GDPR -
Yleinen tietosuoja-asetus

Kyberturvan abc yrittäjille -hanke

Euroopan unioni
Euroopan sosiaalirahasto

Vipuvoimaa EU:lta 2014–2020

Elinkeino-, liikenne- ja ympäristökeskus

XAMK
Kaakkois-Suomen ammattikorkeakoulu

EU:n yleinen tietosuoja-asetus

Suomen yrittäjät ovat kirjoittaneet hyvän oppaan tietosuojasta. Tältä sivulta voit tilata Yrittäjän tietosuojaopas: https://www.yrittajat.fi/oppaat/yrittajan-tietosuojaopas/

GDPR:n on oman yrityksen etu pitää asiakkaiden tiedot turvassa ja sen perusteella saada luottamusta asiakkailta sekä säästä rahaa.

Mitä GDPR tarkoittaa?

GDPR on lyhenne sanoista **G**eneral **D**ata **P**rotection **R**egulations. Suomeksi se tarkoittaa EU:n yleistä tietosuoja-asetusta. GDPR on voimassa kaikissa EU-maissa ja sen tarkoitus on säädellä henkilötietojen käsittelyä. GDPR:n avulla EU on halunnut parantaa henkilötietojen suojaa ja tietosuojaoikeuksia. Laki kehitettiin vastaamaan uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin. Suomessa Tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädäntöä.

Mikä on henkilötieto

Tiettyyn henkilöön (asiakkaaseen/työntekijään/yhteistyökumppaniin) liitettävissä oleva mikä tahansa tieto, kuten yhteystiedot. Ajattele henkilötietoja kuin palapeliä. Yksi pala ei välttämättä kerro paljon, mutta yhdistettynä ne paljastavat elävän kuvan elämästäsi.

Esimerkkejä henkilötiedoista:

- nimi
- kotiosoite
- sähköpostiosoite, kuten etunimi.sukunimi@yritys.fi
- puhelinnumero
- henkilökortin numero
- auton rekisterinumero
- paikannustiedot (esim. matkapuhelimen paikannustiedot)

Suorat tunnisteet sisältävät:

- henkilön koko nimi
- henkilötunnus
- henkilönimen mukainen sähköpostiosoite
- biometriset tunnisteet

Epäsuorat tunnisteet sisältävät:

- Sukupuoli
- Ikä
- Ammatti

GDPR:n keskeiset säännöt

GDPR:n siirtymäaika loppui 25. toukokuuta 2018. GDPR käsittelee tietosuojaperiaatteita, vastuullisuutta, tietosuojaa, sitä milloin sinulla on

lupa käsitellä tietoja, suostumusta, tietosuojavastaavia ja ihmisten yksityisyysoikeuksia.

Vaikka GDPR on EU direktiivi, se velvoittaa organisaatioita ja yrityksiä missä tahansa, kun ne keräävät tietoja EU:n alueella asuvista ihmisistä.

Kun käsittelet tietoja, sinun on tehtävä se GDPR:n seitsemän periaatteen mukaan.

1. Lainmukaisuus, asianmukaisuus ja läpinäkyvyys.
2. Käyttötarkoituksen vastattava rekisterissä ilmoitettua tarkoitusta.
3. Tietojen olennaisuus ja tarpeellisuus.
4. Tietojen käsittelyn oltava turvallista ja luottamuksellista.
5. Tietojen oltava täsmällisiä ja tarvittaessa päivitettyjä.
6. Tietojen säilytys ja käsittely vain niin kauan kuin on tarpeellista.
7. Näiden periaatteiden noudattaminen on voitava osoittaa dokumentaation avulla. Yleensä keskeinen henkilötietojen käsittelyä kuvaava dokumentti on tietosuojaseloste.

Milloin minulla on lupa käsitellä tietoja?

Artikkelissa 6 löytyy tiedot, siitä milloin saat käsitellä tietoja. Alla olevassa listassa löytyy 6 esimerkkiä tietojen käsittelyyn liittyen.

1. Tietty henkilö on antanut sinulle nimenomaisen, yksiselitteisen suostumuksensa tietojen käsittelyyn (esim. markkinointisähköpostitilaus).
2. Käsittely on tarpeen sopimuksen toteuttamiseksi / valmistautumiseksi tietyn henkilön kanssa. (esim. vuokrasopimus).

3. Sinun on käsiteltävä tietoja noudattaaksesi lakisääteisiä velvoitteitasi (esim. tuomioistuimen määräys tai osakeyhtiölain edellyttämä osakasluettelo).
4. Sinun on käsiteltävä tietoja pelastaaksesi jonkun hengen. (esim. ensihoitajat)
5. Käsittely on tarpeen yleisen edun tai julkisen vallan edellyttämän tehtävän suorittamiseksi (esim. olet yksityinen jätehuoltoyritys).
6. Sinulla on oikeutettu etu käsitellä jonkun henkilötietoja. Esimerkiksi asiakas on halunnut tilata sinulta jotakin verkkokaupastasi tai työnantajavelvoitteista huolehtiminen.

Kun olet määrittänyt tietojenkäsittelysi laillisen perustan, sinun on laadittava yrityksellesi tietosuojaseloste, joka sinun tulee saattaa niiden henkilöiden tietoon ja hyväksyttäväksi, joiden tietoja käsittelet.

Jos päätät muuttaa perustelujasi ja tietosuojaselostettasi myöhemmin, sinulla on oltava hyvä syy. Dokumentoi tämä syy ja ilmoita siitä henkilöille, joita muutos koske. Näitä ilmoituksia ovat ne ilmoitukset, joita esimerkiksi ajoittain saat some-tileiltäsi (Voidaksesi jatkaa palvelun käyttämistä, sinun tulee hyväksyä uudet ehtomme tms.).

Suostumus

Suostumuksen suhteen on laadittu tiukat säännöt.

- Suostumuksen on oltava ”vapaasti annettu, täsmällinen, tietoinen ja yksiselitteinen”.
- Suostumuspyyntöjen on oltava selvästi erotettavissa muista asioista.

- Suostumuspyyntöjä on esiteltävä selkeällä muodolla ja selkeällä kielellä.
- Asiakkaat voivat peruuttaa antamansa suostumuksen, mikäli tietojen käsittelyyn ei ole perusteltua syytä.
- Sinun on kunnioitettava heidän päätöstään peruuttaa suostumuksensa. Et voi muuttaa käsittelyn oikeudellista perustetta johonkin muuhun perusteeseen.
- Alle 13-vuotiaat voivat antaa suostumuksen vain vanhemman luvalla.
- Sinun on säilytettävä suostumuksesta asiakirjatodiste.

Rekisteri, rekisterinpitäjä, henkilötietojen käsittelijä

Jokainen yritys, joka säilyttää henkilötietoja, on rekisterinpitäjä. Tämä tarkoittaa käytännössä jokaista yritystä, josta löytyy edes puhelin, jossa on asiakkaiden tietoja.

Rekisteri on mikä tahansa kokoelma henkilötietoja, vaikka ne sijaitsisivat eri paikoissa (esim. sähköpostissa, kännykkäsi yhteystiedoissa ja yrityksen työntekijöiden käytössä olevassa jaetussa Google-taulukossa sekä kaapin perukoille unohdetussa asiakkailta kerätyssä käyntikorttinivaskassa).

Henkilötietojen käsittelijä on yrityksen alihankkija/palveluntoimittaja, joka käsittelee yrityksen puolesta henkilötietoja (esim. työterveys ja tilitoimisto).

Ihmisten yksityisyysoikeudet

Ihmiset lainaavat tietojaan yrityksille. Organisaation on tärkeää ymmärtää heidän oikeutensa.

Asiakkaan (rekisteröidyn) oikeudet

- Saada läpinäkyvästi tietoa henkilötietojensa käsittelystä rekisterinpitäjän toimesta.
- Saada pääsy omiin henkilötietoihinsa. Varmista, että työntekijät ymmärtävät, että esimerkiksi haasteellista asiakasta ei voi kuvata värikkäästi asiakasrekisterissä.
- Oikeus saada virheelliset/puutteelliset korjattua.
- Oikeus tulla unohdetuksi. Tämä tarkoittaa, että organisaatio tai yritys poistaa heidän tietonsa kokonaan tietojärjestelmistä, niiltä osin kuin se on mahdollista (esimerkiksi lakisääteinen velvoite voi estää tämän joiltakin osin).
- Oikeus rajoittaa omien tietojensa käsittelyä.
- Oikeus saada omat tietojen siirretyksi järjestelmästä toiseen.
- Asiakkaalla on oikeus vastustaa henkilötietojensa käsittelyä.
- Asiakkaalla on oikeus olla joutamatta perusteetta automaattisen päätöksenteon kohteeksi.

Arkaluonteiset tiedot eli arkaluonteiset tiedot

Arkaluonteisia tietoja saa kerätä vain, mikäli

- rekisteröity on nimenomaisesti suostunut tähän;
- rekisterinpitäjän tulee tehdä näin lain vaatimuksesta (esim. sosiaalisen suojelun ala);
- se on tarpeen rekisteröidyn elintärkeiden etujen suojelemiseksi (esim. tiedottomuuden vuoksi);

- henkilö on itse tehnyt tiedoista nimenomaisesti julkisia;
- Käsittely tapahtuu asianmukaisin suojatoimin ammattiliiton tai poliittisen, filosofisen, uskonnollisen säätiön tai voittoa tavoittelemattoman yhteisön toimesta.

Arkaluonteisia tietoja ovat

- rotu tai etninen alkuperä
- poliittinen mielipide
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- geneettiset / biometriset tiedot, jotka on kerätty henkilön tunnistamista varten
- terveyttä koskevat tiedot
- seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot

Mitä minun pitää huomioida omassa yrityksessäni?

GDPR:n mukaan sinun tulee toimia seuraavasti:

- Henkilötietojen käsittelyn minimoiminen. Käsittelee juuri niitä tietoja kun tarvitset, älä kerää liika tietoja.
- Henkilötietojen pseudonymisointi (tarkoittaa henkilötietojen käsittelyä siten, että niitä ei voi enää yhdistää tiettyyn henkilöön ilman lisätietoja) mahdollisimman pian.
- Läpinäkyvyys henkilötietojen käyttöön liittyen. Kerro asiakkaille, mihin tarkoitukseen keräät heidän tietojansa.
- Tietojenkäsittelyn seuranta.
- Antaa henkilötietojen käsittelijälle mahdollisuuden luoda ja parantaa suojausominaisuuksia.
- Tuotetta kehitettäessä on otettava huomioon tietosuojalait.

- Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet olisi otettava huomioon myös julkisessa tarjouskilpailussa.
- Ylläpidä yksityiskohtaista dokumentaatiota keräämistäsi tiedoista. Mihin tarvitset niitä tietoja? Missä niitä säilytetään? Kuka on niistä vastuussa?
- Kouluttaa työntekijäsi siten, että he käyttävät hyvää kyberhygieniaa työskennelleessä.
- Tee tietojenkäsittelysopimuksia kolmansien osapuolten kanssa, jotka käsittelevät sinun kerättyjä asiakastietojasi.
- Jos laki vaati, esim. SOTE-ala, nimitä tietosuojavastaava.
- Käytä hyvää suojausta (esim. ota kaksivaiheinen tunnistautuminen eli autentikointi käyttöön.)
- Seuraa säännöllisesti, onko kaikki tietosuojaan liittyvä toiminta ja dokumentaatio ajan tasalla.

Mitä rangaistuksia GDPR:n rikkomisestä määrätään?

Jos yritys tai organisaatio ei noudata yleistä tietosuoja-asetusta, voidaan rangaistuksesi antaa sakkoja, joiden suuruus voi olla jopa **20 miljoona euroa tai 4 % vuosittaisesta liikevaihdosta.**

Esimerkkiä rangaistuksen saaneista yrityksistä Suomessa:

- Yksityishenkilö – 500 euroa
  Yksityishenkilö oli asentanut kiinteistölleen valvontakamerat, jotka tallensivat myös naapurikiinteistöt.
- Matkatoimisto – 6 500 €
  Asiakkaiden täyttämät viisumihakemuslomakkeet olivat julkisesti saatavilla matkatoimiston verkkopalvelimella. Tämä lomake sisälsi muun muassa rekisteröityjen nimet, passin numerot ja yhteystiedot.
- Vastaamo – 608 000 €

Yritys rikkoi yleistä tietosuoja-asetusta laimin lyömällä henkilötietojen turvalliseen käsittelyyn sekä tietoturvaloukkauksesta ilmoittamiseen liittyviä velvollisuuksiaan. Rekisterinpitäjä ei ollut myöskään toteuttanut asianmukaisia toimenpiteitä henkilötietojen käsittelyn turvaamiseksi.

Linkit

GDPR-tarkistuslista: https://gdpr.eu/checklist/ (englanniksi)

EU:n tietosuojaverkkosivu: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fi

Finlex Tietosuojalaki - https://www.finlex.fi/fi/laki/alkup/2018/20181050

Yrittäjän tietosuojaopas - https://www.yrittajat.fi/oppaat/yrittajan-tietosuojaopas/