Analýza · 18. května 2026

← Předchozí·Další →

Schrems II, pět let poté

Rozsudek, který změnil právo v oblasti mezinárodních převodů osobních údajů. O pět let později značná část běžné evropské kancelářské agendy stále funguje, jako by se nic nestalo.

Rozsudek, kterému trvalo tři hodiny, než změnil pravidla

Dne 16. července 2020 kolem čtvrt na jedenáct dopoledne lucemburského času zveřejnil Soudní dvůr Evropské unie (TJUE) rozsudek ve věci C-311/18. Během následujících tří hodin přestal existovat právní režim, který umožňoval každodenní předávání osobních údajů z Evropy do Spojených států — tzv. Privacy Shield v oficiálním názvu. Než evropští pověřenci pro ochranu osobních údajů ten den doobědvali, rámec, v němž jejich společnosti a úřady fungovaly, již nebyl platný.

Rozsudek je dnes znám jako Schrems II podle Maximiliana Schremse, rakouského aktivisty, jehož stížnost na Facebook Ireland ho vyvolala. Stížnost se konkrétně týkala předávání údajů mezi společností Facebook Irsko a Facebook USA. Rozsudek jde v obecné rovině mnohem dále: diktuje, jak a za jakých podmínek může být jakýkoli osobní údaj shromážděný na evropském území předán do Spojených států.

Téměř o šest let později existuje náhradní rámec — EU-US Data Privacy Framework, přijatý v červenci 2023 — a ten je rovněž pod právním tlakem. Připravuje se nové kolo Schrems. Mezitím evropské malé a střední podniky nadále využívají americké cloudové služby pro každodenní úkoly, většinou bez vědomí, že právní otázka, na níž tyto služby spočívají, zůstává otevřená.

Co přesně říkal Schrems II

Rozsudek se opírá o tři pilíře. Prvním je Listina základních práv Evropské unie, zejména její články 7 (soukromý a rodinný život), 8 (ochrana osobních údajů) a 47 (právo na účinnou právní ochranu). Druhým je obecné nařízení o ochraně osobních údajů — RGPD, které si mnozí Evropané pamatují pouze kvůli upozorněním na soubory cookies — konkrétně jeho kapitola V, články 44 až 50 (art. 44 to 50), o předávání údajů do třetích zemí. Třetím jsou americké právní předpisy o zpravodajských službách: oddíl 702 zákona Foreign Intelligence Surveillance Act, v právní hantýrce FISA 702, a prezidentské výkonné nařízení 12333.

Soud postupoval metodou srovnání. Listina základních práv vyžaduje, aby osobní údaje evropských občanů po opuštění Unie požívaly úrovně ochrany v zásadě rovnocenné ochraně zaručené nařízením RGPD. Otázkou tedy bylo, zda Spojené státy tuto v zásadě rovnocennou úroveň nabízejí.

Odpověď byla záporná, a to nikoli kvůli detailům. FISA 702 umožňuje americké vládě shromažďovat komunikaci osob, které nejsou občany USA a nacházejí se mimo území státu, bez předchozího individuálního soudního povolení, bez vyrozumění dotčené osoby a bez účinného prostředku nápravy srovnatelného s evropským. Výkonné nařízení 12333 rozšiřuje tuto pravomoc obdobným způsobem mimo území státu. Soud dospěl k závěru, že evropský občan nemá v americkém právním systému k dispozici v zásadě rovnocennou ochranu, kterou Listina vyžaduje. Rovnocennost tedy neexistuje.

Z toho vyplynul přímý důsledek: rozhodnutí Evropské komise 2016/1250, které potvrdilo Privacy Shield jako odpovídající rámec pro předávání údajů, bylo prohlášeno za neplatné. Jakékoli předávání založené výhradně na tomto rámci zůstalo od téhož okamžiku bez právního základu.

Co přežilo (a za jakých podmínek)

Rozsudek Schrems II nezrušil všechny nástroje. Přežily standardní smluvní doložky — SCC v mezinárodní terminologii, podle anglického Standard Contractual Clauses. Jsou to vzorové smlouvy schválené Evropskou komisí: evropský vývozce a dovozce v cílové zemi je podepíší a zaváží se zpracovávat údaje podle evropského standardu. Společnost, která si myslela, že problém vyřešila 17. července 2020, podepsala SCC se svým poskytovatelem a byla spokojená.

Znepokojení přišlo při pomalém čtení rozsudku. Soud jasně uvedl, že SCC zůstávají platné, ale jejich platnost závisí na podmínce, kterou je třeba zdůraznit: že dovozce údajů je schopen je v praxi dodržet. Pokud mu vnitrostátní právní předpisy cílové země brání klauzule dodržet — například proto, že ho příkaz podle FISA 702 nutí předat údaje, aniž by o tom uvědomil svůj evropský protějšek — pak klauzule ve skutečnosti nechrání. A v takovém případě musí evropský vývozce podle soudu předávání údajů pozastavit.

To zavedlo nový prvek do evropské praxe ochrany osobních údajů: Transfer Impact Assessment neboli analýzu dopadu předávání údajů, známou pod anglickou zkratkou TIA. Pokaždé, když chce evropská společnost předat údaje do USA na základě SCC, musí formálně vyhodnotit, zda příjemce může klauzule dodržet s ohledem na právní předpisy, které se na něj vztahují. Evropský sbor pro ochranu osobních údajů (EDPB) zveřejnil podrobné pokyny k tomu, jak TIA provádět. Poctivá praxe obvykle vede ke stejnému výsledku: pokud je dovozcem americká dceřiná společnost velkého cloudového poskytovatele, upřímná odpověď na TIA zní, že klauzule nelze splnit tak, jak jsou napsány.

Privacy Framework a čekající Schrems III

Dne 10. července 2023 přijala Evropská komise nové rozhodnutí o odpovídající ochraně: 2023/1795. Nahrazuje zaniklý Privacy Shield a funguje pod názvem EU-US Data Privacy Framework. Spojené státy předtím upravily svůj vnitřní režim prostřednictvím výkonného nařízení (Executive Order) 14086, které omezuje rozsah sledování signálů na to, co je „nezbytné a přiměřené“ — terminologie známá evropskému čtenáři, ale méně obvyklá v americké administrativní praxi — a zřizuje kontrolní orgán nazvaný Data Protection Review Court (DPRC). Komise dospěla k závěru, že tyto změny postačují k obnovení v zásadě rovnocenné úrovně ochrany.

Organizace noyb, založená Schremsem, podala 7. září 2023 stížnost proti novému rozhodnutí. Argumenty jsou očekávatelné: DPRC není nezávislý soud ve smyslu článku 47 (art. 47) Listiny; pojmy „nezbytné a přiměřené“ se mechanicky nepřekládají do evropských standardů; a konečně ochrana, která spočívá na výkonném nařízení, může být zrušena následujícím výkonným nařízením. Rozsudek TJUE k novému rozhodnutí — který mnozí s jistou rezignací již nazývají Schrems III — se očekává v příštích letech. Výsledek nelze předjímat. Struktura argumentace v každém případě velmi připomíná tu z roku 2020.

Co evropské malé a střední podniky neslyší

Zatímco velký senát TJUE rozhoduje, středně velká advokátní kancelář nadále komunikuje se svými klienty prostřednictvím Microsoft 365 hostovaného v evropských regionech, ale vlastněného americkou společností podléhající FISA 702. Soukromá ordinace synchronizuje kalendáře prostřednictvím Google Workspace. Daňový poradce zasílá podepsaná přiznání přes DocuSign. Psycholog fakturuje z tabulky v Notion. Pracovněprávní kancelář archivuje spisy v Dropboxu. A prakticky všichni z nich navíc komunikují se svými klienty přes WhatsApp. To vše může fungovat na základě rozhodnutí o odpovídající ochraně 2023/1795, podle vyjádření poskytovatelů. V den, kdy toto rozhodnutí padne v rámci Schrems III, zůstanou všechny tyto vztahy v jediné vteřině nechráněné.

Otázka není řečnická. V letech 2022 až 2024 rozhodlo několik evropských orgánů v případech proti správcům údajů za používání Google Analytics bez odpovídajícího nástroje pro předávání, v doslovné aplikaci úvah TJUE ještě předtím, než vstoupil v platnost Privacy Framework. Francouzský orgán CNIL byl prvním, kdo v roce 2022 formalizoval toto kritérium; rakouský, italský a další orgány následovaly krátce poté. Nedodržování pravidel v rámci současného provozního nastavení evropských malých a středních podniků je dokumentováno v reálném čase před každým, kdo ví, kam se dívat.

TIA jako nástroj, nikoli jako rituál

Značná část TIA, které kolují po evropských kancelářích, jsou při pozorném čtení pouze formální cvičení. Uvádějí smluvní nástroje, vyjmenovávají certifikace poskytovatele, citují technické záruky, odškrtávají políčka. Jen málokdo se vážně ptá, zda by příkaz podle FISA 702 donutil poskytovatele údaje předat. Ještě méně se jich ptá, co by se s tímto předáváním stalo při hypotetické revizi Privacy Framework. Článek 5 (art. 5) nařízení RGPD vyžaduje, aby správce údajů byl schopen doložit soulad. TIA, která není prováděna vážně, nedokazuje nic; dokazuje pouze ochotu plnit pravidla na papíře, zatímco v praxi se dělá opak.

Upřímná verze TIA začíná jednoduchou otázkou: co by se stalo, kdyby zítra tento poskytovatel obdržel příkaz podle FISA 702 k těmto konkrétním údajům? Pokud je poctivá odpověď „musel by je předat, aniž by nás uvědomil“, smluvní klauzule problém neřeší. To, co ho řeší v případech, kdy na otázce skutečně záleží, je nesvěřit údaje do rukou tohoto poskytovatele.

Politická změna jako strukturální riziko

Existuje další, politická vrstva, kterou je třeba pojmenovat bez dramatizace. Rozhodnutí o odpovídající ochraně 2023/1795 spočívá v konečném důsledku na výkonném nařízení 14086, které podepsal prezident Biden v říjnu 2022. Výkonné nařízení podepisuje prezident a následující prezident ho může zrušit, změnit nebo vyprázdnit jeho obsah. Ochrana evropských údajů v USA tak závisí na administrativním rozhodnutí, které nezaručuje ani americký Kongres, ani ho americký právní systém nechrání s takovou pevností, s jakou chrání jiné vnitřní záležitosti. Od ledna 2025 vládne v USA nová administrativa a otázka praktické kontinuity výkonného nařízení 14086 přestala být hypotézou a stala se realitou. Jakýkoli scénář, v němž by se administrativa rozhodla nařízení stáhnout nebo oslabit, by evropské rozhodnutí ponechal bez základu, na němž bylo vybudováno.

Nejedná se o konspirační argument. Je to střízlivé čtení právní konstrukce. Transatlantické rámce ochrany údajů padly již dvakrát: Safe Harbor v roce 2015 (rozsudek Schrems I), Privacy Shield v roce 2020 (Schrems II). Třetí spočívá na křehčím základu než jeho dva předchůdci. Evropská společnost, která dnes sází zpracování svých údajů na tento základ, činí rozhodnutí o řízení rizik, nikoli pouze o prostém dodržování předpisů.

Pro odborné čtenáře

Provozní otázky, které je vhodné si položit před výběrem cloudové služby pro profesionální údaje — s takovou přísností, s jakou by je kladl inspektor ochrany údajů — jsou následující:

1. Kde jsou data fyzicky uložena? Evropský region není dostatečnou odpovědí, pokud je provozovatelem americká společnost.
2. Kdo službu provozuje, v jaké jurisdikci je registrován a jakým právním příkazům může být podroben?
3. Jaký nástroj pro předávání údajů je využíván: rozhodnutí o odpovídající ochraně 2023/1795, SCC s TIA, výjimka podle článku 49 (art. 49) nařízení RGPD? Je tato volba obhajitelná před kontrolou?
4. Pokud by rozhodnutí o odpovídající ochraně zítra padlo, jaký provozní plán existuje pro zachování činnosti?
5. Existuje pro tuto funkci evropská alternativa nebo možnost vlastního hostingu a jaké by byly reálné náklady na migraci?

Ne všechny každodenní funkce v kanceláři vyžadují stejnou odpověď. Tabulka pro vnitřní účetnictví pravděpodobně nezvedá otázku na tuto úroveň. Trestní spis klienta, zdravotní dokumentace, mzdové listy zaměstnanců však ano. Přiměřenost je legitimní; kolektivní setrvačnost, se kterou evropské malé a střední podniky zůstaly u amerických poskytovatelů pro vše — i pro to nejcitlivější — nikoliv.

V červenci uplyne šest let od rozsudku Schrems II. Rozsudek nezměnil každodenní návyky většiny evropských společností. Změnil však mapu rizik, kterým jsou tyto společnosti vystaveny. Když americké administrativní rozhodnutí stojí mezi evropským nařízením a reálným provozem malého či středního podniku, je dobré alespoň vědět, že toto rozhodnutí existuje a že je křehké. My, kteří jsme si zvolili architekturu bez prostředníka — nit, která se vine Cuadernos Lacre — bychom raději nemuseli psát tento druh analýz pokaždé, když se nějaký Schrems rozhodne podat odvolání. Ale budeme v tom pokračovat.

Zdroje a další čtení

- Soudní dvůr Evropské unie (TJUE) — rozsudek ze dne 16. července 2020, věc C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd a Maximillian Schrems*.
- Nařízení (EU) 2016/679, kapitola V, články 44 až 50 — mezinárodní předávání osobních údajů.
- Prováděcí rozhodnutí Komise (EU) 2023/1795 ze dne 10. července 2023 o odpovídající úrovni ochrany osobních údajů v rámci EU-US Data Privacy Framework.
- Evropský sbor pro ochranu osobních údajů (EDPB) — *Doporučení 01/2020 o opatřeních doplňujících nástroje předávání údajů s cílem zajistit soulad s úrovní ochrany osobních údajů v EU*, přijatá dne 18. června 2021.
- noyb.eu — stížnost podaná dne 7. září 2023 proti rozhodnutí (EU) 2023/1795 u evropských orgánů pro ochranu osobních údajů.
- *Foreign Intelligence Surveillance Act*, oddíl 702 (kodifikováno v 50 U.S.C. § 1881a) a výkonné nařízení 12333 o aktivitách amerických zpravodajských služeb mimo území státu.

← PředchozíKdyž není nikdo uprostředDalší →CUADERNOS_LIST_SHA256_TITLE

Nedávné čtení

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vezměte si tento článek tam, kam potřebujete.

↓ Markdown ↓ Prostý text ↓ PDF

Soubor se stáhne do vašeho zařízení. Odtud si jej můžete uložit, importovat do Solo2 nebo sdílet, kdekoli chcete. Cuadernos za vás o cíli nerozhoduje.

Pečeť · SHA-256 c1c30aff41d1b926ec4dd3c47b375ed8aa65be4013bfcf5ddf947d1c91c07038

Cuadernos Lacre · Publikace Menzuri Gestión S.L. ·
napsal R.Eugenio · rediguje tým Solo2.