Fastroin tietopaketti - EU:n yleinen tietosuoja-asetus

Julkaistu 29. huhtikuuta 2020

Sisällysluettelo

Vastuuvapauslauseke

Tämän dokumentin tarkoituksena on esitellä EU:n yleisen tietosuoja-asetuksen (GDPR) keskeisiä käsitteitä, tarjota materiaalia tukemaan Fastroi Oy:n asiakkaita heidän pyrkimyksissään sekä kuvata sitä miten Fastroi toimii yleisen tietosuoja-asetuksen vaatimusten mukaisesti.

Tämän dokumentin tarkoituksena ei ole antaa oikeudellista neuvontaa. Saadaksesi oikeudellista neuvontaa asemaasi tai yleisen tietosuoja-asetuksen asettamiin velvoitteisiin liittyen, tulee sinun kääntyä pätevän lakimiehen puoleen.

Mikäli sinulla on kysyttävää tähän asiakirjaan (Fastroin GDPR-tietopaketti) tai Fastroi Oy:n tietosuoja-asetuksen vaatimustenmukaisuuteen liittyen, voit ottaa yhteyttä tietoturva- ja tietosuojatiimiin lähettämällä sähköpostia osoitteeseen privacy@fastroi.fi.

1 Johdanto EU:n yleiseen tietosuoja-asetukseen (GDPR)

EU:n yleinen tietosuoja-asetus tuli voimaan 25.5.2018. Tietosuoja-asetus tuli suoraan sovellettavaksi kaikissa EU:n jäsenvaltioissa ja se korvasi vanhan vuonna 1995 annetun yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annetun direktiivin (95/46/EY). Asetuksen tavoitteena on yhtenäistää henkilötietojen käsittelemistä koskeva sääntely EU:n alueella.

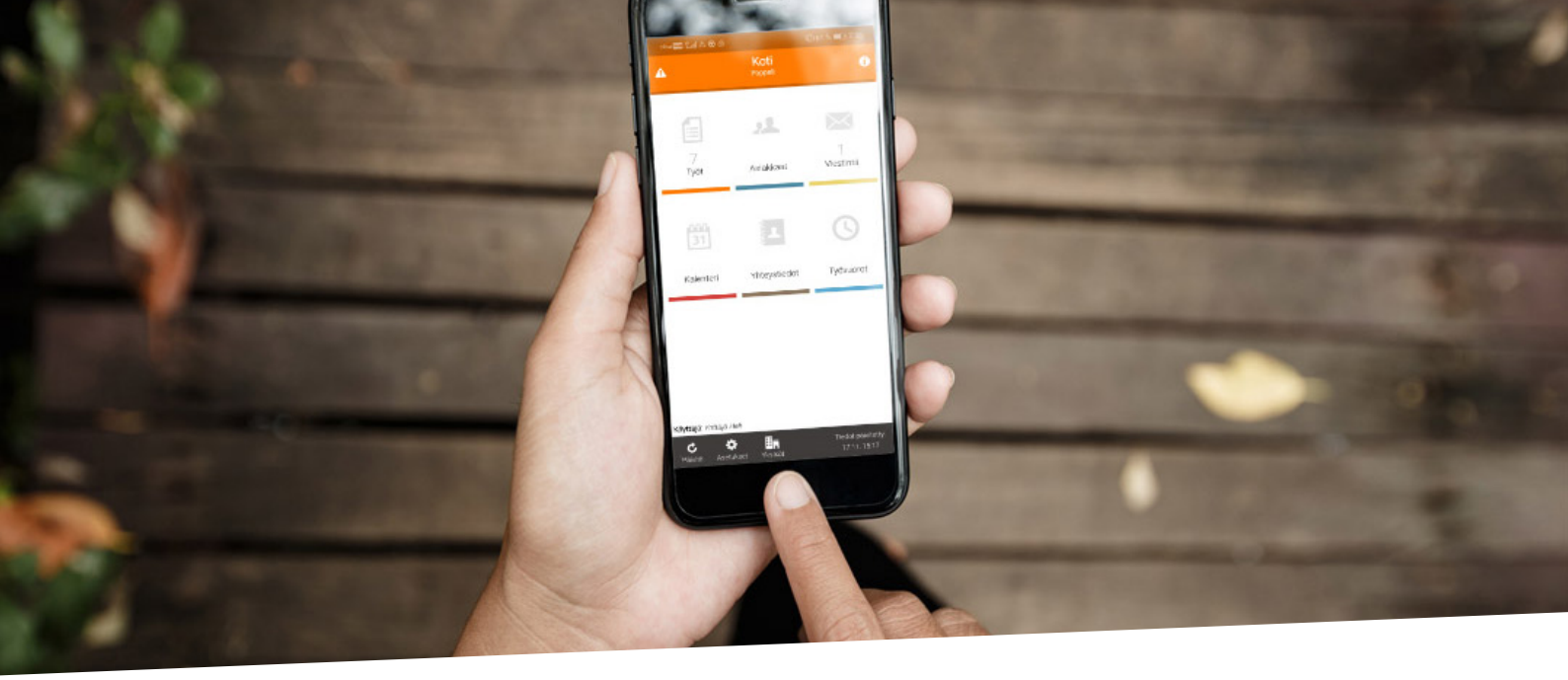
Yleisen tietosuoja-asetuksen tavoitteena on myös vahvistaa EU:n alueella asuvien kansalaisten oikeuksia omiin henkilötietoihinsa (henkilötiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön eli rekisteröityyn). Yleinen tietosuoja-asetus koskee kaikkia EU:n alueella sijaitsevia yrityksiä ja yhteisöjä, jotka käsittelevät henkilötietoja, riippumatta siitä missä itse henkilötietojen käsittely tapahtuu. Henkilötietojen käsittely tarkoittaa kaikkia henkilötietoihin kohdistuvia toimenpiteitä, kuten henkilötietojen keräämistä, käyttöä, siirtämistä, luovuttamista ja poistamista.

Yleisessä tietosuoja-asetuksessa määritetään kaksi olennaista roolia, jotka ovat tärkeitä ymmärtää silloin, kun arvioidaan tietosuoja-asetuksen asettamia velvoitteita ja niiden noudattamista. Tietosuoja-asetus määrittää rekisterinpitäjän ja henkilötietojen käsittelijän roolit, joille molemmille tietosuoja-asetus luo suoria velvoitteita:

Rekisterinpitäjällä tarkoitetaan luonnollista henkilöä, oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä muiden kanssa määrittää henkilötietojen käsittelyn tarkoitukset ja keinot.

Henkilötietojen käsittelijällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Fastroin asiakkaat toimivat tyypillisesti rekisteripitäjinä tai toisen rekisterinpitäjän lukuun käyttäessään Fastroin palveluita. Asiakkaiden käyttäessä Fastroin palveluita, Fastroi on henkilötietojen käsittelijä ja käsittelee henkilötietoja asiakkaidensa lukuun.



2 Mitkä ovat vastuusi Fastroin asiakkaana?

Tämän dokumentin tarkoituksena on ainoastaan antaa yleiskuva EU:n yleisestä tietosuoja-asetuksesta, dokumentin tarkoituksena ei ole tarjota oikeudellista neuvontaa. Suosittelemme tarkempaa perehtymistä EU:n yleiseen tietosuoja-asetukseen ja sen vaatimuksiin. Oikeudellisen neuvonnan osalta suosittelemme kääntymään pätevän lakimiehen puoleen.

Yleisesti ottaen rekisterinpitäjällä on ensisijainen vastuu huolehtia siitä, että henkilötietojen käsittelytoimenpiteet ovat yleisen tietosuoja-asetuksen vaatimusten mukaisia. Rekisterinpitäjän on myös huolehdittava siitä, että henkilötietojen käsittelijöinä käytetään vain sellaisia tahoja, jotka noudattavat henkilötietojen käsittelyssä yleisen tietosuoja-asetuksen asettamia vaatimuksia ja toteuttavat asianmukaisia teknisiä ja organisatorisia toimenpiteitä tietojen suojaamiseksi. Tämän dokumentin tarkoituksena on tarjota tietoa siitä mitä tietosuoja-asetuksen mukaisia teknisiä ja organisatorisia toimenpiteitä Fastroi on toteuttanut tietojen suojaamiseksi. Fastroille on myönnetty on ISO 27001:2013 sertifikaatti virallisen auditoijan DNV GL toimesta.

Yleinen tietosuoja-asetus luo rekisteröidyille erilaisia henkilötietoihinsa liittyviä oikeuksia. Rekisterinpitäjällä on ensisijainen velvollisuus varmistaa rekisteröityjen oikeuksien toteutuminen ja vastata rekisteröityjen esittämiin pyyntöihin heidän käyttäessään henkilötietoihin liittyviä oikeuksiaan. Fastroi on sitoutunut auttamaan asiakkaitaan mahdollisuuksiensa mukaan rekisteröityjen pyyntöihin vastaamisessa.

3 Miten Fastroi on valmistautunut tietosuoja-asetuksen vaatimuksiin

Fastroi yrityksenä suhtautuu yleiseen tietosuoja-asetukseen myönteisesti ja kokee tärkeäksi syventää sitoutumistamme tietosuojaan. Yleisen tietosuoja-asetuksen noudattaminen palveluidemme osalta vaatii sekä kumppanuutta että yhteistyötä Fastroin ja asiakkaidemme välillä palvelujamme käytettäessä. Olemme valmiita auttamaan palveluidemme käyttäjiä tietosuoja-asetuksen vaatimusten täyttämiseen liittyvissä asioissa. Parannamme jatkuvasti palveluitamme ja tuotteitamme sekä dokumentaatiomme tasoa auttaaksemme ja tukeaksemme asiakkaitamme heidän omissa pyrkimyksissään yleisen tietosuoja-asetuksen vaatimusten noudattamisessa. Jäljempänä on tuotu esille muutamia asioita, jotka on hyvä ottaa huomioon Fastroin tarjoamien palvelujen osalta.

3.1 Tietoturvan johtamisjärjestelmä

Olemme ottaneet Fastroilla käyttöön Tietoturvan johtamisjärjestelmän (ISMS) ISO 27001 –standardin asettamien vaatimusten mukaisesti osoittaaksemme, että asiakkaidemme tietojen suojaaminen on meille tärkeää ja varmistaaksemme sen, että ylläpidämme asianmukaista tasoa tietoturvallisuuden osalta. Lisäksi olemme sitoutuneet parantamaan jatkuvasti toimintaamme tietosuojan ja tietoturvallisuuden osalta.

3.2 Tietosuoja- ja tietoturva-vastaavat

Fastroi on nimittänyt tietosuojavastaavan, jotta pystymme täyttämään paremmin tietosuojaa koskevat vaatimukset. Lisäksi olemme nimittäneet tietoturvavastaavan korkeimman mahdollisen tietoturvan takaamiseksi. Tietosuoja- ja tietoturvavastaavan puoleen voi kääntyä ottamalla yhteyttä sähköpostitse osoitteeseen privacy@fastroi.com.

3.3 Salassapitoa koskevat sitoumukset

Kaikki työntekijämme allekirjoittavat salassapitosopimuksen ja suorittavat säännöllisesti työhön liittyviä tietosuoja- ja tietoturvakoulutuksia. Tietoturvapolitiikamme määrittää ne periaatteet, vastuut ja toimintamallit, joita Fastroi noudattaa tietosuojan ja tietoturvan toteuttamisessa ja kehittämisessä.

3.4 Henkilötietojen käsittely

Olemme päivittäneet sopimusehtomme vastaamaan yleisen tietosuoja-asetuksen vaatimuksia. Palveluidemme osalta Fastroi asiakkaat pystyvät näin ollen arvioimaan tietosuoja-asetuksen asettamien vaatimusten täyttymistä. Käsittelemme asiakkaidemme ja heidän käyttäjiensä järjestelmiin tallentamia asiakastietoja henkilötietojen käsittelystä asiakkaan kanssa tehdyn sopimuksen mukaisesti, jossa sovitaan mm. siitä, miten henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun ja toimeksiannosta.

3.5 Tietojen luovuttaminen kolmansille osapuolille

Kuten muutkin yritykset, käytämme kolmansia osapuolia tuottaessamme palveluitamme. Valitsemme kolmannet osapuolet tiukan valintaprosessin kautta, jotta voimme varmistaa, että valittavilla osapuolilla on

tarvittava asiantuntemus sekä kyky toimittaa sellaista palvelua, joka täyttää asianmukaiset tietoturvan ja tietosuojan vaatimukset. Käyttämiemme alihankkijoiden tiedot löytyvät aina henkilötietojen käsittelystä tehdyistä sopimuksista.

3.6 Autamme asiakkaitamme rekisteröityjen oikeuksien toteuttamisessa

Fastroi on tarjoamiensa palveluiden osalta tietojenkäsittelijän roolissa. Autamme omalta osaltamme mahdollisuuksiemme mukaan asiakkaitamme huomioimaan tietosuoja-asetuksen vaatimuksia henkilötietojen käsittelyyn liittyen. Palveluidemme osalta olemme varmistaneet rekisteröityjen oikeuksien toteutumisen toteuttamalla tarvittavat tekniset ominaisuudet. Organisaation tasolla olemme toteuttaneet sisäisesti tarvittavia hallinnollisia toimenpiteitä ja prosesseja henkilötietojen käsittelyyn liittyen.

3.7 Asiakastietojen sijainti ja siirrot kolmansiin maihin

Fastroi voi luovuttaa asiakastietoja voimassaolevan lainsäädännön sallimissa ja velvoittamissa rajoissa. Järjestelmissämme olevat asiakastiedot sijaitsevat kuitenkin EU:n alueella (Suomi). Tietoja ei siirretä Euroopan unionin tai Euroopan talousalueen ulkopuolelle, ellei se ole palvelun toteuttamisen vuoksi tarpeellista. Tällöinkin Fastroi huolehtii riittävästä tietosuojan tasosta lainsäädännön edellyttämällä tavalla mm. hyödyntämällä Euroopan komission mallisopimuslausekkeita tietojen siirrosta kolmansiin maihin. Mallisopimuslausekkeiden avulla vahvistetaan tietojen viejien ja tuojien velvollisuuksia ja varmistetaan tietosuojan riittävä taso siirrettäessä tietoja EU:n tai Euroopan talousalueen ulkopuolelle. Tarkempia tietoja Fastroin palveluita koskevista tiedonsiirroista ja mallisopimuslausekkeista löydät henkilötietojen käsittelystä tehdystä sopimuksesta.

3.8 Palvelujen turvallisuus

Varmistaaksemme, että olemme toteuttaneet asianmukaiset tekniset ja organisatoriset toimenpiteet riskien minimoimiseksi, olemme suorittaneet toiminnoillemme riskienarviointeja sekä tietosuojan osalta vaikutustenarviointeja (DPIA). Riskipohjainen lähestymistapa on osa sitoutumistamme ISO 27001-standardiin. Palvelujemme tietoturvallisuutta kuvataan yleisesti ISO 27001- ja GDPR-tietopaketti -dokumenteissa, jotka löytyvät nettisivuiltamme.

4 Usein kysytyt kysymykset

Mikä on ISO 27001?

ISO 27001 on kansainvälinen standardi, joka määrittelee tietoturvallisuuden hallintajärjestelmän (ISMS) vaatimukset mahdollistaakseen riskien arvioinnin ja tarvittavien ehkäisevien toimenpiteiden toteuttamisen. Lisätietoa ISO 27001 –standardista löytyy kansainvälisen standardisoimisjärjestön (ISO) verkkosivuilta osoitteesta www.iso.org.

Mistä löydän lisätietoa yleisen tietosuoja-asetuksen mukaisista velvoitteista?

EU:n yleinen tietosuoja-asetus löytyy EUR-Lex-sivustolta. Tarkempia tietoja löytyy myös valvontaviranomaisen eli tietosuojavaltuutetun toimiston sivustolta.

Mikä on vaikutustenarviointi (DPIA)?

Tietosuojaa koskeva vaikutustenarviointi (DPIA) on yksi uusista tietosuoja-asetuksen mukanaan tuomista henkilötietojen käsittelyyn liittyvistä velvoitteista. Vaikutustenarvoinnin tarkoituksena on kuvata henkilötietojen käsittely, arvioida henkilötietojen käsittelyn tarpeellisuutta ja oikeasuhtaisuutta sekä tunnistaa ja arvioida henkilötietojen käsittelyyn liittyviä riskejä sekä tarvittavia toimenpiteitä riskien minimoimiseksi.

fastroi

— Caring together —