

Schrems II, pięć lat później

Wyrok, który zmienił prawo w zakresie międzynarodowego transferu danych osobowych. Pięć lat później znaczna część europejskich biur profesjonalnych nadal funkcjonuje tak, jakby nic się nie stało.

Mówiąc prościej: 16 lipca 2020 r., w czwartkowy poranek, europejski trybunał uznał za nielegalną ogromną część sposobu, w jaki firmy przysyłały twoje dane do Stanów Zjednoczonych. Pięć lat później prawie nikt nic nie zmienił. Twoje informacje wciąż latają dokładnie tak samo jak wtedy.

Wyrok, który w trzy godziny zmienił zasady gry

16 lipca 2020 roku, około godziny dziesiątej piętnaście rano czasu luksemburskiego, Trybunał Sprawiedliwości Unii Europejskiej (TJUE) ogłosił wyrok w sprawie C-311/18. W ciągu następujących trzech godzin reżim prawny wspierający codzienny transfer danych osobowych z Europy do Stanów Zjednoczonych — tzw. Tarcza Prywatności (Privacy Shield) — przestał istnieć. Zanim europejscy inspektorzy ochrony danych skończyli tego dnia lunch, ramy prawne, w których operowały ich firmy i urzędy, stały się bezużyteczne.

Wyrok ten znany jest dziś jako Schrems II, od nazwiska Maximiliana Schremsa, austriackiego aktywisty, którego skarga przeciwko Facebook Ireland go wywołała. Skarga w szczególności dotyczyła transferów między Facebook Irlandia a Facebook USA. Wyrok w ujęciu ogólnym idzie znacznie dalej: dyktuje on, jak i pod jakimi warunkami dowolne dane osobowe zebrane na terytorium Europy mogą trafić do Stanów Zjednoczonych.

Prawie sześć lat później istnieją ramy zastępcze — EU-US Data Privacy Framework, przyjęte w lipcu 2023 roku — które również znajdują się pod presją prawną. Przygotowywana jest kolejna runda spraw Schremsa. Tymczasem małe i średnie europejskie przedsiębiorstwa nadal korzystają z amerykańskich usług chmurowych do codziennych zadań, w większości nie wiedząc, że kwestia prawna, na której opierają się te usługi, pozostaje otwarta.

Co dokładnie orzeczono w sprawie Schrems II

Wyrok opiera się na trzech filarach. Pierwszym jest Karta Praw Podstawowych Unii Europejskiej, w szczególności jej artykuły 7 (życie prywatne i rodzinne), 8 (ochrona danych osobowych) i 47 (prawo do skutecznego środka prawnego). Drugim jest ogólne rozporządzenie o ochronie danych — RGPD (RODO), które wielu Europejczyków kojarzy jedynie z komunikatami o ciasteczkach — a konkretnie jego rozdział V, artykuły 44–50, dotyczące transferów międzynarodowych. Trzecim jest amerykańskie ustawodawstwo wywiadowcze: sekcja 702 ustawy Foreign Intelligence Surveillance Act, FISA 702 w żargonie prawniczym, oraz prezydenckie rozporządzenie wykonawcze 12333.

Trybunał postąpił metodą kontrastu. Karta Praw Podstawowych wymaga, aby dane osobowe obywateli europejskich, gdy opuszczają Unię, cieszyły się stopniem ochrony merytorycznie równoważnym temu gwarantowanemu przez RGPD. Pytanie brzmiało zatem, czy Stany Zjednoczone oferują ten merytorycznie równoważny stopień ochrony.

Odpowiedź była przecząca i to nie z powodu drobnych niuansów. FISA 702 pozwala amerykańskiemu rządowi gromadzić komunikację osób niebędących Amerykanami, znajdujących się poza terytorium kraju, bez uprzedniej indywidualnej zgody sądu, bez powiadomienia osoby zainteresowanej i bez skutecznego środka prawnego porównywalnego z europejskim. Rozporządzenie wykonawcze 12333 analogicznie rozszerza te możliwości poza terytorium kraju. Trybunał uznał, że obywatel europejski w obliczu amerykańskiego systemu prawnego nie dysponuje merytorycznie równoważną ochroną, której wymaga Karta. Równoważność zatem nie istnieje.

Stąd bezpośrednia konsekwencja: decyzja Komisji Europejskiej 2016/1250, która uznała Tarczę Prywatności za odpowiednie ramy dla transferów, została uznana za nieważną. Wszelkie transfery oparte wyłącznie na tych ramach pozostały bez podstawy prawnej od tego samego momentu.

Co przetrwało (i pod jakimi warunkami)

Schrems II nie wyeliminował wszystkich instrumentów. Standardowe klauzule umowne — SCC w żargonie międzynarodowym, od Standard Contractual Clauses — przetrwały. Są to wzorcowe umowy zatwierdzone przez Komisję Europejską: unijny eksporter i importer z kraju docelowego podpisują je, zobowiązując się do przetwarzania danych zgodnie z europejskim standardem. Firma, która uznała problem za rozwiązany 17 lipca 2020 roku, podpisała SCC ze swoim dostawcą i uznała sprawę za załatwioną.

Dyskomfort pojawił się przy uważnej lekturze wyroku. Trybunał jasno stwierdził, że SCC pozostają ważne, ale ich ważność zależy od warunku, który warto podkreślić: importer danych musi być w stanie przestrzegać ich w praktyce. Jeśli krajowe ustawodawstwo kraju docelowego uniemożliwia mu przestrzeganie klauzul — ponieważ na przykład nakaz na podstawie FISA 702 zmusza go do wydania danych bez powiadamiania europejskiego kontrahenta — klauzule te w rzeczywistości nie chronią. W takim przypadku, mówi Trybunał, europejski eksporter musi zawiesić transfer.

Wprowadziło to nowy element do europejskiej praktyki ochrony danych: Transfer Impact Assessment, czyli ocenę skutków transferu, znaną pod angielskim skrótem TIA. Za każdym razem, gdy europejska firma chce przesłać dane do Stanów Zjednoczonych na podstawie SCC, musi formalnie ocenić, czy odbiorca jest w stanie przestrzegać klauzul, biorąc pod uwagę przepisy prawa, którym podlega. Europejska Rada Ochrony Danych (EDPB) opublikowała szczegółowe wytyczne dotyczące przeprowadzania TIA. Uczciwa praktyka zazwyczaj prowadzi do tego samego wniosku: jeśli importerem jest amerykańska spółka zależna giganta chmurowego, szczerą odpowiedź w ramach TIA brzmi, że klauzul nie można spełnić w brzmieniu, w jakim zostały zapisane.

Privacy Framework i oczekiwany wyrok Schrems III

10 lipca 2023 roku Komisja Europejska przyjęła nową decyzję o adekwatności: 2023/1795. Zastępuje ona nieistniejącą już Tarczę Prywatności i funkcjonuje pod nazwą EU-US Data Privacy Framework. Stany Zjednoczone uprzednio zmodyfikowały swój wewnętrzny reżim prawny poprzez rozporządzenie wykonawcze (Executive Order) 14086, które ogranicza zakres wywiadu sygnałowego do poziomu „niezbędnego i proporcjonalnego” — to terminologia znana europejskiemu czytelnikowi, ale niekoniecznie amerykańskiej praktyce administracyjnej — oraz tworzy organ odwoławczy o nazwie Data Protection Review Court (DPRC). Komisja uznała, że zmiany te są wystarczające do przywrócenia stopnia ochrony merytorycznie równoważnego standardom unijnym.

Organizacja noyb, założona przez Schremsa, złożyła 7 września 2023 roku skargę na nową decyzję. Argumenty są przewidywalne: DPRC nie jest niezależnym sądem w rozumieniu artykułu 47 Karty; pojęcia „niezbędny i proporcjonalny” nie przekładają się automatycznie na standardy europejskie; i wreszcie, ochrona oparta na rozporządzeniu wykonawczym może zostać cofnięta przez kolejne rozporządzenie wykonawcze. Wyrok TJUE w sprawie nowej decyzji — który wielu nazywa już z pewną rezygnacją Schrems III — spodziewany jest w najbliższych latach. Wyniku nie da się przewidzieć. Struktura argumentacji w każdym razie bardzo przypomina tę z 2020 roku.

Czego nie słyszy europejskie MŚP

Podczas gdy wielka izba TJUE obraduje, średniej wielkości kancelaria prawna nadal wymienia korespondencje ze swoimi klientami za pośrednictwem Microsoft 365, hostowanego w regionach europejskich, ale należącego do amerykańskiej firmy podlegającej pod FISA 702. Prywatna przychodnia lekarska synchronizuje kalendarze przez Google Workspace. Doradca podatkowy wysyła podpisane deklaracje przez DocuSign. Psycholog wystawia faktury z arkusza kalkulacyjnego w Notion. Kancelaria prawa pracy archiwizuje akta w Dropbox. I praktycznie wszyscy oni dodatkowo obsługują klientów przez WhatsApp. Wszystko to, według dostawców, może funkcjonować pod ochroną decyzji o adekwatności 2023/1795. W dniu, w którym decyzja ta upadnie w ramach wyroku Schrems III, wszystkie te relacje zostaną pozbawione ochrony prawnej w jednej sekundzie.

Kwestia ta nie jest retoryczna. W latach 2022–2024 kilka europejskich organów nadzorczych rozstrzygnęło sprawy przeciwko administratorom za korzystanie z Google Analytics bez odpowiedniego instrumentu transferu, stosując dosłowną interpretację rozumowania TJUE jeszcze przed wejściem w życie Privacy Framework. Francuski organ CNIL jako pierwszy sformalizował to kryterium w 2022 roku; organy austriackie, włoskie i inne poszły w jego ślady niedługo później. Brak zgodności, przy obecnym modelu operacyjnym europejskich MŚP, jest dokumentowany w czasie rzeczywistym dla każdego, kto wie, gdzie patrzeć.

TIA jako instrument, a nie rytuał

Znaczna część dokumentów TIA krążących po europejskich biurach to, przy uważnej lekturze, jedynie ćwiczenia formalne. Wymieniają instrumenty umowne, wyliczają certyfikaty dostawcy, przytaczają gwarancje techniczne, zaznaczają odpowiednie pola. Niewielu zadaje sobie na poważnie pytanie, czy nakaz FISA 702 zmusiłby dostawcę do wydania danych. Jeszcze mniej pyta, co stałoby się z tym transferem w przypadku hipotetycznej rewizji Privacy Framework. Artykuł 5 RGPD wymaga od administratora bycia w stanie wykazać zgodność. TIA, która nie jest przeprowadzona rzetelnie, niczego nie dowodzi; dowodzi jedynie woli zachowania pozorów zgodności na papierze przy jednoczesnym robieniu czegoś przeciwnego w praktyce.

Szczera wersja TIA zaczyna się od prostego pytania: co by się stało, gdyby jutro do tego dostawcy dotarł nakaz FISA 702 dotyczący tych konkretnych danych? Jeśli uczciwa odpowiedź brzmi: „musiałby je wydać bez powiadamiania nas”, klauzule umowne nie rozwiązują problemu. Tym, co rozwiązuje problem w przypadkach, gdy pytanie to ma rzeczywiste znaczenie, jest niepowierzenie danych temu dostawcy.

Zmiana polityczna jako ryzyko strukturalne

Istnieje dodatkowa warstwa, polityczna, którą warto nazwać bez zbędnego dramatyzmu. Decyzja o adekwatności 2023/1795 opiera się w ostatecznym rozrachunku na rozporządzeniu wykonawczym 14086, podpisanym przez prezydenta Bidena w październiku 2022 roku. Rozporządzenie wykonawcze podpisuje prezydent i może je cofnąć, zmienić lub pozbawić treści jego następca. Ochrona europejskich danych w Stanach Zjednoczonych zależy zatem od decyzji administracyjnej, której ani Kongres amerykański nie gwarantuje, ani amerykański system prawny nie chroni z taką samą siłą, z jaką chroni inne kwestie wewnętrzne. Od stycznia 2025 roku Stanami Zjednoczonymi rządzi nowa administracja, a pytanie o praktyczną ciągłość EO 14086 przestało być hipotezą, stając się kwestią współczesną. Każdy scenariusz, w którym administracja zdecyduje się wycofać lub osłabić to rozporządzenie, pozbawiłby europejską decyzję fundamentu, na którym została zbudowana.

To nie jest argument spiskowy. To trzeźwa analiza konstrukcji prawnej. Transatlantyckie ramy ochrony danych upadły już dwukrotnie: Safe Harbor w 2015 roku (wyrok Schrems I), Privacy Shield w 2020 roku (Schrems II). Trzeci system opiera się na kruchszych podstawach niż jego dwaj poprzednicy. Europejska firma, która opiera dziś przetwarzanie swoich danych na tym fundamencie, podejmuje decyzję z zakresu zarządzania ryzykiem, a nie jedynie zwykłego przestrzegania przepisów.

Dla czytelnika profesjonalnego

Pytania operacyjne, które warto sobie zadać przed wyborem usługi chmurowej dla danych profesjonalnych — z taką rzetelnością, z jaką postawiłby je inspektor ochrony danych — są następujące:

1. Gdzie dane są fizycznie przechowywane? Region europejski nie jest wystarczającą odpowiedzią, jeśli operatorem jest firma amerykańska.
2. Kto obsługuje usługę, w jakiej jurysdykcji jest ona zarejestrowana i jakim nakazom prawnym może zostać poddana?
3. Na jaki instrument transferu powołuje się dostawca: decyzję o adekwatności 2023/1795, SCC wraz z TIA, czy odstępstwo z artykułu 49 RGPD? Czy wybór ten jest do obrony podczas kontroli?
4. Gdyby decyzja o adekwatności upadła jutro, jaki plan operacyjny istnieje w celu utrzymania ciągłości działania?
5. Czy istnieje europejska lub własna (self-hosted) alternatywa dla danej funkcji i jaki byłby rzeczywisty koszt migracji?

Nie wszystkie funkcje codziennej pracy biurowej wymagają takiej samej odpowiedzi. Arkusz kalkulacyjny do wewnętrznej księgowości prawdopodobnie nie podnosi pytania na ten poziom. Akta karne klienta, historia choroby, listy płac pracowników — już tak. Proporcjonalność jest uzasadniona; zbiorowa inercja, z jaką europejskie MŚP pozostały przy amerykańskich dostawcach we wszystkim — nawet w kwestiach najbardziej wrażliwych — już nie.

Schrems II kończy sześć lat w lipcu tego roku. Wyrok nie zmienił codziennych nawyków większości europejskich firm. Zmienił jednak mapę ryzyk, na które te firmy są narażone. Gdy amerykańska decyzja administracyjna staje pomiędzy europejskim rozporządzeniem a rzeczywistym działaniem MŚP, warto przynajmniej wiedzieć, że ta decyzja istnieje i że jest krucha. Ci z nas, którzy wybrali architekturę bez pośrednika — wątek przewodni Cuadernos Lacre — woleliby nie musieć pisać tego rodzaju analiz za każdym razem, gdy jakiś Schrems postanawia złożyć odwołanie. Będziemy jednak nadal to robić.

Nota redakcyjna: gdy te Cuadernos wymieniają firmy lub produkty, nie robią tego, by oskarżać. Ci, którzy je tworzą, wykonują pracę, z której korzystają i którą doceniają miliony ludzi. To, na co wskazujemy, ma charakter strukturalny — model, a nie marka. Marki pojawiają się jako przykłady, ponieważ są rozpoznawalne dla czytelnika.

Źródła i dodatkowa lektura

- Trybunał Sprawiedliwości Unii Europejskiej — wyrok z 16 lipca 2020 r., sprawa C-311/18, *Data Protection Commissioner przeciwko Facebook Ireland Ltd i Maximillian Schrems*.
- Rozporządzenie (UE) 2016/679, rozdział V, artykuły 44–50 — międzynarodowe przekazywanie danych osobowych.
- Decyzja wykonawcza Komisji (UE) 2023/1795 z dnia 10 lipca 2023 r. w sprawie odpowiedniego stopnia ochrony danych osobowych w ramach EU-US Data Privacy Framework.
- Europejska Rada Ochrony Danych — *Recommendations 01/2020 w sprawie środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych*, przyjęte 18 czerwca 2021 r.
- noyb.eu — skarga złożona 7 września 2023 r. przeciwko decyzji (UE) 2023/1795 do europejskich organów ochrony danych.
- *Foreign Intelligence Surveillance Act*, sekcja 702 (skodyfikowana w 50 U.S.C. § 1881a) oraz rozporządzenie wykonawcze (Executive Order) 12333 dotyczące amerykańskich działań wywiadowczych poza terytorium kraju.

[← Poprzedni](#) [Gdy nie ma nikogo pośrodku](#) [Następny](#) → [Czym naprawę jest SHA-256](#)

Ostatnie lektury

- [Analiza · 18 maja 2026 Prywatność rzeczywista vs pozorna: pytania, które warto sobie zadać](#)
- [Analiza · 18 maja 2026 Self-hosting jako praktyka zawodowa](#)
- [Koncepcja · 18 maja 2026 24 słowa: czym jest tożsamość kryptograficzna](#)

Zabierz ten artykuł tam, gdzie go potrzebujesz.

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

Plik zostanie pobrany na Twoje urządzenie. Stamtąd możesz go zapisać, zaimportować do Solo2 lub udostępnić w dowolnym miejscu. Cuadernos nie decyduje o miejscu docelowym za Ciebie.

Pieczeń lakowa · SHA-256 d550a8848f363496d5cb39611e245eb3e04dc5a53d603b51a80b241304fad01a

Cuadernos Lacre · Publikacja [Menzuri Gestión S.L.](#) ·
napisana przez R.Eugenio · redagowana przez zespół [Solo2](#).

Ta strona nie używa plików cookie i nie ładuje zasobów stron trzecich. Korzysta z anonimowego licznika odwiedzin (Umami, na naszym europejskim serwerze) i minimalnej ilości JavaScript niezbędnej dla dwóch elementów sterujących w nagłówku: motywu jasnego lub ciemnego i wyboru języka. Bez trackerów, bez profilowania, bez udostępniania danych. Jeśli chcesz nas śledzić: [RSS](#).