Аналіз · 18 травня 2026

← Попередній·Наступний →

Schrems II через п'ять років

Судове рішення, яке змінило право міжнародної передачі персональних даних. П'ять років потому значна частина повсякденної європейської офісної роботи продовжує функціонувати так, ніби нічого не сталося.

Судове рішення, якому знадобилося три години, щоб змінити правила

16 липня 2020 року, близько десятої п'ятнадцяти ранку за часом Люксембургу, Суд Європейського Союзу оприлюднив рішення у справі C-311/18. Протягом наступних трьох годин правовий режим, який підтримував щоденну передачу персональних даних з Європи до Сполучених Штатів —так званий «Щит конфіденційності» (Privacy Shield) — припинив своє існування. Коли європейські спеціалісти із захисту даних закінчили свій обід того дня, рамки, за якими працювали їхні компанії та адміністрації, більше не діяли.

Це судове рішення сьогодні відоме як Schrems II на честь Максиміліана Шремса, австрійського активіста, чия скарга проти Facebook Ireland спричинила його. Скарга, зокрема, стосувалася передачі даних між Facebook Ireland та Facebook USA. Рішення, в цілому, йде набагато далі: воно диктує, як і за яких умов будь-які персональні дані, зібрані на території Європи, можуть потрапити до Сполучених Штатів.

Майже через шість років існує рамка на заміну —EU-US Data Privacy Framework, ухвалена в липні 2023 року — і вона також перебуває під юридичним тиском. Готується новий раунд Шремса. Тим часом європейський малий та середній бізнес продовжує використовувати американські хмарні сервіси для повсякденних завдань, здебільшого не знаючи, що юридичне питання, на якому ґрунтуються ці сервіси, все ще залишається відкритим.

Про що саме йшлося в Schrems II

Судове рішення ґрунтується на трьох частинах. Перша — Хартія основних прав Європейського Союзу, зокрема її статті 7 (приватне та сімейне життя), 8 (захист персональних даних) та 47 (ефективний судовий захист). Друга — Загальний регламент про захист даних —GDPR, який багато європейців пам'ятають лише за повідомленнями про файли cookie — зокрема його розділ V, статті 44–50, про міжнародну передачу даних. Третя — американське розвідувальне законодавство: розділ 702 Закону про нагляд за іноземною розвідкою (Foreign Intelligence Surveillance Act), FISA 702 юридичною мовою, та Виконавчий указ президента 12333.

Суд діяв за принципом контрасту. Хартія основних прав вимагає, щоб персональні дані європейських громадян, коли вони залишають Союз, користувалися рівнем захисту, по суті еквівалентним тому, що гарантується GDPR. Відповідно, питання полягало в тому, чи пропонують Сполучені Штати цей по суті еквівалентний рівень.

Відповідь була негативною, і не через нюанси. FISA 702 дозволяє уряду США збирати повідомлення осіб, які не є американцями та перебувають за межами національної території, без попереднього

індивідуального судового дозволу, без повідомлення зацікавленої особи та без ефективного засобу захисту, порівнянного з європейським. Виконавчий указ 12333 розширює цю можливість аналогічним чином за межами національної території. Суд дійшов висновку, що європейський громадянин перед американською правовою системою не має по суті еквівалентного захисту, якого вимагає Хартія. Таким чином, еквівалентності не існує.

Звідси прямий наслідок: рішення Європейської комісії 2016/1250, яке підтвердило Privacy Shield як адекватну базу для передачі, було визнано недійсним. Будь-яка передача, що ґрунтувалася виключно на цій базі, втратила юридичне обґрунтування з того самого моменту.

Що все ж таки вижило (і за яких умов)

Schrems II не усунув усі інструменти. Стандартні договірні умови —SCC за англійською абревіатурою Standard Contractual Clauses — вижили. Це типові контракти, схвалені Європейською комісією: європейський експортер та імпортер з країни призначення підписують їх, зобов'язуючись обробляти дані відповідно до європейських стандартів. Компанія, яка вважала, що вирішила проблему 17 липня 2020 року, підписала SCC зі своїм постачальником і була задоволена.

Дискомфорт з'явився при повільному читанні судового рішення. Суд чітко дав зрозуміти, що SCC залишаються чинними, але їхня дійсність залежить від умови, яку варто підкреслити: щоб імпортер даних міг виконувати їх на практиці. Якщо національне законодавство країни призначення заважає йому виконувати ці умови —оскільки, наприклад, наказ згідно з FISA 702 змушує його надавати дані без повідомлення європейського контрагента — умови насправді не захищають. І тоді, каже суд, європейський експортер повинен припинити передачу.

Це ввело новий об'єкт у європейську практику захисту даних: Transfer Impact Assessment, або оцінка впливу передачі, відома за англійською абревіатурою TIA. Кожного разу, коли європейська компанія хоче передати дані до Сполучених Штатів під егідою SCC, вона повинна формально оцінити, чи може одержувач виконувати ці умови з огляду на законодавство, що до нього застосовується. Європейська рада із захисту даних (EDPB) опублікувала детальні вказівки щодо проведення TIA. Чесна практика зазвичай дає той самий результат: якщо імпортером є американська дочірня компанія хмарного гіганта, щира відповідь на TIA полягає в тому, що умови не можуть бути виконані так, як вони прописані.

Privacy Framework та очікуване рішення Schrems III

10 липня 2023 року Європейська комісія ухвалила нове рішення про адекватність: 2023/1795. Воно замінює покійний Privacy Shield і працює під назвою EU-US Data Privacy Framework. Раніше Сполучені Штати змінили свій внутрішній режим за допомогою Виконавчого указу (Executive Order) 14086, який обмежує обсяг радіотехнічної розвідки тим, що є «необхідним і пропорційним» —термінологія, знайома європейському читачеві, але не дуже поширена в американській адміністративній практиці — і створює орган з перегляду під назвою Data Protection Review Court (DPRC). Комісія визнала, що цих змін достатньо для відновлення суттєво еквівалентного рівня захисту.

Організація noyb, заснована Шремсом, 7 вересня 2023 року подала скаргу проти нового рішення. Аргументи очікувані: DPRC не є незалежним судом у розумінні статті 47 Хартії; поняття «необхідне і пропорційне» не перекладають механічно європейські стандарти; і, нарешті, захист, що ґрунтується на Виконавчому указі, може бути скасований наступним Виконавчим указом. Рішення CJEU щодо нового рішення —яке багато хто вже називає Schrems III з певною смиренністю — очікується в найближчі роки. Результат неможливо передбачити. У будь-якому випадку, структура аргументу дуже нагадує структуру 2020 року.

Те, чого не чує європейський малий бізнес

Поки велика палата CJEU радиться, адвокатське бюро середнього розміру продовжує обмінюватися листуванням зі своїми клієнтами через Microsoft 365, розміщений у європейських регіонах, але такий, що належить американській компанії, що підпадає під дію FISA 702. Приватна медична консультація синхронізує розклади через Google Workspace. Податковий консультант надсилає підписані декларації через DocuSign. Психолог виставляє рахунки за допомогою електронної таблиці в Notion. Трудове бюро архівує справи в Dropbox. І практично всі вони, до того ж, обслуговують своїх клієнтів через WhatsApp. Все це може працювати під егідою рішення про адекватність 2023/1795, за словами постачальників. У той день, коли це рішення впаде в Schrems III, усі ці відносини залишаться без захисту в ту ж секунду.

Питання не є риторичним. У період з 2022 по 2024 рік кілька європейських органів влади вирішили справи проти контролерів даних за використання Google Analytics без відповідного інструменту передачі, буквально застосовуючи аргументацію CJEU ще до того, як Privacy Framework набрав чинності. Французький орган влади, CNIL, був першим, хто офіційно закріпив цей критерій у 2022 році; австрійські, італійські та інші органи влади послідували невдовзі. Недотримання вимог у нинішньому оперативному дизайні європейських малих та середніх підприємств документується в режимі реального часу для тих, хто знає, куди дивитися.

TIA як інструмент, а не як ритуал

Значна частина TIA, що циркулюють в європейських офісах, при уважному читанні є формальними вправами. Вони перераховують договірні інструменти, сертифікати постачальника, цитують технічні гарантії, ставлять галочку. Мало хто серйозно запитує, чи змусить наказ FISA 702 постачальника надати дані. Ще менше запитують, що станеться з цією передачею за умови гіпотетичного перегляду Privacy Framework. Стаття 5 GDPR вимагає від контролера даних бути здатним продемонструвати відповідність. TIA, яка не робиться всерйоз, нічого не демонструє; вона лише демонструє бажання відповідати вимогам на папері, роблячи протилежне на практиці.

Щира версія TIA починається з простого запитання: що сталося б, якби завтра цьому постачальнику надійшов наказ FISA 702 щодо цих конкретних даних? Якщо щира відповідь «він повинен був би надати їх, не попередивши нас», договірні умови не вирішують проблему. Те, що дійсно вирішує її у випадках, коли це питання справді важливе, — це те, що дані не були передані в руки цього постачальника.

Політичні зміни як структурний ризик

Є ще додатковий рівень, політичний, про який варто згадати без зайвого драматизму. Рішення про адекватність 2023/1795 ґрунтується, зрештою, на Виконавчому указі 14086, підписаному президентом Байденом у жовтні 2022 року. Виконавчий указ підписує один президент, і його може скасувати, змінити або позбавити змісту наступний. Таким чином, захист європейських даних у Сполучених Штатах залежить від адміністративного рішення, яке ні американський Конгрес не гарантує, ні американська правова система не захищає з тією міцністю, з якою вона захищає інші внутрішні справи. З січня 2025 року США керує нова адміністрація, і питання про практичну спадкоємність EO 14086 перестало бути гіпотезою і стало сучасністю. Будь-який сценарій, за якого адміністрація вирішить відкликати або пом'якшити указ, залишить європейське рішення без тієї деталі, на якій воно було побудоване.

Це не конспірологічний аргумент. Це тверезе прочитання правового дизайну. Трансатлантичні рамки захисту даних вже руйнувалися двічі: Safe Harbor у 2015 році (рішення Schrems I), Privacy Shield у 2020 році (Schrems II). Третій ґрунтується на більш крихкій деталі, ніж два попередні. Європейська компанія, яка сьогодні ставить свою обробку даних на цю деталь, приймає рішення про управління ризиками, а не про просте дотримання нормативних вимог.

Для професійного читача

Оперативні запитання, які варто поставити собі перед вибором хмарного сервісу для професійних даних —з тією суворістю, з якою їх поставив би інспектор із захисту даних — наступні:

1. Де фізично зберігаються дані? Європейського регіону недостатньо як відповіді, якщо оператор є американським.
2. Хто керує сервісом, у якій юрисдикції він зареєстрований і яким законним наказам він може підпорядковуватися?
3. Який інструмент передачі використовується: рішення про адекватність 2023/1795, SCC з TIA, виключення статті 49 GDPR? Чи можна захистити цей вибір під час перевірки?
4. Якщо завтра рішення про адекватність буде скасовано, який існуючий оперативний план для підтримки діяльності?
5. Чи існує європейська альтернатива або можливість самостійного хостингу для цієї функції, і якою буде реальна вартість міграції?

Не всі функції повсякденної офісної роботи вимагають однакової відповіді. Електронна таблиця для внутрішньої бухгалтерії, ймовірно, не піднімає питання до такого рівня. Кримінальна справа клієнта, медична картка, нарахування заробітної плати працівникам — так. Пропорційність є легітимною; колективна інерція, з якою європейський малий бізнес залишався з американськими постачальниками для всього —навіть для найбільш делікатних речей — ні.

У липні цього року виповнюється шість років рішенню Schrems II. Це судове рішення не змінило повсякденних звичок більшості європейських компаній. Натомість воно змінило карту ризиків, на які ці компанії наражаються. Коли адміністративне рішення США постає між європейським регламентом і реальною роботою малого чи середнього підприємства, варто принаймні знати, що це рішення існує і що воно є крихким. Ті з нас, хто обрав архітектуру без посередника —шлях, яким іде Cuadernos Lacre— воліли б не писати такі аналізи щоразу, коли черговий Шремс сідає подавати апеляцію. Але ми продовжуватимемо це робити.

Джерела та додаткова література

- Суд Європейського Союзу — рішення від 16 липня 2020 року, справа C-311/18, *Data Protection Commissioner проти Facebook Ireland Ltd та Maximillian Schrems*.
- Регламент (ЄС) 2016/679, розділ V, статті 44–50 — міжнародна передача персональних даних.
- Імплементаційне рішення Комісії (ЄС) 2023/1795 від 10 липня 2023 року про адекватний рівень захисту персональних даних у межах EU-US Data Privacy Framework.
- Європейська рада із захисту даних — *Рекомендації 01/2020 щодо заходів, які доповнюють інструменти передачі для забезпечення відповідності рівню захисту персональних даних в ЄС*, ухвалені 18 червня 2021 року.
- noyb.eu — скарга, подана 7 вересня 2023 року проти рішення (ЄС) 2023/1795 до європейських органів захисту даних.
- *Foreign Intelligence Surveillance Act*, розділ 702 (кодифікований у 50 U.S.C. § 1881a), та Виконавчий указ 12333 про розвідувальну діяльність США за межами національної території.

← ПопереднійКоли посередині нікого немаєНаступний →Що насправді таке SHA-256

Останні матеріали

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Візьміть цю статтю з собою куди завгодно.

↓ Markdown ↓ Звичайний текст ↓ PDF

Файл буде завантажено на ваш пристрій. Звідти ви можете зберегти його, імпортувати в Solo2 або поділитися ним де завгодно. Cuadernos не вирішує місце призначення за вас.

Сургучна печатка · SHA-256 ec98ab466356b0f859af69c817b78738d941f86fd3767d5167e98711df13d3e7

Cuadernos Lacre · Видання Menzuri Gestión S.L. ·
автор R.Eugenio · під редакцією команди Solo2.