

Schrems II, пять лет спустя

Решение, изменившее право в области международной передачи персональных данных. Пять лет спустя значительная часть повседневной работы в Европе продолжается так, будто ничего не произошло.

Решение, которое за три часа изменило правила

16 июля 2020 года около десяти пятнадцати утра по люксембургскому времени Суд Европейского союза обнародовал решение по делу C-311/18. В течение следующих трех часов правовой режим, обеспечивавший ежедневную передачу персональных данных из Европы в США — так называемый «Щит конфиденциальности» (Privacy Shield в официальном названии) — прекратил свое существование. Когда в тот день европейские специалисты по защите данных закончили обедать, рамки, в которых работали их компании и ведомства, уже не действовали.

Решение сегодня известно как Schrems II в честь Максимилиана Шремса, австрийского активиста, чья жалоба против Facebook Ireland послужила толчком к судебному разбирательству. Жалоба конкретно касалась передачи данных между Facebook Ireland и Facebook US. Решение в целом идет гораздо дальше: оно диктует, как и на каких условиях любые персональные данные, собранные на территории Европы, могут передаваться в США.

Спустя почти шесть лет существует заменяющая база — EU-US Data Privacy Framework, принятая в июле 2023 года, — и она также находится под юридическим давлением. Готовится новый раунд «дела Шремса». Тем временем малый и средний европейский бизнес продолжает использовать американские облачные сервисы для повседневных задач, в большинстве своем не подозревая, что юридический вопрос, на котором основываются эти сервисы, остается открытым.

Что именно говорилось в Schrems II

Решение опирается на три составляющие. Первая — Хартия Европейского союза об основных правах, в частности ее статьи 7 (уважение частной и семейной жизни), 8 (защита персональных данных) и 47 (право на эффективное средство правовой защиты). Вторая — Хартия Европейского союза об основных правах, в частности ее статьи 7 (уважение частной и семейной жизни), 8 (защита персональных данных) и 47 (право на эффективное средство правовой защиты). Третья — Общий регламент по защите данных (RGPD/GDPR), который многие европейцы помнят только по уведомлениям о файлах cookie, — конкретно его глава V, статьи 44–50, о международной передаче данных. Четвертая — американское законодательство о разведке: раздел 702 Закона о надзоре за иностранными разведками (FISA 702 на юридическом жаргоне) и президентский указ № 12333.

Суд действовал методом противопоставления. Хартия об основных правах требует, чтобы персональные данные европейских граждан при выезде за пределы Союза пользовались уровнем защиты, по существу эквивалентным уровню, гарантированному RGPD. Соответственно, вопрос заключался в том, предлагают ли США такой по существу эквивалентный уровень.

Ответ был отрицательным, причем не из-за нюансов. FISA 702 позволяет правительству США собирать сообщения лиц, не являющихся гражданами США и находящихся за пределами национальной территории, без предварительного индивидуального судебного разрешения, без уведомления пострадавшего лица и без эффективного средства правовой защиты, сопоставимого с европейским. Указ № 12333 аналогичным образом расширяет эти возможности за пределами национальной территории. Суд пришел к выводу, что европейский гражданин перед лицом американской правовой системы не располагает по существу эквивалентной защитой, которой требует Хартия. Таким образом, эквивалентность отсутствует.

Отсюда прямое следствие: решение Европейской комиссии 2016/1250, признавшее Privacy Shield адекватной основой для передачи данных, было признано недействительным. Любая передача данных, основанная исключительно на этой базе, в тот же миг осталась без правовых оснований.

Что выжило (и на каких условиях)

Schrems II не уничтожил все инструменты. Стандартные договорные условия (SCC на международном жаргоне, от английского Standard Contractual Clauses) выжили. Это типовые контракты, утвержденные Европейской комиссией: европейский экспортер и импортер из страны назначения подписывают их, обязуясь обрабатывать данные в соответствии с европейским стандартом. Компания, решившая, что проблема была решена 17 июля 2020 года, подписала SCC со своим поставщиком и осталась довольна.

Дискомфорт возник при внимательном прочтении решения. Суд ясно дал понять, что SCC остаются в силе, но их действительность зависит от условия, которое стоит подчеркнуть: чтобы импортер данных мог выполнять их на практике. Если национальное законодательство страны назначения мешает ему выполнять условия — например, потому что приказ в рамках FISA 702 обязывает его выдать данные без уведомления своего европейского контрагента, — условия на самом деле не защищают. И тогда, говорит суд, европейский экспортер должен приостановить передачу.

Это ввело новый объект в европейскую практику защиты данных: Transfer Impact Assessment, или оценку воздействия передачи, известную под английской аббревиатурой TIA. Каждый раз, когда европейская компания хочет передать данные в США на основании SCC, она должна официально оценить, может ли получатель выполнять условия договора с учетом применяемого к нему законодательства. Европейский совет по защите данных (EDPB) опубликовал подробные рекомендации по проведению TIA. Честная практика обычно дает один и тот же результат: если импортер является американским филиалом облачного гиганта, искренний ответ на TIA заключается в том, что условия не могут быть выполнены в том виде, в котором они написаны.

Privacy Framework и предстоящий Schrems III

10 июля 2023 года Европейская комиссия приняла новое решение о достаточности (Adequacy Decision) № 2023/1795. Оно заменяет ныне покойный Privacy Shield и действует под названием EU-US Data Privacy Framework. США предварительно изменили свой внутренний режим посредством указа № 14086, который ограничивает сферу деятельности радиоэлектронной разведки рамками «необходимого и соразмерного» — терминология, знакомая европейскому читателю, но не столь привычная для американской административной практики — и создает орган по пересмотру под названием Суд по надзору за защитой данных (DPRC). Комиссия сочла, что этих изменений достаточно для восстановления по существу эквивалентного уровня.

Организация поуб, основанная Шремсом, подала жалобу 7 сентября 2023 года против нового решения. Аргументы вполне ожидаемы: DPRC не является независимым судом в смысле статьи 47 Хартии; понятия «необходимый и соразмерный» не переводят механически европейские стандарты; и, наконец, защита, основанная на президентском указе, может быть отменена следующим указом. Решение TJUE по новому Решению — то, которое многие уже с некоторой обреченностью называют Schrems III —

ожидаются в ближайшие годы. Результат нельзя предвидеть заранее. В любом случае структура аргументации очень напоминает структуру 2020 года.

Чего не слышит европейский малый бизнес

Пока большая палата TJUE совещается, юридическая фирма среднего размера продолжает обмениваться перепиской со своими клиентами через Microsoft 365, размещенный в европейских регионах, но принадлежащий американской компании, подпадающей под действие FISA 702. Частная медицинская клиника синхронизирует графики через Google Workspace. Налоговый консультант отправляет подписанные декларации через DocuSign. Психолог выставляет счета из таблицы в Notion. Адвокатское бюро по трудовым спорам архивирует дела в Dropbox. И практически все они, к тому же, общаются с клиентами через WhatsApp. Все это может работать на основании, по утверждению поставщиков, решения о достаточности № 2023/1795. В тот день, когда это решение падет в рамках Schrems III, все эти отношения останутся без защиты в ту же секунду.

Вопрос не риторический. В период с 2022 по 2024 год несколько европейских органов разрешили дела против операторов за использование Google Analytics без надлежащего инструмента передачи, в буквальном применении логики TJUE еще до вступления в силу Privacy Framework. Французский регулятор, CNIL, был первым, кто официально сформулировал этот критерий в 2022 году; вскоре за ним последовали австрийский, итальянский и другие органы. Несоблюдение правил при нынешней операционной модели европейского малого бизнеса документируется в режиме реального времени для любого, кто знает, куда смотреть.

ТИА как инструмент, а не как ритуал

Значительная часть ТИА, циркулирующих в европейских офисах, при внимательном прочтении представляет собой формальные упражнения. В них перечисляются договорные инструменты, указываются сертификаты поставщика, цитируются технические гарантии, ставится галочка. Мало кто всерьез задается вопросом, заставит ли приказ FISA 702 поставщика выдать данные. Еще меньше задаются вопросом, что произойдет с этой передачей при гипотетическом пересмотре Privacy Framework. Статья 5 RGPD требует от оператора способности доказать соблюдение правил. ТИА, сделанная не всерьез, ничего не доказывает; она доказывает лишь желание соблюдать правила на бумаге, делая обратное на практике.

Искренняя версия ТИА начинается с простого вопроса: что произойдет, если завтра этому поставщику поступит приказ FISA 702 в отношении этих конкретных данных? Если честный ответ — «ему придется выдать их, не уведомляя нас», то условия договора не решают проблему. Что ее действительно решает в тех случаях, когда вопрос действительно важен, так это отсутствие передачи данных в руки этого поставщика.

Политическое изменение как структурный риск

Есть еще один слой, политический, о котором стоит упомянуть без драматизма. Решение о достаточности № 2023/1795 в конечном счете опирается на указ № 14086, подписанный президентом Байденом в октябре 2022 года. Президентский указ подписывается одним президентом и может быть отменен, изменен или лишен содержания следующим. Таким образом, защита европейских данных в США зависит от административного решения, которое ни Конгресс США не гарантирует, ни правовая система США не защищает с той прочностью, с которой она защищает другие внутренние вопросы. С января 2025 года в США правит новая администрация, и вопрос о практической преемственности указа № 14086 перестал быть гипотезой и стал реальностью. Любой сценарий, при котором администрация решит отозвать или смягчить указ, оставит европейское решение без той основы, на которой оно было построено.

Это не конспирологический аргумент. Это трезвое прочтение юридической конструкции. Трансатлантические рамки защиты данных уже рушились дважды: Safe Harbor в 2015 году (решение Schrems I), Privacy Shield в 2020 году (Schrems II). Третья попытка опирается на более хрупкую деталь, чем две предыдущие. Европейская компания, которая сегодня делает ставку на эту конструкцию при обработке данных, принимает управленческое решение о рисках, а не просто решение о соблюдении норм.

Для профессионального читателя

Операционные вопросы, которые стоит задать перед выбором облачного сервиса для профессиональных данных — с той строгостью, с которой их задал бы инспектор по защите данных, — следующие:

1. Где физически хранятся данные? Ссылки на европейский регион недостаточно, если оператор американский.
2. Кто управляет сервисом, в какой юрисдикции он зарегистрирован и каким судебным приказам может быть подчинен?
3. Какой инструмент передачи используется: решение о достаточности № 2023/1795, SCC с TIA, исключение из статьи 49 RGPD? Можно ли защитить этот выбор в ходе проверки?
4. Если решение о достаточности завтра падет, какой оперативный план существует для поддержания деятельности?
5. Существует ли европейская или автономная альтернатива для этой функции и какова будет реальная стоимость миграции?

Не все повседневные офисные задачи требуют одинакового ответа. Электронная таблица для внутренней бухгалтерии, вероятно, не поднимает вопрос на этот уровень. Уголовное дело клиента, история болезни, ведомость заработной платы сотрудников — да. Пропорциональность законна; коллективная инерция, с которой европейский малый бизнес остается у американских поставщиков во всем — даже в самом конфиденциальном, — нет.

В июле этого года исполняется шесть лет со дня вынесения решения по делу Schrems II. Решение не изменило повседневных привычек большинства европейских компаний. Оно, однако, изменило карту рисков, которым эти компании подвергаются. Когда американское административное решение встает между европейским регламентом и реальной деятельностью малого и среднего бизнеса, стоит хотя бы знать, что это решение существует и что оно хрупко. Те из нас, кто выбрал архитектуру без посредника-оператора — нить, проходящую через Cuadernos Lacre, — предпочли бы не писать подобный анализ каждый раз, когда некий Шремс решает подать апелляцию. Но мы продолжим это делать.

Источники и дополнительная литература

- Суд Европейского союза — решение от 16 июля 2020 года, дело C-311/18, *Data Protection Commissioner против Facebook Ireland Ltd. и Максимилиана Шремса*.
- Регламент (ЕС) 2016/679, глава V, статьи 44–50 — международная передача персональных данных.
- Исполнительное решение Комиссии (ЕС) 2023/1795 от 10 июля 2023 года об адекватном уровне защиты персональных данных в рамках EU-US Data Privacy Framework.
- Европейский совет по защите данных — *Рекомендации № 01/2020 о мерах, дополняющих инструменты передачи для обеспечения соблюдения уровня защиты персональных данных в ЕС*, принятые 18 июня 2021 года.
- *poyb.eu* — жалоба, поданная 7 сентября 2023 года против Решения (ЕС) 2023/1795 в европейские органы по защите данных.
- *Foreign Intelligence Surveillance Act*, раздел 702 (кодифицирован в 50 U.S.C. § 1881a), и президентский указ № 12333 о разведывательной деятельности США за пределами национальной территории.

Недавние материалы

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

Возьмите эту статью с собой туда, где она вам понадобится.

[↓ Markdown](#) [↓ Простой текст](#) [↓ PDF](#)

Файл будет загружен на ваше устройство. Оттуда вы можете сохранить его, импортировать в Solo2 или поделиться им где угодно. Cuadernos не решает место назначения за вас.

Сургучная печать · SHA-256 4a71c99f349a13f00895982c8d2b321698d54fcc8a8305ff8a19279bb45abdefe

Cuadernos Lacre · Издание [Menzuri Gestión S.L.](#) ·
текст R.Eugenio · под редакцией команды [Solo2](#).

Этот веб-сайт не использует куки-файлы и не загружает ресурсы сторонних лиц. Он использует анонимный счетчик посещений с собственным хостингом (Umami, на нашем европейском сервере) и минимальный объем JavaScript, необходимый для вашего предпочтения светлой/темной темы. Никаких трекеров, никакого профилирования, никакого обмена данными. Если вы хотите следить за нами: [RSS](#).