Analyysi · 16. toukokuuta 2026

← Edellinen·Seuraava →

GDPR ja ammatillinen viestintä: miksi useimmat rikkovat sääntöjä tietämättään

Lähes jokainen toimisto, vastaanotto tai konsulttiyritys lähettää asiakasasiakirjoja sovelluksilla, joiden palvelin sijaitsee Euroopan talousalueen ulkopuolella. Ilman pahaa tarkoitusta, mutta monissa tapauksissa rikkoen asetusta ilman, että kukaan on varoittanut heitä.

Asiakirja, joka matkustaa enemmän kuin luulet

Arkipäivän tilanne: veroasiantuntija saa viestitse asiakirjan, joka sisältää asiakastietoja. Myyjä välittää chatin kautta tarjouksen kollegalleen. Lääkäri jakaa samaa reittiä potilaskertomuksen kollegalleen. Kukaan ei ajattele asiaa kahdesti. Se on normaalia. Se on mukavaa. Sitä tehdään päivittäin jokaisessa toimistossa jokaisessa Euroopan kaupungissa.

Mutta tuo asiakirja on monissa tapauksissa juuri matkustanut palvelimelle Yhdysvaltoihin. Se on tallennettu – vaikka tilapäisestikin, vaikka "levossa salattuna" – pilveen, jota ammattilainen tai hänen asiakkaansa eivät hallitse. Se on kulkenut järjestelmien kautta, jotka voivat teknisesti indeksoida sisältöön liittyviä metatietoja. Ja Euroopan yleisellä tietosuoja-asetuksella on tähän melko selkeää sanottavaa.

Mitä säännökset vaativat

GDPR – ja sen seurauksena Euroopan unionin tuomioistuimen oikeuskäytäntö (erityisesti Schrems II -tuomio, C-311/18, vuodelta 2020) – määrittää, että Euroopan kansalaisten henkilötietojen on oltava asianmukaisesti suojattuja. Jos nämä tiedot poistuvat Euroopan talousalueelta, rekisterinpitäjän on taattava, että vastaanottaja tarjoaa "olennaisesti vastaavan" suojatason kuin Euroopassa. Käytännössä tämä tarkoittaa, että asiakastietojen lähettäminen sellaisten palveluiden kautta, joiden palvelimet ovat Yhdysvaltain lainkäyttövallan alaisia, ilman vaikutustenarvioinnin tekemistä ja täydentävien suojatoimien – vakiosopimuslausekkeiden, teknisten lisätoimien kuten varmennettavan salauksen jne. – toteuttamista, voi olla asetuksen vastainen teko. Vaikka kukaan ei olisi vielä sanonut mitään.

Eikä kyse ole vain viestien sisällöstä. Metatiedot – kuka lähettää mitä kenelle, milloin, kuinka usein, mistä – ovat myös henkilötietoja säännösten mukaan, Euroopan tietosuojaneuvoston toistuvien tulkintojen mukaisesti. Palvelu, joka kerää metatietoja käyttäjän ammatillisesta viestinnästä, käsittelee kyseisen käyttäjän asiakkaiden henkilötietoja ilman, että nämä tietävät siitä tai ovat antaneet suostumustaan tällaiseen käsittelyyn.

Yleinen ajatusmalli – "käytän sovellusta vain kirjoittamiseen; sovellus ei ole asiakkaani tietojen toimittaja" – on oikeudellisesti virheellinen. Jos asiakkaan tiedot kulkevat kolmannen osapuolen infrastruktuurin kautta, tuo kolmas osapuoli käsittelee noita tietoja. Ja jos se käsittelee niitä, on oltava laillinen peruste, tietojenkäsittelysopimus ja asianmukaiset takuut.

Kuka on vastuussa

Kysymys siitä, kuka kantaa oikeudellisen vastuun, ei ole akateeminen. GDPR erottaa *rekisterinpitäjän* (joka päättää mitä tietoja käsitellään ja mihin tarkoitukseen) ja *henkilötietojen käsittelijän* (joka tekee sen konkreettisesti rekisterinpitäjän lukuun). Asiakasasiakirjoja lähettävä ammattilainen on rekisterinpitäjä. Viestintäsovelluksen tarjoaja on monissa tapauksissa tosiasiallinen käsittelijä. Ilman käsittelysopimusta – ja ilman useimpia lausekkeita, joita tällaisen sopimuksen tulisi sisältää – rekisterinpitäjä ei ole täyttänyt velvollisuuttaan.

Lievä tulkinta on: "useimmat ammattilaiset eivät tiedä tätä". Tiukka tulkinta on: "tietämättömyys ei poista vastuuta". Ja jokaisen asiaa koskevan tietosuojaan erikoistuneen asianajajan tulkinta on yleensä se tiukka.

Kenelle tällä on merkitystä konkreettisesti

Kaikille ammattilaisille tai yrityksille, jotka käsittelevät, vaikka vain satunnaisesti, kolmansien osapuolten henkilötietoja:

- Asianajajat, jotka vastaanottavat asiakasdokumentaatiota (sopimukset, kanteet, ilmoitukset, varallisuusraportit).
- Lääkärit ja muut terveydenhuollon ammattilaiset, jotka jakavat terveystietoja – joita pidetään GDPR:n 9 artiklan mukaisina *erityisinä tietoryhminä*, joihin sovelletaan tiukempia sääntöjä –.
- Veroasiantuntijat ja hallinnolliset konsultit, jotka käsittelevät tunnistetietoja sekä vero- ja pankkitietoja.
- Henkilöstöosastot, jotka hallinnoivat työntekijöiden työ- ja henkilöstödokumentaatiota.
- Myyjät, jotka vastaanottavat yhteystietoja ja usein arkaluonteisia kaupallisia tietoja mahdollisilta ja nykyisiltä asiakkailta.

Kaikissa tapauksissa tiedot ovat GDPR:n suojaamia. Kaikissa tapauksissa tavallisessa käytännössä nämä tiedot kulkevat kanavien kautta, joiden lainkäyttövaltaa ei voida todeta "olennaisesti vastaavaksi" Euroopan kehyksen kanssa ilman lisätakuita. Ei pahan tahdon vuoksi. Tavan vuoksi. Ja sellaisen teknologisen infrastruktuurin vuoksi, joka on asettanut mukavuuden vaatimustenmukaisuuden edelle viidentoista vuoden ajan.

Argumentti "kaikki tekevät niin"

On hyvä ennakoida yleisin vastaväite: "jos kaikki tekevät niin, se ei voi olla todellinen ongelma". Se on täysin ymmärrettävä argumentti, eikä sillä ole oikeudellisesti mitään voimaa. Se, että jokin käytäntö on yleinen, ei tee siitä asetuksen mukaista. Tietosuojavaltuutetun toimisto on viime vuosina rankaisut useita yrityksiä juuri sellaisesta viestinnän käytöstä, joka vaikutti vaarattomalta tarkastushetkeen asti.

Nykyinen toiminnallinen todellisuus on, että riski on todennäköisyyden osalta pieni – on hyvin harvinaista, että tietosuojaviranomainen auditoisi keskisuuren toimiston erityiset viestintätyökalut – mutta vaikutusten osalta suuri, jos se toteutuu. Se on riski, jonka useimmat ottavat tietämättään. Eli arvioimatta, onko käytetty työkalu linjassa rekisterinpitäjän oikeudellisen vastuun kanssa.

Digitaalinen jälki on takautuva

On olemassa toinen, lähes edellisen vastakohtainen argumentti, joka on syytä ennakoida: *"jos tämä olisi vakava ongelma, viranomaiset olisivat jo alkaneet tarkastaa sitä"*. Nykyinen havaittu todellisuus antaa tälle pinnallisesti oikeutuksen. Pienten yritysten ja erityisesti yksinyrittäjien viestinnän väärinkäytösten tarkastukset ovat nykyään lähes olemattomia – ei siksi, että toiminta olisi sallittua, vaan siksi, että hallinnolta Suomessa ja suuressa osassa EU:ta puuttuvat tarvittavat henkilöresurssit miljoonien velvollisten auditoimiseksi.

Tämä on se, mitä tänään havaittu käytäntö antaa ymmärtää. Se ei ole se, mitä tuleva vuosikymmen antaa ymmärtää. Kaksi vektoria lähentyy toisiaan muuttaakseen tasapainon suhteellisen lyhyellä aikavälillä.

Ensinnäkin: digitaalinen jälki on takautuva. Jokainen keskuspalvelimella varustetun sovelluksen kautta lähetetty viesti jää rekisteröidyksi – ainakin metatiedoissa – infrastruktuuriin, joka säilyy. Se, mitä lähetettiin kuusi kuukautta sitten, on teknisesti edelleen auditoitavissa tänään. Se, mitä lähetetään tänään, on auditoitavissa vielä viiden vuoden kuluttua. Nykyinen tarkastusten puute ei ole tae tulevasta tarkastusten puutteesta. Se on arvioinnin lykkääminen, ei vapautus.

Toiseksi: hallinnollinen tarkastuskapasiteetti kasvaa kiihtyvällä vauhdilla. Tekoälytyökalujen käyttöönotto tarkastusprosesseissa poistaa inhimillisen pullonkaulan, joka on tähän asti suojellut – tosiasiallisesti, ei oikeudellisesti – pieniä yrityksiä ja yksinyrittäjiä. Järjestelmä, joka pystyy ristiinajamaan massiivisia metatietoja, veroilmoituksia, kaupparekistereitä ja tietomurtojen ilmoitusvelvollisuuksia, ei vaadi tarkastajia: se vaatii pääsyn. Ja pääsy, EU:ssa oikeudellisesti läsnä oleville palveluntarjoajille suunnattujen vaatimusten kautta, on täysin mahdollista nykyisessä normatiivisessa kehyksessä.

Tähän lisätään vähemmän tekninen, mutta yhtä ratkaiseva tekijä: Euroopan valtiot ovat jatkuvassa velkaantumisprosessissa ja niiden on, lähes poikkeuksetta, laajennettava veropohjaansa. GDPR:n noudattamatta jättämisestä aiheutuva hallinnollinen sakko on puhtaasti verotuksellisin termein kasvava ja poliittisesti mukava tulonlähde. Tämä ei ole oletus: se on havaittavissa oleva suuntaus Euroopan tietosuojaviranomaisten vuosikertomuksissa, joissa sakkojen kokonaismäärä on noussut useana peräkkäisenä tilivuotena.

Toiminnallinen johtopäätös rekisterinpitäjälle ei ole hälyttävä vaan kylmä: **päätöstä siitä, miten asiakasviestintää hoidetaan tänään, arvioidaan tarkastusvuoden tarkastuskapasiteettia vasten, ei nykyistä.** Ja tuo kapasiteetti on kohtuullisessa ajassa olennaisesti erilainen kuin tänään. Se, joka alkaa tehdä asiat oikein tänään, ei ole kunnossa vain tästä päivästä alkaen: tästä hetkestä lähtien luotu jälki on säännösten mukainen, ja se suojaa takautuvasti tulevaa ajanjaksoa. Se, joka jatkaa kuten tähän asti, kerää auditoitavaa jälkeä, jonka vaatimustenmukaisuutta arvioidaan tulevien vuosien standardien – ja resurssien – perusteella.

Mikä muuttuu toisenlaisella arkkitehtuurilla

On olemassa teknisiä vaihtoehtoja, joissa tietoja ei tallenneta kolmannen osapuolen infrastruktuuriin, vaan ne matkaavat suoraan lähettäjän laitteesta vastaanottajan laitteeseen. Tässä arkkitehtuurissa GDPR:n noudattaminen kansainvälisten siirtojen osalta ei riipu vakiosopimuslausekkeista, palveluntarjoajan hyvästä tahdosta eikä tulevista auditoinneista. Se riippuu siitä, että *siirtoa ei ole*. Ja sitä, mitä ei ole olemassa, ei voi rikkoa.

Tämä ei ole ainoa ratkaisu eikä ainoa mahdollinen. Mutta se on rakenteellisesti erilainen, ja vaatimustenmukaisuus lakkaa olemasta menettelyllinen liite ja siitä tulee suora seuraus suunnittelusta. Ammattilaiselle, joka ottaa vastuunsa rekisterinpitäjänä vakavasti, tuolla erolla on merkitystä.

Seuraava Cuadernos-julkaisu analysoi yksityiskohtaisesti Schrems II -tuomiota ja sen käytännön vaikutuksia pienille ja keskisuurille yrityksille, jotka tukeutuvat yhdysvaltalaisiin pilvipalveluihin, viisi vuotta sen julkaisemisen jälkeen.

Lähteet ja säädöskehys

- Asetus (EU) 2016/679 (GDPR), erityisesti kansainvälisiä siirtoja koskeva V luku.
- EUT C-311/18 ("Schrems II"), 16. heinäkuuta 2020.
- EDPB – Suositukset 01/2020 siirtovälineitä täydentävistä toimenpiteistä.
- Tietosuojavaltuutetun toimisto – Vuosikertomukset, joissa on tapauksia pikaviestinnän väärinkäytöstä johtuvista sanktioista ammatillisissa ympäristöissä.

← EdellinenAmmattisalaisuus digitaalisella aikakaudellaSeuraava →Kun välissä ei ole ketään

Viimeaikaiset lukemiset

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Ota tämä artikkeli mukaasi minne tarvitset.

↓ Markdown ↓ Pelkkä teksti ↓ PDF

Tiedosto ladataan laitteellesi. Voit tallentaa sen, tuoda sen Solo2-sovellukseen tai jakaa sen haluamallasi tavalla. Cuadernos ei päätä tiedoston kohtaloa puolestasi.

Sinetti · SHA-256 ab4bbfb98c521671571b249e27f4af84b71c32d51fa8557d32bd7973d11caca3

Cuadernos Lacre · Menzuri Gestión S.L. -julkaisu ·
kirjoittanut R.Eugenio · toimittanut Solo2-tiimi.