



# Tietosuojakäytäntö

Olemme keränneet tähän joukon kysymyksiä, joihin vastaamalla saat luotua helposti tietosuojakäytäntödokumentin rungon, joka on EU 2016/679 –asetuksen (GDPR, General Data Protecting Regulation) mukainen.

Täydennämme tätä dokumenttia palutteen perusteella ja tätä saa käyttää vapaasti omalla vastuulla.

## Rekisterinpitäjä

- Yrityksen virallinen nimi, yhteystiedot jne.
- Tietosuojavastaava + yhteystiedot esim. sähköposti, puhelin tmv.

## Kerättyjen tietojen käyttötarkoitus

- Mihin kerättyjä tietoja käytetään. Käytetäänkö niitä esim.
  - o tilausten käsittelyyn
  - o palveluiden tuottamiseen
  - o ylläpitoon
  - o suojaamiseen
  - o käyttäjätilien luomiseen
  - o liiketoimintojen kehittämiseen ja suunnitteluun
  - o personoituihin palveluihin
  - o väärinkäytösten estämiseen
  - o väärinkäytösten tutkimiseen (esim. lokitus)
  - o palveluiden käytettävyyden parantamiseen
  - o kohdennettuun viestintään
  - o markkinointiin
  - o suoramarkkinointiin
  - o johonkin muuhun, mihin?

## Tietolähteet ja keräystavat

- Mitä tietoja kerätään esim.
  - o nimi, osoite, yhteystiedot
  - o sukupuoli, ikä, syntymäaika
  - o sähköpostiosoite
  - o seurantatunnus tai jokin muu yksilöivä tunnus (esim. cookie tmv.)
  - o tilausten tietoja (esim. tuotetietoja ym.)
  - o asiakaspalautteet
  - o kommentit
  - o valokuvat
  - o profiilitietoja (esim. Twitter, Facebook ym.)
  - o luvat, kiellot ja suostumukset
  - o laskituksen tietoja laskutusta varten



- jotain muuta, mitä?
- Mistä lähteistä tietoja kerätään esim.
  - käyttäjältä itseltään (huom. käyttäjän suostumus, miten sen osoitat?)
  - internetistä
  - yhteistyökumppaneilta
  - kolmansilta osapuolilta
  - sähköposteista
  - mobiilisovelluksista
  - jostain muusta lähteestä?
- Olisi hyvä eritellä mitä tietoja eri lähteistä kerätään eli mitä kerätään käyttäjältä itseltään ja mitä esim. yhteistyökumppaneiden tai muiden kanavien kautta.
  - Mitä tietoja kerätään suoraan käyttäjältä
  - Teknisesti kerättyjä tai muuten automaattisesti kerättyä tietoa esim.
    - IP
    - sijaintitiedot
    - laitteiden tunnistekoodit (esim. imei tai muu yksilöivä tunnus)
    - tietoja käytettävästä selaimesta
    - puhelutiedot
  - Kolmansilta osapuolilta kerätyt tiedot esim.
    - analysointidata
    - markkinointidata
    - markkinointikiellot ja -suostumukset
    - Google Analytics, Facebook ym.
- Miten tietoja yhdistellään esim.
  - omia tietoja päivitetään/täydennetään 3. osapuolilta tai toisista rekistereistä saaduilla tiedoilla (esim. Fonecta, Suomen Asiakastieto, viranomaisrekisterit ym.)
- Tietojen käyttö jälkimarkkinointia varten esim.
  - omien tai yhteistyökumppaneiden palveluiden markkinointi
  - suoramarkkinointi ym.

## Tietojen luovutus

- Tietojen luovutuksella pitää olla perusteltu tarkoitus. Mihin tietoja luovutetaan jos luovutetaan esim.
  - kolmansille osapuolille
  - yhteistyökumppaneille
  - markkinointitarkoituksiin
  - palveluiden suojaamiseen
  - yrityskaupan tai ulkoistuksen johdosta
  - suoramarkkinointiin
  - digitaalisen markkinoinnin kohdentamiseen
  - palveluiden tuottamiseen osallistuville tahoille esim. luottokorttiyhtiöille, analysointipalveluiden tuottamiseen ym. vastaavaan
  - viranomaisten käyttöön esim. väärinkäyttötilanteissa
  - palveluiden käyttöehtojen noudattamisen valvontaan



## Käyttäjän palveluihin tuottamien julkisten tietojen käyttö

- Maininta siitä, että käyttäjän tuottamat tiedot saattavat säilyä järjestelmissä asiakassuhteen päättymisen jälkeenkin. Maininta siitä, ettei rekisterinpitäjä ole vastuussa tällaisista henkilötietojen käsittelystä.
  - o julkiset kommentit ja muut julkisesti tuottamat tiedot
  - o käyttäjän julkisesti luovuttamat tiedot esim. kommentit tai välittämät tiedot
  - o nimimerkit ym.

## Seurantatekniikoiden käyttö

- Mitä seurantatekniikoita palvelussa/ järjestelmissä käytetään esim.
  - o evästeet
  - o Google Analytics ym. vastaavat mittaus- ja seurantapalvelut
  - o tekniset tunnisteet ja tunnistetekniikat (voi olla ylimalkainen maininta)
  - o mihin näitä käytetään esim. markkinointiin, sivuliikenteen seuraamiseen/ turvaamiseen, käytettävyyden parantamiseen, analysointiin, käyttäjäprofilointiin ym.
  - o miten käyttäjä voi estää tai tyhjentää seurantatietojen käyttämisen esim. blokkereilla, selaimen asetuksilla ym. vastaavilla menetelmillä. Voiko esim. palvelun asetuksilla muuttaa tätä?

## 3. osapuolten keräämien tietojen käyttö

- Miten 3. osapuolet voivat käyttää tietoja esim.
  - o markkinoinnissa
  - o tietojen hyödyntämisessä esim. asioiden kohdentamiseen tai tarkentamiseen, väärinkäytösten estämiseen ym.
  - o mainonnan kohdistamiseen
  - o liitännäiset esim. Facebookiin, Twitteriin, Instagramiin ym. vastaaviin tahoihin esim. tykkäypainike
  - o maininta, että käyttäjä voi tutustua 3. osapuolten tietosuojakäytäntöihin ja saada niiltä tietoa miten hänen tietojaan käytetään

## Henkilötietojen käsittelijät

- Ketkä käsittelevät henkilötietoja yrityksessä esim.
  - o työntekijät
  - o yhteistyökumppanit (ulkoistetuissa palveluissa)
- Miten heidät on ohjeistettu esim.
  - o DPA-sopimukset yhteistyökumppaneiden kesken (ERITTÄIN TÄRKEÄ!)
  - o Työohjeet



## Tietojen luovutus 3. maihin

- Luovutetaanko tietoja 3. maihin
  - o EU:n tai ETA:n ulkopuolelle
  - o EU:n sisällä
  - o Euroopan Komission mallisopimuslausekkeet?

## Rekisterien suojausperiaatteet

- Miten rekisterit on suojattu esim.
  - o käyttäjätunnusten ja salasanojen taakse
  - o palomuurit
  - o lukitut serverikaapit, kameravalvonta jos on
  - o varmuuskopiointi, raid
  - o kulunvalvonta
  - o pääsyn valvonta

## Käyttäjän oikeudet

- Mitä oikeuksia käyttäjällä on esim.
  - o tietojensa tarkastamiseen, miten
  - o suoramarkkinoinnin kieltäminen tai markkinoinnin kohdentamisen estäminen, miten
  - o suostumusten poistaminen, miten
  - o sijaintitietojen käytön estäminen, miten
  - o tietojen korjaamiseen tai poistamiseen, miten

## Tietojen säilyttäminen

- Miten pitkään tietoja säilytetään, siirretäänkö ne esim. arkistoon asiakassuhteen päättymisen jälkeen tmv.
- Joillekin tiedoille on määritetty minimi- ja maksimisäilytysajat (esim. henkilötietojen käsittelylokit), selvitä ne.

## Muutokset tähän tietosuojakäytäntöön

- Maininta siitä, että tietosuojakäytäntöä voidaan tarkentaa ja muuttaa tarpeen vaatiessa esim. lain muuttuessa.
- Miten muutoksista ilmoitetaan käyttäjälle/rekisteröidylle/sidosryhmille tmv. (esim. pyritään mahdollisuuksien mukaan ilmoittamaan käyttäjälle).