OPAS:

GDPR

ELI TIETOSUOJA-ASETUS

LISTA YRITTÄJÄN
PERUSTEHTÄVISTÄ

Lindblad

Asianajotoimisto Lindblad & Co Oy • www.lindblad.fi

GDPR säätää EU:n kansalaisten oikeuksista tietosuojaan ja omien tietojen luottamukselliseen käsittelyyn

GDPR (General Data Protection Regulation) eli EU:n yleinen tietosuoja-asetus tulee voimaan 25.5.2018 kaikissa EU:n jäsenmaissa. Sitä sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn.

Tietosuoja-asetuksen voimaantulo vaatii useimmilta yrittäjiltä omien käytäntöjen tarkistamista ja päivittämistä. Kokosimme tähän oppaaseen kymmenen kohdan ohjeistuksen tarvittavien toimien tekemistä varten.

1 Tunnista käytössänne olevat henkilötietoryhmät ja tarkista jokaisen ryhmän osalta, että henkilötietojen käsittelyyn on asetuksen mukainen käsittelyperuste.

Henkilötietoryhmä on tietty samankaltainen joukko tietoja: esimerkiksi työntekijätiedot, asiakastiedot, markkinointiin käytettävät henkilötiedot ja alihankintasopimuksiin liittyvät henkilötiedot.

Mikäli henkilötietoryhmä sisältää tietoja henkilön rodusta, etnisestä alkuperästä, poliittisista mielipiteistä, uskonnollisesta tai filosofisesta vakaumuksesta, ammattiliiton jäsenyydestä, terveydentilasta, seksuaalisesta käyttäytymisestä tai suuntautumisesta, geneettistä tai biometristä informaatiota, josta henkilön voi tunnistaa, on tietojen käsittelyyn oltava asetuksen mukainen erityinen peruste.

Asetuksen mukaisia käsittelyperusteita ovat:

- **Suostumus**
  Rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten. Rekisterinpitäjän tulee dokumentoida saatu suostumus, koska se pitää pystyä todentamaan. Suostumus tulee antaa tietoisesti, eli sitä ei voi antaa esimerkiksi valmiiksi rastitetulla ruudulla tai jättämällä jotakin tekemättä.

- **Oikeutettu etu**
  Rekisterinpitäjän ja rekisteröidyn välillä on asianmukainen ja merkityksellinen suhde, kuten esimerkiksi jäsenyys, asiakkuus tai työsuhde.

- **Sopimus**
  Henkilötietojen käsittelyyn on oikeus, kun se on tarpeen sellaisen sopimuksen ehtojen noudattamiseksi, jossa rekisteröity on osapuolena.

- **Lakisääteinen velvoite**
  Henkilötietojen käsittely ilman rekisteröidyn suostumusta on sallittua, kun se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Lakisääteinen velvoite on kyseessä esimerkiksi, kun työnantaja ilmoittaa työntekijöiden palkkatietoja veroviranomaisille ja osakeyhtiölain mukaisen osakasluettelon pitäminen.

- **Elintärkeä tai yleinen etu**
  Henkilötietoja voidaan käsitellä silloin, kun käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Tällainen tarkoitus voi olla esimerkiksi ihmishenkien suojeleminen luonnonkatastrofin yhteydessä.

- **Julkinen tehtävä**
  Henkilötietoja voidaan käsitellä julkisen tehtävän suorittamiseksi.

Kirjoita kunkin rekisterin käsittelyperuste rekisteröidylle ymmärrettävään muotoon.

2. Laadi seloste käsittelytoimista.

Seloste käsittelytoimista on organisaation sisäinen asiakirja, jolla ohjeen kaltaisesti yrityksen sisällä määritellään henkilötietojen käsittelyä. Sen tehtävänä on myös osoittaa esimerkiksi valvontaviranomaisille, että henkilötietoja käsitellään tietosuojalainsäädännön mukaisesti. Seloste käsittelytoimista on pyydettäessä toimitettava valvontaviranomaiselle.

Selosteeseen kirjattavia tietoja:

- rekisterinpitäjän, mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja mahdollisen tietosuojavastaavan nimi ja yhteystiedot

- kuvaus siitä, missä tarkoituksessa henkilötietoja käsitellään

- kuvaukset rekisteröityjen ryhmistä ja henkilötietoryhmistä

- tarvittaessa henkilötietojen vastaanottajien ryhmät, joille henkilötietoja on luovutettu tai luovutetaan

- tarvittaessa tiedot henkilötietojen luovuttamisesta EU-alueen ulkopuolelle

- eri tietoryhmien poistamiseen liittyvä suunnitelma sillä tarkkuudella kuin on mahdollista

- yleinen kuvaus käsittelyn turvallisuuden varmistamiseksi toteutetuista teknisistä ja henkilötasoisista turvatoimista.

Tietosuojavaltuutetun sivulla on tarkempia ohjeita ja mallipohja käsittelytoimien selosteesta.

3. Dokumentoi, miten rekisteröityjä on kunkin rekisterin osalta informoitu.

Henkilötietojen käsittelyn tulee olla läpinäkyvää, ja rekisteröidyille tulee esittää, miten heitä koskevia tietoja kerätään ja miten tietoja käytetään. Tiedot tulee esittää yksinkertaisella ja selkeällä kielellä. Sanotut esitykset henkilötietojen käsittelystä tulee pitää rekisteröidyn saatavilla.

Asetuksen mukaan sanotut tiedot tulee esittää kirjallisesti, suullisesti tai sähköisesti.

Kun rekisteröidyltä kerätään häntä koskevia henkilötietoja, rekisterinpitäjän on toimitettava rekisteröidylle kaikki seuraavat tiedot:

- tietosuojavastaavan yhteystiedot, jos sellainen on nimetty
- henkilötietojen käsittelyn tarkoitukset sekä käsittelyn oikeusperuste eli syy, jonka perusteella yritys saa käsitellä kerättyjä henkilötietoja
- mahdolliset henkilötietojen vastaanottajat tai vastaanottajaryhmät
- onko rekisterinpitäjällä aikomus siirtää henkilötietoja EU:n ulkopuolelle
- rekisteröidyn oikeus pyytää rekisterinpitäjältä pääsy häntä itseään koskeviin henkilötietoihin
- rekisteröidyn oikeus pyytää tietojen oikaisemista, poistamista, tietojensa käsittelyn rajoittamista sekä vastustaa käsittelyä ja oikeus siirtää tiedot järjestelmästä toiseen.

4. Uudista käsittelyn ulkoistamisesta tai tietojen siirtämisestä tehdyt sopimukset asetuksen mukaisiksi.

Ulkoistettuja palveluita, joilla on pääsy henkilötietoihin, voivat olla esimerkiksi IT-tuki, pilvipalvelut, tilitoimistopalvelut ja konsulttipalvelut. Näissä tilanteissa henkilötietojen katsotaan siirtyvän niin sanotulle henkilötietojen käsittelijälle eli sille palveluntarjoajalle, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.

Rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka huolehtivat asianmukaisista suojatoimista ja varmistavat, että käsittely täyttää tietosuoja-asetuksen vaatimukset.

Yrittäjän tulee antaa ohjeet käsittelystä henkilötietojen käsittelijänä toimivalle palveluntarjoajalle. Ohjeet tulee antaa kirjallisina. Ne voi käytännössä liittää osaksi tietojenkäsittelysopimusta, jossa määritetään sekä rekisterinpitäjän että henkilötietojen käsittelijän oikeudet ja velvollisuudet suhteessa käsiteltäviin henkilötietoihin.

Tietojenkäsittelysopimuksessa tulisi sopia ainakin seuraavista asioista:

- Sopimukseen tulisi yksilöidä millaisia tietoja ja keitä henkilöitä (esim. asiakkaat) ulkoistus koskee.
- Henkilötietojen käsittelijän tulee sitoutua käsittelemään henkilötietoja ainoastaan rekisterinpitäjän ohjeiden ja sopimusehtojen mukaisesti.
- Sopimuksessa tulee varmistaa, että henkilötietojen käsittelyyn oikeutetut henkilöt, kuten henkilötietojen käsittelijän työntekijät, ovat sitoutuneet noudattamaan salassapitovelvollisuutta.
- Henkilötietojen käsittelijän on sitouduttava sopimuksessa toteuttamaan riittävät turvatoimet henkilötietojen suojaamiseksi; esimerkiksi tiedot tietokoneiden virustorjunnasta ja palomuureista, toimitilojen kulunvalvonnasta ja palveluntarjoajan organisaatioon liittyvistä seikoista.
- Sopimuksessa tulee sopia, onko henkilötietojen käsittelijän hankittava rekisterinpitäjältä suostumus palveluntarjoajan oman alihankkijan ottamiseksi osaksi tietojenkäsittelyä.
- Sopimuksessa tulee sopia, että käsittelijän on avustettava rekisterinpitäjää täyttämään rekisteröityjen oikeuksiin liittyvät velvollisuutensa.
- Käsittelijän on saatettava rekisterinpitäjän saataville kaikki sellaiset tiedot, jotka ovat tarpeen, jotta voidaan osoittaa rekisterinpitäjän toimineen oikein.
- Käsittelijän on sallittava rekisterinpitäjän tai sen valtuuttaman tahon suorittamat lainmukaisuuden auditoinnit ja osallistuttava niihin.
- Kun käsittelyyn liittyvien palveluiden tarjoaminen päättyy, tulee henkilötietojen käsittelijän poistaa tai palauttaa kaikki henkilötiedot rekisterinpitäjälle, lukuun ottamatta tilanteita joissa käsittelijällä on lakisääteinen velvollisuus säilyttää henkilötietoja.
- Kun rekisterinpitäjä on viime kädessä vastuussa henkilötietojen käsittelyn lainmukaisuudesta, sopimuksessa on tärkeää sopia keskinäisistä korvausvelvollisuuksista vahingon varalta.

5 Tarkista ja dokumentoi henkilötietojen käsittelyn turvallisuus, virustorjunta, palomuuri ja toimitilojen turvallisuus.

Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin. Rekisterinpitäjän ja henkilötietojen käsittelijän on varmistettava, että jokainen, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti.

Rekisterinpitäjän ja henkilötietojen käsittelijän on riittävillä teknisillä ja organisatorisilla toimenpiteillä varmistettava, että käsittelyn turvallisuustaso vastaa riskiä.

Tällaisia toimenpiteitä voivat olla esimerkiksi henkilötietojen salaus, kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus, kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa sekä menetelmät joilla testataan, tutkitaan ja arvioidaan säännöllisesti toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Jos tietojen käsitteleminen aiheuttaa henkilölle korkean riskin, tulee rekisterinpitäjän laatia vaikutusten arviointi (katso tarkemmin tietosuoja-asetuksen artikla 35).

6. Selvitä, tarvitsetko tietosuojavastaavan.

Tietosuoja-asetuksen mukaan yrittäjän ja henkilötietojen käsittelijän on nimitettävä tietosuojavastaava siinä tapauksessa, että rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka luonteensa, laajuutensa tai tarkoitustensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa (katso tarkemmin tietosuoja-asetuksen artikla 37).

7. Suunnittele ja dokumentoi menettely sen varalta, että joudut kertomaan tietomurrosta rekisteröidyille ja valvontaviranomaiselle.

Henkilötietojen tietoturvaloukkaus on tapahtuma, jonka seurauksena tallennettuja tai muuten käsiteltyjä henkilötietoja vahingossa tai lainvastaisesti tuhoutuu, häviää tai muuttuu, tietoja on luovutettu luvattomasti tai joku on luvattomasti päässyt tietoihin.

Rekisterinpitäjän on ilmoitettava henkilötietojen tietosuojaloukkauksesta ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta toimivaltaiselle valvontaviranomaiselle. Näin ei kuitenkaan tarvitse tehdä, jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu riskiä henkilöiden oikeuksille ja vapauksille.

Kun henkilötietojen käsittelijä saa tietää henkilötietojen tietoturvaloukkauksesta, hänen on ilmoitettava siitä rekisterinpitäjälle ilman aiheetonta viivytystä.

Tällaisessa ilmoituksessa tulee kuvata:

- henkilötietojen tietoturvaloukkaus ja mahdollisuuksien mukaan ilmoittaa yksityiskohtaista tietoa asianomaisten rekisteröityjen ryhmistä ja arvioita lukumääristä sekä henkilötietojen sisällöstä.
- henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset
- toimenpiteet, joita rekisterinpitäjä on ehdottaa tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta
- miten mahdollisia haittavaikutuksia lievennetään.

Rekisterinpitäjän tulee dokumentoida kaikki henkilötietojen tietoturvaloukkaukset, niiden vaikutukset sekä korjaavat toimet. Valvontaviranomaisen on voitava tämän dokumentoinnin avulla tarkistaa, että tätä artiklaa on noudatettu (katso tarkemmin tietosuoja-asetuksen 33 artikla).

8. Suunnittele ja dokumentoi menettely rekisteröidyn käyttäessä oikeuksiaan, kuten oikeutta saada pääsy tietoihin, tulla unohdetuksi tai siirtää tiedot järjestelmästä toiseen ja vastustamisoikeutta.

Oikeus tietojen oikaisemiseen

Rekisteröidyllä on oikeus vaatia, että yritys oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot, esimerkiksi toimittamalla rekisterinpitäjälle lisäselvityksiä.

Oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus saada yritys poistamaan häntä koskevat tiedot eli oikeus tulla unohdetuksi seuraavissa tilanteissa:

- Henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä käsiteltiin.
- Henkilötietojen käsittely perustuu suostumukseen ja rekisteröity peruuttaa suostumuksensa.
- Rekisteröity vastustaa käsittelyä. Jos rekisteröity vastustaa muuta käsittelyä kuin käsittelyä suoramarkkinointitarkoituksessa, on lisäedellytyksenä, että käsittelyyn ei ole olemassa perusteltua syytä.
- Henkilötietoja on käsitelty lainvastaisesti.
- Henkilötiedot on poistettava lakisääteisen velvoitteen noudattamiseksi.
- Henkilötiedot on kerätty tarjottaessa sähköisiä palveluja suoraan lapselle.

Yrityksillä voi olla oikeutettu etu henkilötietojen käsittelyyn, jolloin tietoja ei tarvitse poistaa.

9. Yrittäjällä on velvollisuus huolehtia tietosuoja-asetuksen mukaisen dokumentaationsa päivittämisestä kulloinkin vallitsevia olosuhteita vastaaviksi.

Tietosuoja-asetuksessa ei kattavasti yksilöidä dokumentaatiovaatimuksia, vaan vaatimus ilmenee sitä kautta, että rekisterinpitäjän tulee kyetä osoittamaan toimivansa asetuksen vaatimusten mukaisesti. Osoittaminen vaatii ajantasaisen dokumentoinnin laatimista ja ylläpitoa.

10. Laadi tarvittaessa salassapitosopimukset työntekijöiden kanssa.

Salassapitosopimuksella voi tarpeen mukaan korostaa henkilötietojen käsittelyyn osallistuvien sitouttamista yrityksen sisäisiin tietosuojaohjeisiin.

Mikä tieto on henkilötietoa ja millainen toiminta on henkilötiedon käsittelyä?

Henkilötiedolla tarkoitetaan luonnollista henkilöä tai hänen ominaisuuksiaan koskevia tietoja. Lisäksi sillä tarkoitetaan rekisteröidyn elinolosuhteita kuvaavia merkintöjä, jotka voidaan yhdistää häneen, hänen perheeseensä tai hänen kanssaan yhteisessä taloudessa eläviin henkilöihin.

Kyse voi olla esimerkiksi asiakkaiden, työntekijöiden tai yrityskontaktien henkilötiedoista, kuten nimestä, osoitteesta, puhelinnumerosta, auton rekisterinumerosta, tai mistä tahansa tiedosta, jonka voi liittää tiettyyn henkilöön.

Henkilötietojen käsittelyllä tarkoitetaan mm. henkilötietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakemista tietojoukoista, käyttämistä johonkin tarkoitukseen ja tietojen luovuttamista.

TARVITSETKO APUAMME **TIETOSUOJA-ASETUKSEEN** LIITTYEN? AUTAMME MIELELLÄMME.

Asianajotoimisto Lindblad & Co Oy

Helsingin toimisto

Vuorikatu 16 A 5, 00100 Helsinki

020 749 8160

helsinki@lindblad.fi

Katso muiden paikkakuntien yhteystiedot osoitteesta: **lindblad.fi/toimistot**

Lindblad