

Schrems II, pet godina kasnije

Presuda koja je promijenila pravo međunarodnog prijenosa osobnih podataka. Pet godina kasnije, znatan dio europskog svakodnevnog poslovanja nastavlja raditi kao da se ništa nije dogodilo.

Presuda kojoj su trebala tri sata da promijeni pravila

Dana 16. srpnja 2020., oko deset i petnaest ujutro po luksemburškom vremenu, Sud Europske unije (TJUE) objavio je presudu u predmetu C-311/18. U sljedeća tri sata, pravni režim koji je podupirao svakodnevni prijenos osobnih podataka iz Europe u Sjedinjene Države — takozvani Štit privatnosti (Privacy Shield u svom službenom nazivu) — prestao je postojati. Kada su europski službenici za zaštitu podataka tog dana završili s ručkom, okvir pod kojim su njihove tvrtke i uprave poslovale više nije vrijedio.

Presuda je danas poznata kao Schrems II, po Maximilianu Schremsu, austrijskom aktivistu čija ju je tužba protiv Facebooka Ireland potaknula. Tužba se, konkretno, bavila prijenosima između Facebooka Irska i Facebooka Sjedinjene Države. Presuda, općenito, ide mnogo dalje: ona propisuje kako i pod kojim uvjetima bilo koji osobni podatak prikupljen na europskom teritoriju može biti prenesen u Sjedinjene Države.

Gotovo šest godina kasnije, zamjenski okvir postoji — EU-US Data Privacy Framework, usvojen u srpnju 2023. — i on je također pod pravnim pritiskom. Nova runda Schrems se priprema. U međuvremenu, mala i srednja europska poduzeća nastavljaju koristiti američke usluge u oblaku za svakodnevne zadatke, većinom ne znajući da pravno pitanje na kojem te usluge počivaju ostaje otvoreno.

Što je točno govorio Schrems II

Presuda se oslanja na tri dijela. Prvi je Povelja o temeljnim pravima Europske unije, posebno njezini artículos 7 (privatni i obiteljski život), 8 (zaštita osobnih podataka) i 47 (učinkovita sudska zaštita). Drugi je Opća uredba o zaštiti podataka — RGPD koji se mnogi Europljani sjećaju samo po obavijestima o kolačićima — točnije njezino poglavlje V, artículos 44 do 50, o međunarodnim prijenosima. Treći je američko obavještajno zakonodavstvo: odjeljak 702 Zakona o nadzoru stranih obavještajnih službi (Foreign Intelligence Surveillance Act), FISA 702 u pravnom žargonu, i predsjednička Izvršna naredba 12333.

Sud je postupio metodom kontrasta. Povelja o temeljnim pravima zahtijeva da osobni podaci europskih građana uživaju, kada napuste Uniju, razinu zaštite bitno jednakovrijednu onoj koju jamči RGPD. Pitanje je, prema tome, bilo pružaju li Sjedinjene Države tu bitno jednakovrijednu razinu.

Odgovor je bio negativan, i to ne zbog nijansi. FISA 702 dopušta američkoj vladi prikupljanje komunikacija osoba koje nisu Amerikanci, a koje se nalaze izvan nacionalnog teritorija, bez prethodnog pojedinačnog sudskog odobrenja, bez obavijesti pogođenoj osobi i bez učinkovitog pravnog lijeka usporedivog s europskim. Izvršna naredba 12333 analogno proširuje tu sposobnost izvan nacionalnog teritorija. Sud je zaključio da europski građanin, pred američkim pravnim sustavom, nema bitno jednakovrijednu zaštitu koju Povelja zahtijeva. Ekvivalentnost, stoga, ne postoji.

Odatle izravna posljedica: Odluka Komisije 2016/1250, kojom je potvrđen Privacy Shield kao odgovarajući okvir za prijenose, proglašena je nevažećom. Svaki prijenos koji se temeljio isključivo na tom okviru ostao je bez pravne osnove od tog istog trenutka.

Ono što je preživjelo (i pod kojim uvjetima)

Schrems II nije eliminirao sve instrumente. Standardne ugovorne klauzule — SCC u međunarodnom žargonu — preživjele su. To su ogledni ugovori koje je odobrila Europska komisija: europski izvoznik i uvoznik iz zemlje odredišta potpisuju ih obvezujući se na obradu podataka prema europskom standardu. Tvrtka koja je mislila da je riješila problem 17. srpnja 2020. potpisala je SCC sa svojim pružateljem usluga i bila zadovoljna.

Nelagoda se pojavila nakon polaganog čitanja presude. Sud je jasno dao do znanja da SCC-ovi ostaju važeći, ali njihova valjanost ovisi o uvjetu koji treba naglasiti: da ih uvoznik podataka može ispuniti u praksi. Ako mu nacionalno zakonodavstvo zemlje odredišta onemogućuje ispunjavanje klauzula — jer ga, na primjer, nalog pod FISA-om 702 obvezuje na predaju podataka bez obavještanja europske strane — klauzule zapravo ne štite. I tada, kaže Sud, europski izvoznik mora obustaviti prijenos.

To je u europsku praksu zaštite podataka uvelo novi objekt: Procjenu utjecaja prijenosa (Transfer Impact Assessment), poznatu po engleskoj kratici TIA. Svaki put kad europska tvrtka želi prenijeti podatke u Sjedinjene Države pod okriljem SCC-a, mora formalno procijeniti može li primatelj poštivati klauzule s obzirom na zakonodavstvo koje se na njega primjenjuje. Europski odbor za zaštitu podataka (EDPB) objavio je detaljne smjernice o tome kako provesti TIA. Iskrena praksa obično daje isti rezultat: ako je uvoznik američka podružnica velikog pružatelja usluga u oblaku, iskren odgovor na TIA je da se klauzule ne mogu ispuniti onako kako su napisane.

Privacy Framework i neriješeni Schrems III

Dana 10. srpnja 2023. Europska komisija usvojila je novu Odluku o adekvatnosti: 2023/1795. Ona zamjenjuje pokojni Privacy Shield i djeluje pod nazivom EU-US Data Privacy Framework. Sjedinjene Države prethodno su izmijenile svoj unutarnji režim putem Izvršne naredbe (Executive Order) 14086, koja ograničava opseg obavještajnih signala na ono što je „nužno i razmjerno” — terminologija poznata europskom čitatelju, ali ne toliko američkoj administrativnoj praksi — i uspostavlja revizijsko tijelo pod nazivom Data Protection Review Court (DPRC). Komisija je smatrala da su te izmjene dovoljne za ponovnu uspostavu bitno jednakovrijedne razine zaštite.

Organizacija noyb, koju je osnovao Schrems, podnijela je tužbu 7. rujna 2023. protiv nove Odluke. Argumenti su očekivani: DPRC nije neovisni sud u smislu artículo 47 Povelje; koncepti „nužno i razmjerno” ne prevode mehanički europske standarde; i, konačno, zaštita koja počiva na Izvršnoj naredbi može biti opozvana sljedećom Izvršnom naredbom. Presuda TJUE-a o novoj Odluci — koju mnogi već nazivaju, s dozom rezignacije, Schrems III — očekuje se u sljedećim godinama. Ishod se ne može predvidjeti. Struktura argumenta, u svakom slučaju, uvelike podsjeća na onu iz 2020.

Ono što europski PYME ne čuje

Dok veliko vijeće TJUE-a vijeća, odvjetnički ured srednje veličine nastavlja razmjenjivati korespondenciju sa svojim klijentima putem Microsofta 365 ugošćenog u europskim regijama, ali u vlasništvu američke tvrtke podložne FISA-i 702. Privatna medicinska ordinacija sinkronizira kalendare putem Google Workspacea. Porezni savjetnik šalje potpisane prijave putem DocuSigna. Psiholog izdaje račune iz proračunske tablice u Notion-u. Odvjetnički ured za radno pravo arhivira spise u Dropbox-u. I praktički svi oni, osim toga, uslužuju svoje klijente putem WhatsAppa. Sve to može funkcionirati pod okriljem Odluke o adekvatnosti 2023/1795, prema pružateljima usluga. Onog dana kada ta Odluka padne u Schrems-u III, svi ti odnosi ostaju nezaštićeni u istoj sekundi.

Pitanje nije retoričko. Između 2022. i 2024. nekoliko je europskih tijela riješilo predmete protiv voditelja obrade zbog korištenja Google Analyticsa bez odgovarajućeg instrumenta prijenosa, primjenjujući doslovno obrazloženje TJUE-a čak i prije nego što je Privacy Framework stupio na snagu. Francusko tijelo, CNIL, prvo je formaliziralo kriterij 2022.; austrijska, talijanska i druga tijela slijedila su ubrzo nakon toga. Nesukladnost se, pod trenutnim operativnim dizajnom europskog PYME-a, dokumentira u stvarnom vremenu pred onim tko zna kamo gledati.

TIA kao instrument, a ne kao ritual

Znatan dio TIA-ova koji kruže europskim uredima su, pažljivo pročitani, formalne vježbe. Oni navode ugovorne instrumente, nabrajaju certifikate pružatelja usluga, citiraju tehnička jamstva, označavaju kućicu. Rijetki se ozbiljno zapitaju bi li nalog FISA 702 obvezao pružatelja usluga na predaju podataka. Još manje se pitaju što bi se dogodilo s tim prijenosom pod hipotetskom revizijom Privacy Framework-a. Artículo 5 RGPD-a zahtijeva od voditelja obrade da može dokazati sukladnost. TIA koji se ne provodi ozbiljno ne dokazuje ništa; ono što dokazuje je volja za ispunjavanjem na papiru dok se u praksi radi suprotno.

Iskrena verzija TIA-e započinje jednostavnim pitanjem: što bi se dogodilo ako bi sutra ovom pružatelju usluga stigao nalog FISA 702 za ove konkretne podatke? Ako je iskren odgovor „morao bi ih predati bez da nas obavijesti”, ugovorne klauzule ne rješavaju problem. Ono što ga rješava, u slučajevima u kojima je pitanje doista važno, jest ne dati podatke tom pružatelju usluga.

Politička promjena kao strukturni rizik

Postoji dodatni sloj, politički, koji je korisno navesti bez dramatike. Odluka o adekvatnosti 2023/1795 počiva, u konačnici, na Izvršnoj naredbi 14086, koju je potpisao predsjednik Biden u listopadu 2022. Izvršnu naredbu potpisuje jedan predsjednik, a sljedeći je može opozvati, izmijeniti ili isprazniti od sadržaja. Zaštita europskih podataka u Sjedinjenim Državama ovisi, dakle, o administrativnoj odluci koju niti američki Kongres jamči niti američki pravni sustav štiti onom čvrstinom kojom štiti druga unutarnja pitanja. Od siječnja 2025. nova administracija vlada Sjedinjenim Državama, a pitanje o praktičnom kontinuitetu EO 14086 prestalo je biti hipoteza i postalo je suvremeno. Bilo koji scenarij u kojem bi administracija odlučila povući ili ublažiti Naredbu ostavio bi europsku Odluku bez dijela na kojem je izgrađena.

To nije argument zavjere. To je trezveno čitanje pravnog dizajna. Transatlantski okviri za zaštitu podataka već su dva puta pali: Safe Harbor 2015. (presuda Schrems I), Privacy Shield 2020. (Schrems II). Treći počiva na krhkijem dijelu od svoja dva prethodnika. Europska tvrtka koja se danas oslanja na taj dio za svoju obradu podataka donosi odluku o upravljanju rizikom, a ne puku odluku o usklađenosti s propisima.

Za profesionalnog čitatelja

Operativna pitanja koja je korisno postaviti prije odabira usluge u oblaku za profesionalne podatke — uz strogoću kojom bi ih inspektor za zaštitu podataka postavio — su sljedeća:

1. Gdje se podaci fizički pohranjuju? Europska regija nije dovoljan odgovor ako je operater Amerikanac.
2. Tko upravlja uslugom, u kojoj je jurisdikciji registriran i kojim pravnim nalogima može biti podvrgnut?
3. Koji se instrument prijenosa priziva: Odluka o adekvatnosti 2023/1795, SCC s TIA, odstupanje iz artículo 49 RGPD-a? Je li taj izbor obranjiv pred inspekcijom?
4. Ako Odluka o adekvatnosti sutra padne, koji operativni plan postoji za održavanje aktivnosti?
5. Postoji li europska ili samostalno ugošćena alternativa za tu funkciju i koliki bi bio stvarni trošak migracije?

Ne zahtijevaju sve svakodnevne uredske funkcije isti odgovor. Proračunska tablica za interno računovodstvo vjerojatno ne podiže pitanje na ovu razinu. Kazneni dosje klijenta, medicinska povijest, platna lista zaposlenika,

da. Razmjernost je legitimna; kolektivna inercija s kojom je europski PYME ostao kod američkih pružatelja usluga za sve — čak i za ono najosjetljivije — nije.

Schrems II ovog srpnja navršava šest godina. Presuda nije promijenila svakodnevne navike većine europskih tvrtki. Promijenila je, međutim, mapu rizika kojima su te tvrtke izložene. Kada se američka administrativna odluka isprieči između europske regulative i stvarnog poslovanja malog ili srednjeg poduzeća (PYME), korisno je barem znati da je ta odluka tu i da je krhka. Mi koji smo odabrali arhitekturu bez operatera u sredini — nit koja prožima Cuadernos Lacre — radije ne bismo morali pisati ovakve analize svaki put kad Schrems sjedne podnijeti žalbu. Ali nastaviti ćemo ih pisati.

Izvori i dodatno štivo

- Sud Europske unije — presuda od 16. srpnja 2020., predmet C-311/18, *Data Protection Commissioner protiv Facebook Ireland Ltd. i Maximilliana Schremsa*.
- Uredba (UE) 2016/679, poglavlje V, artículos 44 do 50 — međunarodni prijenosi osobnih podataka.
- Provedbena odluka Komisije (UE) 2023/1795 od 10. srpnja 2023. o odgovarajućoj razini zaštite osobnih podataka u okviru EU-US Data Privacy Framework-a.
- Europski odbor za zaštitu podataka — *Preporuke 01/2020 o mjerama koje dopunjuju instrumente prijenosa kako bi se osigurala usklađenost s razinom zaštite osobnih podataka u EU-u*, usvojene 18. lipnja 2021.
- noyb.eu — tužba podnesena 7. rujna 2023. protiv Odluke (UE) 2023/1795 europskim tijelima za zaštitu podataka.
- *Foreign Intelligence Surveillance Act*, odjeljak 702 (kodificiran u 50 U.S.C. § 1881a), i Izvršna naredba 12333 o američkim obavještajnim aktivnostima izvan nacionalnog teritorija.

[← Prethodno](#)[Kada nema nikoga u sredini](#)[Sljedeće](#) → [CUADERNOS LIST SHA256 TITLE](#)

Nedavna čitanja

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

Ponesite ovaj članak sa sobom gdje god vam zatreba.

[↓ Markdown](#) [↓ Obični tekst](#) [↓ PDF](#)

Datoteka će se preuzeti na vaš uređaj. Od tamo je možete spremiti, uvesti u Solo2 ili dijeliti gdje god želite. Cuadernos ne odlučuje o odredištu umjesto vas.

Voštani pečat · SHA-256 edc1205fa761a25df4d4a4682bb49974e3d2e503edd9884b8ed57ba9f9642487

Cuadernos Lacre · Publikacija [Menzuri Gestión S.L.](#) · napisao R.Eugenio · uredio tim [Solo2](#).

Ova web stranica ne koristi kolačiće i ne učitava resurse trećih strana. Koristi samostalno hostiran anonimni brojač posjeta (Umami, na našem europskom poslužitelju) i minimalnu količinu JavaScripta potrebnu za vašu postavku svijetle/tamne teme. Bez trackera, bez profiliranja, bez dijeljenja podataka. Ako nas želite pratiti: [RSS](#).