Sopimus henkilötietojen käsittelystä (DPA)

Sopimuksen osapuolet

Tämä sopimus on osa CardPlus Oyn yleisiä toimitusehtoja. Tämä sopimus tulee voimaan, kun rekisterinpitäjä tai tämän edustaja, toimittaa henkilötietoaineiston toimittajalle.

Asiakas
Jäljempänä "Asiakas"

CardPlus Oy
Y-tunnus: 2784644-4
Jäljempänä "Toimittaja"

Jäljempänä yhdessä "Osapuolet"

Yleiset sopimusehdot

Tällä sopimuksella osapuolet sopivat henkilötietojen toimittamisesta, säilyttämisestä, prosessoinnista sekä tuhoamisesta.

Toimittajan asema, oikeudet ja velvollisuudet

Toimittaja ja asiakas sopivat tällä sopimuksella käyttöoikeuksien antamisesta asiakkaan toimittamiin henkilötietoihin. Näiden henkilötietojen perusteella toimittajan tehtävänä on valmistaa ja toimittaa asiakkaalle tilatut tunnisteet. Tunnisteiden valmistamiseksi, toimittajalle toimitetaan tietoaineisto, joka sisältää henkilötietoja. Toimittaja säilyttää näitä henkilötietoja omassa järjestelmässään toimeksiannon ajan. Toimittaja on henkilötietolain tarkoittama käsittelijä.
Toimittaja avustaa asiakasta mahdollisuuksien mukaan rekisteröityjen oikeuksien toteuttamisessa.

Henkilötietoja käytetään vain tilattujen tunnisteiden valmistamiseksi. Toimittajan vastuulla on varmistaa, että toimittajan valmistamille tunnisteille painetaan henkilötietorekisteristä saatavien tietojen mukaiset tiedot. Toimittaja voi tämän tarkoituksen toteuttamiseksi suorittaa tarpeellisia käsittelytoimenpiteitä, kuten esimerkiksi tarkastella, poistaa tai muokata toimitettuja henkilötietoja.

Toimittaja huolehtii siitä, että toimittajan tuotanto- ja varastotiloihin pääsevät vain toimittajan nimeämät henkilöt. Toimittajan henkilöstöllä on salassapitovelvollisuus ja he ovat allekirjoittaneet vaitiolositoumuksen. Toimittajan tietokoneiden virustorjunta ja palomuurit ja toimitilojen kulunvalvonta on järjestetty tarkoituksenmukaisesti. Tietoturvariskejä hallitaan erikseen määriteltävän ja kuvattavan riskienhallinta-prosessin avulla. Hyväksyttävän riskitason määrittelee Toimittajan johtoryhmä riskianalyysin tulosten perusteella ja yhteisesti valmisteltujen kriteereiden ja mittarien avulla.

Toimittajan henkilöstöä on riittävä määrä ja se on saanut perehdytyksen ja koulutuksen sekä tietosuojaan että tietoturvaan liittyen. Toimittaja tekee säännöllisesti vaikutusten arviointia toiminnastaan. Toimittaja

sitoutuu siihen, että kyseisiä henkilötietoja tuotannossa ja varastossa käsittelevät vain ne henkilöt, joiden työtehtävien hoitaminen sitä edellyttää. Toimittaja vastaa siitä, että toimittajan muut asiakkaat eivät pääse käsiksi asiakkaan tietoihin.

Toimittaja toteuttaa tarpeelliset tekniset ja organisatoriset toimenpiteet käsittelyn turvallisuuden varmistamiseksi. Asiakkaalla on oikeus saada tietoja henkilötietojen käytöstä ja säilytyksestä. Toimittaja antaa pyynnöstä lisätietoja käytössä olevista teknisistä ja organisatorisista turvatoimista ja sallii niiden tarkastukset erikseen sovittavalla tavalla. Toimittaja hyväksyy asiakkaan tai muun sen valtuuttaman auditoijan suorittamat auditoinnit ja toimittaja osallistuu niihin. Ulkopuolinen auditoiva taho ei kuitenkaan saa olla kilpaileva yritys.

Toimittajalla on mahdollisuus käyttää alihankkijoita tai siirtää sopimus kolmannelle osapuolelle asiakkaan kirjallisella suostumuksella. Mahdollisia alihankkijoita koskevat tietosuojan ja tietoturvan osalta samat vaatimukset kuin varsinaista toimittajaa.

Toimittajalle kuuluvat rekisterinkäsittelyyn liittyvät tehtävät henkilötietojen käsittelyssä. Toimittajan on huolehdittava henkilötietojen ylläpidosta, suojaamisesta, tietoturvallisuudesta ja tietojen säilyttämisestä asiakkaan lukuun, sekä tarkastusoikeuden toteuttamisesta. Toimittaja vastaa siitä, että se toteuttaa osaltaan tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi, asiattomien pääsyn tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta luvattomalta käsittelyltä.

Toimittaja ei saa käyttää tietoja hyväkseen tai luovuttaa henkilötietoja kenellekään muuten kuin sopimuksen tarkoittamassa laajuudessa ja sopimuksen mukaista tehtävää hoitaessaan ilman kirjallista ennakkolupaa, ellei tähän ole lakiin perustuvaa velvollisuutta. Toimittaja voi käyttää tietoja vain toimeksiantosopimuksessa määritellyillä tavoilla ja sopimuksessa määriteltyihin tarkoituksiin.

Toimittaja avustaa Asiakasta mahdollisuuksien mukaan täyttämään velvollisuuden vastata GDPR:ssä määriteltyihin pyyntöihin, koskien rekisteröidyn oikeuksien käyttämistä, kuten:

a) oikeus saada pääsy henkilötietoihin;
b) oikeus henkilötietojen oikaisemiseen ja poistamiseen;
c) oikeus henkilötiedon käsittelyn rajoittamiseen;
d) oikeus siirtää henkilötietoja järjestelmästä toiseen;
e) oikeus vastustaa henkilötietojen käsittelyä.

sekä GDPR:ssä määriteltyjen rekisterinpitäjän velvollisuuksien täyttämisessä, kuten:

f) asianmukaisten teknisten ja organisatoristen toimenpiteiden toteuttaminen;
g) avustaminen tietoturvaloukkauksista ilmoittamisessa valvontaviranomaiselle ja rekisteröidylle;
h) osallistuminen tarvittaessa tietosuojaa koskevan vaikutustenarvioinnin tekemiseen ja valvontaviranomaisen ennakkokuulemiseen.

Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit Toimittajan on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten:

i) henkilötietojen pseudonymisointi ja salaus;
j) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;
k) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;

l) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Toimittaja avustaa yllä mainituissa tapauksissa Asiakasta tämän esittämän pyynnön ja ilmoittamien tietojen perusteella käyttäen omia teknisiä ratkaisuja ja tietoturvaohjeitaan. Toimittaja ilmoittaa Asiakkaalle, mikäli rekisteröity on ilmoittanut suoraan Toimittajalle oikeuksiensa käyttämisestä. Osapuolet sopivat yhdessä siitä, miten tällaisiin pyyntöihin reagoidaan käytännössä ja kumpi taho pyyntöihin vastaa.

Toimittajalla on oikeus laskuttaa Asiakasta Toimittajan tehtäväksi sovituista sekä yllä mainituista toimenpiteistä palveluhinnastonsa mukaisesti.

Asiakkaan asema, oikeudet ja velvollisuudet

Asiakas, jonka nimissä sopimus syntyy toimii asiakkaan rekisterinpitäjäjänä ja hänellä on siihen valtuudet ellei erikseen kirjallisesti muuta ilmoita.

Asiakas toimii henkilötietoaineiston toimittajana. Aineisto on toimitettava toimittajalle tietoturvallisesti.

a) Ensisijaisesti Toimittajan tilausjärjestelmän kautta
b) Toissijaisesti SFTP –palvelimen kautta
c) Muu tietoturvallinen erikseen sovittu tapa

Asiakas vastaa siitä, että tietojen korjaukset, poistot ja muutokset henkilötietoihin toimitetaan toimittajalle. Asiakkaan velvollisuutena on huolehtia siitä, että henkilötietojen keräämiseen on saatu lupa.

Asiakas on henkilötietolain tarkoittama rekisterinpitäjä, jonka käyttöä varten rekisteri on perustettu ja jolla on oikeus määrätä sen käytöstä. Asiakkaalla on mahdollisuus valvoa henkilötietojen käsittelyä ja antaa sitä koskevia määräyksiä ja ohjeita toimittajalle.

Henkilötietojen sisältö

Asiakas ylläpitää tunnisteiden valmistuksessa käytettäviä tietoja ensijijaisesi erillisessä liitteessä 2. Toissijaisesti vastaavan sähköisen dokumentin mukaan.
Tietojen muuttuessa Asiakas toimittaa päivitettyn liitteen Toimittajalle.

Mikäli Asiakas ei toimita erittelyä tiedoista, niin Toimittaja käsittelee saadut tietueet oletusarvoisesti perushenkilötietoina. Toimittaja pidättää tällöin oikeuden kieltäytyä käsitellä sellaista tietoa, joka voidaan katsoa arkaluonteiseksi tai perusteettomaksi.

Tietosuojaloukkaukset ja tietosuojavastaava

Tietojen käsittelyn lainmukaisuuden seuranta- ja valvontatehtäviä varten toimittajalla tulee olla nimetty tietosuojavastaava. Tietosuojavastaavan lakisääteisenä tehtävänä on henkilötietojen lainmukaiseen käyttöön ja tietosuojaan liittyvä seuranta ja valvonta.

Toimittaja ilmoittaa ilman aiheetonta viivästystä tietoonsa tulleesta tietoturvaloukkauksesta asiakkaalle. Tämän lisäksi toimittaja antaa pyynnöstä hallussaan olevat, kohtuullisesti toimitettavissa olevat ja tarpeelliset tiedot tietosuoja-asetuksen 33 artiklan 1 kohdan mukaisen ilmoituksen tekemiseksi.
Mikäli Asiakas havaitsee tietoturvaloukkauksen, tulee tämän ilmoittaa siitä Toimittajalle ilman aiheetonta viivästystä.

Asiakkaan antamassa ilmoituksessa on:

a) kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;
b) ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;

c) kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;

d) kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Mikäli tietoja ei ole mahdollista toimittaa samanaikaisesti, tiedot voidaan toimittaa vaiheittain ilman aiheetonta viivytystä.

Asiakas on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, mukaan lukien henkilötietojen tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet. Asiakas vastaa tarvittavien ilmoitusten tekemisestä viranomaiselle. Toimittaja voi avustaa Asiakasta tässä kappaleessa kuvattujen velvollisuuksien hoitamisessa tarpeen mukaan.

Mikäli tietoturva- ja/tai tietosuojaloukkaus johtuu Asiakkaan vastuulla olevasta seikasta, Toimittajalla on oikeus laskuttaa Asiakasta loukkauksesta ja sen selvittämisestä aiheutuvista kustannuksista.

Toimittajan tietosuojavastaavana toimii Mikael Strang, mikael.strang@cardplus.fi, 040-4554301.

Sopimuksen voimassaolo

Tämä sopimus tulee voimaan, kun rekisterinpitäjä tai tämän edustaja, toimittaa henkilötietoaineiston toimittajalle. Tämä sopimus on voimassa niin kauan, kun toimittaja käsittelee sopimuksen tarkoittamia henkilötietoja rekisterinpitäjän lukuun. Toimitettuja henkilötietoja voidaan käsitellä tämän sopimuksen perusteella niin kauan, kuin on tarpeen edellä mainitun tarkoituksen toteuttamiseksi.

Sopimuksen päättäminen/päättyminen

Mikäli aineiston toimittaja ei ole esittänyt erillistä pyyntöä aineiston palauttamisesta, toimittaja poistaa toimitetun aineiston ja siitä tehdyt jäljennökset 30 päivänä sisällä tämän sopimuksen mukaisen käsittelyn päätyttyä.

Mikäli toimeksianto peruutetaan tai puretaan ja mikäli aineiston toimittaja ei ole esittänyt erillistä pyyntöä aineiston palauttamisesta, toimittaja poistaa toimitetun aineiston ja siitä tehdyt jäljennökset 30 päivänä sisällä tämän sopimuksen mukaisen käsittelyn päätyttyä.

Toimittaja sitoutuu pitämään luottamuksellisina saamansa aineistot ja tiedot sekä olemaan käyttämättä niitä muihin kuin sopimuksen mukaisiin tarkoituksiin myös sopimussuhteen päättymisen jälkeenkin.

Virhetilanteet ja vastuu

Vastuu henkilötietojen tietoturvallisesta säilyttämisestä siirtyy asiakkaalle toimitusehdon mukaisesti, toimittaja ei ole vastuussa mahdollisista henkilötietojen loukkauksista tämän jälkeen.

Yleiset sopimusehdot

Mikäli näissä ehdoissa ei ole muuten sovittu sovelletaan CardPlus Oy:n yleisiä toimitusehtoja.

Liite 2: Henkilötietojen kuvaus