Reflexió · 2026. május 16.

← Előző·Következő →

A szakmai titoktartás a digitális korban

Ha a szakember és ügyfele közötti kommunikáció technikailag alkalmatlan csatornán zajlik, a titok nem a szivárgás napján törik meg. Már sokkal korábban, az eszköz kiválasztásának pillanatában megtört.

Egy probléma, amelyet szinte senki sem lát

Egy ügyvéd bizalmas dokumentumot kap az ügyfelétől a telefonjára. Egy orvos kényes diagnózist beszél meg egy kollégájával. Egy pszichológus pszichiáterrel egyezteti egy páciens kezelését. Egy adótanácsadó felülvizsgálatra váró bevallás adatait küldi el. Mindannyian azonnali üzenetküldőn keresztül teszik ezt. És szinte senki sem áll meg elgondolkodni azon, hogy ezek az üzenetek valójában hol kötnek ki.

A válasz a legtöbb esetben ugyanaz: egy olyan szerveren, amelyet a szakember nem ellenőriz, egy olyan országban, amelynek jogszabályait nem feltétlenül ismeri, egy olyan vállalat kezelésében, amelynek üzleti modellje – közvetlen gazdasági értelemben – az adatok felhalmozása. Az üzenet lehet titkosítva a továbbítás során. De amint eléri a szervert, az egy harmadik fél infrastruktúrájában tárolt másolat, amely e harmadik fél operatív, jogi és kereskedelmi döntéseinek van kitéve. Nem a szakemberének.

Amit a jogszabályok mondanak

Az európai általános adatvédelmi rendelet egyértelmű a 32. cikkében: bárki, aki személyes adatokat kezel, köteles „megfelelő” technikai és szervezési intézkedéseket végrehajtani a kockázat mértékének megfelelő szintű biztonság garantálása érdekében. Az intézkedések megfelelőségét nem az alapján mérik, hogy „mit állít az alkalmazás magáról”, hanem a tényleges kockázat alapján. Ha az ügyfél adatai olyan szerveren kötnek ki, amelynek joghatósága nem garantál az Európai Gazdasági Térséggel egyenértékű védelmi szintet, az adatkezelő – azaz a szakember – olyan kockázatot vállal, amelynek valószínűleg nincs teljes mértékben tudatában.

És ez nem csak a GDPR. Az ügyvédekre, orvosokra, pszichológusokra, könyvvizsgálókra, újságírókra és másokra vonatkozó szakmai titoktartási szabályok megkövetelik, hogy az ügyféllel folytatott kommunikáció bizalmas legyen. Nem „lehetőleg bizalmas”. Feltétel nélkül bizalmas. Ha az alkalmazott technikai csatorna ezt nem tudja garantálni, a szakember olyan kockázatot vállal, amelyet hivatása etikája nem tesz lehetővé.

A paradoxon az, hogy a kockázat láthatatlan. Senki nem auditálja az irodai üzenetküldést. Senki nem kéri el a chat-szolgáltatótól az adatfeldolgozási szerződést. A kockázat csak akkor derül ki, amikor már késő: egy szivárgás, egy nyilvánosságra került feltörés, vagy egy másik kontinensen végrehajtott bírósági végzés, amelyről a felhasználót nem is értesítik.

Mire van szüksége technikailag egy szakembernek

Amire egy titoktartásra kötelezett személynek szüksége van, az a követelmények szempontjából valójában meglepően egyszerű:

- Egy csatorna, ahol az üzenetek közvetlenül a küldő eszközéről a fogadó eszközére kerülnek, anélkül, hogy áthaladnának egy másolatokat tároló közvetítő szerveren.
- Egy olyan infrastruktúra, amelynek joghatósága és szabályozása tervezésénél fogva összhangban van a GDPR-ral, nem pedig nyilatkozatok alapján.
- Egy mód a beszélgetőpartnerrel való azonosításra anélkül, hogy a szakmai kapcsolatokat (ügyfélnevek, telefonszámok, névjegyzék) át kellene adni egy harmadik félnek.
- Egy ellenőrizhető rendszer – nem a szolgáltató szavára alapozva –, amellyel megerősíthető, hogy az üzenet a megfelelő személyhez érkezett meg.

Ez nem egy igényes lista. Tulajdonképpen ez az, amit a digitális kor előtti szakmai kommunikációban magától értetődőnek vettek. Egy ajánlott levél minden ilyen kritériumnak megfelelt. Egy telefonhívás az iroda központjából az ügyfél központjába szintén. Nem az a furcsa, hogy ma is elvárjuk ezeket a garanciákat: az a furcsa, hogy a digitális csatornára való áttéréskor ezek elvesztek anélkül, hogy bárki észrevette volna.

Különbség a titkosítás és a nem-tárolás között

Van egy hasznos metafora. Egy üzenet titkosítása és szerveren való tárolása megfelel annak, mintha egy dokumentumot széfbe tennénk, és a széfet egy ismeretlen házában hagynánk. A széf jó. A dokumentum elvileg nem olvasható. De a dokumentum *továbbra is valaki más házában van*. És ez a valaki kaphat bírósági végzést, érheti kibertámadás, megváltoztathatja a szolgáltatási feltételeit, megveheti egy másik, más etikájú cég, vagy holnap megszűnhet.

A strukturális alternatíva – nem eljárási, nem bizalmi alapon – az, hogy a dokumentum soha nem hagyja el az irodát. Hogy közvetlenül a szakember asztaláról az ügyfél asztalára utazik, bármiféle közvetítő nélkül. Ez az, amit az eszközök közötti pont-pont kommunikáció technikailag tesz: kiiktatja a közvetítőt. Nem mintha a közvetítő gonosz lenne. Csak arról van szó, hogy a szakmai titoktartás esetében a közvetítő *felesleges*. És ami felesleges, azt minden biztonságra törekvő rendszerben elvi alapon el kell távolítani.

A felelősség kérdése

Végső soron az a kérdés, amelyre minden titoktartásra kötelezett szakembernek határozott igennel kellene tudnia válaszolnia, a következő:

> Ha holnap kiszivárogna egy beszélgetés az egyik ügyfelemmel, és egy bíróság vagy szakmai kamara megkérdezné, hogyan kezelem a bizalmasságot, tudom-e technikailag bizonyítani, hogy az általam használt csatorna nem tárol másolatokat harmadik felek infrastruktúrájában? Tudom-e bizonyítani, hogy az adatok soha nem hagyták el a beszélgetésben részt vevő két személy eszközeit? Tudom-e bizonyítani, egy másik kontinensről származó cég szavára való hagyatkozás nélkül, hogy a bizalmasságot az architektúra garantálta, nem pedig egy ígéret?

Ha a válasz nem, a probléma nem a konkrét eszközben van. A probléma az, hogy az eszközre olyan felelősséget ruháztak, amelynek támogatására az eszközt nem tervezték. Olyan ez, mintha bizalmas iratokat tennénk egy átlátszó borítékba, és bíznánk abban, hogy a postás nem néz bele.

Az az eszköz, amelyet egy szakember az ügyfeleivel való kommunikációra választ, sokat elárul arról, hogyan becsüli meg a bizalmukat. Vannak eszközök, amelyeket úgy terveztek, hogy ez a bizalom ne ígéretektől, hanem az architektúrától függjön. És vannak eszközök, amelyek nem ilyenek. A különbség ismerete a munka része.

Hivatkozott jogi keret

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR), különösen az 5., 25. (beépített adatvédelem) és 32. cikke (az adatkezelés biztonsága).

- Magyarországi jogszabályok a szakmai titoktartásról (pl. 2017. évi LXXVIII. törvény az ügyvédi tevékenységről, 1997. évi CLIV. törvény az egészségügyről).
- 2012. évi C. törvény a Büntető Törvénykönyvről, 223. § (Titoktartási kötelezettség megszegése).
- Az ügyvédi hivatás etikai szabályai a titoktartásra és a hivatási titokra vonatkozóan.

← ElőzőA titkosítás nem azonos a magánélettel: mit árulnak el Önről a metaadatokKövetkező →A GDPR és a professzionális üzenetküldés: miért sértik meg a legtöbben tudtukon kívül a szabályokat

Legutóbbi olvasmányok

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vigye magával ezt a cikket, ahová csak szüksége van rá.

↓ Markdown ↓ Egyszerű szöveg ↓ PDF

A fájl letöltődik az Ön eszközére. Onnan elmentheti, importálhatja a Solo2-be, vagy megoszthatja bárhol. A Cuadernos nem dönt Ön helyett a fájl sorsáról.

Viaszpecsét · SHA-256 381fc50975c4a9d183d205bb73fe8f7e38cd25bfac653cf3db8d69ccd54546e0

Cuadernos Lacre · A Menzuri Gestión S.L. kiadványa ·
írta R.Eugenio · szerkesztette a Solo2 csapata.