GDPR in profesionalno sporočanje: zakaj večina krši pravila, ne da bi se tega zavedala

Skoraj vsaka pisarna, ordinacija ali svetovalno podjetje pošilja dokumente strank prek aplikacij, katerih strežnik se nahaja zunaj Evropskega gospodarskega prostora. Brez slabega namena, a v mnogih primerih v kršitvi uredbe, ne da bi jih kdo na to opozoril.

Dokument, ki potuje dlje, kot si mislite

Vsakodnevna situacija: davčna svetovalka prek sporočanja prejme dokument s podatki stranke. Prodajnik prek klepeta posreduje ponudbo kolegu. Zdravnica na isti način deli klinično poročilo s kolegico. Nihče ne pomisli dvakrat. To je normalno. To je priročno. To se počne vsak dan v vsaki pisarni v vsakem mestu v Evropi.

Toda ta dokument je v mnogih primerih pravkar odpotoval na strežnik v Združene države. Bil je shranjen – čeprav začasno, čeprav "šifrirano v mirovanju" – v oblaku, ki ga ne nadzoruje niti strokovnjak niti njegova stranka. Prešel je sisteme, ki lahko tehnično indeksirajo metapodatke, povezane z vsebino. In evropska splošna uredba o varstvu podatkov ima o tem povedati nekaj precej jasnega.

Kaj zahteva norma

GDPR – in posledično sodna praksa Sodišča Evropske unije (zlasti sodba Schrems II, C-311/18, iz leta 2020) – določa, da morajo biti osebni podatki evropskih državljanov ustrezno zaščiteni. Če ti podatki zapustijo Evropski gospodarski prostor, mora upravljavec zagotoviti, da prejemnik ponuja raven varstva, ki je "v bistvu enakovredna" evropski. V praksi to pomeni, že pošiljanje podatkov strank prek storitev, katerih strežniki so pod jurisdikcijo ZDA, brez opravljene ocene učinka in izvedenih dopolnilnih zaščitnih ukrepov – standardnih pogodbenih klavzul, dodatnih tehničnih ukrepov, kot je preverljivo šifriranje itd. – lahko pomeni kršitev uredbe. Tudi če do zdaj nihče ni rekel ničesar.

In ne gre le za vsebino sporočil. Metapodatki – kdo pošilja kaj komu, kdaj, kako pogosto, od kod – so po predpisih in po večkratni interpretaciji Evropskega odbora za varstvo podatkov prav tako osebni podatki. Storitev, ki zbira metapodatke iz poklicne komunikacije uporabnika, obdeluje osebne podatke strank tega uporabnika, ne da bi te o tem vedele ali dale kakršno koli privolitev za takšno obdelavo.

Splošna miselna shema – "aplikacijo uporabljam le za pisanje; aplikacija ni ponudnik podatkov moje stranke" – je pravno napačna. Če podatki stranke gredo skozi infrastrukturo tretje osebe, ta tretja oseba obdeluje te podatke. In če jih obdeluje, mora obstajati pravna podlaga, pogodba o obdelavi podatkov in ustrezna jamstva.

Kdo je odgovoren

Vprašanje, kdo nosi pravno odgovornost, ni akademsko. GDPR razlikuje med *upravljavcem* (tistim, ki odloča, kateri podatki se obdelujejo in za kakšen namen) in *obdelovalcem* (tistim, ki to počne materialno v imenu upravljavca). Strokovnjak, ki pošilja dokumente strank, je upravljavec. Ponudnik aplikacije za sporočanje je v

mnogih primerih dejansko obdelovalec. Brez pogodbe o obdelavi – in brez večine klavzul, ki bi jih taka pogodba morala vsebovati – upravljavec ni izpolnil svoje obveznosti.

Blaga interpretacija je: "večina strokovnjakov tega ne ve". Stroga interpretacija je: "nepoznavanje prava ne opravičuje kršitve". In interpretacija katerega koli specializiranega odvetnika za varstvo podatkov, ki je zaprošen za mnenje o tem, je običajno stroga.

Za koga je to konkretno pomembno

Za vsakega strokovnjaka ali podjetje, ki čeprav le občasno operira z osebnimi podatki tretjih oseb:

- Odvetniki, ki prejemajo dokumentacijo strank (pogodbe, tožbe, izjave, poročila o premoženju).
- Zdravniki in drugi zdravstveni delavci, ki delijo zdravstvene podatke – ki po 9. členu GDPR veljajo za *posebne vrste podatkov* s strožjim režimom varstva –.
- Davčni svetovalci in upravni managerji, ki operirajo z identifikacijskimi, davčnimi in bančnimi podatki.
- Oddelki za človeške vire, ki upravljajo z delovno in osebno dokumentacijo zaposlenih.
- Tržniki, ki prejemajo kontaktne podatke in pogosto občutljive poslovne informacije od potencialnih in obstoječih strank.

V vseh primerih so informacije zaščitene z GDPR. V vseh primerih v običajni praksi te informacije tečejo prek kanalov, katerih jurisdikcija ne dovoljuje njihove razglasitve za "v bistvu enakovredne" evropskemu okviru brez dodatnih jamstev. Ne zaradi slabega namena. Iz navade. In zaradi tehnološke infrastrukture, ki je petnajst let dajala prednost priročnosti pred skladnostjo.

Argument "vsi to počnejo"

Pametno je predvideti najpogostejši ugovor: "če vsi to počnejo, to ne more biti resnična težava". To je popolnoma razumljiv argument in pravno nima nobene teže. Dejstvo, da je neka praksa razširjena, je ne naredi skladne z uredbo. Nadzorni organi za varstvo podatkov so v zadnjih letih sankcionirali več podjetij prav zaradi načinov uporabe sporočanja, ki so se do trenutka revizije zdeli neškodljivi.

Trenutna operativna realnost je, da je tveganje glede verjetnosti nizko – zelo redko se zgodi, da revizija nadzornega organa revidira specifična orodja za sporočanje srednje velike pisarne – a visoko glede učinka, če se uresniči. To je tveganje, ki ga večina sprejme, ne da bi vedela, da ga sprejme. Se pravi, ne da bi ocenili, ali je uporabljeno orodje v skladu s pravno odgovornostjo upravljavca.

Digitalna sled je retroaktivna

Obstaja drugi argument, skoraj simetričen prejšnjemu, ki ga je vredno predvideti: *"če bi bila to resna težava, bi uprava to že začela nadzorovati"*. Trenutna opažena realnost mu daje površno prav. Nadzora zaradi neustrezne uporabe sporočanja v majhnih podjetjih in predvsem pri samostojnih podjetnikih danes skorajda ni – ne zato, ker bi bilo vedenje dovoljeno, temveč zato, ker upravi v večjem delu EU primanjkuje človeških virov, potrebnih za revizijo milijonov zavezancev.

To nakazuje današnja opažena praksa. Ni pa to, kar nakazuje naslednje desetletje. Dva vektorja se stekata, da bi spremenila ravnovesje v razmeroma kratkih rokih.

Prvič: digitalna sled je retroaktivna. Vsako sporočilo, poslano prek aplikacije s centralnim strežnikom, ostane registrirano – vsaj v metapodatkih – v infrastrukturi, ki traja. Kar je bilo poslano pred šestimi meseci, je tehnično še vedno mogoče revidirati danes. Kar bo poslano danes, bo mogoče revidirati čez pet let. Odsotnost trenutnega nadzora ni jamstvo za odsotnost prihodnjega nadzora. Gre za odlog presoje, ne za oprostitev.

Drugič: zmogljivost upravne revizije bo rasla pospešeno. Uvedba orodij umetne inteligence v nadzorne procese odpravlja človeško ozko grlo, ki je do zdaj – dejansko, ne pravno – ščitilo majhna podjetja in samostojne podjetnike. Sistem, sposoben navzkrižnega preverjanja masovnih metapodatkov, davčnih napovedi, trgovinskih registrov in obveznosti obveščanja o kršitvah varnosti, ne potrebuje inšpektorjev: potrebuje dostop. Dostop pa je prek zahtev ponudnikom s pravno prisotnostjo v EU v okviru sedanjega normativnega okvira popolnoma izvedljiv.

K temu se doda manj tehničen, a enako odločilen dejavnik: evropske države so v procesu nenehno rastočega zadolževanja in morajo, skoraj brez izjeme, razširiti svojo davčno osnovo. Upravna sankcija, ki izhaja iz neskladnosti z GDPR, je v čisto fiskalnih terminih rastoč in politično udoben vir prihodkov. To ni domneva: je opazen trend v letnih poročilih evropskih nadzornih organov za varstvo podatkov, kjer skupni obseg sankcij narašča že več zaporednih proračunskih let.

Operativni zaključek za upravljavca ni alarmanten, temveč trezen: **odločitev o tem, kako se danes upravlja komunikacija s strankami, se presoja glede na zmogljivost nadzora v letu, ko nadzor pride, ne pa glede na trenutno.** In ta zmogljivost bo v razumnem roku bistveno drugačna kot danes. Kdor danes začne delati stvari prav, ne bo v redu le od danes: sled, ki se ustvari od tega trenutka naprej, bo skladna s predpisi, kar retroaktivno ščiti prihajajoči odsek poti. Kdor bo nadaljeval kot doslej, bo kopičil revizijsko sled, katere skladnost se bo ocenjevala po standardih – in virih – prihodnjih let.

Kaj se spremeni z drugačno arhitekturo

Obstajajo tehnične alternative, pri katerih se podatki ne shranjujejo v infrastrukturi tretjih oseb, temveč potujejo neposredno z naprave pošiljatelja na napravo prejemnika. V tej arhitekturi skladnost z GDPR glede mednarodnih prenosov ni odvisna od standardnih pogodbenih klavzul, niti od dobre volje ponudnika niti od prihodnjih revizij. Odvisna je od tega, da *prenosa ni*. In tistega, kar ne obstaja, ni mogoče prekršiti.

To ni izključna rešitev niti edina možna. Je pa strukturno drugačna in skladnost s predpisi neha biti postopkovni dodatek, temveč postane neposredna posledica zasnove. Za strokovnjaka, ki svojo odgovornost kot upravljavec jemlje resno, ta razlika pomeni razliko.

Naslednja številka Cuadernos bo podrobno analizirala sodbo Schrems II in njene praktične posledice za mala in srednja podjetja, odvisna od ameriških storitev v oblaku, pet let po njeni objavi.

Viri in pravni okvir

- Uredba (EU) 2016/679 (GDPR), zlasti poglavje V o mednarodnih prenosih.
- SEU C-311/18 ("Schrems II"), 16. julij 2020.
- EDPB – Priporočila 01/2020 o ukrepih, ki dopolnjujejo orodja za prenos.
- Informacijski pooblaščenec (in drugi nadzorni organi) – Letna poročila s primeri sankcij zaradi neustrezne uporabe trenutnega sporočanja v poklicnem okolju.

← PrejšnjiPoklicna skrivnost v digitalni dobiNaslednji →Ko vmes ni nikogar

Zadnja branja

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vzemite ta članek s seboj, kamor koli ga potrebujete.

↓ Markdown ↓ Navadno besedilo ↓ PDF

Datoteka bo prenesena v vašo napravo. Od tam jo lahko shranite, uvozite v Solo2 ali delite, kjer koli želite. Cuadernos ne odloča o cilju namesto vas.

Voščeni pečat · SHA-256 5df2c5901d6b0d585f77a8965e86c78f4b98fa562c3064d5496caf07234b7cb8

Cuadernos Lacre · Publikacija podjetja Menzuri Gestión S.L. ·
napisal R.Eugenio · uredila ekipa Solo2.