Schrems II, fünf Jahre danach

Das Urteil, das das Recht der internationalen Übermittlung personenbezogener Daten veränderte. Fünf Jahre danach arbeitet ein beträchtlicher Teil des europäischen Kanzleialltags weiter, als wäre nichts geschehen.

Das Urteil, das drei Stunden brauchte, um die Regeln zu ändern

Am 16. Juli 2020 gegen Viertel nach zehn Uhr morgens Luxemburger Zeit veröffentlichte der Gerichtshof der Europäischen Union das Urteil in der Rechtssache C-311/18. In den folgenden drei Stunden hörte die Rechtsordnung, die den täglichen Transfer personenbezogener Daten von Europa in die USA stützte — das sogenannte Privacy Shield (Datenschutzschild in seiner offiziellen Bezeichnung) —, auf zu existieren. Als die europäischen Datenschutzbeauftragten an diesem Tag ihr Mittagessen beendeten, war der Rahmen, unter dem ihre Unternehmen und Verwaltungen arbeiteten, nicht mehr gültig.

Das Urteil ist heute als Schrems II bekannt, benannt nach Maximilian Schrems, dem österreichischen Aktivisten, dessen Beschwerde gegen Facebook Ireland es auslöste. Die Beschwerde befasste sich im Konkreten mit den Übermittlungen zwischen Facebook Irland und Facebook USA. Das Urteil geht im Allgemeinen viel weiter: Es schreibt vor, wie und unter welchen Bedingungen personenbezogene Daten, die auf europäischem Territorium erhoben wurden, in die USA gelangen dürfen.

Fast sechs Jahre später existiert der Ersatzrahmen — das im Juli 2023 verabschiedete EU-US Data Privacy Framework — und steht ebenfalls unter juristischem Druck. Eine neue Runde Schrems bereitet sich vor. In der Zwischenzeit nutzen europäische kleine und mittlere Unternehmen weiterhin US-Cloud-Dienste für alltägliche Aufgaben, meist ohne zu wissen, dass die juristische Frage, auf der diese Dienste beruhen, weiterhin offen ist.

Was Schrems II genau besagte

Das Urteil stützt sich auf drei Teile. Der erste ist die Charta der Grundrechte der Europäischen Union, insbesondere die Artikel 7 (Achtung des Privat- und Familienlebens), 8 (Schutz personenbezogener Daten) und 47 (Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht). Der zweite ist die Datenschutz-Grundverordnung — die DSGVO, an die sich viele Europäer nur wegen der Cookie-Banner erinnern —, insbesondere Kapitel V, Artikel 44 bis 50, über Datenübermittlungen in Drittländer. Der dritte ist die US-Geheimdienstgesetzgebung: Abschnitt 702 des Foreign Intelligence Surveillance Act, in der juristischen Fachsprache FISA 702, und die präsidiale Executive Order 12333.

Das Gericht ging nach dem Kontrastprinzip vor. Die Grundrechtecharta verlangt, dass personenbezogene Daten europäischer Bürger beim Verlassen der Union ein Schutzniveau genießen, das dem durch die DSGVO garantierten Niveau im Wesentlichen gleichwertig ist. Die Frage war folglich, ob die USA dieses im Wesentlichen gleichwertige Niveau bieten.

Die Antwort war negativ, und zwar nicht aufgrund von Nuancen. FISA 702 erlaubt es der US-Regierung, Mitteilungen von Nicht-US-Bürgern außerhalb des Staatsgebiets ohne vorherige individuelle gerichtliche Genehmigung, ohne Benachrichtigung der Betroffenen und ohne einen wirksamen Rechtsbehelf, der mit dem europäischen vergleichbar wäre, zu sammeln. Die Executive Order 12333 erweitert diese Kapazität analog

außerhalb des Staatsgebiets. Das Gericht kam zu dem Schluss, dass der europäische Bürger gegenüber dem US-Rechtssystem nicht über den im Wesentlichen gleichwertigen Schutz verfügt, den die Charta verlangt. Die Gleichwertigkeit existiert daher nicht.

Daraus folgte die direkte Konsequenz: Der Beschluss 2016/1250 der Europäischen Kommission, der das Privacy Shield als angemessenen Rahmen für Übermittlungen validiert hatte, wurde für ungültig erklärt. Jede Übermittlung, die sich ausschließlich auf diesen Rahmen stützte, war ab diesem Moment ohne Rechtsgrundlage.

Was überlebte (und unter welchen Bedingungen)

Schrems II hat nicht alle Instrumente eliminiert. Die Standardvertragsklauseln — in der internationalen Fachsprache SCC nach dem englischen Standard Contractual Clauses — überlebten. Es handelt sich um von der Europäischen Kommission genehmigte Musterverträge: Ein europäischer Exporteur und ein Importeur im Bestimmungsland unterzeichnen sie und verpflichten sich, die Daten nach europäischem Standard zu behandeln. Das Unternehmen, das dachte, das Problem am 17. Juli 2020 gelöst zu haben, unterzeichnete SCC mit seinem Anbieter und gab sich zufrieden.

Das Unbehagen kam beim langsamen Lesen des Urteils. Das Gericht stellte klar, dass die SCC weiterhin gültig sind, ihre Gültigkeit jedoch von einer Bedingung abhängt, die man unterstreichen sollte: dass der Importeur der Daten sie in der Praxis einhalten kann. Wenn die nationale Gesetzgebung des Bestimmungslandes ihn daran hindert, die Klauseln einzuhalten — weil ihn beispielsweise eine Anordnung unter FISA 702 dazu verpflichtet, die Daten herauszugeben, ohne seinen europäischen Vertragspartner zu benachrichtigen —, schützen die Klauseln in Wirklichkeit nicht. Und dann, so das Gericht, muss der europäische Exporteur die Übermittlung aussetzen.

Dies führte ein neues Objekt in die europäische Datenschutzpraxis ein: die Transfer Impact Assessment (Transfer-Folgenabschätzung), bekannt unter ihrem englischen Kürzel TIA. Jedes Mal, wenn ein europäisches Unternehmen Daten auf Grundlage von SCC in die USA übermitteln möchte, muss es formell bewerten, ob der Empfänger die Klauseln angesichts der für ihn geltenden Gesetzgebung einhalten kann. Der Europäische Datenschutzausschuss (EDPB) veröffentlichte detaillierte Leitlinien zur Durchführung der TIA. Die ehrliche Praxis führt meist zum selben Ergebnis: Wenn der Importeur eine US-Tochtergesellschaft eines Cloud-Giganten ist, lautet die aufrichtige Antwort auf die TIA, dass die Klauseln so, wie sie geschrieben stehen, nicht eingehalten werden können.

Das Privacy Framework und das ausstehende Schrems III

Am 10. Juli 2023 verabschiedete die Europäische Kommission einen neuen Angemessenheitsbeschluss: 2023/1795. Er ersetzt das verstorbene Privacy Shield und operiert unter dem Namen EU-US Data Privacy Framework. Die USA hatten zuvor ihre interne Regelung durch die Executive Order 14086 geändert, die den Umfang der Signalaufklärung auf das „Notwendige und Angemessene“ beschränkt — eine dem europäischen Leser vertraute Terminologie, weniger jedoch der US-Verwaltungspraxis — und ein Überprüfungsorgan namens Data Protection Review Court (DPRC) schafft. Die Kommission war der Ansicht, dass diese Änderungen ausreichten, um ein im Wesentlichen gleichwertiges Schutzniveau wiederherzustellen.

Die von Schrems gegründete Organisation noyb reichte am 7. September 2023 eine Beschwerde gegen den neuen Beschluss ein. Die Argumente sind erwartbar: Der DPRC ist kein unabhängiges Gericht im Sinne von Artikel 47 der Charta; die Begriffe „notwendig und angemessen“ lassen sich nicht mechanisch in europäische Standards übersetzen; und schließlich kann ein Schutz, der auf einer Executive Order beruht, durch die nächste Executive Order widerrufen werden. Ein Urteil des EuGH über den neuen Beschluss — das viele bereits mit einer gewissen Resignation Schrems III nennen — wird für die nächsten Jahre erwartet. Das Ergebnis lässt sich nicht vorhersagen. Die Struktur des Arguments erinnert jedenfalls stark an die von 2020.

Was das europäische KMU nicht hört

Während die Große Kammer des EuGH berät, tauscht die mittelgroße Anwaltskanzlei weiterhin Korrespondenz mit ihren Mandanten über Microsoft 365 aus, das in europäischen Regionen gehostet wird, aber einem US-Unternehmen gehört, das FISA 702 unterliegt. Die private Arztpraxis synchronisiert Termine über Google Workspace. Der Steuerberater versendet unterschriebene Erklärungen über DocuSign. Der Psychologe rechnet über eine Tabellenkalkulation in Notion ab. Die Arbeitsrechtskanzlei archiviert Akten in Dropbox. Und praktisch alle von ihnen betreuen ihre Kunden zusätzlich über WhatsApp. All dies kann nach Angaben der Anbieter auf Grundlage des Angemessenheitsbeschlusses 2023/1795 betrieben werden. An dem Tag, an dem dieser Beschluss in Schrems III fällt, stehen all diese Beziehungen im selben Moment im Freien.

Die Frage ist nicht rhetorisch. Zwischen 2022 und 2024 entschieden mehrere europäische Behörden Verfahren gegen Verantwortliche wegen der Nutzung von Google Analytics ohne angemessenes Übermittlungsinstrument, in wörtlicher Anwendung der Argumentation des EuGH, noch bevor das Privacy Framework in Kraft trat. Die französische Behörde CNIL war 2022 die erste, die das Kriterium formalisierte; die österreichischen, italienischen und andere Behörden folgten kurz darauf. Die Nichteinhaltung wird unter dem aktuellen operativen Design des europäischen KMU in Echtzeit für jeden dokumentiert, der hinzusehen weiß.

Die TIA als Instrument, nicht als Ritual

Ein beträchtlicher Teil der TIA, die in europäischen Kanzleien zirkulieren, sind bei aufmerksamer Lektüre formale Übungen. Sie listen die vertraglichen Instrumente auf, zählen die Zertifizierungen des Anbieters auf, zitieren die technischen Garantien, setzen das Häkchen. Nur wenige fragen sich ernsthaft, ob eine Anordnung nach FISA 702 den Anbieter zur Herausgabe der Daten zwingen würde. Noch weniger fragen sich, was mit dieser Übermittlung im Falle einer hypothetischen Revision des Privacy Framework passieren würde. Artikel 5 der DSGVO verlangt vom Verantwortlichen den Nachweis der Einhaltung. Eine TIA, die nicht ernsthaft durchgeführt wird, beweist nichts; was sie beweist, ist der Wille, auf dem Papier die Vorschriften einzuhalten, während in der Praxis das Gegenteil getan wird.

Die aufrichtige Version der TIA beginnt mit einer einfachen Frage: Was würde passieren, wenn morgen eine Anordnung nach FISA 702 bezüglich dieser spezifischen Daten bei diesem Anbieter eingehen würde? Wenn die ehrliche Antwort lautet „er müsste sie herausgeben, ohne uns zu benachrichtigen“, lösen die Vertragsklauseln das Problem nicht. Was es jedoch löst, in den Fällen, in denen die Frage wirklich wichtig ist, ist, die Daten gar nicht erst in die Hände dieses Anbieters gegeben zu haben.

Politischer Wandel als strukturelles Risiko

Es gibt eine zusätzliche politische Ebene, die man ohne Dramatik benennen sollte. Der Angemessenheitsbeschluss 2023/1795 beruht letztendlich auf der Executive Order 14086, die im Oktober 2022 von Präsident Biden unterzeichnet wurde. Eine Executive Order wird von einem Präsidenten unterzeichnet und kann vom nächsten widerrufen, geändert oder inhaltlich ausgehöhlt werden. Der Schutz europäischer Daten in den USA hängt somit von einer administrativen Entscheidung ab, die weder der amerikanische Kongress garantiert noch das amerikanische Rechtssystem mit der Solidität schützt, mit der es andere interne Angelegenheiten schützt. Seit Januar 2025 regiert eine neue Administration die USA, und die Frage nach der praktischen Kontinuität der EO 14086 ist keine Hypothese mehr, sondern Gegenwart. Jedes Szenario, in dem die Administration beschließt, die Order zurückzuziehen oder abzuschwächen, würde den europäischen Beschluss des Kernstücks berauben, auf dem er aufgebaut wurde.

Dies ist kein verschwörungstheoretisches Argument. Es ist die nüchterne Lesart des rechtlichen Designs. Die transatlantischen Datenschutzrahmen sind bereits zweimal gefallen: das Safe Harbor 2015 (Schrems I-Urteil), das Privacy Shield 2020 (Schrems II). Das dritte beruht auf einem fragileren Stück als seine beiden Vorgänger.

Ein europäisches Unternehmen, das heute seine Datenverarbeitung auf dieses Stück setzt, trifft eine Entscheidung des Risikomanagements, nicht nur der bloßen Einhaltung von Vorschriften.

Für den professionellen Leser

Die operativen Fragen, die man sich vor der Wahl eines Cloud-Dienstes für berufliche Daten stellen sollte — mit der Strenge, mit der ein Datenschutzprüfer sie stellen würde —, sind folgende:

1. Wo werden die Daten physisch gespeichert? Eine europäische Region ist keine ausreichende Antwort, wenn der Betreiber US-amerikanisch ist.
2. Wer betreibt den Dienst, in welcher Rechtsordnung ist er ansässig und welchen rechtlichen Anordnungen kann er unterworfen werden?
3. Welches Übermittlungsinstrument wird herangezogen: Angemessenheitsbeschluss 2023/1795, SCC mit TIA, Ausnahme nach Artikel 49 der DSGVO? Ist diese Wahl bei einer Prüfung vertretbar?
4. Falls der Angemessenheitsbeschluss morgen fallen würde, welcher operative Plan existiert, um die Tätigkeit aufrechtzuerhalten?
5. Gibt es eine europäische oder selbstgehostete Alternative für diese Funktion, und was wären die tatsächlichen Kosten für eine Migration?

Nicht alle Funktionen des Kanzleialltags erfordern dieselbe Antwort. Eine Tabellenkalkulation für die interne Buchhaltung hebt die Frage wahrscheinlich nicht auf dieses Niveau. Die Strafakte eines Mandanten, die Krankenakte, die Gehaltsabrechnung der Mitarbeiter hingegen schon. Verhältnismäßigkeit ist legitim; die kollektive Trägheit, mit der das europäische KMU bei US-Anbietern für alles geblieben ist — selbst für das Sensibelste —, ist es nicht.

Schrems II wird in diesem Juli sechs Jahre alt. Das Urteil hat die Alltagsgewohnheiten der meisten europäischen Unternehmen nicht verändert. Es hat jedoch die Risikolandschaft verändert, der diese Unternehmen ausgesetzt sind. Wenn eine administrative Entscheidung der USA zwischen der europäischen Verordnung und dem tatsächlichen Betrieb eines KMU steht, sollte man zumindest wissen, dass diese Entscheidung existiert und dass sie fragil ist. Diejenigen von uns, die sich für eine Architektur ohne zwischengeschalteten Betreiber entschieden haben — der rote Faden, der sich durch Cuadernos Lacre zieht —, würden es vorziehen, nicht jedes Mal eine solche Analyse schreiben zu müssen, wenn sich ein Schrems hinsetzt, um Rechtsmittel einzulegen. Aber wir werden sie weiterhin erstellen.

Quellen und weiterführende Literatur

- Gerichtshof der Europäischen Union — Urteil vom 16. Juli 2020, Rechtssache C-311/18, *Data Protection Commissioner gegen Facebook Ireland Ltd. und Maximillian Schrems*.
- Verordnung (EU) 2016/679, Kapitel V, Artikel 44 bis 50 — Internationale Übermittlungen personenbezogener Daten.
- Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10. Juli 2023 über das angemessene Schutzniveau für personenbezogene Daten im Rahmen des EU-US Data Privacy Framework.
- Europäischer Datenschutzausschuss — *Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungsinstrumenten zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten*, angenommen am 18. Juni 2021.
- noyb.eu — Beschwerde vom 7. September 2023 gegen den Beschluss (EU) 2023/1795 bei den europäischen Datenschutzbehörden.
- *Foreign Intelligence Surveillance Act*, Abschnitt 702 (kodifiziert in 50 U.S.C. § 1881a), und Executive Order 12333 über US-Geheimdienstaktivitäten außerhalb des Staatsgebiets.

← ZurückWenn niemand dazwischen istWeiter →CUADERNOS_LIST_SHA256_TITLE

Aktuelle Lektüre

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Nehmen Sie diesen Artikel mit, wohin Sie ihn brauchen.

↓ Markdown ↓ Klartext ↓ PDF

Die Datei wird auf Ihr Gerät heruntergeladen. Von dort aus können Sie sie speichern, in Solo2 importieren oder teilen, wo immer Sie möchten. Cuadernos entscheidet nicht über den Zielort für Sie.

Siegellack-Siegel · SHA-256 0e4e06dd4674d9f04cd5b006ae7b05f562e61618cfebe2d8834b4cee25a1c284

Cuadernos Lacre · Eine Publikation von Menzuri Gestión S.L. ·
geschrieben von R.Eugenio · herausgegeben vom Team von Solo2.