Elemzés · 2026. május 16.

← Előző·Következő →

A GDPR és a professzionális üzenetküldés: miért sértik meg a legtöbben tudtukon kívül a szabályokat

Szinte minden iroda, rendelő vagy tanácsadó cég küld ügyfél-dokumentumokat olyan alkalmazásokon keresztül, amelyek szervere az Európai Gazdasági Térségen kívül található. Rossz szándék nélkül, de sok esetben a rendeletet megsértve, anélkül, hogy bárki figyelmeztette volna őket.

A dokumentum, amely messzebbre utazik, mint gondolná

Egy mindennapi helyzet: egy adótanácsadó üzenetküldőn kap egy ügyféladatokat tartalmazó dokumentumot. Egy üzletkötő chaten továbbít egy ajánlatot egy kollégájának. Egy orvos ugyanezen az úton oszt meg klinikai jelentést egy munkatársával. Senki nem gondol bele kétszer. Ez a normális. Ez kényelmes. Ezt teszik minden nap minden irodában Európa minden városában.

De ez a dokumentum sok esetben éppen most utazott el egy szerverre az Egyesült Államokba. Tárolták – ha csak ideiglenesen is, ha „titkosítva” is –, egy olyan felhőben, amelyet sem a szakember, sem az ügyfele nem ellenőriz. Olyan rendszereken haladt keresztül, amelyek technikailag képesek indexelni a tartalomhoz kapcsolódó metaadatokat. Az európai általános adatvédelmi rendeletnek pedig erről meglehetősen egyértelmű mondanivalója van.

Amit a norma megkövetel

A GDPR – és következésképpen az Európai Unió Bíróságának joggyakorlata (különösen a 2020-as Schrems II ítélet, C-311/18) – megállapítja, hogy az európai polgárok személyes adatait megfelelően védeni kell. Ha ezek az adatok elhagyják az Európai Gazdasági Térséget, az adatkezelőnek garantálnia kell, hogy a címzett az európaival „lényegileg egyenértékű” védelmi szintet kínál. A gyakorlatban ez azt jelenti, hogy az ügyféladatok küldése olyan szolgáltatásokon keresztül, amelyek szerverei amerikai joghatóság alá tartoznak, hatásvizsgálat elvégzése és kiegészítő garanciák – általános szerződési feltételek, további technikai intézkedések, például ellenőrizhető titkosítás stb. – bevezetése nélkül a rendelet megsértését jelentheti. Még akkor is, ha eddig senki nem szólt érte.

És nem csak az üzenetek tartalmáról van szó. A metaadatok – ki mit küld kinek, mikor, milyen gyakran, honnan – az előírások szerint, az Európai Adatvédelmi Testület ismételt értelmezése szerint szintén személyes adatok. Egy olyan szolgáltatás, amely metaadatokat gyűjt egy felhasználó szakmai kommunikációjáról, a felhasználó ügyfeleinek személyes adatait kezeli anélkül, hogy azoknak tudomása lenne erről, vagy bármilyen hozzájárulást adtak volna az ilyen adatkezeléshez.

A bevett gondolati séma – „csak írásra használom az alkalmazást; az alkalmazás nem az ügyfelem adatszolgáltatója” – jogilag téves. Ha az ügyfél adatai áthaladnak egy harmadik fél infrastruktúráján, az a harmadik fél kezeli ezeket az adatokat. Ha pedig kezeli őket, akkor kell lennie jogalapnak, adatfeldolgozási szerződésnek és megfelelő garanciáknak.

Ki a felelős

Az a kérdés, hogy ki viseli a jogi felelősséget, nem akadémiai. A GDPR megkülönbözteti az *adatkezelőt* (aki eldönti, hogy milyen adatokat milyen célból kezelnek) és az *adatfeldolgozót* (aki ezt ténylegesen az adatkezelő nevében teszi). Az ügyfél-dokumentumokat küldő szakember az adatkezelő. Az üzenetküldő alkalmazás szolgáltatója sok esetben tényleges adatfeldolgozó. Adatfeldolgozási szerződés nélkül – és a legtöbb olyan kikötés nélkül, amelyet egy ilyen szerződésnek tartalmaznia kellene – az adatkezelő nem teljesítette kötelezettségét.

A megengedő értelmezés szerint: „a legtöbb szakember ezt nem tudja”. A szigorú értelmezés szerint: „a törvény nem ismerete nem mentesít a felelősség alól”. És minden, a témában konzultált adatvédelmi szakjogász értelmezése általában a szigorú.

Kinek fontos ez konkrétan

Minden olyan szakembernek vagy vállalatnak, amely akár csak alkalmanként harmadik felek személyes adataival dolgozik:

- Ügyvédek, akik ügyfél-dokumentációt kapnak (szerződések, keresetek, nyilatkozatok, vagyonnyilatkozatok).
- Orvosok és más egészségügyi szakemberek, akik egészségügyi adatokat osztanak meg – amelyek a GDPR 9. cikke szerint *különleges kategóriának* minősülnek, fokozott védelmi rendszerrel –.
- Adótanácsadók és közigazgatási ügyintézők, akik azonosító, adó- és banki adatokkal dolgoznak.
- HR osztályok, amelyek munkavállalói és személyügyi dokumentációt kezelnek.
- Értékesítők, akik elérhetőségi adatokat és gyakran kényes üzleti információkat kapnak leendő és meglévő ügyfelektől.

Minden esetben az információkat a GDPR védi. Minden esetben a bevett gyakorlatban ezek az információk olyan csatornákon áramlanak, amelyek joghatósága nem teszi lehetővé, hogy kiegészítő garanciák nélkül az európai kerettel „lényegileg egyenértékűnek” nyilvánítsák őket. Nem rossz szándékból. Megszokásból. És egy olyan technológiai infrastruktúra miatt, amely tizenöt éven át a kényelmet a megfelelőség elé helyezte.

A „mindenki így csinálja” érv

Érdemes megelőzni a leggyakoribb kifogást: „ha mindenki így csinálja, az nem lehet valódi probléma”. Ez egy teljesen érthető érv, de jogilag semmi ereje nincs. Az a tény, hogy egy gyakorlat elterjedt, nem teszi azt a rendelettel összhangban lévővé. Az adatvédelmi hatóságok (Magyarországon a NAIH) az elmúlt években több vállalatot is szankcionáltak pontosan olyan üzenetküldési módok miatt, amelyek az ellenőrzés pillanatáig ártalmatlannak tűntek.

A jelenlegi operatív valóság az, hogy a kockázat valószínűsége alacsony – nagyon ritka, hogy egy hatósági ellenőrzés egy közepes méretű iroda konkrét üzenetküldő eszközeit auditálja –, de a hatása nagy, ha bekövetkezik. Ez egy olyan kockázat, amelyet a legtöbben anélkül vállalnak, hogy tudnának róla. Vagyis anélkül, hogy értékelték volna, hogy az alkalmazott eszköz összhangban van-e az adatkezelő jogi felelősségével.

A digitális lábnyom visszamenőleges

Van egy második, az előzővel szinte ellentétes érv, amelyet érdemes megelőzni: *„ha ez komoly probléma lenne, a közigazgatás már elkezdte volna ellenőrizni”*. A jelenlegi tapasztalt valóság felületesen neki ad igazat. A kisvállalkozásoknál és főként az egyéni vállalkozóknál az üzenetküldés nem megfelelő használata miatti ellenőrzések ma szinte nem léteznek – nem azért, mert a magatartás megengedett lenne, hanem azért, mert a közigazgatásból Magyarországon és az EU nagy részén hiányoznak a több millió kötelezett auditálásához szükséges emberi erőforrások.

Ezt sugallja a ma tapasztalt gyakorlat. De nem ezt sugallja a következő évtized. Két vektor fut össze, hogy relatíve rövid időn belül megváltoztassa az egyensúlyt.

Először is: a digitális lábnyom visszamenőleges. Minden üzenet, amelyet központi szerverrel rendelkező alkalmazáson keresztül küldenek el, regisztrálva marad – legalábbis a metaadatokban – egy fennmaradó infrastruktúrában. Amit hat hónappal ezelőtt küldtek, az technikailag ma is auditálható. Amit ma küldenek, az öt év múlva is auditálható lesz. A jelenlegi ellenőrzés hiánya nem garancia a jövőbeli ellenőrzés hiányára. Ez az értékelés elhalasztása, nem pedig mentesség alóla.

Másodszor: a közigazgatási ellenőrzési kapacitás gyorsulva fog nőni. A mesterséges intelligencia eszközeinek bevezetése az ellenőrzési folyamatokba megszünteti azt az emberi szűk keresztmetszetet, amely eddig – ténylegesen, nem jogilag – védte a kisvállalkozásokat és az egyéni vállalkozókat. Egy olyan rendszernek, amely képes keresztbevetni hatalmas metaadat-állományokat, adóbevallásokat, cégnyilvántartásokat és az adatvédelmi incidensek bejelentési kötelezettségeit, nincs szüksége ellenőrökre: hozzáférésre van szüksége. A hozzáférés pedig az EU-ban jogi jelenléttel rendelkező szolgáltatók felé intézett megkereséseken keresztül a jelenlegi normatív keretek között teljesen megvalósítható.

Ehhez járul egy kevésbé technikai, de ugyanolyan meghatározó tényező: az európai államok a folyamatosan növekvő eladósodás folyamatában vannak, és szinte kivétel nélkül bővíteniük kell az adóalapjukat. A GDPR nemteljesítéséből eredő közigazgatási szankció tisztán fiskális értelemben növekvő és politikailag kényelmes bevételi forrás. Ez nem feltételezés: ez egy megfigyelhető trend az európai adatvédelmi hatóságok éves jelentéseiben, ahol a szankciók összvolumene több egymást követő pénzügyi év óta emelkedik.

Az operatív következtetés az adatkezelő számára nem riogató, hanem kijózanító: **az ügyfelekkel folytatott kommunikáció mai kezeléséről szóló döntést az ellenőrzés évének ellenőrzési kapacitása alapján ítélik meg, nem a jelenlegi alapján.** Ez a kapacitás pedig belátható időn belül lényegesen más lesz, mint a mai. Aki ma elkezdi jól csinálni a dolgokat, az nemcsak mától lesz rendben: az ettől a pillanattól generált lábnyom összhangban lesz a normával, és ez visszamenőlegesen védi az elkövetkező időszakot. Aki úgy folytatja, mint eddig, az egy olyan auditálható lábnyomot halmoz fel, amelynek megfelelőségét a jövő éveinek standardjai – és erőforrásai – alapján fogják megítélni.

Mi változik egy másfajta architektúrával

Léteznek olyan technikai alternatívák, ahol az adatok nem harmadik felek infrastruktúrájában tárolódnak, hanem közvetlenül a küldő eszközéről a fogadó eszközére utaznak. Ebben az architektúrában a GDPR nemzetközi adattovábbításra vonatkozó szabályainak betartása nem az általános szerződési feltételektől, nem a szolgáltató jóindulatától és nem a jövőbeli auditoktól függ. Attól függ, hogy *nincs adattovábbítás*. Amit pedig nem létezik, azt nem lehet megsérteni.

Ez nem az egyetlen megoldás, és nem is az egyetlen lehetséges. De strukturálisan más, és a megfelelőség megszűnik eljárási függeléknek lenni, és a tervezés közvetlen következményévé válik. Egy olyan szakember számára, aki komolyan veszi adatkezelői felelősségét, ez a különbség sokat számít.

A Cuadernos következő száma részletesen elemzi a Schrems II ítéletet és annak gyakorlati következményeit az amerikai felhőszolgáltatásoktól függő kis- és középvállalkozások számára, öt évvel a közzététele után.

Források és jogi keret

- Az EU 2016/679 rendelete (GDPR), különösen a nemzetközi adattovábbításról szóló V. fejezet.
- EUB C-311/18 ítélet („Schrems II”), 2020. július 16.
- EDPB – 01/2020. számú ajánlás az adattovábbítási eszközöket kiegészítő intézkedésekről.
- NAIH (és más felügyeleti hatóságok) – Éves jelentések az üzenetküldés szakmai környezetben történő nem megfelelő használatáért kiszabott szankciók eseteivel.

← ElőzőA szakmai titoktartás a digitális korbanKövetkező →Amikor nincs senki középen

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 cc142356f23a985592e8e4409e173755075f1a9b14921f5865cfe5e8f85cb26f

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