HELLEWI

Tietojärjestelmäkuvaus

Käyttöoikeussopimuksen liitenumero 2

Versio 2.6 – 16.5.2018

Yleistä

Tämä dokumentti on jaettu kolmeen osaan. Ensimmäisessä osassa käsitellään Hellewi-järjestelmän palvelininfrastruktuuria ja siihen liittyviä ohjelmistoja, toimintoja ja kokoonpanoja. Toisessa osassa käsitellään Hellewi-järjestelmän tietoturvakäytäntöjä Hellewi-ohjelmiston osalta. Kolmannessa osassa käsitellään Hellewi-järjestelmän tietosuojakäytäntöjä EU:n tietosuojadirektiivin (GDPR) kannalta.

Dokumentin versio ja viimeisimmät muutokset:

Versio	Päivämäärä	Viite
2.6	16.5.2018	Lisätty sopimuksen liitenumero. Täydennetty tietosuojaliitteen kuvausta.
2.5	19.3.2018	Lisätty tietosuojaliite, jossa käsitellään Hellewi-järjestelmän tietosuojakäytäntöjä 25.5.2018 voimaan tulevan EU:n tietosuojadirektiivin (GDPR) kannalta.
2.4	1.1.2018	Vaihdettu palvelin- ja ohjelmistoympäristön tilannevalvontajärjestelmä sekä logien seuranta- ja analysointijärjestelmä.
2.3	1.6.2017	Nostettu arkipäivän kapasiteettia kantapalvelimien osalta ja lisätty ruuhkahuippujen mukaan suunniteltu mahdollisten edustapalvelimien lukumäärä kahdeksaan.
2.2	29.1.2016	Nostettu arkipäivän kapasiteettia. Lisätty valvontapalveluiden järjestelmät.

Voimassaolo

Tämä kuvaus koskee kaikkia Hellewi-asiakkaita 25.5.2018 alkaen. Tämä kuvaus liitetään Hellewin käyttöoikeussopimukseen liitenumerolla 2.

Termejä

Toimittaja = Wildfrost Oy, Hellewi-järjestelmän kehittäjä
Asiakas = Hellewi-järjestelmän tilaaja
Rekisteröity = On henkilö jonka tiedot on tallennettu Asiakkaan Hellewi-järjestelmään

Palvelinympäristö

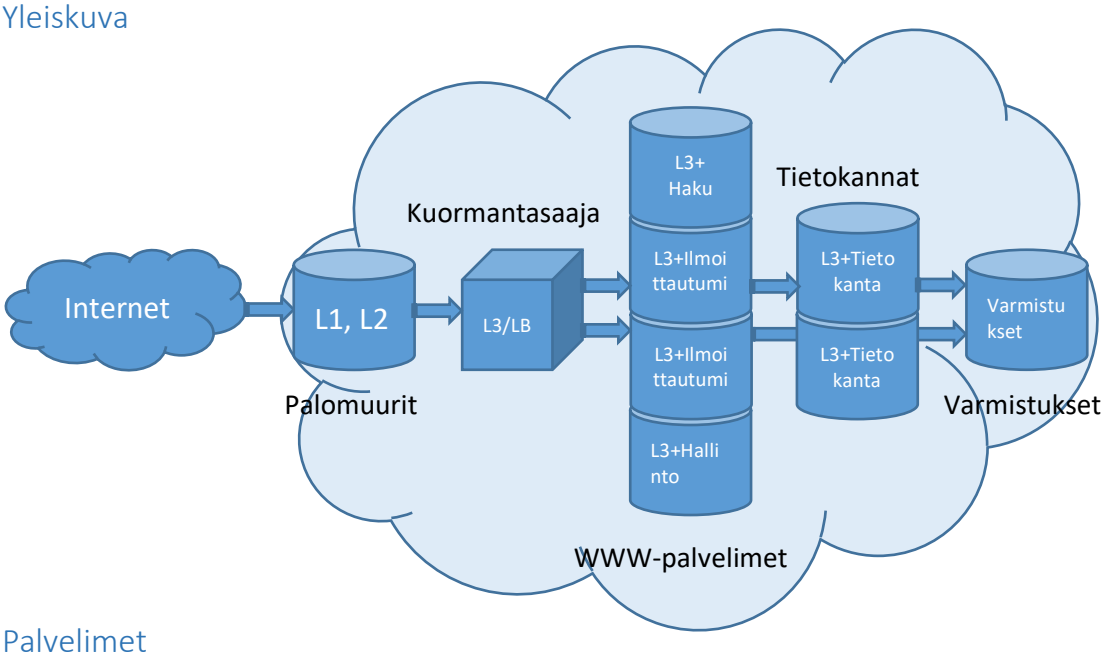
Toimittaja

Palvelinympäristön toimittaa UpCloud Oy (https://www.upcloud.com/). UpCloud Oy on Suomeen rekisteröity, kansainvälisillä markkinoilla toimiva, palvelinkapasiteettia tarjoava toimija. UpCloud Oy on Sigmatic Oy:stä vuonna 2011 omaksi yritykseksi perustettu ja Sigmatic Oy:n osittain omistama pilvipalveluihin erikoistunut yritys.

Sijainti

Hellewi-järjestelmän palvelinympäristö sijaitsee Helsingissä, Suomessa. Palvelinympäristön kaikkia asiakastietoja säilytetään Suomessa, eikä tietoja siirretä Suomen rajojen ulkopuolelle. Palvelinympäristö on auditoitu Viestintäviraston toimesta Oikeusministeriön käyttöön ja täyttää VAHTI-perustason vaatimukset.

Yleiskuva



Palvelimet

Hellewin palvelinympäristö koostuu pilvipalvelimista, joiden kokoonpanoja ja lukumääriä säädellään tarvittavan suorituskyvyn mukaan. Hiljaisina ajankohtina ylimääräisiä resursseja poistetaan käytöstä. Suorituskyvyn lisäksi useilla palvelimilla saavutetaan vikasietoisuutta ongelmatilanteiden sekä huoltojen varalle.

Palvelinkohtainen suorituskyky voidaan nostaa tarvittaessa tasolle 20xCPU ja 131072MB muistia.

Palvelimien lukumäärää voimme nostaa ilman rajoituksia. Ruuhkatilanteita varten suorituskyvyn nostolle on valmis toimintamalli ilman huoltokatkoja. Alla esimerkki normaalista kokoonpanosta arkipäivisin.

Palvelin	Lkm	Ohjelmistot	Kokoonpano
Kuormantasaus	1	Debian Linux 8.0, HAProxy	1xCPU, 1024MB, 30GB SSD
Ilmoittautuminen	8	Debian Linux 8.0, Nginx, PHP	2xCPU, 2048MB, 30GB SSD
Hallinto, Uusi versio	1	Debian Linux 8.0, Nginx, Nodejs	2xCPU, 4096MB, 50GB SSD
Hallinto, Vanha Versio	1	Windows Server 2012 R2 DC, IIS	2xCPU, 4096MB, 50GB SSD
Tietokanta #1	1	Debian Linux 8.0, MariaDB	16xCPU, 24576MB, 100GB SSD
Tietokanta #2	1	Debian Linux 8.0, MariaDB	6xCPU, 16384MB, 100GB SSD
Hakupalvelu	1	Debian Linux 8.0, Solr, Nginx, Nodejs	2xCPU, 2048MB, 30GB SSD
VPN	1	Debian Linux 8.0	1xCPU, 1024MB, 30GB SSD

Palomuurit

Hellewin palvelinympäristö on suojattu ympäristötasolla kolmella palomuuritasolla (L1, L2, L3), joista kahta ensimmäistä tasoa ylläpitää UpCloud Oy ja kolmatta tasoa Hellewin kehittäjät UpCloudin tarjoamien työkalujen avulla.

L1-palomuurilla ehkäistään yleisimmät tietoliikennehyökkäykset mukaan lukien DDoS-hyökkäysyritykset.

L2-palomuuri eristää UpCloud Oy:n asiakkaat omiin verkkoympäristöihin. Hellewi-ympäristön kanssa samassa verkkoympäristössä ei siis ole muita käyttäjiä. Palomuurilla ehkäistään myös L2-tason hyökkäysyritykset kuten ARP-väärennökset. Kaikki tietoliikenne Hellewi-palvelimilta ja -palvelimille kulkee tämän palomuurin läpi.

Jokainen Hellewin-järjestelmän palvelin on edellä mainittujen palomuurien lisäksi suojattu vielä L3-tason palomuurilla palvelinkohtaisilla ja whitelist -perusteisilla säännöillä. Muu kuin sallittu liikenne hylätään palomuuritasolla. Valituilta palvelimilta tarpeettomat julkiset IP-osoitteet on poistettu kokonaan.

Verkko

Tietoliikenne on varmennettu useiden eri tietoliikenneoperaattorien yhteyksillä. Hellewi-järjestelmän palvelimet ovat yhteydessä julkiseen internet-verkkoon 500 Mbps –nopeudella.

Hellewi-järjestelmän palvelimien välinen sisäverkko toimii 1000 Mbps -nopeudella. Kaikki tietoliikenne palvelimien välisessä sisäverkossa on salattu mukaan lukien www-palvelimien ja tietokantapalvelimien välinen tietoliikenne.

Kuormantasaus

Käytössämme on Linux-pohjainen HAProxy-kuormantasaaja (http://www.haproxy.org/), jolla tietoliikenne jaetaan palvelimille http-pyynnön perusteella. Jos http-pyyntö kohdistuu palveluun, josta on käytössä useampia palvelimia, tietoliikennekuorma jaetaan tasan palvelinten kesken.

Yksittäinen palvelun käyttäjä ohjataan aina samalle palvelimelle ensimmäisen pyynnön jälkeen, paitsi vikatilanteissa, jolloin pyyntö reitittyy automaattisesti toimivalle palvelimelle.

Saatavuus

UpCloud Oy takaa 100% SLA:n ja on velvoitettu korvaamaan Hellewi-järjestelmän ylläpitäjille vikatilanteessa palveluajan 50-kertaisesti. UpCloud Oy:n palvelinympäristöjen status-sivu löytyy osoitteesta: http://status.upcloud.com/. Sivulta voi tilata sähköpostipalvelun, jolla ilmoitetaan aina, jos palvelinympäristössä on häiriötilanne.

Vikasietoisuus

Kaikki palvelinympäristön komponentit on varmistettu N+1 –vikasietoisuusperiaatteella. Palvelinsalissa on useita verkkoyhteyksien toimittajia, useita sähkönsyöttöjä, vikasietoisia reititinpareja ja vikasietoisia tallennusjärjestelmiä.

Hellewi-järjestelmän tärkeimmät palvelimet on kahdennettu myös normaalikäytössä ja esimerkiksi ilmoittautumispalvelimet ovat monistettavissa alle minuutin vasteajalla. Palvelimia voidaan perustaa etukäteen ongelma- ja ruuhkatilanteiden varalle, jolloin vasteaika palvelimen käyttöönotolle on noin puoli minuuttia.

Siirrettävyys

Hellewi palvelinympäristön hallinnassa käytetään Ansible-automaatiotyökalua (https://www.ansible.com/), jolla palvelinympäristö voidaan automatisoidusti perustaa Linux- ja Windows-palvelimia tarjoavaan kapasiteettipalveluun tai tarvittaessa fyysisille palvelimille. Windows-palvelimien perustaminen suoritetaan manuaalisesti. Tarkoitukseen sopivia palveluntarjoajia on Suomessa useita. Ympäristöissä voi olla eroja esimerkiksi sisäverkon salauksen suhteen.

Siirto voidaan tehdä vain siinä tapauksessa, että Hellewi-järjestelmän ylläpitäjät ovat katsoneet nykyisen palveluntarjoajan olevan estynyt toimittamaan luvattua palvelinympäristöä ja palvelutasoa tai jos palvelinympäristön ylläpito muuten kilpailutetaan Hellewi-järjestelmän ylläpitäjien toimesta. Siirtoja ei tehdä Asiakaskohtaisesti ilman erillistä sopimusta.

Levyt ja varmistukset

Kaikki tuotantopalvelimet käyttävät SSD-levyjä kaikessa tiedon tallennuksessa. Kaikki järjestelmään tallennettu tieto on tallennettu UpCloud Oy:n toimesta kahdelle eri tallennusratkaisulle samassa palvelinkeskuksessa.

Tämän lisäksi tietokannat on varmistettu ajastetusti erikseen Hellewi-ylläpitäjien toimesta, erilliselle kolmannelle tallennusratkaisulle samassa palvelinkeskuksessa. Varmistuksissa käytetään kolmen viikon kiertoa, eli tiedot ovat palautettavissa kolmen viikon ajalta. Tämän lisäksi säilytämme puolen vuoden ajan kerran kuukaudessa otettua levykuvaa tietokantapalvelimista.

Muut palvelimet ja niiden asetukset ovat perustettavissa levykuvista ja palvelimien ohjelmistot asennetaan versiohallinnasta. Windows-palvelin perustetaan varmistuksesta ja muut palvelimet Ansible-työkalulla valmiilla skriptiohjelmalla.

Kun palvelinympäristön käyttö lopetetaan, UpCloud Oy takaa tietojen hävityksen ylikirjoittamalla kaikki levyt scrubbing-tekniikalla.

Hellewi

Tietoturvakäytännöt

Hellewissä sovelletaan Defence in depth -käytäntöä järjestelmän suunnittelussa. Käytäntöjä sovelletaan monella eri tasolla varmistaaksemme tiedon eheyden ja salassapidon myös mahdollisten tietoturva-aukkojen varalta.

Kehitystyössä hyödynnetään useita eri laajasti käytettyjä tietoturvakirjastoja. Emme suunnittele itse omia tietoturvakäytäntöjä, jos tarvittavaan toimintoon on olemassa laajasti käytetty ratkaisu.

Hellewi -Asiakkaat on eristetty toisistaan omiin tietokantoihin sekä omiin käyttöoikeusympäristöihin. Yhden Asiakkaan käyttöoikeudet on jaettu tietokantojen osalta asiakaskohtaisesti viiteen eri käyttöoikeustasoon, riippuen toimintojen käyttötarkoituksesta. Kantahauissa käytetään parametrisoituja kyselyitä.

Hellewi -järjestelmän ohjelmalliset käyttöoikeudet voidaan määritellä organisaatiokohtaisesti rajattomalla määrällä erilaisia tasoja. Ohjelmallisia käyttöoikeuksia valvotaan toimintokohtaisesti ja em. kantaoikeuksilla. Esimerkiksi tuntiopettajan käyttämillä ohjelmilla ei ole ohjelmallisia eikä kantatason oikeuksia hallintotason ohjelmiin.

Ilmoittautumisjärjestelmästä tai Hellewiin liitetyistä lisäpalveluista kuten hakupalvelu Linnunrata.fi:stä ei ole pääsyä rekisteröityjä identifioiviin henkilötietoihin.

Hellewissä käytetään kriittisten tietojen osalta tiivisteitä (Hash). Tiivisteitä luodessamme käytämme hitaaksi suunniteltua tiivistealgoritmia tiivistekohtaisesti vaihtuvalla suolauksella (Salt) silloin kun tiivisteitä käytetään salassa pidettävän tiedon vertailuun. Järjestelmään tallennetut henkilötiedot ja muut salassa pidettävät tiedot säilytetään levyllä salattuna ja salaus puretaan ja suoritetaan aina tietojen haun ja tallennuksen yhteydessä. Muut kuin henkilötiedot tai muut salassa pidettävät tiedot, säilytetään salaamattomina tästä seuraavan suorituskykyhyödyn takia.

Tietoliikenne

Tietoliikenne on aina salattu Hellewi-palvelimille (HTTPS, useita eri SSL-sertifikaattien toimittajia) sekä palvelinympäristön sisäverkossa. HTTP-pyynnöt suodatetaan (http-request-filtter) ja puhdistetaan (input sanitation).

Pääsy Hellewi-palvelinympäristön ylläpitoon on rajattu VPN -ympäristöllä. Pääsy VPN-ympäristöön on rajattu IP-osoitteiden perusteella. UpCloud Oy:n henkilökunnalla ei ole pääsyä Hellewi-järjestelmän palvelimille.

Testaus

Testaamme järjestelmää sekä kuormitus- että penetraatiotyökaluilla. Kuormitustestejä suoritetaan Loader.io -työkalulla. Tietoturvahaavoittuvuuksia testaamme käyttämällä useita ohjelmistoja mukaan lukien, mutta ei rajoittuen seuraaviin sovelluksiin: SQLNinja, NTOSpider, Backtrack, WebScarap, NMAP, Nessus, Firefox (Web Developer-, Tamper Data expansions) sekä Metasploit. Tämän lisäksi testaamme järjestelmää myös manuaalisesti.

Valvonta

Seuraamme aktiivisesti tietoturvaan liittyvää uutisointia, tekniikan kehitystä ja tietoturvatiedotteita. Tiedotamme asiakkaitamme Hellewiin liittyvistä tietoturvauutisista. Järjestelmää kehittäessämme noudatamme alalla yleisesti noudatettuja parhaita käytäntöjä.

Käytämme palvelin- ja ohjelmaympäristön tilannevalvontaan sekä logien seurantaan ja analysointiin Datadog-valvontajärjestelmää (https://www.datadoghq.com/). Toimintaa seurataan lisäksi PM2-managerilla (https://keymetrics.io/). Ostamme lisäksi valvontapalvelua palveluntarjoajaltamme. Ostopalvelun valvontajärjestelmänä on Zabbix (http://www.zabbix.com/). Järjestelmät lähettävät poikkeavasta toiminnasta hälytykset ylläpitäjille.

Tietosuojaliite

Tämä Tietosuojaliite on erottamaton osa Asiakkaan ja Wildfrost Oy:n (myöh. Toimittajan) välillä allekirjoitettua Hellewi-palvelusopimusta. Jos alkuperäinen sopimus ja sen muut liitteet ovat ristiriidassa tämän Tietosuojaliitteen kanssa, sovelletaan Asiakkaan ja Toimittajan välillä henkilötietojen käsittelyyn liittyen ensisijaisesti tässä Tietosuojaliitteessä sovittua riippumatta siitä, mitä Sopimukseen tai sen muihin liitteisiin on kirjattu. Tässä liitteessä käytetyt termit vastaavat Euroopan Unionin tietosuoja-asetuksessa määriteltyjä termejä. Toimittajalla on oikeus muuttaa näitä ehtoja, mikäli se lainsäädännössä tai sen tulkinnassa tapahtuneen muutoksen tai Toimittajan toimintaympäristössä tai liiketoiminnassa tapahtuneiden muutosten vuoksi on perusteltua.

Rekisterinpitäjä ja henkilötietojen käsittelijä

Rekisterin pitäjänä toimii Asiakas. Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä on siis se henkilö tai organisaatio, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä. Rekisterin pitäjä ei ole Hellewi-järjestelmä, Wildfrost Oy tai Wildfrost Oy:n henkilökunta.

Henkilötietojen käsittely tarkoittaa toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä.
Toimittaja käsittelee Sopimuksen perusteella henkilötiedon käsittelijänä varsinaisena rekisterinpitäjänä toimivan Asiakkaan lukuun ja määrittämässä tarkoituksessa sekä ohjeistuksen mukaisesti tässä liitteessä määritettyjä henkilötietoja ja niistä muodostuvaa henkilörekisteriä.

Henkilörekisterin tarkoituksena on mahdollistaa:

1) Asiakkaan järjestämiin koulutuksiin ja tapahtumiin ilmoittautuneiden henkilöiden tietojen kerääminen koulutuksen tai tapahtuman toteuttamisen edellyttämässä laajuudessa
2) Erilaisten kyselyiden tuottamien tietojen käsittely mukaan luettuna Opetushallituksen vaatimat kalenterivuosikohtaiset tilastot osallistumisista opetukseen sekä vaihtuvasti kausittain tehtävät kyselyt osallistujien taustatiedoista (koulutustausta ja pääasiallinen toiminta), ikä-, kieli- ja sukupuolijakaumista
3) Edellä mainittujen tietojen muu analysointi Asiakkaan määrittämässä lain hyväksymässä tarkoituksessa.

Kerättävät henkilötiedot

Asiakas määrittää kuhunkin koulutukseen tai tapahtumaan liittyen mitä tietoja kerätään. Toimittaja kerää ja säilyttää kuhunkin koulutukseen tai tapahtumaan liittyen käsittelyn kohteena olevat Asiakkaan määrittämät ja Asiakkaan käsittelytoimista laatiman tietosuojaselosteen mukaiset kustakin henkilöstä ilmoitetut tiedot. Tällaisia tietoja voivat olla esimerkiksi henkilön

nimi, tarvittavat yhteystiedot ja tarvittaessa ikä sekä muut tapahtumaan ilmoittautumisen, osallistumisen ja maksamisen mahdollistamiseksi välttämättömät tiedot. Tietoja käsitellään kunkin koulutuksen tai tapahtuman osalta Asiakkaan määrittämän ajan.

Asiakas vastaa siitä, että rekisteröidyistä henkilöistä ei säilytetä takautuvasti taustatietoja ja että jokainen henkilö esiintyy rekisterissä ainoastaan yhden kerran.

Henkilötietojen käsittelyn periaatteet

Asiakas vastaa siitä, että sillä on oikeus ja tarvittavat suostumukset henkilötietojen käsittelyyn. Asiakas vastaa rekisteröidyn henkilön iän varmentamisesta. Asiakas vastaa käsittelytoimiin liittyvän rekisteriselosteen laatimisesta ja saatavilla pidosta sekä rekisteröityjen informoinnista. Toimittaja vastaa siitä, että se käsittelee henkilötietoja asianmukaisia tietoturvaprosesseja noudattaen ainoastaan voimassa olevan lainsäädännön, Asiakkaan tässä Sopimuksessa vahvistamien kirjallisten ohjeiden sekä Asiakkaan Hellewi-järjestelmään tekemien määritysten mukaisesti. Toimittaja on velvollinen ilmoittamaan Asiakkaalle, mikäli Asiakkaan antamat ohjeet Toimittajan arvion mukaan ovat lainvastaisia. Toimittaja toimii tarvittaessa yhteistyössä Asiakkaan tietosuojasta ja -turvallisuudesta vastaavan henkilöstön kanssa.

Asiakas vastaa siitä että, järjestelmän sisältämien tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään. Käytännössä tämä tehdään mm. käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä, henkilökunnan koulutuksella ja ohjeistamisella sekä henkilökunnan sopimusjärjestelyillä.

Henkilörekisteri ja Hellewi-järjestelmä sijaitsevat EU:n alueella, mutta Toimittaja ei takaa, että kaikki tiedonsiirto Asiakkaan tai rekisteröidyn ja Toimittajan välillä tapahtuisi EU:n alueen sisällä Internetin rakenteen ja toimintaperiaatteen takia. Toimittaja hyödyntää palvelun järjestämiseksi kolmansien osapuolien tuotteita, palveluita ja järjestelmiä ja vastaa että kolmansien osapuolien tuotteet, palvelut ja järjestelmät noudattavat tietosuoja-asetuksen velvoitteita, niiltä osin joilta Asiakkaan tietojen käsittely tätä edellyttää. Toimittajalla on oikeus vaihtaa käyttämiään kolmansien osapuolien tuotteita, palveluita tai järjestelmiä toiseen ilman erillistä ilmoitusta. Toimittaja auttaa Asiakasta tietosuoja-asetuksen rekisterinpitäjälle asettamien vaatimusten noudattamisessa, mihin liittyen Toimittajalla on oikeus periä kohtuullinen korvaus, mikäli avun antaminen edellyttää Toimittajan normaalista toiminnasta poikkeavia toimia.

Henkilötietojen siirto muihin järjestelmiin

Asiakas vastaa siitä että, rekisteröidylle henkilölle ilmoitetaan yksiselitteisesti ja selkeästi henkilön tietojen tallentamisen yhteydessä, mihin muihin järjestelmiin henkilön tietoja mahdollisesti siirretään. Rekisteröidylle henkilölle on ilmoitettava mahdollisesta tietojen siirrosta esimerkiksi lasku-, maksu- ja perintäjärjestelmiin ja markkinointijärjestelmiin.

Tietojen säilytys ja elinkaari

Ellei esimerkiksi maksunvälittämiseen tai muuhun syyhyn liittyen Toimittajan oikeutetun edun toteuttamiseksi tai lain velvoittamana jotakin henkilötietoa ole välttämätöntä säilyttää pidempään, henkilötiedot poistetaan viimeistään, kun Asiakas niin edellyttää tai kun Sopimus lakkaa olemasta voimassa. Tietojen säilytysvelvollisuudesta ja -ajasta määrätään henkilötietolaissa sekä arkistolaissa.

Toimittaja palauttaa Asiakkaalle kaikki henkilötiedot, mikäli saa sitä koskevan pyynnön ennen kuin tiedot on tämän edellä lausutun mukaisesti poistettu. Toimittaja saa käsittelyn aikana ja sen päätyttyä säilyttää ja käyttää hyväksi henkilötiedoista anonymisoimalla syntyneitä tietoja toimintansa ja tuotteidensa kehittämisessä. Anonymisoinnilla tarkoitetaan tietojen muokkaamista siten, ettei niistä voida millään toimenpiteillä enää tunnistaa henkilöitä.

Käsittelyn suorittajat

Toimittaja vastaa siitä, että Henkilötietoja käsittelevät ainoastaan henkilöt, jotka ovat sitoutuneet pitämään käsittelemänsä tiedot salassa. Asiakas suostuu siihen, että Henkilötietoja käsitellään Toimittajan harkinnan mukaisesti muidenkin kuin Toimittajan ja sen henkilöstön toimesta. Mikäli tietoja käsitellään tällaisen kolmannen osapuolen toimesta, Toimittaja vastaa siitä, että kyseinen taho sitoutuu tämän Tietosuojaliitteen mukaisiin Toimittajaa koskeviin vastuisiin.

Rekisteröidyn oikeudet

Toimittaja auttaa tarjoamillaan teknisillä rajapinnoilla Asiakasta täyttämään rekisterinpitäjän velvollisuuden vastata pyyntöihin, jotka koskevat rekisteröidyn oikeuksien käyttämistä sekä auttaa rekisterinpitäjää varmistamaan, että ottaen huomioon henkilötiedon luonteen, käsittelyn turvallisuus on asianmukaisesti hoidettu. Toimittaja ilmoittaa välittömästi Asiakkaalle tietoonsa tulleista henkilötietoon liittyvistä tietoturvaloukkauksista sekä mahdollisuuksien mukaan auttaa tietoturvaloukkauksen ilmoittamisesta tarvittaessa myös rekisteröidyille. Toimittaja avustaa Asiakasta soveltuvin osin tietosuojaa koskevassa vaikutustenarvioinnissa, ja on oikeutettu laskuttamaan Asiakkaalta siitä aiheutuneet ylimääräiset kulut.

Tietojen palautus

Toimittajalla on mahdollisuus palauttaa muuttuneita tai poistettuja tietoja jokaiselta päivältä viimeisen kolmen viikon ajalta (21 päivää), siitä hetkestä, kun Asiakas tietojen palautusta pyytää. Edellä mainitun lisäksi tietoja on mahdollista palauttaa puolen vuoden ajalta (6kk) kerran kuukaudessa tehdystä levykuvausta yhteensä kuudesta eri ajankohdasta. Mainittuja ajankohtia vanhemmat varmuuskopiot tuhotaan ylikirjoittamalla, eikä vanhentuneiden varmuuskopioiden tietoja ole mahdollista palauttaa millään toimin. Toimittaja on oikeutettu laskuttamaan tietojen palautuksesta aiheutuneet ylimääräiset kulut.

Jos Asiakas pyytää tietojen palautusta varmistuksista, joissa tietojen poistoa pyytäneen rekisteröidyn henkilön tietoja vielä on, tietojen poistamista pyytäneet rekisteröidyn tietoja ei palauteta muiden tietojen palautuksen yhteydessä järjestelmään, ellei tietojenpalautuspyyntö nimenomaisesti kohdistu virheellisesti järjestelmästä poistetun rekisteröidyn henkilön tietoihin.

Tietosuojan varmistaminen

Toimittaja toimittaa Asiakkaalle pyydettäessä tarpeelliset asiakirjat ja sallii auditoinnit ja avustaa niissä sen osoittamiseksi, että Toimittaja noudattaa tämän liitteen määräyksiä. Auditoinnin suorittajan on sitouduttava pitämään salassa auditoinnin yhteydessä saamansa tiedot. Toimittajalla on oikeus kieltäytyä auditoinnista, mikäli sen suorittajaksi on osoitettu Toimittajan suoraksi tai välilliseksi kilpailijaksi katsottava taho tai sellainen taho, jonka asiantuntemusta tai luotettavuutta voidaan perustellusti epäillä. Asiakas vastaa kaikista auditointien kustannuksista. Toimittaja ohjaa kaikki Asiakkaaseen liittyvät tietosuojaviranomaisten tiedustelut myös Asiakkaalle. Toimittaja ei edusta Asiakasta eikä toimi Asiakkaan puolesta tietosuojaan liittyvissä asioissa.

Vastuu vahingoista

Toimittajan palvelu on vakuutettu mahdollisten tietoturvamurtojen, -rikosten ja vahinkojen varalta. Toimittaja ei vastaa Asiakkaan toiminnallaan aiheuttamista vahingoista. Mahdolliset vahingonkorvausvastuut tai niiden rajoitukset on sovittu tarkemmin Hellewi-palvelun toimitussopimuksessa, jonka liite tämä dokumentti on.

Tietoturva

Toimittaja vastaa siitä, että sen henkilötietojen käsittelyyn liittyvään toimintaan sovelletaan asianmukaisia riskienhallinta- ja tietoturvaprosesseja. Toimittaja toteuttaa tietosuojalainsäädännön ja tämän sopimuksen määräämät riittävät tekniset ja organisatoriset suojatoimenpiteet käsittelemiensä henkilötietojen suojaamiseksi. Ottaen huomioon Asiakkaan määrittämän henkilötietojen arkaluontoisuuden sekä niihin liittyvän riskitason, toimittaja suojaa henkilötietojen käsittelyssä käytettävät järjestelmät ja tietoliikenteen asianmukaisilla tietoturvaratkaisuilla sen varmistamiseksi, että henkilötietojen luottamuksellisuus, eheys ja saatavuus on turvattu siihen saakka, että henkilötiedot on tämän sopimuksen mukaisesti poistettu Toimittajan järjestelmästä.

Lokit

Järjestelmän käytöstä muodostuu useita eritasoisia lokitapahtumia. Ensimmäinen lokitaso on järjestelmän kuormantasaajilla, toinen jokaisella järjestelmään liitetyllä www-palvelimella ja kolmas lokitaso muodostuu Hellewi-järjestelmän kirjautumis- ja käyttölokista. Asiakkaalla on pääsy Hellewi-järjestelmän lokeihin. Toimittajalla on pääsy Hellewi-järjestelmän lokien lisäksi myös kuormantasaajan ja www-palvelimien lokeihin. Lokien tietoja voidaan yhdistää toisiinsa. Asiakas voi pyytää Toimittajalta apua lokien perusteella tehtävästä mahdollisten ongelma- tai rikostilanteiden selvityksistä. Toimittajalla on oikeus periä kohtuullinen korvaus avun antamisesta.

Kuormantasaajien ja www-palvelimien lokit muodostuvat http-pyyntökohtaisesti ja niihin kerätään seuraavat tiedot:

- Http-pyynnön aikaleima
- Http-pyynnön lähde ja kohde (referer ja request)
- IP-osoite
- Käytetyn selaimen tai sovelluksen User Agent

Listattujen tietojen perusteella on mahdollista selvittää järjestelmän käyttäjän käyttämän Internet-yhteyden operaattori ja käytetty käyttöjärjestelmä, sovellus sekä laite versionumerotasolla huomioiden, että edellä mainittujen tietojen väärentäminen ja peittäminen on mahdollista.

Kirjautumisloki

Hellewi-järjestelmän kirjautumisloki kirjaa järjestelmään kirjautuneet henkilöt. Myös epäonnistuneet kirjautumiset kirjataan lokiin sekä syy kirjautumisen epäonnistumisesta. Lokiin kirjataan seuraavat tiedot:

- Lokitapahtuman tunniste
- Lokitapahtuman järjestysnumero
- Sisäänkirjautumisaika
- Uloskirjautumisaika
- Tunnistautumistapa, jos käytössä on useita eri tunnistautumistapoja
- Käyttäjänimi
- Käyttöoikeustaso
- IP-osoite
- Istuntotunniste
- Metatietoja käytettävästä laitteesta ja sovelluksesta jonka kautta järjestelmään kirjaudutaan

Lokitapahtumaan liittyvät tiedot on yksilöitävissä riittävällä tarkkuudella, että uskottava valvonta on mahdollista. Kirjautumislokista ei voi poistaa tietoja ja kirjautumislokin eheyttä voidaan seurata ja valvoa lokitapahtumien tunnisteen ja järjestysnumeron perusteella.

Lokitietojen luottamuksellisuus, eheys ja saatavuus on turvattu siihen saakka, kunnes Asiakas lopettaa järjestelmän käytön. Kirjautumislokin tietoja kerätään järjestelmän käyttöönotosta lähtien eikä kirjautumislokin tietoja poisteta ajastetusti, ellei tästä Asiakkaan kanssa toisin sovita.

Käyttöloki

Hellewi-järjestelmän käyttölokiin kirjataan merkintä sekä tietosisältö kaikista järjestelmään kohdistuvista toimenpiteistä. Lokimerkintä tehdään siis aina, kun järjestelmästä joko näytetään, muokataan tai poistetaan tietoa. Käyttölokiin kirjataan seuraavat tiedot:

- Lokitapahtuman tunniste
- Lokitapahtuman järjestysnumero
- Aikaleima
- Käyttäjätunniste
- Käsitellyn tiedon tyyppi

- Käsitellyn tiedon tunniste
- Tapahtuman tyyppi (katselu, päivitys, tuhoaminen)
- Käsitelty tietosisältö kokonaisuudessaan

Käyttölokin tietoja kerätään järjestelmän käyttöönotosta lähtien eikä käyttölokin tietoja poisteta ajastetusti, ellei tästä Asiakkaan kanssa toisin sovita. Jos rekisteröity pyytää tietojensa poistamista järjestelmästä ja tiedot pyynnön jälkeen poistetaan, poistetaan rekisteröidyn identifioivat tiedot kokonaisuudessaan myös käyttölokista.

Tietojen poistaminen rekisteröidyn pyynnöstä

Rekisteröidyllä henkilöllä on oikeus pyytää tietojen poistamista osittain tai kokonaan rekisteristä. Mikäli estettä tietojen poistamiselle ei ole, voidaan tiedot poistaa ja muuttaa niin, ettei niistä tunnisteta enää henkilöä. Henkilön tietoja ei tämän jälkeen voida palauttaa järjestelmään millään tavalla edes Asiakkaan tai rekisteröidyn henkilön pyynnöstä. Jos henkilö rekisteröidään tietojen poistamisen jälkeen uudestaan järjestelmään, käsitellään henkilöä uutena henkilönä.

Asiakas vastaa siitä, että rekisteröidyn tietojen poistamiselle ei ole mahdollista estettä esimerkiksi siinä tapauksessa, että rekisteröidyllä henkilöllä on muihin järjestelmiin siirrettyjä avoimia laskuja. Asiakas vastaa siitä, että rekisteröidyn tietojen poistamiselle ei ole lain edellyttämiä esteitä. Tällainen este voi olla esimerkiksi tilastointivelvollisuus. Rekisteröidyn henkilön tiedot on kuitenkin poistettava sen jälkeen, kun tilastointivelvollisuus on täytetty. Tästä johtuen Hellewi-järjestelmässä ajantasaisesti haettavat historiatilastot voivat vääristyä. Tilastotiedoista on mahdollisuus tallentaa ote, jonka tiedot eivät muutu, vaikka järjestelmästä poistetaan henkilötietoja.

Asiakas vastaa siitä, että rekisteröidyistä henkilöistä ei säilytetä takautuvasti taustatietoja ja että jokainen henkilö esiintyy rekisterissä ainoastaan yhden kerran.

Tietojen siirtäminen rekisteröidyn pyynnöstä

Jos rekisteröity henkilö haluaa siirtää tietonsa johonkin muuhun järjestelmään, tietojen poiston yhteyteen on tehty tietojen vienti koneellisesti luettavassa muodossa. Toimittaja määrittää koneellisesti luettavien tietojen muodon. Asiakas toimittaa tiedot rekisteröidylle henkilölle sähköisessä muodossa Asiakkaan määrittämällä turvallisella tavalla.