Sisukord

Directo kasutamine GDPR kontekstis

Üldine

GDPR ehk General Data Protection Regulation (EU direktiiv 2016/679) reguleerib eraisikust EU residentide andmete töötlemist. Kõik Directo kliendid, kellel on plaan mingiski ulatuses isikuandmeid töödelda, peaks arvesse võtma teatud asjaolusid ja vajadusel kohaldama oma Directo kasutamist puudutavaid protsesse vastavalt oma rollile.

Rollid

1. Data Controller ehk andmete vastutav 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 ehk nn volitatud töötleja. 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 või õigustatud huvist. 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. Loe ka Andmekaitse Inspektsiooni (AKI) juhiseid korrektseks nõusoleku küsimiseks: http://www.aki.ee/et/andmekaitse-reform/nousoleku-kontrollnimekiri
- 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.
- Andmete töötlemiseks EI ole vaja küsida subjekti nõusolekut juhul, kui see on vajalik kehtiva lepingu täitmiseks. Seda on oluline teada ka seetõttu, et kõik ettevõtted, mis Directot kasutavad, teevad seda kehtiva litsentsilepingu alusel ning seetõttu pole neil vaja anda Directole eraldi nõusolekut selliseks andmete töötlemiseks, mis toimub lepingu tingimuste kohaselt Directot kasutades.
- Sõltuvalt sellest, milliseid isikuandmeid Directo klient töötleb, võib tal tekkida täiendavaid kohustusi, näiteks kohustus määrata andmekaitsespetsialist või pidada töötlemistoimingute registrit. Loe lähemalt oma võimalike kohustuste kohta siit: http://www.aki.ee/et/andmekaitse-reform/andmetootleja-kohustused

Andmete säilitamine

- Directo kasutamise käigus tekkivaid andmeid (mis võivad, aga ei pruugi sisaldada isikuandmeid) hoitakse Telia Eesti AS andmekeskustes.
- Andmete, sh nendest koostatud varukoopiate säilitamise asukoht on Tallinn, Eesti Vabariik
- Directo litsentsilepingu tingimuste kohaselt koostatakse varukoopia iga 24 tunni tagant ning säilitatakse seitset viimast varukoopiat. See tähendab, et juhul, kui andmete töötleja kustutab või anonümiseerib isikuandmeid, kulub seitse kalendripäeva, enne kui muutub võimatuks ka nende taastamine varukoopiast
- Andmete säilitamise eest vastutavate isikute töökohustuste täitmise asukoht on Tallinn, Eesti Vabariik
- Telia Eesti AS infoturbe juhtimissüsteem on sertifitseeritud Bureau Veritas poolt ISO 27001 standardi alusel. GDPR seatud andmete säilitamise nõuded on ISO 27001 alamosa
- Kuna Directo on 100% pilveteenus, ei hoita kasutaja arvutis mingeid andmeid. See tähendab muuhulgas, et juhul, kui Directot kasutatakse EU kodanike andmete töötlemiseks väljaspool EU piire, ei hoiustata selle käigus kunagi isikuandmeid väljaspool EU territooriumit.

Andmelekked

Juhul, kui andmete töötlejal on infot võimaliku isikuandmete lekke kohta, palun sellest teavitada Directo andmekaitse inspektorit (Data Protection Officer) dpo@directo.ee et me saaks teid igakülgselt abistada juhtumi uurimisel ning vajadusel määruses ette nähtud subjektide teavitamisel.