

TIETOSUOJASOPIMUS (DPA – Data Processing Agreement)

Tämä tietosuojasopimus (jäljempänä "Sopimus") on liite T:mi Timo Mätön / Digi Turun (jäljempänä "Käsittelijä") ja asiakkaan (jäljempänä "Rekisterinpitäjä") väliseen pääsopimukseen tai tilaussopimukseen, joka koskee verkkosivujen ylläpitoa, hosting-palveluita tai muita digitaalisia palveluita.

1. Tausta ja tarkoitus

Tällä Sopimuksella sovitaan EU:n yleisen tietosuoja-asetuksen (2016/679, "GDPR") edellyttämistä ehdoista, joiden mukaisesti Käsittelijä käsittelee henkilötietoja Rekisterinpitäjän lukuun tuottaessaan pääsopimuksen mukaisia palveluita.

Rekisterinpitäjä vastaa siitä, että sillä on lainmukainen oikeus ja peruste käsitellä ja siirtää henkilötietoja Käsittelijälle.

2. Käsittelyn luonne, tarkoitus ja kohteena olevat tiedot

- **Käsittelyn tarkoitus ja luonne:** Henkilötietojen säilyttäminen, varmuuskopiointi, ylläpito ja tekninen tuki Rekisterinpitäjän verkkosivustolla ja siihen liittyvillä palvelimilla.
- **Henkilötietoryhmät:** Riippuu Rekisterinpitäjän sivuston sisällöstä (esim. verkkokaupan asiakkaat tai lomakkeen täyttäjät), tyypillisesti: nimi, sähköpostiosoite, puhelinnumero, IP-osoite sekä mahdolliset tilaustiedot.
- **Rekisteröityjen ryhmät:** Rekisterinpitäjän asiakkaat, potentiaaliset asiakkaat tai verkkosivuston käyttäjät.

3. Käsittelijän yleiset velvollisuudet

Käsittelijä sitoutuu:

1. Käsittelemään henkilötietoja ainoastaan Rekisterinpitäjän dokumentoitujen ohjeiden ja pääsopimuksen mukaisesti.
2. Varmistamaan, että henkilötietoja käsittelevät henkilöt ovat sitoutuneet noudattamaan salassapitovelvollisuutta.
3. Toteuttamaan kaikki GDPR:n 32 artiklan mukaiset vaadittavat tekniset ja organisatoriset toimenpiteet tietoturvan varmistamiseksi (esim. tietoliikenteen salaaminen, päätelaitteiden suojaukset ja monivaiheinen tunnistautuminen pääsynhallinnassa).

4. Alihankkijoiden käyttö (Alikäsittelijät)

Rekisterinpitäjä antaa Käsittelijälle yleisen ennakkoluvan käyttää alikäsittelijöitä palvelun tuottamisessa. Sopimuksen tekohetkellä Käsittelijä käyttää seuraavia keskeisiä infrastruktuurin ja tiedonhallinnan alikäsittelijöitä:

- **Miss Hosting AB:** Palvelintilan ja konesali-infrastruktuurin tuottaminen asiakkaiden sivustoille (sijainti: EU/ETA).
- **Microsoft Ireland Operations Ltd:** Operatiivisen dokumentaation, taulukoiden ja ylläpitotietojen tallennus Microsoft 365 ja OneDrive -ympäristöissä (sijainti: EU/ETA).

- **Google Ireland Limited:** Projektitiedostojen, vedosten ja satunnaisten aineistojen jakaminen asiakkaiden ja sidosryhmien kesken Google Driven kautta (sijainti: EU/ETA).

Käsittelijä vastaa alihankkijoidensa toiminnasta kuin omastaan. Mikäli Käsittelijä vaihtaa tai lisää uusia alikäsittelijöitä, tästä ilmoitetaan Rekisterinpitäjälle, jolla on oikeus vastustaa muutosta perustellusta syystä. Käsittelijä ei syötä Rekisterinpitäjän henkilötietoja kielimalleihin tai tekoälytyökaluihin (esim. Google AI Pro) ilman erillistä lupaa.

5. Tietoturvaloukkauksista ilmoittaminen

Käsittelijän on ilmoitettava Rekisterinpitäjälle henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan **48 tunnin kuluessa** sen havaittuaan. Ilmoituksessa on kuvattava loukkauksen luonne, todennäköiset seuraukset sekä toimenpiteet, joihin on ryhdytty haittavaikutusten lieventämiseksi.

6. Avustamisvelvollisuus

Käsittelijä avustaa Rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä, jotta Rekisterinpitäjä voi täyttää velvollisuutensa vastata rekisteröityjen oikeuksia koskeviin pyyntöihin (esim. tietojen poistaminen tai siirtäminen). Käsittelijällä on oikeus laskuttaa tästä avustamisesta normaalin tuntiveloituksensa mukaisesti, ellei kyse ole Käsittelijän omasta virheestä.

7. Tietojen palauttaminen ja poistaminen

Kun henkilötietojen käsittelyä koskevat palvelut päättyvät, Käsittelijä Rekisterinpitäjän valinnan mukaan joko poistaa tai palauttaa kaikki henkilötiedot Rekisterinpitäjälle, sekä poistaa olemassa olevat jäljennökset (esim. varmuuskopiot), ellei lainsäädäntö vaadi henkilötietojen säilyttämistä.

8. Auditoinnit

Rekisterinpitäjällä tai sen valtuuttamalla kolmannella osapuolella on oikeus auditoida Käsittelijän toiminta tämän Sopimuksen noudattamisen todentamiseksi. Auditointi suoritetaan ensisijaisesti tarkastamalla Käsittelijän toimittamaa kirjallista dokumentaatiota (esim. "Tietoturvakäytännöt ja NIS2-valmius" -dokumentti). Mikäli Rekisterinpitäjä vaatii laajempaa teknistä auditointia, Rekisterinpitäjä vastaa auditoinnin aiheuttamista kustannuksista.