

Usein kysyttyä EU:n tietosuoja-asetuksesta

Mikä GDPR?

GDPR tulee sanoista General Data Protection Regulation (yleinen tietosuoja-asetus). Se on uusi henkilötietojen käsittelyä sääntelevä laki, jota sovelletaan kaikissa EU-maissa 25.5.2018 alkaen.

GDPR antaa paremman suojan henkilötiedoillesi ja enemmän keinoja hallita tietojesi käsittelyä.

Miksi tietosuojalait muuttuvat?

Uuden lainsäädännön tavoitteena on

- parantaa henkilötietojen suojaa ja tietosuojaoikeuksia
- vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin
- yhtenäistää tietosuojasääntelyä kaikissa EU-maissa
- edistää digitaalisten sisämarkkinoiden kehittymistä.

Mitä tietosuojaoikeuksia minulla on?

Sinulla on oikeus

- tietää mitä henkilötietoja organisaatiolla on sinusta
- tietää miten ja mihin tarkoitukseen henkilötietojasi käsitellään
- pyytää virheellisten, epätarkkojen ja puutteellisten henkilötietojesi korjaamista
- pyytää henkilötietojesi poistamista
- vastustaa henkilötietojesi käsittelyä
- pyytää henkilötietojesi käsittelyn rajoittamista
- siirtää tietosi toiselle organisaatiolle
- olla joutumatta perusteetta automaattisen päätöksenteon kohteeksi.

Mistä tiedän, mitä tietoja organisaatiolla on minusta?

Voit kysyä, onko organisaatiolla henkilötietojasi. Sinulla on oikeus saada vahvistus siitä, että henkilötietojasi ei käsitellä. Jos yrityksellä on henkilötietojasi, sinulla on oikeus

- saada pääsy tietoihin
- saada lisätietoja tietojesi käsittelystä, kuten mihin tarkoitukseen niitä käytetään.

Organisaation on toimitettava tiedot yleisesti käytetyssä sähköisessä muodossa, jollet pyydä toisin.

Organisaation ei kuitenkaan tarvitse antaa jäljennöstä tiedoistasi, jos se vaikuttaa haitallisesti muiden oikeuksiin ja vapauksiin.

Mitä teen, jos organisaatiolla on virheellisiä henkilötietoja itsestäni?

Voit pyytää organisaatiota korjaamaan henkilötietosi, jos huomaat niiden olevan virheellisiä, puutteellisia tai epätarkkoja. Tietyissä tilanteissa sinulla on oikeus täydentää puutteellisia henkilötietoja. Organisaation on vastattava pyyntöön kuukauden kuluessa.

Voinko pyytää organisaatiota poistamaan henkilötietoni?

Voit pyytää henkilötietojesi poistamista organisaatiolta esimerkiksi silloin, kun tietoja ei enää tarvita tai tietojasi on käytetty laittomasti. Organisaation on poistettava tietosi, jos sillä ei ole laillista perustetta käsitellä niitä.

Mikä on henkilötieto?

Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön.

Henkilötietoja ovat esimerkiksi

- nimi
- kotiosoite
- sähköpostiosoite, kuten etunimi.sukunimi@yritys.com
- puhelinnumero
- henkilökortin numero
- auton rekisterinumero
- paikannustiedot
- IP-osoite
- potilastiedot
- isovanhempien perinnöllisiä sairauksia koskevat tiedot.

Saako organisaationi käsitellä henkilötietoja?

Saat käsitellä henkilötietoja, jos sille on laissa määritelty peruste.

Peruste voi olla

- rekisteröidyn suostumus
- sopimus
- rekisterinpitäjän lakisääteinen velvoite
- elintärkeiden etujen suojaaminen
- yleinen etu ja julkinen valta
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.

Henkilötietojen käsittelyssä on noudatettava aina lakia ja tietosuojaperiaatteita. Arkaluonteisia tietoja saa käsitellä vain poikkeustapauksissa.

Lue lisää: [Milloin henkilötietoja saa käsitellä?](#)

Onko organisaationi nimitettävä tietosuojavastaava?

Tietosuojavastaava on nimitettävä, jos

- ydintehtävänne edellyttävät arkaluonteisten tietojen laajamittaista käsittelyä

- ydintehtävänne edellyttävät ihmisten laajamittaista, säännöllistä ja järjestelmällistä seuranta
- organisaationne on julkishallinnon toimija.

Tietosuojavastaava on organisaation sisäinen asiantuntija tietosuoja-asioissa sekä rekisteröityjen ja tietosuojaviranomaisen yhteyshenkilö.

Lue lisää: [Tietosuojavastaavat](#)

Onko organisaationi laadittava seloste henkilötietojen käsittelytoimista?

Jos organisaatiossanne on yli 250 työntekijää, teidän on laadittava seloste käsittelytoimista. Jos organisaatiossanne on alle 250 työntekijää, seloste käsittelytoimista on laadittava, kun

- henkilötietojen käsittely organisaatiossa ei ole satunnaista
- organisaation vastuulla oleva henkilötietojen käsittely todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille tai
- organisaatiossa käsitellään arkaluonteisia tietoja.

Lue lisää: [Seloste käsittelytoimista](#)

Mitä tietoja organisaationi on kerrottava heille, joiden henkilötietoja aiomme käsitellä?

Ilmoita avoimesti ja selkeästi vähintään

- organisaatiosi nimi, yhteystiedot ja mahdollisen tietosuojavastaavan yhteystiedot
- mitä tietoja organisaatiosi aikoo käsitellä
- mihin tarkoitukseen organisaatiosi käsittelee henkilötietoja
- henkilötietojen käsittelyn oikeusperuste
- kuinka kauan tietoja säilytetään
- mikä toinen organisaatio tai henkilö voi saada tiedot
- siirretäänkö henkilötietoja EU:n ulkopuolelle
- henkilön tietosuojaoikeudet
- oikeus tehdä valitus tietosuojaviranomaiselle
- oikeus milloin tahansa peruuttaa suostumus, jos käsittely perustuu suostumukseen
- tiedot automaattisesta päätöksenteosta ja käsittelyyn liittyvästä logiikasta.

Lue lisää: [Informointikäytännöt](#)

Mitä tietosuojaperiaatteilla tarkoitetaan?

Tietosuojaperiaatteiden mukaan henkilötietoja on

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- käsiteltävä luottamuksellisesti ja turvallisesti

- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

Tietosuojaperiaatteita on noudatettava henkilötietojen käsittelyn kaikissa vaiheissa.

Rekisterinpitäjän on pystyttävä osoittamaan, että se noudattaa tietosuojaperiaatteita.