Sisukord

Directo ja GDPR eli EU:n yleinen tietosuoja-asetus (EU-direktiivi 2016/679)

Yleistä

EU:n tietosuoja-asetus (GDPR) astuu voimaan toukokuun 25.5.2018. Asetuksen tavoite on tuoda läpinäkyvyyttä yritysten ja organisaatioiden henkilötietojen käsittelyyn. Asetuksen mukaan kaikilla yksityishenkilöillä on oikeus tietää, miten hänen henkilötietojaan, kuten nimi, osoite, sähköposti, syntymäaika tai terveystiedot, käsitellään organisaatioissa. Se tarkoittaa, että henkilötietoja säilyttävien yritysten ja yhteisöjen täytyy jatkossa pystyä seuraamaan muun muassa, missä kaikkialla henkilötietoja säilytetään, mihin niitä käytetään ja kuka niitä on katsellut. Lisäksi jokaisen organisaation on tarjottava yksityishenkilöille, hänen sitä pyytäessä, tarkka selvitys henkilötietojen käsittelystä.

Rekisterinpitäjän vastuu

Jokainen organisaatio, jolla on henkilötietorekisteri, toimii sen osalta rekisterinpitäjänä. Rekisterinpitäjällä on siis aina vastuu tietosuoja-asetuksen noudattamisesta. Helpottaaksemme rekisterinpitäjän vastuuta toteuttaa rekisteröidyn oikeuksia, Directo henkilötietojen käsittelijänä toimivana ohjelmistotalona auttaa siinä, että asiat on mahdollista tarkistaa meidän ohjelmistostamme.

Roolit

1. Rekisterinpitäjä (data controller) Henkilötietorekisteristä vastaa rekisterinpitäjä, joka voi olla yritys, viranomainen, yhdistys, laitos tai säätiö. Rekisterinpitäjä on juridisessa vastuussa rekisteristä, määrää rekisterin käytöstä sekä on taho, jonka käyttöä varten rekisteri on luotu. Rekisterinpitäjän on lain mukaan laadittava rekisteriseloste, josta käy ilmi muun muassa rekisterin käyttötarkoitus, kerättävät tiedot ja niiden tietolähteet, rekisterin suojaus sekä rekisterinpitäjän yhteystiedot.
2. Henkilötietojen käsittelijä (data processor) Henkilötietojen käsittelijä on taho, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta. Esimerkiksi digitaalisten palveluiden toimittajat käsittelevät usein asiakasyritystensä asiakkaiden tietoja toimittamissaan palveluissa. Verkkokauppoihin ja kirjautumista vaativiin palveluihin syntyy väistämättä henkilötietorekisteri.
3. Data Processor ehk andmete säilitaja. Selles rollis on Directo poolt valitud kesksüsteemiteenuse pakkuja ehk Telia Eesti AS. Andmete säilitamise juures tuleb järgida erinevaid füüsilise ja protseduurilise kaitse reegleid.

Henkilötietojen käsittely

- käsittely voi tapahtua ainoastaan, kun on saatu henkilön itsensä antama suostumus henkilötietojensa keräämiseen ja käsittelyyn. Tämä suostumus pitää olla rekisterinpitäjällä dokumentoituna, paitsi jos käsittely on tarpeen muiden säädösten tai lakien perusteella, esim. viranomaisrekisterit. Suostumus voidaan liittää esim. tiedostona Directon asiakaskortille.
- rekisteröidyllä yksityishenkilöllä on oikeus tietää mitä tietoa hänestä on rekisteröity, mihin,

miten ja kenen toimista tietoja on käytetty. Directon käyttäjäloki on muutettu loputtomaksi ja sieltä löytyy nyt tiedot, joilla voidaan vastata edellä mainittuihin kysymyksiin.
- Rekisteröidyllä on oikeus pyytää henkilötietojensa poistamista rekisteristä. Tässä tapauksessa rekisterinpitäjän on poistettava tiedot, paitsi silloin, kun niiden (osittainen) säilyttäminen säädetään toisessa laissa. Esimerkki. Yksittäisiä asiakkaita, jotka ovat hankkineet palveluyritys monta vuotta, vaatii loppuun heidän tietojaan käsitellään. Hakemistot poistavat asiakaskortin, jolloin Directo tarvitsee korvaavan koodin. Oletetaan, että tähän on saatavilla 1111 asiakasta. Kun olet poistanut asiakas ei ole enää yksityinen Directon asiakastietoja tai yksikään liittyvät toimintaan enemmän kuollut henkilö. AGA - kirjanpitosyistä täytyy säilyttää kirjanpito lähde, joka voidaan toistaa muodossa, mikä tarkoittaa sitä, että esimerkiksi asiakas laskun poistamaan hänen nimeään ei käytetä.
- Erikseen kannattaa arvioida ne riskit, jotka voivat liittyä siihen, että käyttäjä vie Directosta ulos tietoja ja tallentaa sen paikallisesti esim. tietokoneensa kovalevylle. Esimerkki: Directon käyttäjä tarkistaa yhtiön yksityinen asiakaskortin, jolloin käyttäjälokiin syntyy vastaava merkintä. Nyt on kuitenkin mahdollista, että käyttäjä Leikkaa-Liimaa henkilökohtaisia tietoja asiakaskortilta ja tallentaa ne tietokoneelle. Tällaisesta toimenpiteestä ei jää mitään tietoja Directoon ja nyt käyttäjä on luonut mahdollisesti uuden henkilörekisterin. Tällaisten riskien merkitys kasvaa, jos Directoa käyttää henkilöä EU: n ulkopuolella, koska tietojen siirrosta EU:n ulkopuolelle on aina pyydettävä erillinen lupa.

Tietojen säilyttäminen

- Directoon tallennettu data, joka saattaa sisältää henkilötietoja, on fyysisesti tallennettu Telia Eesti AS palvelinkeskukseen Tallinnassa.
- varmuuskopiot sijaitsevat Tallinnassa Virossa.
- varmuuskopioista vastuulliset henkilöt asuvat Tallinnassa Virossa.
- Directon käyttämän palvelinkeskuksen Telia Eesti AS:n toiminta on sertifioitu kaikilta osin Bureau Veritaksen toimesta ISO 27001 standardin mukaisesti toimivaksi. GDPR:n vaatimukset ovat yhteneviä ISO 27001 standardin kanssa.
- Koska Directo on 100% pilvipalveluna toteutettu, niin käyttäjän omalle koneelle ei tallenneta mitään tietoja.