Sopimus henkilötietojen käsittelystä (DPA – Data Processing Agreement)

TÄYTÄ PUNAISELLA MERKITYT KOHDAT

Osapuolet

Rekisterinpitäjä (asiakas)

ASIAKKAAN NIMI (y-tunnus: FI)
Tietosuojavastaava:

Asiakkaan valtuuttama yhteyshenkilö

Sama kuin rekisterinpitäjä (voi hyväksyä liitteeseen tehtävät muutokset)

Tietojen käsittelijä (toimittaja)

Koodiperhonen Oy (y-tunnus: FI24598609)
Tietosuojavastaava: Jukka Ratilainen, jukka.ratilainen@koodiperhonen.com, +358 44 2007 444

Yleiset sopimusehdot

Tämä on asiakkaan ja toimittajan välinen sopimus henkilötietojen käsittelystä, jossa toimittaja käsittelee henkilötietoja asiakkaan puolesta. Osapuolet sitoutuvat toiminnassaan noudattamaan EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 mukaista vaatimustasoa.

Sopimus astuu voimaan kun asiakas on hyväksynyt sopimuksen allekirjoittamalla tai muuten kirjallisesti esim. sähköpostilla.

Asiakas omistaa tai on muutoin oikeutettu siirtämään/antamaan henkilötiedot käsiteltäväksi. Asiakas vastaa tietojen tarkkuudesta, paikkansapitävyydestä, sisällöstä, luotettavuudesta ja lainsäädännön vaatimusten täyttämisestä. Asiakas on velvollinen ilmoittamaan lainsäädännössä vaadittavalla tavalla viranomaisille ja/tai tietojen kohteelle rikkomuksesta tai henkilötietojen luvattomasta luovuttamisesta.

Sopimuksen sisältö on määritetty tarkemmin tämän sopimuksen liitteessä (DPA-SOPIMUKSEN TIETOSUOJALIITE), jota osapuolet sitoutuvat pitämään ajan tasalla. Molempien osapuolien pitää hyväksyä liitteeseen tehtävät muutokset kirjallisesti esim. sähköpostilla, jonka jälkeen muutokset astuvat voimaan. Merkintä muutoksista on tehtävä liitteeseen.

Henkilötietoja on aina käsiteltävä luottamuksellisina ja salassa pidettävinä, riippumatta siitä onko osapuolten välillä voimassa olevaa erillistä salassapitosopimusta.

_____ _____

Asiakkaan allekirjoitus Toimittajan allekirjoitus

Kommentti [T1]: Kirjoita tähän rekisterinpitäjän tiedot ja nimetyn tietosuojavastaavan tiedot yhteystietoineen.

Kommentti [T2]: Kirjoita tähän yhteyshenkilön tiedot, joka voi hyväksyä liitteeseen tehtävät muutokset. Tämä helpottaa sopimuksen päivittämistä.

Yhteyshenkilönä kannattaa olla sellainen henkilö, joka oikeasti tietää miten tietoja käsitellään. Tietosuojavastaava tai allekirjoittaja ei välttämättä tiedä teknisiä yksityiskohtia.

Kommentti [T3]: Kirjoita tähän tietoja käsittelevän yrityksen tiedot.

Varsinaiset tietoja käsittelevät henkilöt tai ryhmät pitää listata tietosuojaliitteessä.

Kommentti [T4]: Sopimusta ei tarvitse välttämättä allekirjoittaa fyysisesti, riittää kun siitä on olemassa molemminpuoliset hyväksyntäsähköpostit. Ne kannattaa laittaa talteen.

Tällä on tarkoitus helpottaa sopimuksen tekemistä, koska oikeiden allekirjoitusten hankkiminen voi viedä tarpeettomasti aikaa.

Kommentti [T5]: Huomioi, että sopimusta pitää ylläpitää ja täydentää kun tilanteet muuttuvat.

Tässä on sama idea kuin itse sopimuksessakin eli molemminpuolinen hyväksyntäsähköposti on helpoin tapa täydentää sopimuksen liitettä.

DPA-SOPIMUKSEN TIETOSUOJALIITE

Päivityshistoria

XX.XX.2018 Sopimus ja liite on hyväksytty.

Kommentti [T6]: Tähän kannattaa laittaa sopimuksen ja liitteen hyväksyntämerkintä.

Muista lisätä tähän merkintä jos teet liitteeseen muutoksia.

Liitteen tarkoitus

Tämä tietosuojaliite määrittelee ja ohjeistaa tietojenkäsittelyn periaatteet.

Molemmat osapuolet ovat velvollisia pitämään tämä liite ajan tasalla, jotta henkilötietojen käsittely säilyy turvallisena. Päivityksistä on tehtävä merkintä tähän liitteeseen ja molempien osapuolien pitää hyväksyä muutokset kirjallisesti esim. sähköpostilla.

Asiakkaan puolelta hyväksynnän (liitteeseen tehtäville muutoksille) voi antaa allekirjoittanut, asiakkaan tietosuojavastaava tai asiakkaan valtuuttama yhteyshenkilö (asiakkaan oman sisäisen ohjeistuksen mukaisesti). Toimittajan puolelta muutokset voi hyväksyä toimittajan tietosuojavastaava.

Kommentti [T7]: Tämä kohta kannattaa lukea ajatuksella kuka saa ja voi tehdä liitteeseen/sopimukseen muutoksia. Tarkoitus on helpottaa muutosten tekemistä, koska niitä tulee pakostakin tilanteiden muuttuessa.

Itse kannatan sitä, että asiakas valtuuttaa tähän yhteyshenkilön, joka voi hyväksyä muutoksia liitteeseen.

Tietojenkäsittelyn tarkoitus ja perustelut

Tietojenkäsittelyn tarkoituksena on ylläpitää ja kehittää asiakkaan järjestelmiä, neuvoa niiden käyttöä ja selvittää erilaisia ongelmatilanteita.

Kommentti [T8]: Tämä on tärkeä kohta, koska henkilötietojen käsittelylle täytyy olla selkeä tarkoitus ja selkeät perusteet:

Miksi tietoja käsitellään?

Henkilötietojen käsittelijät

Henkilötietoja saa käsitellä vain tässä listatut toimittajan henkilöt

- Jukka Ratilainen, jukka.ratilainen@koodiperhonen.com, +358 44 2007 444

Henkilötietojen sisältö (rekisteröityjen ryhmät ja henkilötietojen tyypit)

Järjestelmä 1

- Henkilöasiakkaat (palveluita tilanneet asiakkaat)
    - Tunnistetiedot, nimi ja yhteystiedot, laskututustietoja, web-sivustojen tunnistetiedot.
- Omat työntekijät ()
    - Tunnistetiedot, nimi ja yhteystiedot, työsuhde- ja palkkatietoja, sosiaaliturvatunnus.

Kommentti [T9]: Parasta olisi jos varsinaiset tietojenkäsittelijät pystytään nimeämään. Tässä voi tietysti käyttää myös ryhmiä esim. asiakaspalvelu, mutta silloin kannattaa lisätä hieman lisätietoja esim. ”jotka on koulutettu tehtäviinsä ja ovat tietoisia tämän liitteen sisällöstä” tai viitata erilliseen ohjeistukseen.

Tietojenkäsittelijöiden on tiedettävä tämän liitteen sisältö ja myös siihen tulevat päivitykset.

Henkilötietoja pitää säilyttää aina asiakkaan järjestelmissä. Joskus voi tulla tilanne, että henkilötietoja joudutaan siirtämään väliaikaisesti toimittajan koneelle esim. eräajojen tekemistä varten tai koko tietokanta ongelmien tutkimista varten. Tiedot pitää poistaa toimittajan koneelta välittömästi työn päättymisen jälkeen, mikäli ne sisältävät tunnistettavissa olevia henkilötietoja.

Asiakas vastaa tietojen poistamisesta rekistereistä tai arkistoinnista säilytysaikojen puitteissa. Toimittaja on velvollinen huolehtimaan omalta osaltaan samojen velvoitteiden täyttymisestä, noudattamalla tässä liitteessä annettuja ohjeita.

Kommentti [T10]: Järjestelmä voi olla esim. taloushallinto-ohjelmisto tmv. joka sisältää henkilötietoja.

Järjestelmät kannattaa nimetä, jotta tiedetään mistä järjestelmästä on kysymys.

Tietoturva

Asiakas vastaa omien järjestelmiensä tietoturvasta ja toimittaja omistaan. Molempien osapuolien pitää ottaa huomioon tietoturvassaan henkilötietojen arkaluontoisuus sekä niihin liittyvä riskitaso.

- Toimittaja vastaa siitä, että sen henkilötietojen käsittelyyn liittyvään toimintaan sovelletaan dokumentoituja asianmukaisia riskienhallinta- ja tietoturvaprosesseja.

Kommentti [T11]: Listaa tähän henkilöryhmät, joiden henkilötietoja käsitellään.

Käytännössä nämä ovat asiakasryhmiä tai muita vastaavia henkilöryhmiä.

- Toimittaja on velvollinen toteuttamaan tietosuojalainsäädännön ja tämän sopimuksen määräämät riittävät tekniset ja organisatoriset suojatoimenpiteet tietojen/henkilötietojen suojaamiseksi.
- Molempien osapuolien pitää ottaa huomioon tietoturvassaan henkilötietojen arkaluontoisuus sekä niihin liittyvä riskitaso.

Tietojenkäsittelyssä käytettävät järjestelmät

Molempien osapuolien pitää suojata tietojenkäsittelyssä käytettävät järjestelmät ja tietoliikenne asianmukaisilla tietoturvaratkaisuilla. Tässä on listattu minimivaatimukset.

- Järjestelmät pitää olla suojattu henkilökohtaisin käyttäjätunnuksin ja salasanoin. Niitä ei saa luovuttaa muille.
- Tietokoneille pitää olla asennettuna toimiva virustorjunta ja haittaohjelmien poistotyökalu.
- Järjestelmien pitää olla palomuurilla suojattuja.
- Toimittaja ei saa asentaa (tai poistaa) ohjelmistoja asiakkaan järjestelmiin tai muuttaa tietoturvaan liittyviä asetuksia ilman asiakkaan lupaa, vaikka hänellä olisi siihen oikeudet.

Etäyhteydet

Etäyhteyksiä käytettäessä pitää aina käyttää suojattua yhteyttä (vpn-yhteys, teamviewer tai vastaavaa) jos yhteys otetaan asiakkaan lähiverkon ulkopuolelta.

- Asiakkaan lähiverkon sisällä voidaan käyttää suojaamatonta yhteyttä (esim. RDP)
- Etäyhteyden saa muodostaa vain toimittajan tai asiakkaan hallinnassa olevilta tietokoneilta. Muilta tietokoneilta yhteyksien ottaminen on ankarasti kielletty.
- Tietokone (tai etäyhteys) tulee aina sulkea tai lukita käsittelyn päätteeksi tai jos se on ollut käyttämättömänä 30 minuuttia (ns. automaattilukitus).
- Etäyhteyksissä tulee huomioida myös ympäristö, josta tai johon etäyhteys otetaan. Ulkopuoliset eivät saa nähdä ruuduilla näkyvää tietoa. Asiakas vastaa omista järjestelmistä ja toimittaja omistaan.
- Teamviewer-etäyhteyksissä pitää olla aina lokitus päällä, jotta voidaan nähdä milloin etäyhteyksiä on käytetty.
- Asiakkaan järjestelmiin (esim. palvelimille tai työasemiin) saa ottaa väliaikaisen etäyhteyden vain jos asiakas antaa siihen luvan ja avaa yhteyden.

Valvomattomat etäyhteydet tarkoittavat sellaisia etäyhteyksiä, joihin toimittaja pystyy ottamaan yhteyden ilman asiakkaan toimenpiteitä (esim. Teamviewer-host –yhteydet).

- Asiakkaan käyttämät tietokoneet, joihin toimittaja saa ottaa etäyhteyksiä tarvittaessa
  -
- Toimittajan käyttämät tietokoneet, joista etäyhteyksiä saa ottaa
  -

Tietokannat

Tietokannasta voidaan siirtää varmuuskopio VÄLIAIKAISESTI toimittajan koneelle ongelmien tutkimista tai ohjelmien kehittämistä varten.

- Asiakkaalta pitää olla tähän kirjallinen suostumus tai toimeksianto esim. sähköpostilla.
- Toimittajan tulee tuhota tietokantakopio luotettavasti toimeksiannon jälkeen esim. käyttäen Shredder-ohjelmistoa, joka ylikirjoittaa poistetun kannan kiintolevyltä. Tuhoamisesta pitää ilmoittaa kirjallisesti asiakkaalle esim. sähköpostilla.
- Asiakas on vastuussa tietokantojen varmuuskopioinnista ja niiden asianmukaisesta säilyttämisestä.
- Toimittaja voi palauttaa tiedot varmuuskopiosta vain asiakkaan toimeksiannosta.

Kommentti [T12]: Etäyhteydet kannattaa listata tarkasti, koska ne muodostavat selkeän tietoturvauhkan.

Tässä kannattaa olla tarkkana.

Kommentti [T13]: Käytännössä tietokantoja joudutaan siirtämään välillä koneelta toiselle esim. ongelmien selvittämiseksi. Tämä muodostaa selkeän tietoturvauhkan.

Tietokannan varmuuskopioiden käsittelyyn kannattaa kiinnittää erityistä huomiota, ettei varmuuskopioita jää lojumaan vääriin paikkoihin. Tietokannat eivät saa joutua vääriin käsiin ja kopioiden asianmukaisesta tuhoamisesta kannattaa huolehtia tarkkaan.

Henkilötietojen siirto tai luovutus

Toimittaja ei saa siirtää tai luovuttaa henkilötietoja eteenpäin.

Rekisterinpitäjää tukevat toimenpiteet, joilla turvataan rekisteröidyn oikeuksien toteutuminen

Tämä kohta liittyy tietosuoja-asetuksen (EU) 2016/679 artikloihin 32-36: käsittelyn turvallisuus, tietoturvaloukkauksista ilmoittamiseen, tietosuojaa koskevien vaikutusten arviointiin (automaattikäsittelyt tai laajat tietojen käsittelyt) ja valvontaviranomaisen ennakkokuuleminen.

Kommentti [T14]: Tässä suojataan rekisterinpitäjää siltä, että esim. pilvipalvelussa tai tietokannan hostaajalla oleviin tietoihin ja lokeihin päästään varmasti käsiksi silloin jos pitää selvittää tietoturvaloukkausta.

Tässä on tarkoitus velvoittaa pilvipalvelun toimittaja (tai hostaaja) edesauttamaan selvitystyössä ja ilmoittamaan etukäteen havaituista tietoturvauhkista.

Toimittaja on velvollinen auttamaan asiakasta kaikissa toimenpiteissä, joilla turvataan rekisteröityjen oikeuksien toteutuminen. Asiakas on puolestaan velvollinen informoimaan toimittajaa vastaavissa tapauksissa. Tähän on listattu oleellisimmat toimenpiteet

- Asiakas on vastuussa tietoturvaloukkauksen ilmoittamisesta (viranomaisille ja/tai rekisteröidylle).
- Toimittaja on velvollinen ilmoittamaan asiakkaalle tietoonsa tulleista tietoturvauhkista tai tietoturvaloukkauksista. Tämä on tehtävä välittömästi.
- Asiakas on velvollinen ilmoittamaan toimittajalle tietoonsa tulleista tietoturvauhkista, jotka liittyvät toimittajaan tietojen käsittelijänä. Tämä on tehtävä välittömästi.
- Asiakkaan tulisi (jos se on mahdollista) ilmoittaa etukäteen toimittajalle muutoksista, jotka voivat vaikuttaa toimittajan ja asiakkaan väliseen tietojenkäsittelyyn.
- Toimittajan on autettava asiakasta tietoturvaloukkauksen ilmoittamisesta (vaatii asiakkaan toimeksiannon).
- Toimittaja on velvollinen avustamaan asiakasta tietosuojaa koskevassa vaikutusten arvioinnissa (esim. lokitietojen selvittely ja viranomaistahoille kerättävään informaatioon tai dokumentointiin). Toimittaja on oikeutettu laskuttamaan selvittelystä aiheutuvat ylimääräiset kulut.
- Toimittaja ei saa antaa mitään tietoja suoraan (esim. rekisteröidyille tai viranomaisille) ilman asiakkaan toimeksiantoa tai oikeuden päätöstä.

Salassapito

Henkilötietoja on aina käsiteltävä luottamuksellisina ja salassa pidettävinä, riippumatta siitä onko osapuolten välillä voimassa olevaa erillistä salassapitosopimusta.