Sisukord

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

Yleistä

EU:n tietosuoja-asetus (GDPR) astuu voimaan toukokuun lopulla 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 mahdollisuus pyytää selvitystä ja pyynnön saavuttua myös toimitettava 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. Data Controller ehk andmete töötleja. Sellesse rolli võib sattuda Directot kasutav ettevõte, juhul kui kogutakse eraisikute andmeid. Directo universaalsest arhitektuurist tulenevalt on teoreetiliselt võimalik regulatsioonile alluvaid andmeid salvestada suvalisse süsteemi osasse ja seetõttu peab andmete töötleja olema kindel, et ta tegutseb reeglite kohaselt.
2. 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.

Andmete töötlemine

- Andmete töötlemine saab toimuda ainult andmete omaniku dokumenteeritud nõusolekul, välja arvatud juhul, kui töötlemise kohustus tuleneb mõnest muust õigusaktist. Nõusolekut kinnitav dokument peab olema taasesitatav. Juhul, kui andmete töötlemiseks kasutatakse Directot, soovitame me nõusoleku dokumente samuti hoida Directos. Näide: eraisik soovib liituda püsikliendiprogrammiga ja allkirjastab vastava avalduse, mille raames annab ta nõusoleku oma andmete töötlemiseks. Allkirjastatud dokument lisatakse Directosse kliendikaardi manuseks. Juhul, kui tekib küsimus, miks on antud isiku andmeid töötlema asutud, on nõusolek andmekirjega 1:1 seotud.
- Andmete omanikul on õigus esitada küsimus, kes ja millal on tema andmeid töödelnud. Kõikidest toimingutest, mis Directos tehakse, jääb maha kasutuslogi, mida säilitatakse igavesti. Vastava aruande abil saab tulevikus vastata küsimustele, KES, MILLAL ja KUST on andmeid

vaadanud või muutnud. See viimane, ehk KUST (IP aadress) võib osutuda oluliseks juhul, kui andmeid töödeldakse väljaspool EU-d

- Andmete omanikul on õigus esitada nõudmine oma andmete töötlemine lõpetada. Sellisel puhul tuleb andmed töötleja valdusest kõrvaldada, välja arvatud juhul, kui nende (osaline) säilitamine on reguleeritud mõne muu õigusaktiga. Näide. Eraisikust klient, kes on aastaid ettevõttelt teenuseid ostnud, nõuab oma andmete töötlemise lõpetamist. Directos kustutatakse sellisel puhul kliendi kaart, mille puhul Directo nõuab mingit asenduskoodi. Oletame, et selleks on 1111 Klient. Pärast kliendi kustutamist ei ole Directos enam eraisikust kliendi kirjet ega ole ükski temaga seotud toiming enam isikuliselt tuvastatav. AGA - Raamatupidamisseaduse nõuetest tulenevalt peavad olema raamatupidamise algdokumendid säilitatud taasesitamist võimaldaval kujul, mis tähendab, et näiteks kliendile esitatud arve pealt tema nime eemaldada ei tohi.
- Oluline on tähele panna, et andmete töötlemise vajadus võib tekkida ka muus olukorras kui eraisikust klienti teenindades. Näiteks kui ettevõte kasutab Directot selleks, et töötajale töötasu arvestada, on tegemist andmete töötlemisega ja selleks on vaja andmete omaniku nõusoleku kinnitust.
- Eraldi tasub hinnata riske, mis võivad kaasneda sellega, et Directot kasutav isik salvestab andmeid lokaalselt mingeid sõltumatuid vahendeid kasutades. Näide: Directo kasutaja XXX vaatab ettevõtte eraisikust kliendi kaarti Directos. Logis on vastav kirje. Ekraanil avatud kliendi andmetest võtab töötaja Copy-Paste meetodil isiku koduse aadressi ja salvestab selle oma arvutis olevasse Exceli faili. Sellise toimingu kohta ei ole kuskil ühtegi kirjet ja ei saagi olla, aga andmete töötlemine on laienenud väljapoole Directot. Selliste riskide tähtsus suureneb juhul, kui Directot kasutav isik asub väljaspool EU piire.

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.