GDPR ja professionaalne sõnumside: miks enamik rikub reegleid seda teadmata

Peaaegu iga büroo, praksis või nõustamisettevõte saadab kliendidokumente rakenduste kaudu, mille server asub väljaspool Euroopa Majanduspiirkonda. Ilma kurja kavatsuseta, kuid paljudel juhtudel määrust rikkudes, ilma et keegi oleks neid hoiatanud.

Dokument, mis reisib rohkem kui arvate

Igapäevane olukord: maksunõustaja saab sõnumside kaudu kliendiandmetega dokumendi. Müügiesindaja saadab chati kaudu pakkumise kolleegile edasi. Arst jagab samal viisil kliinilist raportit kolleegiga. Keegi ei mõtle sellele kaks korda. See on normaalne. See on mugav. See on see, mida tehakse iga päev igas büroos igas Euroopa linnas.

Kuid see dokument on paljudel juhtudel just reisinud serverisse Ameerika Ühendriikidesse. See on salvestatud – kasvõi ajutiselt, kasvõi "puhkeolekus krüpteeritult" – pilve, mida ei professionaal ega tema klient ei kontrolli. See on läbinud süsteeme, mis saavad tehniliselt indekseerida sisuga seotud metaandmeid. Ja Euroopa isikuandmete kaitse üldmäärusel on selle kohta üsna selget öelda.

Mida norm nõuab

GDPR – ja selle tulemusena Euroopa Liidu Kohtu kohtupraktika (eriti Schrems II otsus, C-311/18, aastast 2020) – sätestab, et Euroopa kodanike isikuandmed peavad olema asjakohaselt kaitstud. Kui need andmed väljuvad Euroopa Majanduspiirkonnast, peab vastutav töötleja garanteerima, et vastuvõtja pakub kaitsetaset, mis on "sisuliselt samaväärne" Euroopa omaga. Praktikas tähendab see, et kliendiandmete saatmine teenuste kaudu, mille serverid alluvad USA jurisdiktsioonile, ilma mõjuhinnangut läbi viimata ja täiendavaid tagatisi rakendamata – standardselepingu klauslid, tehnilised lisameetmed nagu kontrollitav krüpteerimine jne – võib kujutada endast määruse rikkumist. Isegi kui siiani pole keegi midagi öelnud.

Ja küsimus pole ainult sõnumite sisus. Metaandmed – kes saadab mida kellele, millal, kui sageli, kust – on eeskirjade kohaselt ja Euroopa Andmekaitsenõukogu korduva tõlgenduse kohaselt samuti isikuandmed. Teenus, mis kogub metaandmeid kasutaja ametialasest suhtlusest, töötleb selle kasutaja klientide isikuandmeid, ilma et neil oleks sellest teadmist või nad oleksid andnud nõusoleku selliseks töötlemiseks.

Tavaline mõttemuster – "kasutan rakendust ainult kirjutamiseks; rakendus pole mu kliendi andmete tarnija" – on juriidiliselt vale. Kui kliendi andmed läbivad kolmanda osapoole infrastruktuuri, töötleb see kolmas osapool neid andmeid. Ja kui ta neid töötleb, peab olema juriidiline alus, andmetöötlusleping ja asjakohased garantiid.

Kes on vastutav

Küsimus, kes kannab juriidilist vastutust, pole akadeemiline. GDPR eristab *vastutavat töötlejat* (kes otsustab, milliseid andmeid ja mis eesmärgil töödeldakse) ja *volitatud töötlejat* (kes teeb seda materiaalselt vastutava

töötleja nimel). Kliendi dokumente saatev professionaal on vastutav töötleja. Sõnumirakenduse pakkuja on paljudel juhtudel faktiliselt volitatud töötleja. Ilma volituse lepinguta – ja ilma enamiku klausliteta, mida selline leping peaks sisaldama – pole vastutav töötleja oma kohustust täitnud.

Leebe tõlgendus on: "enamik professionaale ei tea seda". Range tõlgendus on: "seaduse mittetundmine ei vabasta vastutusest". Ja iga selles küsimuses konsulteeritud andmekaitsele spetsialiseerunud advokaadi tõlgendus on tavaliselt range.

Kellele see konkreetselt oluline on

Igale professionaalile või ettevõttele, kes kasvõi aeg-ajalt opereerib kolmandate isikute isikuandmetega:

- Advokaadid, kes saavad kliendidokumentatsiooni (lepingud, hagid, deklaratsioonid, varaaruanded).
- Arstid ja muud tervishoiutöötajad, kes jagavad terviseandmeid – mida peetakse GDPR-i art 9 kohaselt *eriliiki isikuandmeteks* koos tugevdatud kaitsekorraga –.
- Maksunõustajad ja haldusjuhid, kes opereerivad tuvastus-, maksu- ja pangandatmetega.
- Personaliosakonnad, kes haldavad töötajate töö- ja isiklikku dokumentatsiooni.
- Müügiesindajad, kes saavad kontaktandmeid ja sageli tundlikku äriteavet potentsiaalsetelt ja olemasolevatelt klientidelt.

Kõigil juhtudel on teave GDPR-iga kaitstud. Kõigil juhtudel liigub see teave tavapärases praktikas kanalite kaudu, mille jurisdiktsioon ei luba neid deklareerida "sisuliselt samaväärseks" Euroopa raamistikuga ilma täiendavate garantiideta. Mitte kurjast tahtest. Harjumusest. Ja tehnoloogilise infrastruktuuri tõttu, mis on viisteist aastat seadnud mugavuse vastavusest ettepoole.

Argument "kõik teevad nii"

Tasub ennetada kõige sagedasemat vastuväidet: "kui kõik nii teevad, ei saa see olla tegelik probleem". See on täiesti mõistetav argument ja juriidiliselt pole sellel mingit jõudu. Fakt, et tava on levinud, ei muuda seda määrusega kooskõlas olevaks. Andmekaitseasutused on viimastel aastatel karistanud mitmeid ettevõtteid just sõnumside kasutusviiside eest, mis tundusid kontrolli hetkeni kahjutud.

Praegune operatiivne reaalsus on see, et risk on tõenäosuse mõttes madal – juhtub väga harva, et andmekaitseinspektsiooni kontroll auditeerib keskmise suurusega büroo spetsiifilisi sõnumside tööriistu –, kuid mõju mõttes kõrge, kui see realiseerub. See on risk, mille enamik võtab teadmata, et nad seda teevad. Ehk siis hindamata, kas kasutatav tööriist on kooskõlas vastutava töötleja juriidilise vastutusega.

Digitaalne jälg on tagasiulatuv

On olemas teine, peaaegu sümmeetriline argument eelmisega, mida tasub ennetada: *"kui see oleks tõsine probleem, oleks administratsioon seda juba kontrollima hakanud"*. Praegune vaadeldav reaalsus annab talle pealiskaudselt õiguse. Sõnumside väärkasutuse kontrollid väikeettevõtetes ja eriti füüsilisest isikust ettevõtjate juures on täna peaaegu olematud – mitte sellepärast, et käitumine oleks lubatud, vaid sellepärast, et administratsioonil Eestis ja suures osas EL-ist puuduvad vajalikud inimressursid miljonite kohustatute auditeerimiseks.

Seda sugereerib tänane vaadeldav praktika. See pole aga see, mida sugereerib järgmine kümnend. Kaks vektorit koonduvad, et muuta tasakaalu suhteliselt lühikese aja jooksul.

Esiteks: digitaalne jälg on tagasiulatuv. Iga kesksserveriga rakenduse kaudu saadetud sõnum jääb registreerituks – vähemalt metaandmetesse – infrastruktuuri, mis püsib. See, mis saadeti kuus kuud tagasi, on tehniliselt täna veel auditeeritav. See, mis saadetakse täna, on auditeeritav veel viie aasta pärast. Praegune

kontrolli puudumine ei ole garantii tulevase kontrolli puudumise kohta. See on hindamise edasilükkamine, mitte vabastus.

Teiseks: administratiivne auditeerimisvõimekus kasvab kiirenevas tempos. Tehisintellekti tööriistade kasutuselevõtt kontrolliprotsessides eemaldab inimliku kitsaskoha, mis on seni – faktiliselt, mitte juriidiliselt – kaitsnud väikeettevõtteid ja füüsilisest isikust ettevõtjaid. Süsteem, mis suudab ristkasutada massiivseid metaandmeid, maksudeklaratsioone, äriregistreid ja rikkumistest teatamise kohustusi, ei vaja inspektoreid: ta vajab juurdepääsu. Ja juurdepääs on EL-is juriidilist kohalolekut omavatele pakkujatele suunatud nõuete kaudu praeguses normatiivses raamistikus täiesti teostatav.

Sellele lisandub vähem tehniline, kuid sama määrav tegur: Euroopa riigid on pidevalt kasvava võlgnevuse protsessis ja nad peavad peaaegu ilma eranditeta oma maksubaasi laiendama. GDPR-i mittetäitmisest tulenev haldussanktsioon on puhtalt fiskaalses mõttes kasvav ja poliitiliselt mugav tulunõu. See pole oletus: see on vaadeldav trend Euroopa andmekaitseasutuste aastaaruannetes, kus sanktsioonide kogumaht tõuseb mitu majandusaastat järjest.

Operatiivne järeldus vastutavale töötlejale pole alarmistlik, vaid kaine: **otsust selle kohta, kuidas täna kliendisuhtlust hallatakse, hinnatakse kontrolli toimumise aasta kontrollivõimekuse järgi, mitte praeguse järgi.** Ja see võimekus on mõistliku aja jooksul oluliselt teistsugune kui täna. Kes hakkab asju õigesti tegema täna, ei ole korras ainult alates tänasest: sellest hetkest genereeritud jälg on normiga kooskõlas ja see kaitseb tagasiulatuvalt tulevat lõiku. Kes jätkab nagu seni, kuhjab auditeeritavat jälge, mille vastavust hinnatakse tulevaste aastate standardite – ja ressursside – järgi.

Mis muutub teistsuguse arhitektuuriga

On olemas tehnilised alternatiivid, kus andmeid ei salvestata kolmandate osapoolte infrastruktuuri, vaid need reisivad otse saatja seadmest vastuvõtja seadmesse. Selles arhitektuuris ei sõltu GDPR-i järgimine rahvusvaheliste edastuste osas standardsetest lepingutingimustest, pakkuja heast tahtest ega tulevastest audititest. See sõltub sellest, et *edastamist ei toimu*. Ja seda, mida pole olemas, ei saa rikkuda.

See pole ainus lahendus ega ainus võimalik. Kuid see on struktuurselt teistsugune ja normatiivne vastavus lakkab olemast protseduuriline lisa ning muutub disaini otseseks tagajärjeks. Professionaali jaoks, kes võtab oma vastutust töötlejana tõsiselt, on see erinevus oluline.

Järgmine Cuadernose väljaanne analüüsib üksikasjalikult Schrems II otsust ja selle praktilisi mõjusid USA pilveteenustest sõltuvatele väike- ja keskmise suurusega ettevõtetele viis aastat pärast selle avaldamist.

Allikad ja juriidiline raamistik

- Määrus (EL) 2016/679 (GDPR), eriti V peatükk rahvusvaheliste edastuste kohta.
- ELKo C-311/18 ("Schrems II"), 16. juuli 2020.
- EDPB – Soovitused 01/2020 edastamisvahendeid täiendavate meetmete kohta.
- Andmekaitseinspektsioon (ja teised järelevalveasutused) – Aastaaruanded koos kaasustega sanktsioonide kohta sõnumside väärkasutuse eest ametialases keskkonnas.

← EelmineAmetisaladus digiajastulJärgmine →Kui kedagi ei ole vahel

Viimased lugemised

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Võtke see artikkel endaga kaasa kuhu iganes vaja.

↓ Markdown ↓ Lihttekst ↓ PDF

Fail laaditakse alla teie seadmesse. Sealt saate selle salvestada, importida Solo2-sse või jagada kus iganes soovite. Cuadernos ei otsusta sihtkohta teie eest.

Lakipitsat · SHA-256 d4cb5e965b87e07df293e9a3cde8330224ac7b66bc0beba99d3b804ba8a6b48d

Cuadernos Lacre · Ettevõtte Menzuri Gestión S.L. väljaanne ·
kirjutanud R.Eugenio · toimetanud Solo2 meeskond.