämä yhdistetään yhdeksi moniulotteiseksi taulukoksi.

```
// Get orders
$order_ids  = wc_get_orders( $order_args );
$order_data = [];

foreach ( $order_ids as $order_id ) :

    $order                                = wc_get_order( $order_id );
    $order_temp_data                      = $order->get_data();
    $order_data[ $order_temp_data['id'] ] = $order_temp_data;

    // Loop products the order includes
    foreach ( $order->get_items() as $item_key => $item_values ) :
        $order_data[ $order_temp_data['id'] ]['products'][ $item_values->get_id() ] = $item_values->get_data();
    endforeach;

endforeach;
```

Kuvio 9. Tilaustietojen hakeminen WooCommercen funktioilla ja moniuloitteisen taulukon luonti.

Moniulotteinen taulukko sisälsi jonkin verran dataa, jolla ei ollut mitään arvoa lopullisen ladattavan JSON-tiedoston kannalta. Esimerkiksi avaimen timezone_type numeroarvolla ei ole mitään merkitystä, koska se ei kerro mitään, ja koska lopulliseen dataan tulee kuitenkin avaimella ”timezone” käyttäjän aikavyöhykkeen esimerkkisijainti. Koska moniulotteisesta taulukosta piti saada poistettua tarpeettomia avaimia, lisäosaan luotiin uusi funktio tuota tarkoitusta varten. Funktiolle annetaan parametrina taulukko, musta lista, joka sisältää ei-toivotut avaimet, ja mikäli avain sijaitsee taulukossa taulukon sisällä, ilmaistaan polku avaimeen mustan listan taulukon sisälle omana taulukkonaan. Mustalle listalle määritellyt avaimet ja kaikki taulukossa hierarkkisesti niiden alapuolella olevat datat poistetaan aina datan hakemisen jälkeen.

4.6.5 WordPressin tietyn käyttäjän henkilötietojen haku

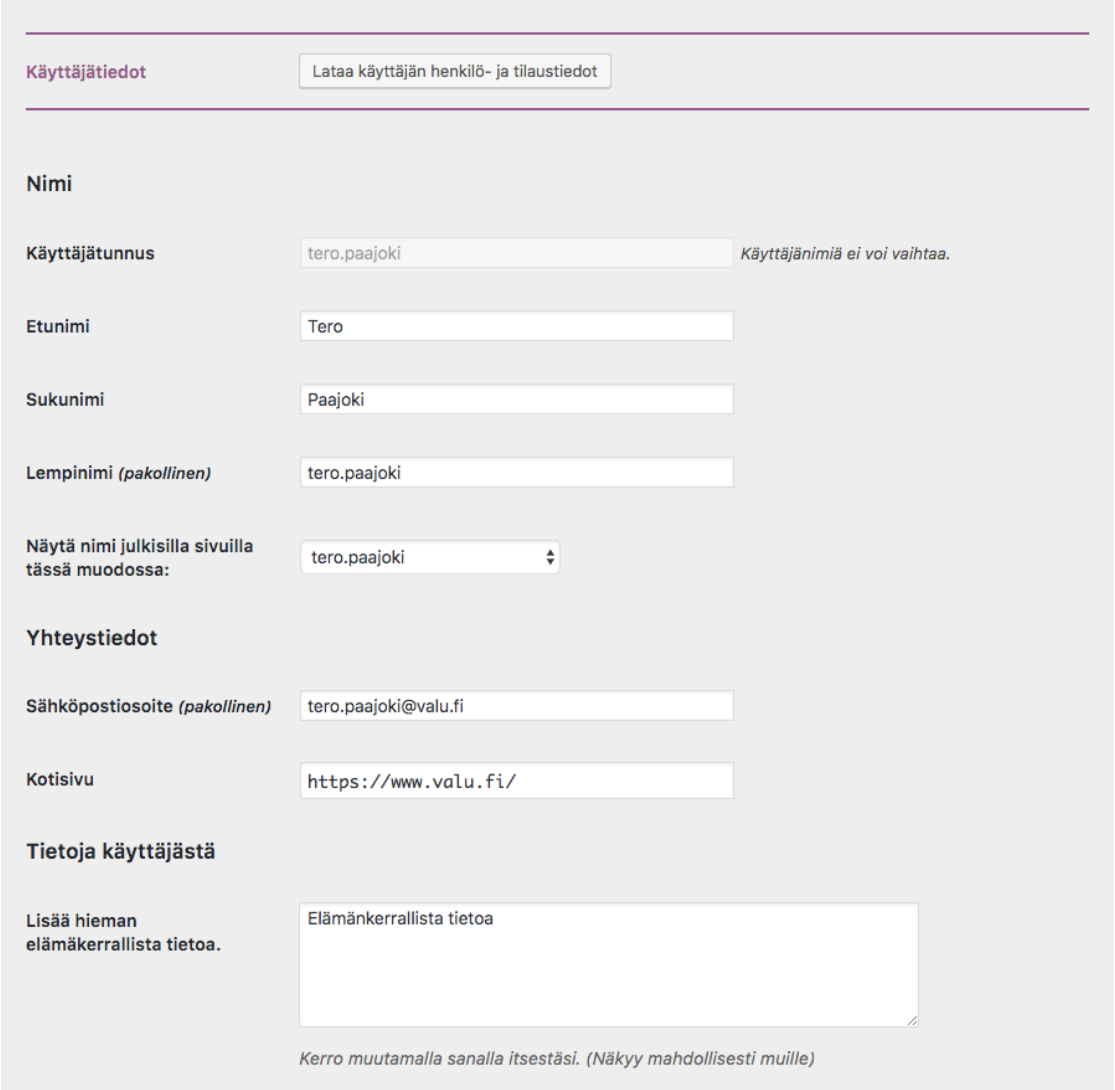
Käyttäjän tilausten lisäksi samaan pakettiin haluttiin käyttäjän henkilötiedot, jotka löytyvät käyttäjänhallintasivulta heti luodun latauspainikkeen alta. Lisäosa hakee nuo

tiedot get_user_meta -funktiolla, joka käyttää, aivan kuten wc_get_orders, käyttäjän id:tä käyttäjän tunnisteena.

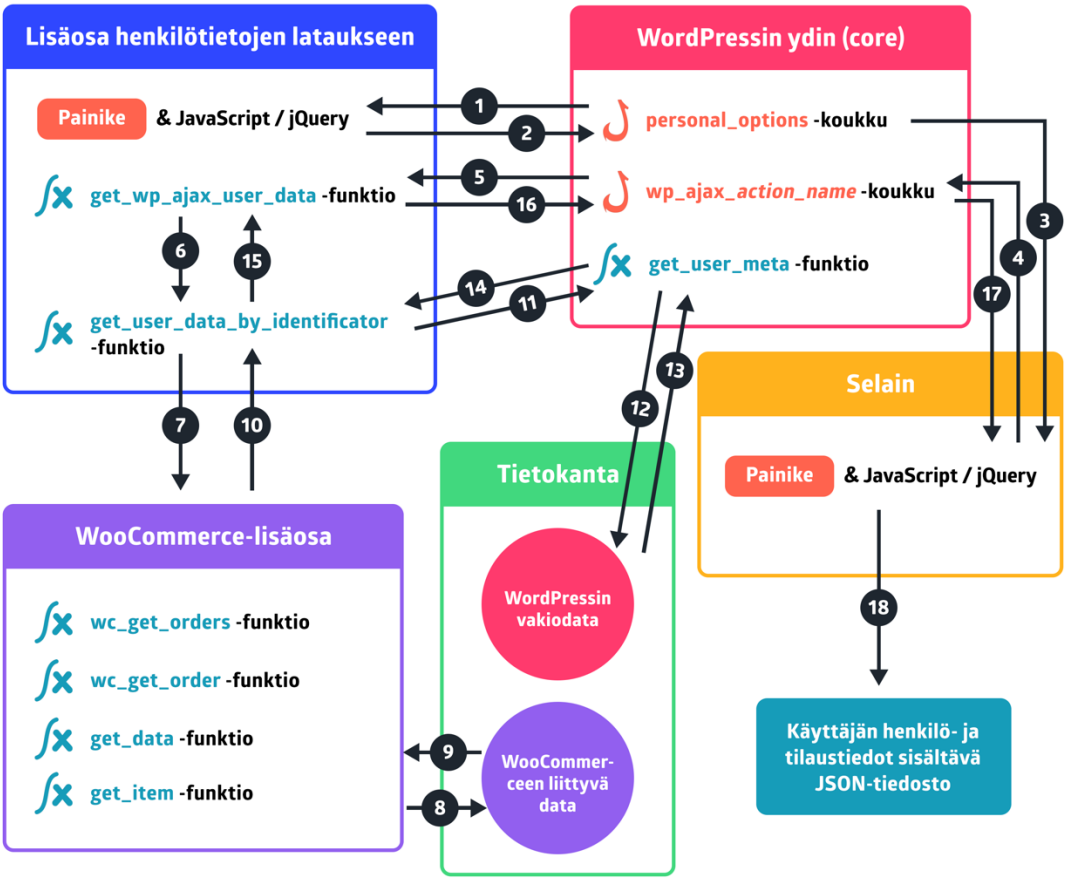
```
// Get user meta
$user_meta = get_user_meta( $identificator );
$user_meta = array_diff_key( $user_meta, array_flip( $blacklist_of_user_meta_keys ) );
```

Kuvio 10. WordPressin käyttäjätietojen hakeminen ja mustan listan avainten poisto.

Myös henkilötiedot sisälsivät tarpeetonta dataa, esimerkiksi hallintasivujen väriteeman nimi taulukon avaimella ”admin_color”. Mutta koska taulukko ei ollut moniulotteinen, mustan listan avainten poistoon ei tarvinnut käyttää omaa funktiota, vaan poisto saatiin toimimaan PHP:n omalla array_diff_key -funktiolla. Mustan listan avaimet poistetaan aina datan hakemisen jälkeen.



Kuvio 11. WordPress-käyttäjän henkilötiedot ovat näkyvillä ja osittain muokattavissa käyttäjänhallintasivulla.



1. & 2. & 3. Käyttäjänhallintasivun latautuessa WordPressin ytimestä, uudesta lisäosasta haetaan personal_options -koukun kohdalla painike ja skripti selaimeen.

4. Skriptin AJAX-pyyntö lähtee liikkeelle painiketta klikattaessa. Selain jää odottamaan.

5. Painikkeen klikkaus määrittelee WordPressin ytimen wp_ajax_action_name -hookin ajallisen sijainnin klikkaushetkeen, joten lisäosassa tuohon koukutettu funktio get_wp_ajax_user_data suoritetaan.

6. Funktio kutsuu lisäosan toista funktiota get_user_data_by_identificator, joka hakee kaiken käyttäjädatan käyttäjän id:n perusteella.

7. & 8. & 9. Funktio get_user_data_by_identificator kutsuu ensimmäiseksi WooCommerce -lisäosan funktioita tarpeellisessa järjestyksessä, jotta haettua saadaan niin käyttäjän tilaukset kuin niiden sisältämät tuotteetkin. WooCommercen funktiot hakevat datan tietokannasta WooCommercen itsensä luomasta datasta.

10. WooCommerce palauttaa tilaukset taulukkona

11. & 12. & 13. & 14. Funktio get_user_data_by_identificator kutsuu WordPressn ytimen funktiota get_user_meta. Funktio hakee WordPressin tietokannan perustauluista käyttäjän tiedot ja palauttaa tiedot taulukkona.

15. & 16. & 17. Funktion get_user_data_by_identificator yhdistämä käyttäjädata palautuu funktiolle get_wp_ajax_user_data, joka muuttaa palautuvan taulukon JSON-objektiksi ja tulostaa sen selaimeen, jolloin selaimen AJAX-kutsu saa JSON-objektin responsena.

18. Skripti luo responsen latauslinkin, jota se klikkaa itse automaattisesti sillä seurauksella, että JSON-tiedoston lataus käynnistyy.

Kuvio 12. Lisäosan toiminta vaihe vaiheelta kuvattuna.

4.6.6 Sanitointi ja validointi

Kaikki $_POST- ja $_GET-pyynnöt tulee sanitoida ja validoida suodattimella tietoturvasyistä. Sanitoinnilla puhdistetaan palautuva arvo sanitoinnin määrityksen mukaan ja validoinnilla varmistetaan palautuvan arvon oikeamuotoisuus niin ikään validoinnin määrityksen mukaan. Sanitointi ja validointi määritellään siis palautuvan arvon mukaan ja tämän lisäosan tapauksessa tarvitsi sanitoida ja validoida vain yksi $_POST-pyyntö: käyttäjän id. Id:lle käytettiin filter_var -funktiossa suodattimia FILTER_ SANITIZE _NUMBER_INT ja FILTER_VALIDATE_INT.

4.6.7 AJAX-kutsun lähteen tarkistus

Funktion get_wp_ajax_user_data alkuun lisättiin WordPressin funktio check_ajax_referer, joka tarkistaa tuleeko AJAX-kutsu sieltä, mistä on tarkoitus. Check_ajax_referer -funktiolle asetettiin parametreiksi custom_user_profile_fields -funktiossa wp_create_nonce -funktiolla määritellyn tokenin nimi sekä AJAX-kutsun se avain, jonka arvo token on. Jos check_ajax_referer ei tunnista tokenia asetetuksi, kutsu estetään. Käytännössä siis, jos kutsu on peräisin muualta kuin käyttäjänhallintasivulta, se estetään heti aluksi. Toimenpide vähensi huomattavasti tietoturvariskejä.

```
/**
 * Function for WP ajax to get WooCommerce user data
 *
 */
public function get_wp_ajax_user_data() {
    // Check if ajax-check nonce is set
    check_ajax_referer( action: 'ajax-check', query_arg: 'security' );
    if ( isset( $_POST['user_id'] ) ) :
        $customer_id = filter_var( $_POST['user_id'], filter: FILTER_SANITIZE_NUMBER_INT );
        if ( filter_var( $customer_id, filter: FILTER_VALIDATE_INT ) === 0 || ! filter_var( $customer_id, filter: FILTER_VALIDATE_INT ) === false ) :
            echo json_encode( $this->get_user_data_by_identificator( $customer_id, $by_id = true ), JSON_UNESCAPED_UNICODE | JSON_PRETTY_PRINT );
        else :
            echo '';
        endif;
    else :
        echo '';
    endif;

    wp_die();
}
```

Kuvio 13. $_POST-pyyntö validoitiin ja sanitoitiin sekä token tarkistettiin wp_ajax_get_user_data -koukun kutsumassa get_wp_ajax_user_data -funktiossa.

4.6.8 Omien suodatinkoukkujen lisääminen

Lisäosan kehittämisessä on hyvä ottaa aina huomioon myös se, että lisäosan käyttäjä saattaisi haluta päästä käsiksi joihinkin lisäosan kohtiin koskematta kuitenkaan lisäosan koodiin. Ja tätä vartenhan suodatin- ja toimintakoukut ovat olemassa.

Tähän lisäosaan lisättiin kolme suodatinkoukkua apply_filters -funktiolla: molemmille poistettavien avainten taulukoille eli mustille listoille sekä moniulotteisen taulukon avainten poistoon tarkoitetun funktion palautusarvolle. Kehittäjällä on siis mahdollisuus luoda omat mustat listansa omaan WordPress-teemaan tai toiseen lisäosaan. Niin ikään kehittäjällä on mahdollisuus toteuttaa, omaan teemaan tai lisäosaan, moniulotteisen taulukon avainten poistoon tarkoitettu funktio jotenkin toisella tavalla ja ohittaa tapa, jolla se tähän on toteutettu.

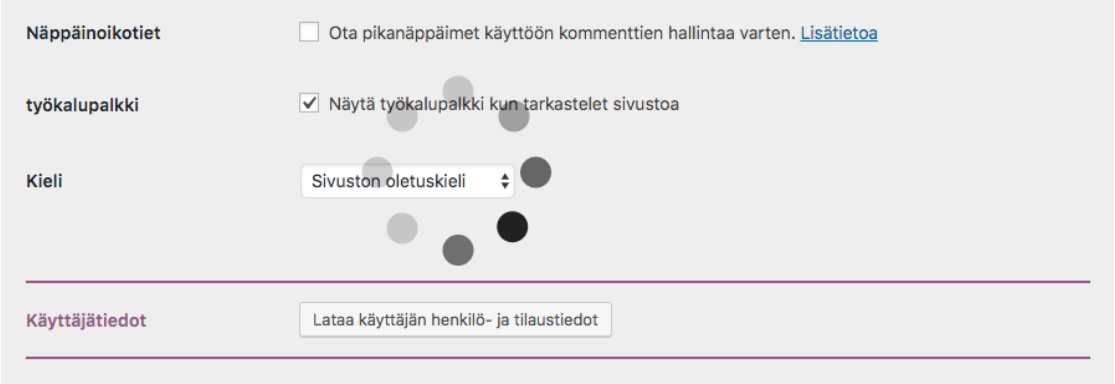
```
// Keys to remove from user meta data.
$blacklist_of_user_meta_keys = array(
    'rich_editing',
    'syntax_highlighting',
    'comment_shortcuts',
    'admin_color',
    'use_ssl',
    'show_admin_bar_front',
);

$blacklist_of_user_meta_keys = apply_filters( 'valu_woouser_blacklist_of_user_meta_keys', $blacklist_of_user_meta_keys );
```

Kuvio 14. Suodatinkoukut lisättiin apply_filters -funktiolla.

4.6.9 Tyylien lisääminen

WordPress Plugin Boilerplate -lisäosapohjassa on valmiiksi omat CSS-tiedostot sekä admin- että public-puolelle. Koska tässä tapauksessa haluttiin muokata hieman käyttäjänhallintasivulle lisätyn painikkeen ympäristöä, jotta painike erottuisi lomakkeen muista kentistä, tehtiin CSS-määrittelyjä admin-puolen CSS:ään. Lisäksi admin-puolen CSS:ään määriteltiin animoitu loader-ikoni, joka ilmestyy näkyviin aina painikkeen klikkauksen ja latauksen alkamisen väliseksi ajaksi.



Kuvio 15. CSS:llä määritelty ja animoitu loader-ikoni.

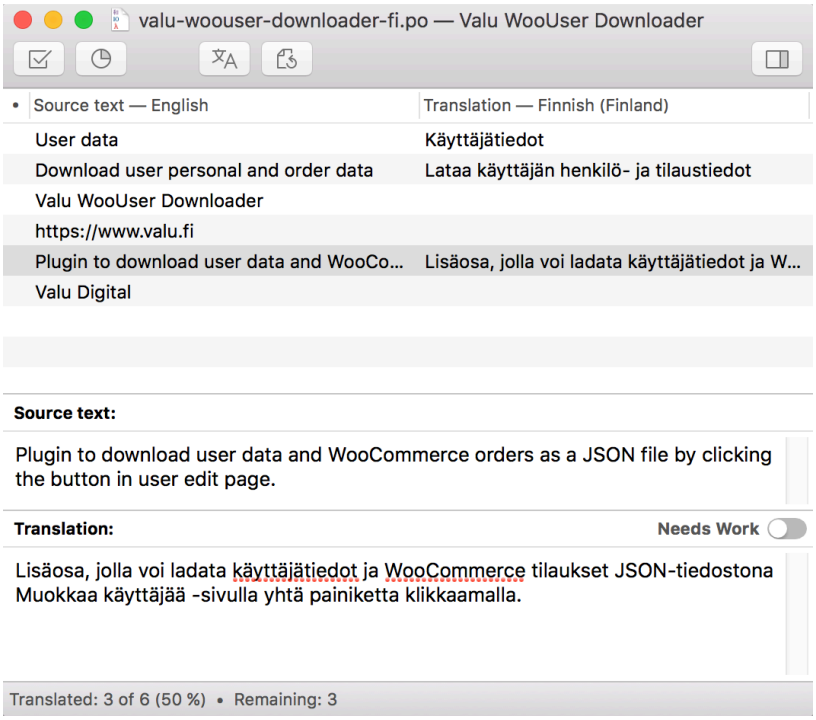
4.6.10 Käännökset

Lisäosan muutamat käyttäjänhallintasivulla näkyvät tekstipätkät käännettiin suomeksi. Yleinen käytäntö on, että koodiin kirjoitettavat alkuperäiset tekstit kirjoitetaan englanniksi ja englanninkielisten tekstien pohjalta tehdään muiden kielten käännökset.

Poedit on loistava työkalu tekstikäännösten tekemiseen sovelluksiin ja sivustoihin, jotka käyttävät Gettext:ä lokalisointiin (https://poedit.net/). WordPress Plugin Boilerplate -lisäosapohja käyttää WordPressin Gettext:ä ja esimerkiksi painikkeen teksti voitiin hakea käännettäväksi WordPressin funktiolla _e ja lisäosan domain-attribuutilla valu-woouser-downloader. Poedit loi valu-woouser-downloader-fi.po ja valu-woouser-downloader-fi.mo -tiedostot, joissa varsinaiset käännökset sitten sijaitsivat. Itse kääntäminen tapahtui mutkattomasti Poeditin käyttöliittymässä. Riippuen käyttäjän kielivalinnasta WordPressin asetuksissa, näytetään käyttäjälle joko suomen- tai englanninkieliset tekstit.

```
<div id="clickMe" class="button woo-user-downloader__button" onclick="get_user_data();">
    <?php _e( text: 'Download user personal and order data', domain: 'valu-woouser-downloader' ); ?>
</div>
```

Kuvio 16. Käännettäväksi halutut tekstit sijoitettiin _e -funktion ensimmäiseksi parametriksi.



Kuvio 17. Lisäosan tekstit käännettiin Poeditillä.

5 Tulokset

Opinnäytetyön tehtävänä oli käsitellä EU:n tietosuoja-asetus GDPR:n vaikutusta Valu Digitalissa toteutettavaan WordPress-kehitykseen. Ensimmäisenä tavoitteena oli käsitellä laajasti tietoperustaa ja sen myötä muodostaa selväkielinen tietopaketti GDPR:stä. Lisäksi tavoitteena oli kehittää WordPress-lisäosa, joka mahdollistaa verkkokauppalisäosa WooCommercen sekä WordPressin tallentaman tiettyyn henkilöön identifioitavissa olevan datan hakemisen ja lataamisen konekielisessä muodossa.

Tuloksena syntyi dokumentin tietoperustaosioon kohtalaisen laaja, mutta napakka, tietopaketti GDPR:n keskeisimmistä teemoista. Tietopaketti sisältää selvitykset asetuksen kattavuudesta, aikataulusta, valvonnasta, henkilötietojen käsittelyä koskevista perusperiaatteista, rekisteröidyn oikeuksista sekä henkilötietojen käsittelijöiden ja rekisterinpitäjien velvoitteista, haasteista ja hyödyistä.

Toisena tuloksena syntyi WordPress-lisäosa, joka mahdollistaa käyttäjän käyttäjätietojen lataamisen JSON-tiedostona käyttäjänhallintasivulta yhdellä painikkeen klikkauksella. Ladattavat käyttäjätiedot sisältävät WooCommerce-lisäosan tallentamat

käyttäjän tilaustiedot sekä WordPressin yleiset käyttäjän henkilötiedot. Lisäosa on rakennettu ja tiedot haetaan tietoturvallisesti ja suositeltujen standardien mukaisesti.

6 Pohdinta

Opinnäytetyölle asetetuissa tavoitteissa onnistuttiin hyvin. Tietoperustan GDPR tietopaketista todella muodostui tiivis ja helposti ymmärrettävä kokonaisuus. Paketti on käyttökelpoinen työkalu GDPR:n perusasioiden haltuunottoon.

Toisena tuloksena syntynyt lisäosa täyttää täysin tehtävänsä olla osaltaan vastaamassa GDPR:n asettamiin vaatimuksiin, “Oikeus saada pääsy tietoihin” ja “Oikeus siirtää tiedot järjestelmästä toiseen”, WordPress-kehityksessä. Hyvään lopputulokseen päädyttiin joidenkin huonompien ratkaisujen kautta. Alun kompuroinnit ja pohdinnat käytettävästä tiedonhakutavasta tarvittiin, jotta paremmat toimintatavat löydettiin, ymmärrettiin ja saatiin toteutettua.

Lisäosa toteutettiin toimeksiantajan, Valu Digitalin, käyttöön ja sen voidaan olettaa vahvistavan asiakkaiden luottamusta yritykseen. Lisäosa, ja siten yrityksen osoitus GDPR:n huomioon ottamisesta, antaa yritykselle kilpailuetua esimerkiksi tulevaisuuden tarjouskilpailuissa. Lisäosan mukanaan tuoma hyöty on siis merkittävä.

Lisäosaa voisi jatkokehittää laajentamalla siihen muitakin toiminnallisuuksia. Esimerkiksi toiminnallisuus, joka poistaisi käyttäjän WooCommerce-verkkokaupan tilaustiedot, olisi GDPR:n vaatimuksen ”Oikeus tulla unohdetuksi” kannalta erittäin oleellinen. Olisi myös järkevää ja perusteltua yhdistää se tähän lisäosaan. Mikäli, ilman tuota toiminnallisuutta, loppukäyttäjä pyytäisi tietojensa poistoa rekisterinpitäjältään, tulisi rekisterinpitäjän ottaa yhteyttä henkilötietojen käsittelijään ja henkilötietojen käsittelijä kävisi sitten poistamassa tiedot manuaalisesti tietokannasta. Prosessi olisi täysin mahdollinen ja periaatteessa toimiva, mutta käytännössä turhan tehoton.

Lähteet

AJAX in Plugins. N.d. WordPressin Codex-verkkosivusto. Viitattu 7.5.2018. https://codex.wordpress.org/AJAX_in_Plugins.

All around the world, Building a new web, and a New workplace. N.d. Atomatticin verkkosivut. Viitattu 27.4.2018. https://automattic.com/about.

B2/Cafelog - Where WordPress Started. N.d. Sisältösivu WhoIsHostingThis-verkkosivuilla. Viitattu 27.4.2018. https://www.whoishostingthis.com/resources/b2-cafelog.

Bałazińska, E. 2016. 8 Privacy Principles to Live By, According to OECD Guidelines. Artikkeli Piwik Pro -verkkosivuilla. Viitattu 15.11.2017. https://piwik.pro/blog/privacy-principles/.

Biglione, K. 2016. What is WordPress? Blogikirjoitus WP Apprentice -verkkosivuilla. Viitattu 27.4.2018. https://wpapprentice.com/blog/what-is-wordpress.

Chapter 3. Test credentials. N.d. Paytrailin verkkosivut. Viitattu 7.5.2018. https://docs.paytrail.com/en/ch03.html.

Direktiivi 2000/31/EY. Direktiivi sähköisestä kaupankäynnistä. Viitattu 13.12.2017. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32000L0031&from=FI.

Ecommerce Usage Statistics. N.d. Built With -verkkosivut. Viitattu 27.4.2018. https://trends.builtwith.com/shop.

EU:n tietosuojauudistus. 2017. Viitattu 11.1.2018. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html.

EU:n tietosuojauudistus ja sen kansallinen täytäntöönpano. 2017. Eduskunnan verkkosivut. Viitattu 11.1.2018. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx.

EU:n yleinen tietosuoja-asetus (GDPR): keskeisimmät muutokset. N.d. Artikkeli Laki24-verkkosivustolla. Viitattu 13.5.2018. https://www.laki24.fi/eun-yleinen-tietosuoja-asetus-gdpr-keskeisimmat-muutokset.

EU:n yleisen tietosuoja-asetuksen (GDPR) täytäntöönpano – Uusi tietosuojalaki. 2018. Eduskunnan verkkosivut. Viitattu 9.5.2018. https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/EUn-tietosuojauudistus/Sivut/EUn-yleinen-tietosuoja-asetus.aspx.

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. 2017. Viitattu 11.1.2018. http://julkaisut.valtioneuvosto.fi/handle/10024/80098.

EU-tietosuojan kokonaisuudistus. 2016. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän VAHTI-raportti. Viitattu 31.1.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128.

Euroopan ihmisoikeussopimus. 1998. Annettu 4.11.1950. Viim. muutos 1.11.1998. Viitattu 4.1.2018. http://www.echr.coe.int/Documents/Convention_FIN.pdf.

GDPR Timeline of Events. N.d. EUGDPR:n verkkosivut. Viitattu 15.11.2017. https://www.eugdpr.org/gdpr-timeline.html.

Happonen, I. GDPR termit infografiikkana. Isoltan verkkosivut. Viitattu 10.5.2018. https://www.isolta.fi/gdpr-termit-infografiikkana.

HE 49/1986. Hallituksen esitys Eduskunnalle henkilörekisterilaiksi ja siihen liittyviksi laeiksi. Viitattu 15.11.2017. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_49+1986.pdf.

HE 9/2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Viitattu 9.5.2018. https://www.finlex.fi/fi/esitykset/he/2018/20180009.

HE 96/1998. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi. Viitattu 15.11.2017. https://www.finlex.fi/fi/esitykset/he/1998/19980096.

Henkilörekisterilaki 471/1987. Viitattu 15.11.2017. https://www.finlex.fi/fi/laki/alkup/1987/19870471.

Hilmansson, A. 2017. Lopeta pelottelu! Näin voit hyötyä EU:n laajuisesta GDPR-tietosuoja-asetuksesta. Blogikirjoitus APSIS:n verkkosivuilla. Viitattu 10.5.2018. https://www.apsisfinland.fi/blogi/lopeta-pelottelu-nain-voit-hyotya-eun-laajuisesta-gdpr-tietosuoja-asetuksesta.

Ihmiskeskeinen tiedonhallinta, omadata eli MyData. 2017. Korkeakoulujen valtakunnallisen tietovarannon VIRTA-opintotietopalvelu. Viitattu 31.1.2018. https://confluence.csc.fi/display/VIRTA/Omien+opintotietojen+hallinta.

Introduction to Vagrant. N.d. Vagrant-verkkosivut. Viitattu 7.5.2018. https://www.vagrantup.com/intro.

Kattilakoski, M. 2017. Vieraskirjoitus: Paperiarkistot ja tietosuoja-asetus. Kirjoitus Avoine-verkkosivuilla. Viitattu 10.5.2018. https://blog.avoine.fi/kirjoitukset/paperiarkistot-ja-tietosuoja-asetus.

Kerttula, T. 2017. Tietosuoja-asetuksen mukainen siirto-oikeus – mitä se tarkoittaa? Blogikirjoitus IABlogissa. Viitattu 10.5.2018. https://www.iab.fi/iablogi/2017-postaukset/iablogi/tietosuoja-asetuksen-mukainen-siirto-oikeus-mita-se-tarkoittaa.html.

Lehto, L. 2017. GDPR tulee, oletko valmis? Uutinen COSS:n verkkosivuilla. Viitattu 10.5.2018. https://coss.fi/uutiset/gdpr-tulee-oletko-valmis.

Meet WordPress. N.d. WordPress.org verkkosivut. Viitattu 27.4.2018. https://wordpress.org.

Mitä jokaisen kuuluu tietää EU:n uudesta tietosuoja-asetuksesta GDPR. N.d. Findwisen verkkosivuilla. Viitattu 15.11.2017. https://findwise.com/en/gdpr-fi.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 1980. OECD:n verkkosivuilla. Viitattu 4.1.2018. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat ohjeet (WP 242 rev.01). 2017. EU:n tietosuojatyöryhmän ohjeistus. Viitattu 31.8.2018. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/UpTS0GArv/Oikeus_siirtaa_tiedot_jarjestelmasta_toiseenwp242rev01_fi.pdf.

Perko, J. 2016. 5 väärää luuloa EU:n tietosuoja-asetuksesta. Blogikirjoitus ASML-verkkosivuilla. Viitattu 31.1.2018. https://www.asml.fi/blogi/eu-tietosuoja-5-luuloa.

Pisto, V. 2018. Miten käy kerrostalojen saunavuorolistojen? 6 kysymystä tietosuoja-uudistuksesta. 2017. Artikkeli YLE:n verkkosivuilla. Viitattu 3.4.2018. https://yle.fi/uutiset/3-10074402.

Plugin API. N.d. WordPressin Codex-verkkosivusto. Viitattu 7.5.2018. https://codex.wordpress.org/Plugin_API.

Plugins. N.d. WordPress.org verkkosivut. Viitattu 27.4.2018. https://wordpress.org/plugins.

Puranen, K. 2017. EU tietosuoja-asetus (GDPR) – vipuvarsi parempaan vai kehityksen jarru. Blogikirjoitus Goforen verkkosivuilla. https://gofore.com/eu-tietosuoja-asetus-gdpr-vipuvarsi-parempaan-vai-kehityksen-jarru.

The most customizable eCommerce platform for building your online business. N.d. WooCommercen verkkosivut. Viitattu 27.4.2018. https://woocommerce.com.

Tietopaketti yrityksille: On tärkeätä valmistautua EU:n tietosuoja-asetukseen. N.d. Tietopaketti Elinkeinoelämän keskusliiton verkkosivuilla. Viitattu 7.5.2018. https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen.

Tietosuojadirektiivi (EU) 2016/680. Asetus luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta. Viitattu 4.1.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L0680&from=FI.

Tietosuojavastaavat. 2017. Viitattu 3.4.2018. http://www.tietosuoja.fi/fi/index/eun-tietosuojauudistus/ohjeitarekisterinpitajalle/tietosuojavastaavat.html.

Toolbox of the Smart WordPress Developer: The WordPress Plugin Boilerplate. 2015. Tutoriaali Envato Tuts -verkkosivuilla. Viitattu 27.4.2018. https://code.tutsplus.com/tutorials/toolbox-of-the-smart-wordpress-developer-the-wordpress-plugin-boilerplate--cms-23873.

Wc_get_orders and WC_Order_Query. N.d. GitHub-versionhallintapalvelu. Viitattu 7.5.2018. https://github.com/woocommerce/woocommerce/wiki/wc_get_orders-and-WC_Order_Query.

What Are WordPress Plugins? And How Do They Work? 2017. Blogikirjoitus WPBeginner-verkkosivuilla. Viitattu 27.4.2018. http://www.wpbeginner.com/beginners-guide/what-are-wordpress-plugins-how-do-they-work.

WooCommerce Checkout.fi. N.d. WooCommercen verkkosivut. Viitattu 7.5.2018. https://docs.woocommerce.com/document/checkout-fi.

WordPress Plugin Boilerplate. N.d. GitHub-versionhallintapalvelu. Viitattu 27.4.2018. https://github.com/DevinVinson/WordPress-Plugin-Boilerplate.

WordPress Plugin Boilerplate Generator. N.d. WordPress Plugin Boilerplate Generatorin verkkosivu. Viitattu 7.5.2018. https://wppb.me.

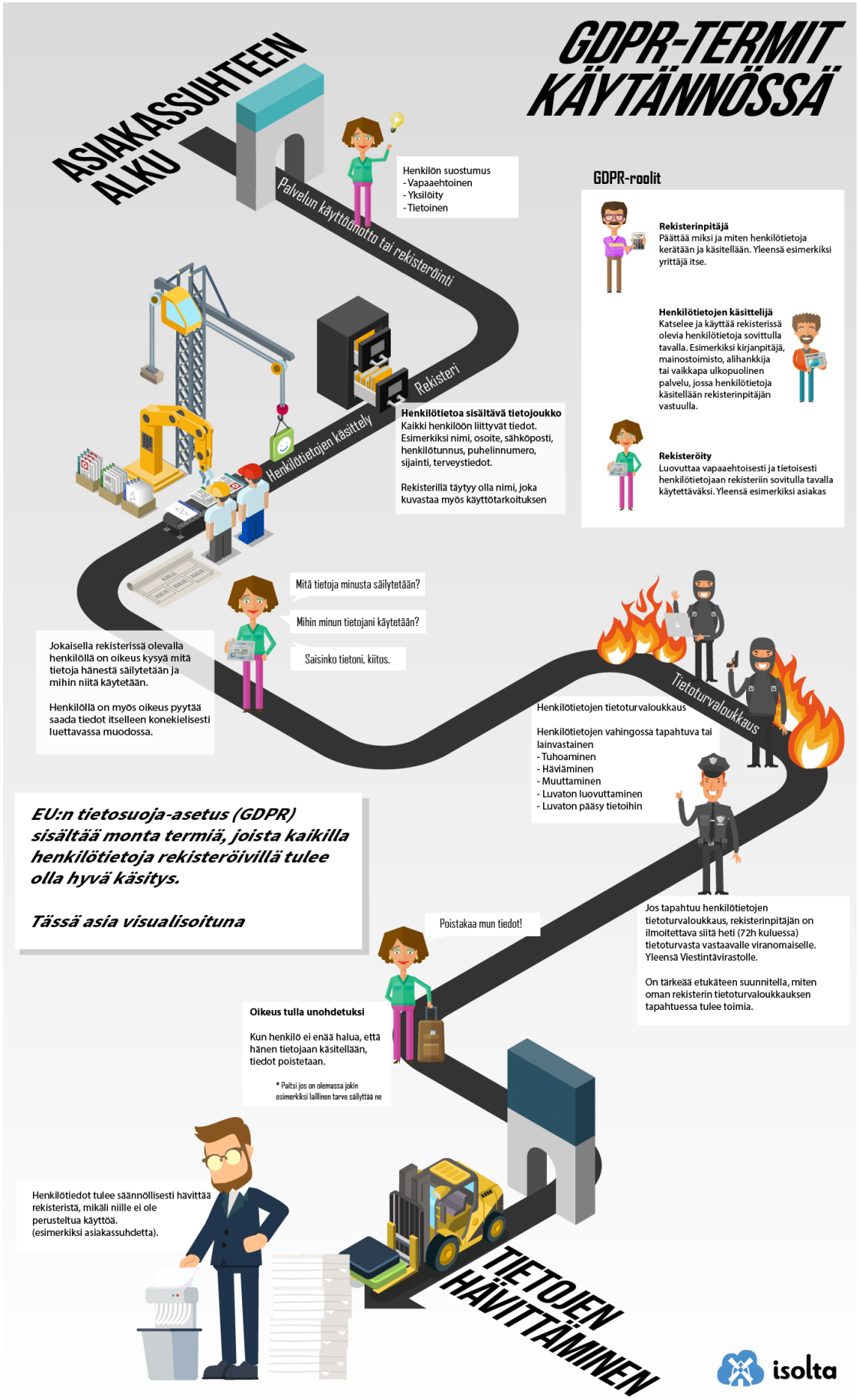
Yleinen tietosuoja-asetus (EU) 2016/679. Asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta. Viitattu 4.1.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

Ylipartanen, A. & Andreasson, A. 2015. EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt. Viitattu 4.1.2018. https://opitietosuojaa.fi/index.php/fi/oikeus/lait/eu-n-tietosuoja-asetus/23-eun-tietosuoja-asetus.

Yritys. N.d. Valun verkkosivut. Viitattu 15.11.2017. https://www.valu.fi/yritys.

Liitteet

Liite 1. GDPR termit infografiikkana



Liite 2. Esimerkki ladatun JSON-tiedoston sisällöstä


```
{
    "2794": {
        "user": {
            "nickname": [
                "tero.paajoki"
            ],
            "first_name": [
                "Tero"
            ],
            "last_name": [
                "Paajoki"
            ],
            "description": [
                "Elämänkerrallista tietoa"
            ],
            "locale": [
                ""
            ],
            "wp_capabilities": [
                "a:1:{s:8:\"customer\";b:1;}"
            ],
            "wp_user_level": [
                "0"
            ],
            "session_tokens": [

"a:1:{s:64:\"3ff55d173eb7cf9f0520c4de634157fa8105b5a96c1ee2cd95b8552a92bcb75a\";a:4:{s:10:\"ex
piration\";i:1526724207;s:2:\"ip\";s:12:\"192.168.50.1\";s:2:\"ua\";s:82:\"Mozilla\/5.0 (Mac-
intosh; Intel Mac OS X 10.12; rv:52.0) Gecko\/20100101 Fire-
fox\/52.0\";s:5:\"login\";i:1525514607;}}"
            ],
            "last_update": [
                "1526045549"
            ],
            "billing_first_name": [
                "Tero"
            ],
            "billing_last_name": [
                "Paajoki"
            ],
            "billing_address_1": [
                "Keksittykatu 10 HC"
            ],
            "billing_city": [
                "Keksittypostitoimipaikka"
            ],
            "billing_postcode": [
                "56700"
            ],
            "billing_country": [
                "FI"
            ],
            "billing_email": [
                "tero.paajoki@valu.fi"
            ],
            "billing_phone": [
                "0501234567"
            ],
            "shipping_first_name": [
                "Tero"
            ],
            "shipping_last_name": [
                "Paajoki"
            ],
            "shipping_address_1": [
                "Keksittykatu 10 HC"
            ],
            "shipping_city": [
                "Keksittypostitoimipaikka"
            ],
            "shipping_postcode": [
```

```
            "56700"
        ],
        "shipping_country": [
            "FI"
        ],
        "paying_customer": [
            "1"
        ],
        "billing_company": [
            "Keksitty Yritys Oy"
        ],
        "billing_address_2": [
            "Osoiterivi 2"
        ],
        "billing_state": [
            ""
        ],
        "shipping_company": [
            "Keksitty Yritys Oy"
        ],
        "shipping_address_2": [
            "Osoiterivi 2"
        ],
        "shipping_state": [
            ""
        ],
        "user_profile_image": [
            ""
        ],
        "_user_profile_image": [
            "field_5809edeb3dace"
        ],
        "shipping_method": [
            ""
        ],
        "_woocommerce_persistent_cart_1": [
            "a:1:{s:4:\"cart\";a:0:{}}"
        ]
    },
    "orders": {
        "115263": {
            "id": 115263,
            "status": "processing",
            "currency": "EUR",
            "date_created": {
                "date": "2018-05-11 16:32:29.000000",
                "timezone_type": 3,
                "timezone": "Europe\/Helsinki"
            },
            "date_modified": {
                "date": "2018-05-11 16:32:54.000000",
                "timezone": "Europe\/Helsinki"
            },
            "discount_total": "0",
            "discount_tax": "0",
            "shipping_total": "6.45",
            "shipping_tax": "1.55",
            "cart_tax": "1.36",
            "total": "14.98",
            "total_tax": "2.91",
            "billing": {
                "first_name": "Tero",
                "last_name": "Paajoki",
                "company": "Keksitty Yritys Oy",
                "address_1": "Keksittykatu 10 HC",
                "address_2": "Osoiterivi 2",
                "city": "Keksittypostitoimipaikka",
                "state": "",
                "postcode": "56700",
                "country": "FI",
                "email": "tero.paajoki@valu.fi",
                "phone": "0501234567"
            },
            "shipping": {
                "first_name": "Tero",
                "last_name": "Paajoki",
```

```
                    "company": "Keksitty Yritys Oy",
                    "address_1": "Keksittykatu 10 HC",
                    "address_2": "Osoiterivi 2",
                    "city": "Keksittypostitoimipaikka",
                    "state": "",
                    "postcode": "56700",
                    "country": "FI"
                },
                "payment_method": "checkout_fi_shop_in_shop",
                "payment_method_title": "Checkout.fi",
                "transaction_id": "",
                "customer_ip_address": "192.168.50.1",
                "customer_user_agent": "mozilla\/5.0 (macintosh; intel mac os x 10.12;
rv:52.0) gecko\/20100101 firefox\/52.0",
                "created_via": "checkout",
                "customer_note": "",
                "date_completed": null,
                "date_paid": {
                    "date": "2018-05-11 16:32:54.000000",
                    "timezone": "Europe\/Helsinki"
                },
                "cart_hash": "550f86b5f34d54ecf58d58dc6d03e451",
                "number": "115263",
                "meta_data": [
                    {
                        "id": 3144889,
                        "key": "_tribe_has_tickets",
                        "value": "1"
                    }
                ],
                "line_items": {
                    "9394": [],
                    "9395": []
                },
                "tax_lines": {
                    "9397": []
                },
                "shipping_lines": {
                    "9396": []
                },
                "fee_lines": [],
                "coupon_lines": [],
                "products": {
                    "9394": {
                        "id": 9394,
                        "order_id": 115263,
                        "name": "Pekonijäätelö",
                        "product_id": 115258,
                        "variation_id": 0,
                        "quantity": 1,
                        "tax_class": "",
                        "subtotal": "4.024194",
                        "subtotal_tax": "0.965806",
                        "total": "4.024194",
                        "total_tax": "0.965806",
                        "taxes": {
                            "total": {
                                "1": "0.965806"
                            },
                            "subtotal": {
                                "1": "0.965806"
                            }
                        },
                        "meta_data": []
                    },
                    "9395": {
                        "id": 9395,
                        "order_id": 115263,
                        "name": "Makkarakone",
                        "product_id": 115257,
                        "variation_id": 0,
                        "quantity": 1,
                        "tax_class": "",
                        "subtotal": "1.604839",
                        "subtotal_tax": "0.385161",
                        "total": "1.604839",
```

```
                        "total_tax": "0.385161",
                        "taxes": {
                            "total": {
                                "1": "0.385161"
                            },
                            "subtotal": {
                                "1": "0.385161"
                            }
                        },
                        "meta_data": []
                    }
                }
            }
        }
    }
}
```