HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVA SOPIMUSLIITE

1 JOHDANTO

Tämä henkilötietojen käsittelyä koskeva sopimusliite ("Liite") sovelletaan Oikio Digital Oy:n ja Oikio Oy:n (jäljempänä "Toimittaja") ja asiakkaan ("Asiakas") välillä solmittuihin sopimuksiin, liittyen Toimittajan tuotteisiin ja palveluihin, joissa käsitellään Asiakkaiden henkilötietoja ("Sopimus").

Tässä Liitteessä sovitaan Asiakkaan henkilötietojen tietosuojasta ja tietoturvasta Toimittajan palveluissa. Tämä Liite muodostaa osapuolten välille EU:n yleisen tietosuoja-asetuksen (EU 679/2016) mukaisen kirjallisen sopimuksen henkilötietojen käsittelystä.

Jos tämän Liitteen ja Sopimuksen henkilötietojen käsittelyä koskevat ehdot ovat ristiriidassa keskenään, osapuolet soveltavat ensisijaisesti tämän Liitteen ehtoja.

2 MÄÄRITELMÄT

Tässä Liitteessä tarkoitetaan EU:n tietosuoja-asetuksen mukaisesti:

"rekisterinpitäjällä" Asiakasta, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

"käsittelijällä" Toimittajaa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun Sopimuksen perusteella.

"käsittelyllä" toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin 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.

"henkilötiedoilla" kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä "rekisteröityyn", liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

"henkilötietojen tietoturvaloukkauksella" tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

3 TIETOSUOJA JA HENKILÖTIETOJEN KÄSITTELY

3.1 TOIMITTAJAN JA ASIAKKAAN VASTUUT

Toimittaja käsittelee Asiakkaan henkilötietoja Asiakkaan lukuun ja tämän toimeksiannosta Sopimuksen perusteella. Henkilötietoja voivat olla esim. työntekijöitä, asiakkaita taikka muita luonnollisia henkilöitä koskevat tiedot. Asiakas on palvelussa käsiteltävien henkilötietojensa rekisterinpitäjä ja Toimittaja käsittelijä. Osapuolet sitoutuvat noudattamaan Suomessa ja EU:ssa kulloinkin voimassa olevaa henkilötietojen käsittelyä koskevaa lainsäädäntöä, asetuksia sekä viranomaisten määräyksiä ja ohjeistuksia ja tarvittaessa muuttamaan tämän Liitteen ehtoja niiden mukaiseksi.

Rekisterinpitäjänä Asiakas on vastuussa siitä, että sillä on tarvittavat oikeudet ja suostumukset Sopimuksen mukaiseen henkilötietojen käsittelyn. Asiakas vastaa selosteen laatimisesta ja saatavilla pidosta sekä rekisteröityjen informoinnista ja ilmoituksista tietosuojaviranomaisille. Asiakas vastaa Toimittajalle antamiensa henkilötietojen oikeellisuudesta.

Asiakkaalla on oikeus ja velvollisuus määrittää henkilötietojen käsittelyn tarkoitus ja keinot. Käsittelyn kohde, luonne ja tarkoitus on tarkemmin määritelty Sopimuksessa. Oikion palveluissa käsiteltävien henkilötietojen tyypit ja rekisteröityjen ryhmät on määritelty Liitteessä 1 tai palvelukuvauksessa/palvelusopimuksessa.

Toimittajalla on oikeus käsitellä Asiakkaan henkilötietoja ja muita Asiakkaan tietoja vain Sopimuksen, tämän Liitteen ja Asiakkaan kirjallisten ohjeiden mukaisesti ja vain siltä osin ja siten kuin on tarpeellista palveluiden toimittamiseksi. Toimittaja ilmoittaa Asiakkaalle, mikäli ohjeissa havaitaan EU:n tai Suomen tietosuojasäännösten vastaisuutta ja tällöin Toimittaja voi välittömästi kieltäytyä ja lopettaa soveltamasta Asiakkaan ohjeita.

Toimittaja ylläpitää palvelun kuvausta tai muuta EU:n tietosuoja-asetuksen vaatimaa selostetta palvelussa suoritettavista käsittelytoimista. Toimittajalla on oikeus kerätä Sopimuksen mukaisten palvelujen käytöstä anonyymiä ja tilastollista tietoa, joka ei yksilöi Asiakasta eikä rekisteröityjä ja käyttää sitä palvelujensa analysointiin ja kehittämiseen.

3.2 TIETOJEN POISTO/PALAUTTAMINEN

Sopimuksen päätyttyä Toimittaja palauttaa tai poistaa, Asiakkaan antaman ohjeistuksen mukaisesti, kaikki Asiakkaan henkilötiedot Asiakkaalle sekä poistaa olemassa olevat jäljennökset, ellei sovellettava lainsäädäntö edellytä henkilötietojen säilyttämistä.

3.3 ALIHANKKIJAT

Toimittajalla on oikeus käyttää alihankkijoita Asiakkaan henkilötietojen käsittelyssä. Toimittaja vastaa alihankkijoiden toimista kuin omistaan ja laatii alihankkijoiden kanssa vastaavat kirjalliset sopimukset henkilötietojen käsittelystä. Palvelusopimuksessa tai palvelukuvauksessa on lista alihankkijoista, joita Toimittaja aikoo käyttää Sopimuksen mukaiseen henkilötietojen käsittelyyn. Asiakkaalla on perustellusta syystä oikeus vastustaa uuden alihankkijan käyttöä.

3.4 TOIMITTAJAN AVUSTAMISVELVOLLISUUS

Toimittaja siirtää Asiakkaalle kaikki Rekisteröidyiltä saamansa henkilötietojen tarkastamista, oikaisemista, poistamista tai niiden käsittelyn kieltämistä koskevat pyynnöt tai muut Rekisteröidyltä saamansa pyynnöt. Asiakkaan velvollisuutena on huolehtia ko. pyyntöihin vastaamisesta. Ottaen huomioon käsittelytoimen luonteen, Toimittaja auttaa Asiakasta asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään Asiakkaan velvollisuuden vastata Rekisteröidyn pyyntöihin.

Toimittaja on velvollinen, ottaen huomioon henkilötietojen käsittelyn luonteen ja sen saatavilla olevat tiedot, auttaa Asiakasta varmistamaan, että sille laissa asetettuja velvollisuuksia noudatetaan. Nämä velvollisuudet voivat käsittää tietoturvallisuutta, tietoturvaloukkauksista ilmoittamista, tietosuojaa koskevaa vaikutustenarviointia ja ennakkokuulemista koskevia velvoitteita. Toimittaja on velvollinen avustamaan Asiakasta ainoastaan sovellettavan tietosuojalainsäädännön henkilötiedon käsittelijälle asettamien velvoitteiden mukaisessa laajuudessa. Ellei toisin sovita, Toimittajalla on oikeus laskuttaa tämän sopimuskohdan mukaisista toimista aiheutuvat kustannukset voimassa olevan hinnastonsa mukaisesti.

Toimittaja ohjaa kaikki tietosuojaviranomaisten tiedustelut suoraan Asiakkaalle, eikä Toimittajalla ei ole valtuuksia edustaa Asiakasta tai toimia Asiakkaan puolesta Asiakasta valvovien tietosuojaviranomaisten kanssa.

4 KÄSITTELY EU:N / ETA:N ULKOPUOLELLA

Pääsääntöisesti henkilötietoja ei siirretä Euroopan talousalueen (ETA) ulkopuolelle. Käsittelemme henkilötietoja ensisijaisesti EU/ETA-alueella sijaitsevilla palvelimilla.

Mikäli poikkeuksellisesti käytämme palveluntarjoajia, joiden palvelimet sijaitsevat EU/ETA-alueen ulkopuolella, varmistamme tietosuojan riittävän tason seuraavilla mekanismeilla: EU:n komission hyväksymät vakiosopimuslausekkeet (SCC), EU–US Data Privacy Framework -sertifiointi tai muu vastaava siirtomekanismi sekä tarvittaessa täydentävät suojatoimet.

5 AUDITOINTI

Asiakkaalla tai tämän valtuuttamalla auditoijalla (joka ei kuitenkaan saa olla Toimittajan kilpailija) on oikeus auditoida Liitteen alainen toiminta. Sopijapuolet sopivat auditoinnin ajankohdasta ja muista yksityiskohdista hyvissä ajoin ja vähintään 14 työpäivää ennen tarkastusta. Auditointi tulee suorittaa tavalla, joka ei haittaa Toimittajan ja sen alihankkijoiden sitoumuksia kolmansiin osapuoliin nähden. Asiakkaan edustajien ja auditoijan on allekirjoitettava tavanomaiset salassapitositoumukset. Osapuolet vastaavat omalta osaltaan auditoinnista aiheutuvista kustannuksista.

6 TIETOTURVA

Toimittaja toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet Asiakkaan henkilötietojen suojaamiseksi ottaen huomioon käsittelyn sisältämät riskit, erityisesti

siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen tahaton tai laiton tuhoaminen, hävittäminen, muuttaminen, luvaton luovuttaminen tai henkilötietoihin pääsy.

Suojatoimenpiteiden järjestämisessä otetaan huomioon saatavilla olevat tekniset vaihtoehdot ja niiden kustannukset suhteessa käsillä olevaan tietojenkäsittelyyn liittyviin erityisiin riskeihin sekä käsiteltävien henkilötietojen arkaluonteisuuteen.

Asiakas on velvollinen varmistamaan, että Toimittajalle tiedotetaan kaikista niistä Asiakkaan toimittamiin henkilötietoihin liittyvistä seikoista, kuten riskiarvioinneista sekä erityisten henkilöryhmien käsittelystä, jotka vaikuttavat tämän Liitteen mukaisiin teknisiin ja organisatorisiin toimenpiteisiin. Toimittaja varmistaa, että henkilötietojen käsittelyyn osallistuva Toimittajan tai Toimittajan käyttämän alihankkijan henkilöstö noudattaa asianmukaista salassapitovelvollisuutta.

7 TIETOTURVALOUKKAUKSESTA ILMOITTAMINEN

Toimittajan on ilmoitettava Asiakkaalle kaikista henkilötietoihin kohdistuneista tietoturvaloukkauksista ilman aiheetonta viivytystä loukkauksesta tiedon saatuaan tai kun Toimittajan käyttämä alihankkija on saanut loukkauksen tietoonsa.

Asiakkaan pyynnöstä Toimittajan tulee ilman aiheetonta viivytystä toimittaa Asiakkaalle kaikki asiaankuuluva tietoturvaloukkaukseen liittyvä tieto. Siltä osin kuin kyseinen tieto on Toimittajan saatavilla, Toimittajan on Asiakkaalle tehtävässä ilmoituksessa kuvattava vähintään:

a) tapahtunut tietoturvaloukkaus,

b) mahdollisuuksien mukaan rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvoidut lukumäärät,

c) kuvaus tietoturvaloukkauksen aiheuttamista todennäköisistä seurauksista, ja

d) kuvaus korjaavista toimenpiteistä, jotka Toimittaja on suorittanut tai tulee suorittamaan tietoturvaloukkausten ennaltaehkäisemiseksi jatkossa, sekä tarvittaessa myös toimenpiteet mahdollisten tietoturvaloukkauksen haittavaikutusten minimoimiseksi.

Toimittaja dokumentoi ja raportoi selvityksen tulokset ja suoritetut toimenpiteet Asiakkaalle. Asiakas vastaa tarvittavista ilmoituksista tietosuojaviranomaisille.

8 MUUT EHDOT

Jos henkilölle aiheutuu EU:n tietosuoja-asetuksen tai Liitteen loukkauksista aineellista tai aineetonta vahinkoa, Toimittaja on vastuussa vahingosta vain siltä osin, kuin se ei ole noudattanut nimenomaisesti henkilötietojen käsittelijöille osoitettuja EU:n tietosuoja-asetuksen tai tämän Liitteen velvoitteita. Kumpikin osapuoli on velvollinen maksamaan määrätyistä vahingonkorvauksista ja hallinnollista sakoista vain sen osan, joka vastaa sille

tietosuojavalvontaviranomaisen tai tuomioistuimen lainvoimaisessa päätöksessä vahvistettua vastuuta vahingosta. Muilta osin osapuolten vastuu määräytyy Sopimuksen perusteella.

Toimittaja tiedottaa Asiakasta kirjallisesti kaikista muutoksista, jotka saattavat vaikuttaa sen kykyyn tai mahdollisuuksiin noudattaa tätä Liitettä ja Asiakkaan antamia kirjallisia ohjeita.

Toimittaja voi muuttaa tämän Liitteen sisältöä perustellusta syystä ilmoittamalla siitä Asiakkaalle kirjallisesti kaksi (2) viikkoa ennen muutoksen voimaanastumista.

Tämä Liite on voimassa (i) niin pitkään kuin Sopimus on voimassa tai (ii) osapuolilla on henkilötietojen käsittelytoimiin perustuvia velvoitteita toisiaan kohtaan. Velvoitteet, joiden on niiden luonteen vuoksi tarkoitus säilyä voimassa tämän Liitteen voimassaolon päättymisestä riippumatta, jäävät voimaan Liitteen päättymisen jälkeen.

LIITE 1

Toimittajan palveluissa käsiteltävien henkilötietojen tyypit ja rekisteröityjen ryhmät*

TOIMITTAJAN PALVELU	REKISTERÖITYJEN RYHMÄ	HENKILÖTIETOJEN TYYPIT
KAIKKI PALVELUT		
Kaikki palvelut	Oikion asiakas	Nimi, yhteystiedot, rooli, käyttäjätunnus ja salasana
Tuotteistetut markkinointipalvelut		
Mainontakone	Oikion asiakkaan asiakas	Evästeet
Kotisivukone	Oikion asiakkaan asiakas	Evästeet, verkkotunnistetiedot, välitystiedot, asiakasviestit
Sähköpostipalvelut	Oikion asiakas	
ASIANTUNTIJAPALVELUT		
Hakukone- ja tekoälyoptimointi	Oikion asiakkaan asiakas	Evästeet
Mainonnan optimointi	Oikion asiakkaan asiakas	Yhteystiedot, Evästeet
Analytiikka	Oikion asiakkaan asiakas	Evästeet

*Lista ei sisällä kaikkia Toimittajan palveluita, vaan henkilötietojen tyypeistä ja rekisteröityjen ryhmistä voidaan sopia Asiakkaan kanssa erikseen myös palvelusopimuksella tai muulla sopimuksella.

LIITE 2

TOIMITTAJAN TIETOTURVAKÄYTÄNNÖT

Toimittaja noudattaa Sopimukseen liittyvässä henkilötietojen käsittelyssään tässä liitteessä esitettyjä tietoturvakäytäntöjä. Toimittaja on sitoutunut jatkuvasti kehittämään tietoturvakäytäntöjä. Toimittaja pidättää oikeuden muuttaa tietoturvakäytäntöjään vastatakseen esimerkiksi lainsäädäntöön, muuttuvaan teknologiaan tai liiketoimintarpeeseen.

1. TIETOTURVAN HALLINNAN PERIAATTEET

Toimittajan tietoturvan hallinnan roolit ja vastuut ovat seuraavat:

- **Johto**
    - Vastuu määritellä Toimittajan tietoturvapolitiikalle asetetut vaatimukset ja tavoitteet, jotka ovat olennaisia riskienhallinnalle ja turvallisuusajattelun kehittämiselle Toimittajan organisaation yleisen politiikan ja tavoitteiden mukaisesti.
    - Vastuu arvioida ja mitata tietoturvakäytäntöjä ja niiden toteutumista.
- **Tietoturvapäällikkö ja esimiehet**
    - Vastuu toteuttaa, kehittää ja seurata tietoturvapolitiikkaa ja siihen liittyviä turvamekanismeja, prosesseja ja menettelytapoja.
- **Tietoturvapäällikkö**
    - Vastuu ryhtyä ehkäiseviin ja korjaaviin toimenpiteisiin tietoturvaloukkauksiin ja tietoturvan puutteisiin liittyen sekä toteuttaa katselmuksia ja toimia johdon ohjeistuksen mukaisesti tavoitteena Toimittajan tietoturvallisuuden jatkuvan parantaminen.
- **Henkilöstö**
    - Vastuu on noudattaa sovittuja menettelytapoja ja ohjeita huolellisesti käsitellessään Asiakkaiden henkilötietoa omassa toiminnassaan.
    - Jokainen Toimittajan työntekijä allekirjoittaa osana työsopimusta salassapitosopimuksen, jossa mm. sitoutuu noudattamaan Toimittajan luottamuksellisen aineiston käsittelypolitiikkaa.

2. TIETOTURVA PALVELUISSA

Toimittaja huolehtii palveluidensa tietoturvasta käyttäen asianmukaisia teknisiä ja hallinnollisia menettelyjä. Palveluiden ylläpito hoidetaan hyvien tietoturvakäytäntöjen mukaan, mm.

suojaamalla IT-ympäristöt palomuureilla sekä huolehtimalla käyttöjärjestelmien ja ohjelmistojen tietoturvapäivityksistä asianmukaisesti. Toimittajan palvelut tuotetaan moderneissa pilviympäristöissä, joissa on toteutettu korkea tietoturvallisuus. Palvelinympäristöinä käytettäviltä pilviympäristöiltä vaaditaan asianmukaista tietoturvasertifiointia. Henkilötietojen suojaamiseen ja tietoturvaan kiinnitetään erityistä huomiota palveluita suunniteltaessa ja toteutettaessa.

3. JÄRJESTELMIEN JA IT-INFRASTRUKTUURIN TIETOTURVALLISUUS

Pääsy tuotantoympäristöihin sekä tietokantoihin on vain erikseen nimetyillä henkilöillä, jotka tarvitsevat toimenkuvansa takia pääsyn ympäristöihin. Kaikki liikennöinti ympäristöihin tehdään henkilökohtaisilla tunnuksilla ja käyttäen salattua yhteyttä. Toimittajalla on asianmukainen käyttäjätunnusten hallintaprosessi, jolla hallinnoidaan käyttäjien pääsyä IT-infrastruktuuriin.

- Käyttäjätunnusten hallintaprosessi sisältää mm. seuraavat asiat:
    - käyttäjätunnukset ovat yksilöllisiä siten, että järjestelmiä käyttäneet henkilöt voidaan tunnistaa;
    - salasanoja varten on hallintapolitiikka, joka pitää sisällään vaatimukset salasanojen vahvuudesta, käyttöajoista ja suojatusta toimittamisesta;
    - käyttäjätunnuksia seurataan säännöllisesti ja tarpeettomat käyttäjätunnukset poistetaan tai jäädytetään;
    - käyttäjäoikeudet määritetään niin, että ne annetaan vain käyttäjän hyväksyttävään tarpeeseen;
    - järjestelmävalvojan ja normaalikäytön tunnukset on eriytetty;
    - oletustunnistautumistietoja ei käytetä missään tietojärjestelmissä.

Toimittaja arvioi säännöllisesti tietoturvan tasoa ja päivittää tietoturvakäytäntöjään tarpeen mukaan. Lisäksi Toimittajalla on palveluiden sisältö ja luonne huomioon ottaen riittävä varmistus- ja palautussuunnitelma. Toimittaja huolehtii varmuuskopioinnista ja pyrkii varmistamaan asianmukaisesti varmuuskopioiden eheyden ja palautettavuuden.

Toimittaja suunnittelee sen ICT-infrastruktuurin ja verkkoyhteydet sekä niiden hallinnan siten, että ne suojaavat tietojärjestelmiä, informaatiota, käyttäjiä ja sähköistä viestintää.

Toimittaja valvoo, analysoi ja pitää kirjaa sovelluksia, tietojärjestelmiä ja verkkoja koskevista tietoturvatapahtumista ja ongelmista.

Toimittaja suojaa Asiakkaan tiedot asianmukaisin teknisin järjestelyin. Toimittajalla on muun muassa riittävät järjestelmät ja toimintamallit tietomurtojen havaitsemiseen ja estämiseen

sekä virus- ja haittaohjelmistoilta suojautumiseen. Lisäksi Toimittaja valvoo sovellusten ja IT-infrastruktuurin haavoittuvuutta ja konfiguraatioiden turvallisuusvaatimusten mukaisuutta.

Toimittaja käyttää standardoituja konfiguraatioita palvelimissa ja niiden ylläpitojärjestelmissä. Lisäksi Toimittaja huolehtii riittävästä haavoittuvuuksien hallintaprosessista ja varmistaa säännölliset tietoturvapäivitykset. Toimittaja asentaa automatisoidun, ajantasaisen ja toimivan haittaohjelmien suojan Toimittajan työasemiin.

4. TIETOTURVATAPAHTUMIEN HALLINTA JA TIETOTURVALOUKKAUKSET

Toimittajalla on tietoturvatapahtumien yleinen hallintaprosessi, jota Toimittaja pitää yllä ja täydentää tarpeen mukaan. Tietoturvatapahtumien hallintaprosessilla Toimittaja pyrkii valvomaan, tutkimaan ja estämään Asiakkaaseen vaikuttavia tietoturvallisuuden vaarantavia tapahtumia. Henkilötietojen käsittelyssä käytettävien järjestelmien käytettävyys ja vikasietoisuus on varmistettu sen estämiseksi, etteivät henkilötiedot pääse tuhoutumaan, häviämään tai muuttumaan. Henkilötiedot suojataan siten, että ne pystytään palvelusta riippuen palauttamaan fyysisen tai teknisen vian sattuessa. Toimittaja suorittaa tietoturvatarkastuksia ja turvallisuusarviointeja hyödyntäen ulkopuolisia tietoturvan arvioijia. Mahdollisissa tietoturvaloukkauksissa Toimittaja auttaa Asiakasta tunnistamaan ja ratkaisemaan tietoturvapoikkeamat ilman aiheetonta viivästystä.