ZEITSCHRIFT FÜR DATENSCHUTZ
EDITORIAL
ZD
11/2020

Schrems-II-Urteil des EuGH und die USA: Mehr Licht!

Lesedauer: 8 Minuten

Bei der Debatte um die Folgen der Schrems-II-Entscheidung kommt einem der Spruch des deutschen Juristen und Aufklärers *Adolph Freiherr v. Knigge* (1752–1796) in den Sinn: „Man vergesse nicht, dass das, was wir Aufklärung nennen, anderen vielleicht als Verfinsterung scheint." Zu der in der ZD ausführlich dargestellten *EuGH*-Entscheidung Schrems II (ZD 2020, 511 m. Anm. *Moos/Rothkegel*) haben sich so gut wie alle Datenschutzbehörden mindestens einmal geäußert. Hinzu kommen die zahlreichen Beiträge hier in der ZD, im Beck-Blog und in den gedruckten Medien, Web-Postings, Memos von Anwaltskanzleien, Stellungnahmen von *Schrems* selbst usw.

101 Dalmatiner gepostet, aber sonst wenig passiert

Wirklich passiert ist seitdem herzlich wenig – zum Leidwesen von *Schrems* und seinen Mitstreitern. Darüber können auch die putzigen 101 Dalmatiner auf der Webseite der von *Schrems* gegründeten Organisation *NOYB* („None of your business") schwer hinwegtäuschen – stellvertretend für 101 von *NYOB* bei allen Datenschutzbehörden in der EU gezielt eingereichten Beschwerden. Nach dem Säbelrasseln der Datenschützer aus Berlin hat sich der *LfDI Baden-Württemberg* mit konkreten, aber leider wenig praxisreifen Vorschlägen aus der Deckung gewagt. In Deutschland finden es manche Kommentatoren unverantwortlich, dass der *EuGH* dieses politische Thema auf die Wirtschaft überwälzt (u.a. *Hansch*, DSB 2020, 212). Der *EuGH* moniert Lücken im Rechtsschutz für die EU-Bürger bei Überwachungsmaßnahmen in den USA. *Härting* hat in seinem NJW-Editorial v. 24.8.2020 auf die „Ironie" hingewiesen, dass Europäer sich gegenüber europäischen Nachrichtendiensten weder auf die DS-GVO noch auf die Grundrechte-Charta berufen können. Wie wird wohl die vom *EuGH* gewollte fallbezogene Risikoanalyse der EU-Datenexporteure für Großbritannien ab dem 1.1.2021 ausfallen? Kommt es noch in der 90. Minute des BREXIT-Finales zu einer Einigung über die Angemessenheit des Datenschutzes?

Dr. Axel Spies
ist Rechtsanwalt bei Morgan, Lewis & Bockius LLP in Washington DC und Mitherausgeber der ZD.

Manche bringen vor, die Schrems-II-Entscheidung sei für die Europäer ein Gewinn, weil nunmehr deren Daten in der EU abgespeichert würden. Das ist Augenwischerei.

- Erstens lassen sich Dienstleister in den meisten Fällen nicht wie Schuhe wechseln. Am Datenstrom ändert sich deshalb mittelfristig nicht viel.
- Zweitens gibt es in den meisten Fällen der EU-Speicherung doch einen Zugriff aus den USA (z.B. bei konzerninternen Datenbasen), was auch *NOYB* messerscharf erkannt hat.
- Drittens sind die propagierten EU-Cloud-Lösungen noch nicht so weit.

Die *Bundesregierung* hat in ihrer Antwort auf eine Kleine Anfrage v. 14.7.2020 zum Projekt GAIA-X verdeutlicht: „GAIA-X ist eine dezentrale, föderale Dateninfrastruktur der nächsten Generation und wird keine eigenständige Cloudlösung im klassischen Sinne sein. Die Bundesregierung hat nicht die Absicht, einen ‚europäischen Cloud-Anbieter' zu entwickeln."

Die neue Initiative der *Telekom* und des französischen Unternehmens *OVHcloud* zu einer europäischen Cloud für sensible Daten wird Zeit brauchen, bis sie verlässlich funktioniert.

Verfinsterung aus Luxemburg?

In den USA haben seit der Ankündigung des *US Department of Commerce*, das Privacy-Shield-Abkommen weiter offen zu halten und Verstöße zu sanktionieren, kaum Unternehmen den Privacy Shield verlassen. Der *EuGH* hat keine Sheriffs ausgesandt, um den Hahn für den Datenfluss in die USA zuzudrehen. Die überlastete *irische Datenschutzbehörde* beabsichtigt eine Suspendierung des US-Datenflusses eines großen Social-Media-Anbieters, aber wann es in Irland zu einer unanfechtbaren Entscheidung kommt, weiß keiner. Manche in den USA sehen auch ohne Tweets aus dem *Weißen Haus* die *EuGH*-Entscheidung als Mittel der EU im Kampf um Märkte an. Bei vielen Praktikern ist die Enttäuschung über „Schrems II" groß, weil sich der in den Orkus gesandte Privacy Shield in der Praxis in den drei Jahren seit seinem Bestehen als praxistauglich erwiesen hat. Sicher, es gab einige Schwarze Schafe – Unternehmen, die z.B. wider besseren Wissens mit einer nicht vorhandenen Privacy Shield Compliance geworben haben. Die *Federal Trade Commission (FTC)* hätte noch mehr tun können, um die öffentlich einsehbaren Selbstverpflichtungen des Privacy-Shield-Abkommens durchzusetzen. Aber immerhin hat das Privacy-Shield-Abkommen dazu geführt, dass sich mehr als 5.000 US-Unternehmen freiwillig unter den von der *FTC* beaufsichtigten Privacy Shield begeben haben. Dies hat das Bewusstsein der US-Unternehmen für den behutsamen Umgang mit personenbezogenen Daten aus der EU gestärkt. In vielen Fällen haben die Datenimporteure ihren US-Kunden dieselben Rechte wie den EU-Kunden eingeräumt.

Seit den *Snowden*-Enthüllungen vor sieben Jahren hat sich in den USA einiges im Datenschutz getan. Der CCPA in Kalifornien und die Nichtverlängerungen einiger *NSA*-Überwachungsbe-

fugnisse durch den *Kongress* sind Beispiele dafür (vgl. zum neuen Consumer Privacy Rights Act in Kalifornien *Spies*, ZD-Aktuell 2020, 04414). Gegenwärtig wird im *US-Senat* ein den kalifornischen Vorschriften nachgestaltetes neues Bundesgesetz (SAFE DATA Act) debattiert. Ein Berufungsgericht (*Court of Appeals for the Ninth Circuit*) entschied Anfang September 2020, dass die Sammlung der Telefon-Metadaten durch die nationale Sicherheitsbehörde *NSA*, wie sie 2013 von *Snowden* aufgedeckt wurde, rechtswidrig und möglicherweise verfassungswidrig sei. In einer einstimmigen Entscheidung aus der Feder der Richterin *Berzon* befand das Richterkollegium, dass eine exzessive Datensammlung der *NSA* gegen FISA (Foreign Intelligence Surveillance Act) und möglicherweise auch gegen den Vierten Zusatzartikel der Verfassung verstoße. Das *Gericht* bezeichnet die „extrem große Zahl von Personen", von denen die *NSA* Daten gesammelt hat, als „problematisch". Ohne hier im Detail auf das US-Recht eingehen zu wollen, ist es keine Majestätsbeleidigung, zu fragen, ob die *EuGH-Richter* und das *vorlegende Gericht* die komplizierten US-Vorschriften wie FISA und die US-Rechtsentwicklung in den letzten Jahren richtig verstanden haben. Das bezweifelt auch die *NTIA*, eine dem US-Handelsministerium zugeordnete Behörde, in einem ausführlichen White Paper v. 25.9.2020, das u.a. Sec. 702 FISA aus ihrer Sicht auslegt. Weiter fällt negativ auf: Warum kommt es in der Entscheidung so sehr auf die „Unionsbürger" und ihre Rechtsmittel in den USA an, während ansonsten in der DS-GVO die Staatsbürgerschaft keine Rolle spielt?

Was wird aus den Standardvertragsklauseln?

Der Kollateralschaden von Schrems II liegt aber ganz woanders, nämlich bei den Unternehmen in der EU, die zu Tausenden mit US-Unternehmen als Datenimporteure Standardvertragsklauseln (SDK) abgeschlossen haben, die uns aus der grauen Vorzeit vor der DS-GVO überliefert worden sind. Beim Versenken des Privacy Shield hat der *EuGH* die SDK ins Rettungsboot gepackt. Land ist aber nicht in Sicht. Auf Grund von „Schrems II" müssen die Daten exportierenden Unternehmen diese Verträge aus den Schubladen holen, in denen sie allzu oft nach der Unterzeichnung verschwunden sind, und sie eventuell ergänzen. Das wäre einfacher, wenn die Unternehmen wüssten, was jetzt zu tun ist. Sie rufen jetzt nach Schwimmwesten, um im Bild zu bleiben. Daran hapert es aber, trotz aller guten Ratschläge von Beratern. Es gibt viele offene Fragen (s. *Schröder*, DB 2020, 1945): Wer ist z.B. der Normadressat der Art. 44 ff. DS-GVO? Wer muss die Anforderungen von „Schrems II" erfüllen und bußgeldbewehrt das Datenschutzniveau im Einzelfall prüfen (vgl. dazu *Golland*, NJW 2020, 2593 (2595))? Das Ausspannen und die Verwaltung eines weltumspannenden, fein gewebten Netzes von SDK ist schon für ein mittelgroßes Unternehmen ein Problem. Jetzt kommt auch noch die Risikoanalyse für alle mit ins Boot. Interessiert sich die *NSA* wirklich für die individuellen Bestellungen, die die Familie Schrems aus ihrem Salzburger Schmuckladen in die USA schickt? Nach Auskunft von EU-Justizkommissar *Reynders* vor dem *LIBE-Komitee des EU-Parlaments* v. 3.9.2020 soll es neue SDK frühestens zu Weihnachten geben. Die neuen SDK sollten dann Konstellationen wie Datenflüsse des EU-Datenverarbeiters an einen Datenverarbeiter in einem Drittland und „komplexe Ketten der Übertragung von personenbezogenen Daten" abbilden. Die Unternehmen sind gespannt, wie diese neuen SDK aussehen werden. Vermutlich wird das ein komplexes Vertragswerk. Von „Klauseln" zu reden ist reiner Euphemismus.

Der EU-US-Datenfluss bricht sich Bahn

Mittlerweile schwillt der Chor derer an, die die Riskoanalyse nach „Schrems II" für die SDK sanft abfedern wollen. *Hansch* (a.a.O.) meint z.B., dass bei der Übermittlung von konzerninternen HR-Daten in die USA „der Einsatz von SDK ohne weitere Maßnahmen durchaus als statthaft zu bewerten ist." *Schrems* vertrat in der genannten Anhörung des *LIBE-Ausschusses* wenig überraschend eine strenge Auslegung, wonach z.B. die SDK überhaupt nicht „für Unternehmen, die unter das US-Überwachungsrecht fallen", verwendbar seien – u.a. für alle Anbieter elektronischer Kommunikationsdienste, da diese unter Sec. 702 FISA fielen. Die Unsicherheit bleibt. *Golland* bezeichnet die Lage als „Experiment SCC+", das „stets unter dem Damoklesschwert einer Intervention der Aufsicht steht" (a.a.O., S. 2596).

Auch bei dem eigentlich als strenge Ausnahmevorschrift gedachten Art. 49 Abs. 1 DS-GVO gibt es Weichspül-Tendenzen. *Moos/Fleming* weisen z.B. in ihrer Urteilsbesprechung zu Schrems II (ZD 2020, 522) darauf hin, dass die vom *EDSA* gewollte Einschränkung „occasional" ausschließlich in den Erwägungsgründen der DS-GVO, nicht aber im Normentext des Art. 49 DS-GVO genannt ist. So oder so, es ist durchaus möglich, dass sich der Datenfluss ins Ausland über Art. 49 DS-GVO Bahn brechen wird – z.B. über Einwilligungen („informed consents"), wie sie im Gesundheitsbereich gang und gäbe sind. *Weiß* hat ebenfalls in ihrem Editorial (ZD 2020, 486) auf die Bedeutung des Art. 49 DS-GVO für den internationalen Datenfluss hingewiesen. Wie viele Unternehmen haben jetzt schon gem. Art. 49 Abs. 1 UAbs. 2 DS-GVO eine Übermittlung in die USA nach Interessenabwägung bei einer Datenschutzbehörde angezeigt – mit der nicht aus der Luft gegriffenen Hoffnung, nie von der Behörde zu hören?

Convention 108+ statt SDK+

Der Leidensdruck der US-Unternehmen ist nicht hoch genug für eine Änderung des US-Rechts zu Gunsten der überwachten Europäer. Die Spatzen pfeifen es von den Dächern: *Schrems* und seine Mitstreiter werden ohnehin etwaige Kompromisslösungen der US- und EU-Delegationen wieder vor Gericht bringen. Ein Ausweg ist vielleicht die vom *Europarat* vorgeschlagene Unterzeichnung der „Convention 108+" durch die USA (Statement v. 7.9.2020). Damit ist das Straßburger Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten gemeint. Das Übereinkommen steht nach Ratifizierung allen Staaten zur Unterzeichnung offen. Denkbar ist auch ein Angemessenheitsbeschluss der *EU-Kommission* nur für Kalifornien. Das ist gem. Art. 45 Abs. 1 DS-GVO („Gebiet") durchaus möglich, hätte aber erhebliche politische Konsequenzen. Auch praktisch ist schwer vorstellbar, dass ein deutsches Unternehmen Daten ohne weiteres ins Silicon Valley schicken darf, nicht aber nach New York.