Elemzés · 2026. május 18.

← Előző·Következő →

Schrems II, öt évvel később

Az ítélet, amely megváltoztatta a személyes adatok nemzetközi továbbításának jogát. Öt évvel később az európai irodai mindennapok jelentős része úgy zajlik tovább, mintha mi sem történt volna.

Az ítélet, amelynek három óra kellett a szabályok megváltoztatásához

2020. július 16-án, luxemburgi idő szerint délelőtt negyed tizenegy körül az Európai Unió Bírósága (TJUE) közzétette a C-311/18. sz. ügyben hozott ítéletét. A következő három órában megszűnt az a jogi rendszer, amely az Európából az Egyesült Államokba irányuló napi személyesadat-továbbítást támogatta — az úgynevezett Adatvédelmi Pajzs (hivatalos nevén Privacy Shield). Mire az európai adatvédelmi tisztviselők befejezték aznapi ebédjüket, az a keret, amelyben vállalataik és közigazgatási szerveik működtek, már nem volt érvényes.

Az ítélet ma Schrems II néven ismert, Maximilian Schrems osztrák aktivista után, akinek a Facebook Ireland elleni panasza kiváltotta azt. A panasz konkrétan a Facebook Írország és a Facebook Egyesült Államok közötti adattovábbításokkal foglalkozott. Az ítélet általánosságban sokkal messzebbre megy: rögzíti, hogyan és milyen feltételekkel továbbítható az Egyesült Államokba bármely európai területen gyűjtött személyes adat.

Közel hat évvel később létezik a helyettesítő keret — a 2023 júliusában elfogadott EU-US Data Privacy Framework —, és ez is jogi nyomás alatt áll. Újabb Schrems-forduló készül. Eközben a kis- és középvállalkozások továbbra is amerikai felhőszolgáltatásokat használnak a mindennapi feladatokhoz, legtöbbjük anélkül, hogy tudná, hogy az a jogi kérdés, amelyen ezek a szolgáltatások nyugszanak, továbbra is nyitott.

Mit mondott pontosan a Schrems II

Az ítélet három darabra támaszkodik. Az első az Európai Unió Alapjogi Chartája, különösen annak artículo 7 (magán- és családi élet), 8 (személyes adatok védelme) és 47 (hatékony jogorvoslathoz való jog) cikke. A második az általános adatvédelmi rendelet — az RGPD, amelyre sok európai csak a süti-értesítések miatt emlékszik —, konkrétan annak V. fejezete, a nemzetközi adattovábbításról szóló artículo 44–50 cikkek. A harmadik az amerikai hírszerzési jogszabályok: a Foreign Intelligence Surveillance Act 702. szakasza, a jogi szakzsargonban FISA 702, valamint az 12333. sz. elnöki rendelet.

A bíróság az összehasonlítás módszerével járt el. Az Alapjogi Charta megköveteli, hogy az európai polgárok személyes adatai az Unió elhagyásakor lényegileg az RGPD által garantált védelemmel egyenértékű szintet élvezzenek. A kérdés következésképpen az volt, hogy az Egyesült Államok kínálja-e ezt a lényegileg egyenértékű szintet.

A válasz nemleges volt, és nem árnyalatnyi különbségek miatt. A FISA 702 lehetővé teszi az amerikai kormány számára, hogy előzetes egyedi bírói engedély nélkül, az érintett értesítése nélkül és az európaihoz hasonló hatékony jogorvoslat nélkül gyűjtse a nemzeti területen kívül tartózkodó nem amerikaiak kommunikációját. Az 12333. sz. elnöki rendelet analóg módon kiterjeszti ezt a képességet a nemzeti területen kívülre. A bíróság megállapította, hogy az európai polgár az amerikai jogrendszerrel szemben nem rendelkezik a Charta által megkövetelt lényegileg egyenértékű védelemmel. Az egyenértékűség tehát nem áll fenn.

Ebből következik a közvetlen következmény: az Európai Bizottság 2016/1250 határozatát, amely a Privacy Shield-et az adattovábbítás megfelelő kereteként ismerte el, érvénytelennek nyilvánították. Minden, kizárólag ezen a kereten alapuló adattovábbítás ugyanabban a pillanatban jogalap nélkül maradt.

Ami túlélte (és milyen feltételekkel)

A Schrems II nem szüntette meg az összes eszközt. Az általános szerződési feltételek — a nemzetközi szakzsargonban SCC-k — túléltek. Ezek az Európai Bizottság által jóváhagyott mintaszerződések: egy európai exportőr és a célország egy importőre aláírja őket, kötelezettséget vállalva az adatok európai szabvány szerinti kezelésére. Az a vállalat, amely azt hitte, hogy 2020. július 17-én megoldotta a problémát, SCC-t írt alá szolgáltatójával, és elégedett volt.

A kényelmetlenség az ítélet lassú elolvasásakor jelentkezett. A bíróság világossá tette, hogy az SCC-k továbbra is érvényesek, de érvényességük egy hangsúlyozandó feltételtől függ: attól, hogy az adatimportőr a gyakorlatban be tudja-e tartani azokat. Ha a célország nemzeti jogszabályai megakadályozzák a kikötések betartását — mert például egy FISA 702 szerinti végzés arra kötelezi, hogy az adatok átadásáról ne értesítse európai partnerét —, akkor a kikötések valójában nem védenek. És ekkor, mondja a bíróság, az európai exportőrnek fel kell függesztenie az adattovábbítást.

Ez egy új fogalmat vezetett be az európai adatvédelmi gyakorlatba: a továbbítási hatásvizsgálatot (Transfer Impact Assessment), amelyet angol betűszóval TIA-ként ismernek. Minden alkalommal, amikor egy európai vállalat SCC-k védelme alatt akar adatokat továbbítani az Egyesült Államokba, formálisan értékelnie kell, hogy a címzett be tudja-e tartani a kikötéseket a rá vonatkozó jogszabályok fényében. Az Európai Adatvédelmi Testület (EDPB) részletes iránymutatást adott ki a TIA lefolytatásáról. Az őszinte gyakorlat általában ugyanarra az eredményre vezet: ha az importőr egy felhőalapú óriásvállalat amerikai leányvállalata, a TIA-ra adott őszinte válasz az, hogy a kikötések nem tarthatók be úgy, ahogy le vannak írva.

A Privacy Framework és a függőben lévő Schrems III

2023. július 10-én az Európai Bizottság új megfelelőségi határozatot fogadott el: a 2023/1795 számút. Ez váltja fel a megszűnt Privacy Shield-et, és EU-US Data Privacy Framework néven működik. Az Egyesült Államok korábban a 14086. sz. elnöki rendelettel (Executive Order) módosította belső rendszerét, amely a jelfelderítés hatókörét a „szükségesre és arányosra” korlátozza — ez az európai olvasó számára ismerős terminológia, az amerikai közigazgatási gyakorlat számára kevésbé —, és létrehozott egy Data Protection Review Court (DPRC) nevű felülvizsgálati szervet. A Bizottság úgy ítélte meg, hogy ezek a módosítások elegendőek a lényegileg egyenértékű szint visszaállításához.

A Schrems által alapított noyb szervezet 2023. szeptember 7-én panaszt nyújtott be az új határozat ellen. Az érvek várhatóak: a DPRC nem független bíróság a Charta artículo 47 értelmében; a „szükséges és arányos” fogalmak nem fordítják le mechanikusan az európai szabványokat; és végül, egy elnöki rendeleten alapuló védelem a következő elnöki rendelettel visszavonható. A TJUE ítélete az új határozatról — amelyet sokan már bizonyos beletörődéssel Schrems III-nak neveznek — a következő években várható. Az eredmény nem jósolható meg. Az érvelés szerkezete mindenesetre erősen emlékeztet a 2020-asra.

Amit az európai kkv nem hall meg

Miközben a TJUE nagykamarája tanácskozik, egy közepes méretű ügyvédi iroda továbbra is a Microsoft 365-ön keresztül levelezik ügyfeleivel, amelyet európai régiókban tárolnak, de egy FISA 702 hatálya alá tartozó amerikai vállalat tulajdonában van. Egy magánorvosi rendelő a Google Workspace-en keresztül szinkronizálja naptárát. Az adótanácsadó a DocuSign-on keresztül küldi el az aláírt bevallásokat. A pszichológus egy Notion táblázatból számláz. A munkajogi iroda a Dropbox-ban archiválja az aktákat. És gyakorlatilag mindannyian WhatsApp-on keresztül is tartják a kapcsolatot ügyfeleikkel. A szolgáltatók szerint mindez a 2023/1795

megfelelőségi határozat védelme alatt működhet. Azon a napon, amikor ez a határozat a Schrems III-ban elbukik, mindezek a kapcsolatok ugyanabban a másodpercben védelem nélkül maradnak.

A kérdés nem költői. 2022 és 2024 között több európai hatóság is eljárt adatkezelők ellen, mert megfelelő adattovábbítási eszköz nélkül használták a Google Analytics-et, a TJUE érvelésének szó szerinti alkalmazásával, még a Privacy Framework hatálybalépése előtt. A francia hatóság, a CNIL formalizálta először a kritériumot 2022-ben; az osztrák, az olasz és más hatóságok röviddel ezután követték. A szabályok be nem tartása az európai kkv-k jelenlegi operatív kialakítása mellett valós időben dokumentálható bárki számára, aki tudja, hová nézzen.

A TIA mint eszköz, nem mint rituálé

Az európai irodákban keringő TIA-k jelentős része, figyelmesen elolvasva, formális gyakorlat. Felsorolják a szerződéses eszközöket, felsorolják a szolgáltató tanúsítványait, hivatkoznak a technikai garanciákra, kipipálják a négyzetet. Kevesen kérdezik meg komolyan, hogy egy FISA 702 végzés kötelezné-e a szolgáltatót az adatok átadására. Még kevesebben kérdezik meg, mi történne ezzel az adattovábbítással a Privacy Framework egy hipotetikus felülvizsgálata esetén. Az RGPD artículo 5 előírja az adatkezelő számára, hogy képes legyen bizonyítani a megfelelést. Egy TIA, amelyet nem komolyan végeznek el, nem bizonyít semmit; azt bizonyítja, hogy papíron meg akarnak felelni, miközben a gyakorlatban az ellenkezőjét teszik.

A TIA őszinte változata egy egyszerű kérdéssel kezdődik: mi történne, ha holnap érkezne egy FISA 702 végzés ehhez a szolgáltatóhoz ezekre a konkrét adatokra vonatkozóan? Ha az őszinte válasz az, hogy „át kellene adnia őket anélkül, hogy értesítene minket”, a szerződéses kikötések nem oldják meg a problémát. Ami megoldja — azokban az esetekben, amikor a kérdés valóban számít —, az az, hogy nem adjuk át az adatokat annak a szolgáltatónak.

A politikai változás mint strukturális kockázat

Van egy további, politikai réteg is, amelyet érdemes dráma nélkül megnevezni. A 2023/1795 megfelelőségi határozat végső soron a 14086. sz. elnöki rendeleten alapul, amelyet Biden elnök írt alá 2022 októberében. Egy elnöki rendeletet egy elnök ír alá, és a következő visszavonhatja, módosíthatja vagy kiüresítheti. Az európai adatok védelme az Egyesült Államokban így egy olyan közigazgatási döntéstől függ, amelyet sem az amerikai kongresszus nem garantál, sem az amerikai jogrendszer nem véd olyan szilárdsággal, mint amilyen szilárdsággal más belügyeket véd. 2025 januárja óta új adminisztráció irányítja az Egyesült Államokat, és az EO 14086 gyakorlati folytonosságával kapcsolatos kérdés hipotézisből jelenné vált. Bármely forgatókönyv, amelyben az adminisztráció a rendelet visszavonása vagy enyhítése mellett döntene, az európai határozatot azon darab nélkül hagyná, amelyre épült.

Ez nem egy összeesküvés-elmélet. Ez a jogi kialakítás józan olvasata. A transzatlanti adatvédelmi keretek már kétszer elbuktak: a Safe Harbor 2015-ben (Schrems I ítélet), a Privacy Shield 2020-ban (Schrems II). A harmadik egy törékenyebb darabon nyugszik, mint két elődje. Egy európai vállalat, amely ma erre a darabra teszi fel adatkezelését, kockázatkezelési döntést hoz, nem pedig pusztán jogi megfelelési döntést.

A szakmai olvasó számára

Az operatív kérdések, amelyeket érdemes feltenni egy professzionális adatokhoz használt felhőszolgáltatás kiválasztása előtt — olyan szigorral, amellyel egy adatvédelmi felügyelő feltenné őket —, a következők:

1. Hol tárolják fizikailag az adatokat? Egy európai régió nem elegendő válasz, ha az operátor amerikai.
2. Ki üzemelteti a szolgáltatást, melyik joghatóság alá tartozik, és milyen jogi utasításoknak vethető alá?
3. Milyen adattovábbítási eszközt alkalmaznak: a 2023/1795 megfelelőségi határozatot, SCC-t TIA-val, az RGPD artículo 49 alóli mentességet? Megvédhető ez a választás egy ellenőrzés során?
4. Ha a megfelelőségi határozat holnap elbukna, milyen operatív terv létezik a tevékenység fenntartására?

5. Létezik-e európai vagy saját gazdagépen futó (self-hosted) alternatíva erre a funkcióra, és mekkora lenne a migráció valós költsége?

Nem minden mindennapi irodai funkció igényel azonos választ. Egy belső könyveléshez használt táblázat valószínűleg nem emeli a kérdést erre a szintre. Egy ügyfél büntetőjogi aktája, orvosi kórtörténete, az alkalmazottak bérlistája igen. Az arányosság jogos; az a kollektív tehetetlenség, amellyel az európai kkv-k mindenre — még a legérzékenyebb dolgokra is — amerikai szolgáltatóknál maradtak, nem az.

A Schrems II idén júliusban lesz hatéves. Az ítélet nem változtatta meg a legtöbb európai vállalat mindennapi szokásait. Megváltoztatta viszont a kockázati térképet, amelynek ezek a vállalatok ki vannak téve. Amikor egy amerikai közigazgatási döntés az európai szabályozás és egy kkv (PYME) tényleges működése közé áll, érdemes legalább tudni, hogy a döntés ott van, és törékeny. Mi, akik olyan architektúrát választottunk, ahol nincs közvetítő operátor — ez a szál fut végig a Cuadernos Lacre-en —, jobban szeretnénk, ha nem kellene minden alkalommal ilyen elemzéseket írnunk, amikor egy Schrems leül fellebbezést benyújtani. De továbbra is meg fogjuk tenni.

Források és további olvasnivalók

- Az Európai Unió Bírósága — 2020. július 16-i ítélet, C-311/18. sz. ügy, *Data Protection Commissioner kontra Facebook Ireland Ltd. és Maximillian Schrems*.
- Az (UE) 2016/679 rendelet V. fejezete, artículo 44–50 — személyes adatok nemzetközi továbbítása.
- A Bizottság (UE) 2023/1795 végrehajtási határozata (2023. július 10.) a személyes adatok megfelelő szintű védelméről az EU-US Data Privacy Framework keretében.
- Európai Adatvédelmi Testület — *01/2020. sz. ajánlások az adattovábbítási eszközöket kiegészítő intézkedésekről az EU személyesadat-védelmi szintjének való megfelelés biztosítása érdekében*, elfogadva 2021. június 18-án.
- noyb.eu — 2023. szeptember 7-én az (UE) 2023/1795 határozat ellen az európai adatvédelmi hatóságoknál benyújtott panasz.
- *Foreign Intelligence Surveillance Act*, 702. szakasz (az 50 U.S.C. § 1881a pontban kodifikálva), és az 12333. sz. elnöki rendelet az Egyesült Államok nemzeti területén kívüli hírszerzési tevékenységéről.

← ElőzőAmikor nincs senki középenKövetkező →CUADERNOS_LIST_SHA256_TITLE

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 fbfa5f5b7a1675a5e549a4f19a5c8567c732bccbbbc06a243ebd39ac3988bc6e

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

beállításához szükséges minimális JavaScriptet. Nincsenek trackerek, nincs profilalkotás, nincs adatmegosztás. Ha követni szeretne minket: RSS.