Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems („Schrems II“)

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Autor: Dr. Bernd Schütze
Stand: 04. September 2020

Inhaltsverzeichnis

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Zusammenfassung

Am 16. Juli 2020 urteilte Gerichtshofs der Europäischen Union (EuGH) im Rechtsstreit „Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems“, d. h. in einem Rechtsstreit zwischen einer Privatperson und Facebook. Das Urteil hat jedoch nicht nur Auswirkungen auf die Verarbeitung personenbezogener Daten durch Facebook in den USA, sondern berührt letztlich jede Verarbeitung in einem Drittland, also einem Land außerhalb des EWR. Auch im Gesundheitswesen erfolgt regelmäßig die Verarbeitung personenbezogener Daten in Drittländern, sodass das Urteil auch Prozesse in deutschen Forschung- und Versorgungseinrichtungen beeinflussen kann.

Kernaussage des Urteils: Alle Artikel in Kapitel V DS-GVO müssen im Licht von Art. 44 DS-GVO ausgelegt werden. Insbesondere ist das Bestehen wirksamer Rechtsbehelfe im betreffenden Drittland im Kontext einer Übermittlung personenbezogener Daten in dieses Drittland daher besonders wichtig und zwingend zu gewährleisten. U. a. dies wird durch den Privacy Shield nicht gewährleistet. Der EuGH kam zu dem Schluss, dass der Angemessenheitsbeschluss bzgl. des Privacy Shield kein der DS-GVO gleichwertiges Schutzniveau gewährleistet und somit ungültig ist. Auf dem Privacy Shield basierende Datenübermittlungen in die USA sind daher seit dem 16. Juli 2020 nicht mehr möglich.

Standardvertragsklauseln bleiben gültig. Werden personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt, so müssen diese aber ein dem EU-Recht genügendes Schutzniveaus sowohl bei der Übermittlung als auch bei der Verarbeitung in einem Drittland gewährleisten: Es muss durch die Standardvertragsklauseln ein Schutzniveau gewährleistet werden, welches dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist.

Dies wird durch vertragliche Gestaltung bei amerikanischen Unternehmen, welche unter Section 702 des FISA fallen, regelhaft nicht möglich sein. Der EuGH stellte fest, dass seitens des europäischen (deutschen) Vertragspartners geprüft werden muss, ob der amerikanische Vertragspartner US-amerikanischem Recht unterliegt, welches einen vertraglichen Schutz personenbezogener Daten in den USA nicht erlauben. In diesen Fällen können allenfalls technische Maßnahmen, welche sicher einen Zugriff des amerikanischen Dienstleisters auf personenbezogene Daten ausschließen, ein entsprechendes Schutzniveau gewährleisten. Ist eine technische Absicherung auch nicht möglich, so kann eine Übermittlung der Daten in die USA nicht rechtskonform erfolgen.

1 Warum sich mit diesem Urteil beschäftigen?

Im Rechtsstreit „Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems“ geht es zunächst darum, in wieweit Facebook Daten einer Privatperson (Maximilian Schrems) in den USA bearbeiten darf. Das Urteil hat jedoch nicht nur Auswirkungen auf die Verarbeitung personenbezogener Daten durch Facebook in den USA, sondern berührt letztlich jede Verarbeitung in einem Drittland, also einem Land außerhalb des EWR.

Auch im Gesundheitswesen erfolgt regelmäßig die Verarbeitung personenbezogener Daten in Drittländern, sodass das Urteil auch Prozesse in deutschen Forschung- und Versorgungseinrichtungen beeinflussen kann.

2 Im Urteil in der Rechtssache C-311/18 enthaltene Aussagen

2.1 Allgemein

Am 16. Juli 2020 urteilte Gerichtshofs der Europäischen Union (EuGH) in der Rechtssache C-311/18 und beurteilte die Konformität des EU-US-Datenschutzschilds (Privacy Shield) mit den rechtlichen Vorgaben der Europäischen Union (EU) und stellte fest, dass der Privacy Shield nicht vereinbar ist mit den Werten der EU[1]. Insbesondere stellte der EuGH fest:

- Übermittlungen personenbezogener Daten zwischen zwei juristischen Personenfallen grundsätzlich nicht unter Art. 2 Abs. 2 DS-GVO und somit gelten die Ausnahmetatbestände wie z. B. ausschließlich persönlicher oder familiärer Tätigkeiten nicht.
- Die in Art. 4 Abs. 2 EUV enthaltene Bestimmung, wonach innerhalb der Union die nationale Sicherheit in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt, betrifft ausschließlich die Mitgliedstaaten der Union; Sicherheitsinteressen anderer Staaten können somit nicht unter Bezugnahme auf diesen Artikel Datenzugriffe legitimieren und insbesondere die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) außer Kraft setzen.
- Insbesondere kann die Möglichkeit, dass personenbezogene Daten, die zwischen zwei Wirtschaftsteilnehmern zu gewerblichen Zwecken übermittelt werden, bei ihrer Übermittlung oder im Anschluss daran von den Behörden des betreffenden Drittlands für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates verarbeitet werden, nicht dazu führen, dass ihre Übermittlung und die damit verbundenen Möglichkeiten einer behördlichen Nutzung vom Anwendungsbereich der DS-GVO ausgenommen wären.
- Alle Artikel in Kapitel V DS-GVO müssen im Licht von Art. 44 DS-GVO ausgelegt werden. D. h . bei einer Verarbeitung und insbesondere bei einer Übermittlung in ein Drittland muss sichergestellt werden, dass das durch die DS-GVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.
- Nach ständiger Rechtsprechung ist es dem Wesen eines Rechtsstaats inhärent, dass eine wirksame, zur Gewährleistung der Einhaltung des Unionsrechts dienende gerichtliche Kontrolle vorhanden sein muss. Daher verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz.
- Das Bestehen solcher wirksamer Rechtsbehelfe im betreffenden Drittland ist im Kontext einer Übermittlung personenbezogener Daten in dieses Drittland daher besonders wichtig und zu gewährleisten.

2.2 Standardvertragsklauseln

Zur Anwendung von Standardvertragsklauseln (Standard Contractual Clauses, SCC) bemerkte der EuGH in seinem Urteil insbesondere:

- Werden personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt, so müssen diese daher den Fortbestand des hohen Schutzniveaus sowohl bei der Übermittlung als auch bei der Verarbeitung in einem Drittland gewährleisten.

[1] Urteil des Gerichtshofs (Große Kammer) vom 16. Juli 2020. Zitiert 2020-09-03, Online unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62018CJ0311

- D. h. werden personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt, so muss ein Schutzniveau gewährleistet werden, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist.
- Bei der im Zusammenhang mit einer Drittland-Übermittlung erforderlichen Beurteilung sind insbesondere die vertraglichen Regelungen zu berücksichtigen, die zwischen dem in der Union ansässigen Verantwortlichen bzw. seinem dort ansässigen Auftragsverarbeiter und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, sowie die maßgeblichen Elemente der Rechtsordnung dieses Landes, soweit diese einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten betreffen.
- Weiterhin ist es gemäß Art. 46 Abs. 1 DS-GVO Sache des in der Union ansässigen Verantwortlichen bzw. des dort ansässigen Auftragsverarbeiters ist, insbesondere geeignete Garantien vorzusehen und zu prüfen, ob durch diese Maßnahmen ein der DS-GVO gleichwertiges Schutzniveau erreicht wird.
- Insbesondere muss basierend auf der in Art. 46 Abs. 2 Buchst. c DS-GVO durch die Möglichkeit der vertragliche Gestaltung innewohnenden Eigenverantwortlichkeit, der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung – prüfen, ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet.
- Kann der in der Union ansässige Verantwortliche bzw. sein dort ansässiger Auftragsverarbeiter keine hinreichenden zusätzlichen Maßnahmen ergreifen, um einen solchen Schutz zu gewährleisten, ist er – bzw. in zweiter Linie die zuständige Aufsichtsbehörde – verpflichtet, die Übermittlung personenbezogener Daten in das betreffende Drittland auszusetzen oder zu beenden.

2.3 Privacy Shield

Zum Angemessenheitsbeschluss der Europäischen Kommission bzgl. der Übermittlung personenbezogener Daten auf Basis des Privacy Shield befand der EuGH:

- Abschnitt I.5 des Anhangs II Privacy Shield ausgeführt, dass die Einhaltung der Grundsätze u. a. insoweit begrenzt sein können, „als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss“. Aufgrund dieses Vorrangs sind die selbstzertifizierten US-Organisationen, die aus der Union personenbezogene Daten erhalten, ohne jede Einschränkung verpflichtet, diese Grundsätze unangewendet zu lassen, wenn sie in Widerstreit zu den genannten Erfordernissen stehen und sich deshalb als mit ihnen unvereinbar erweisen.
- Solche Eingriffe können insbesondere daraus resultieren, dass die amerikanischen Behörden auf die aus der Union in die Vereinigten Staaten übermittelten personenbezogenen Daten zugreifen und sie verwenden.
- Dies kann sowohl im Rahmen der auf Section 702 des Foreign Intelligence Surveillance Acts[2] (FISA) gestützten Überwachungsprogramme PRISM und UPSTREAM als auch auf der Grundlage der Executive Order (E. O.) 12333[3] geschehen.

[2] GovTrack.us: Foreign Intelligence Surveillance Acts (FISA). Zitiert 2020-09-03, Online unter https://www.govtrack.us/congress/bills/110/hr6304/text

- Weiterhin stellte die Kommission in ihrem Angemessenheitsbeschluss im ErwGr. 115. hinsichtlich der E. O. 12333 das Fehlen jeglichen Rechtsbehelfs fest. Dies steht den in der Charta verbürgten Rechten entgegen.
- Die Europäische Kommission verkannte bei ihrer Feststellung hinsichtlich der Angemessenheit des durch den Privacy Shield bereitgestellten Schutzniveaus die Anforderungen, die sich aus Art. 45 Abs. 1 der DS-GVO im Licht der Artt. 7, 8 und 47 der Charta ergeben.
- Der Angemessenheitsbeschluss gewährleistet daher kein der DS-GVO gleichwertiges Schutzniveau und ist ungültig.

2.4 Datenübermittlung in die USA

Hinsichtlich des möglichen Schutzes personenbezogener Daten bei der Übertragung in die USA erwog der EuGH insbesondere folgende Punkte:

- Section 702 des FISA lässt in keiner Weise erkennen, dass für die darin enthaltene Ermächtigung zur Durchführung von Überwachungsprogrammen zum Zweck der Auslandsaufklärung Einschränkungen bestehen.
- Section 702 des FISA enthält für potenziell von diesen Programmen erfasste Nicht-US-Personen keine Garantien.
- Section 702 des FISA sind somit nicht geeignet, ein Schutzniveau zu gewährleisten, welches dem durch die Charta[4] garantierten Niveau der Sache nach gleichwertig ist.
- Insbesondere erlauben auf Section 702 des FISA gestützten Überwachungsprogramme es somit auch nicht, ein Schutzniveau zu gewährleisten, welches den Anforderungen der DS-GVO gleichwertig ist.
- Gleiches gilt für auf E. O. 12333 gestützte Überwachungsprogramme.

3 Fazit aus dem Urteil

3.1 Grundsätzliches zu den Rahmenbedingungen bei US-Vertragspartnern

Vertragliche Vereinbarungen zur Gewährleistung eines dem europäischen Recht entsprechenden Schutzniveaus können nur dort funktionieren, wo die Vertragsparteien eine Dispositionsmöglichkeit haben. Dies scheidet jedoch im Recht der nationalen Sicherheit aus: Hier können die Vertragsparteien sich nicht über das für sie geltende Recht hinwegsetzen oder dieses ändern.

Section 702 des FISA gilt für „Electronic Communication Service Provider“ im Sinne von 50 U.S. Code § 1881[5]. Dort findet sich in Absatz 4:

---

[3] Hinweis: am 27. August 2004 wurde E. O. 12333 durch E. O. 13355 geändert, am 30. Juli 2008 änderte wiederum E. O. 13470 die E. O. 12333

- E. O. 12333--United States intelligence activities vom 4. Dezember 1981. Zitiert 2020-09-03, Online unter https://www.archives.gov/federal-register/codification/executive-order/12333.html
- E. O. 13355: Strengthened Management of the Intelligence Community vom 27. August 2004. Zitiert 2020-09-03, Online unter https://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040827-6.html
- E. O. 13470 vom 30. Juli 2008. Zitiert 2020-09-03, Online unter https://fas.org/irp/offdocs/eo/eo-13470.htm

[4] Charta der Grundrechte der Europäischen Union. Zitiert 2020-09-03, Online unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:12012P/TXT

[5] 50 U. S. Code § 1881. Definitions. Zitiert 2020-09-03, Online unter https://www.law.cornell.edu/uscode/text/50/1881

(4) Electronic communication service provider

The term “electronic communication service provider” means—

(A) a telecommunications carrier, as that term is defined in section 153 of title 47;

(B) a provider of electronic communication service, as that term is defined in section 2510 of title 18;

(C) a provider of a remote computing service, as that term is defined in section 2711 of title 18;

(D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

(E) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

Demzufolge unterliegen nicht alle Unternehmen in den USA Section 702 des FISA, aber Anbieter von Cloud-Dienstleistungen, Anbieter von Cloud-Services und natürlich Kommunikationsanbieter beispielsweise fallen darunter.

Bekannterweise belegen US-amerikanischen Geheimdienste Anweisungen an US-amerikanische Vertragspartner europäischer Unternehmen zur Offenlegung oder zum Zugang zu Informationen und Daten in der Regel mit Geheimhaltungsverpflichtungen, sog. Gag Orders[6]. Die solcherart zur Verschwiegenheit verpflichten können ihren aus den Standardvertragsklauseln resultierenden vertraglichen Pflichten zur Information des europäischen Vertragspartners nicht nachkommen, somit können in diesen Fällen.

Der Clarifying Lawful Overseas Use of Data Act[7] (CLOUD Act) verpflichtet amerikanischen Firmen, amerikanischen Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt, sondern beispielsweise auf Servern innerhalb der EU. Dabei steht dem von der Herausgabeverpflichtung betroffenen Unternehmen im Einzelfall ein Widerspruchsrecht gegen die Anordnung zur Herausgabe personenbezogener Daten zu, wenn

- der Eigentümer der Daten kein US-Bürger ist,
- nicht in den USA lebt und
- das Unternehmen durch die Herausgabe der Daten gegen geltendes Recht in anderen Ländern verstößt.

Allerdings gilt dieses Einspruchsrecht nur, wenn das jeweilige Land mit den USA ein Abkommen unter dem CLOUD Act (“Executive Agreement“) abgeschlossen haben. Ein Executive Agreement soll eigentlich beiden Vertragsparteien die Herausgabe von im Ausland befindlichen Unterlagen zur Bekämpfung von Straftaten gewährleisten, aber der CLOUD Act sieht nur Anforderungen an die Rechtsstaatlichkeit und das Rechtssystem der anderen Vertragspartei eines Executive Agreements vor, nicht jedoch für die USA; wahrscheinlich weil die USA sich im umgekehrten Fall schützen wollen, z. B. wenn ein Gericht im Vertragsland Unterlagen verlangt, die sich in den USA befinden. Bisher vereinbarte von den europäischen Staaten ausschließlich Großbritannien ein entsprechendes Abkommen, sodass für alle anderen EU-Länder amerikanische Firmen kein Widerspruchsrecht bei

[6] Lejeune M. (2020) Datentransfer personenbezogener Daten in die USA vor dem Aus?! Kritische Anmerkungen zur EuGH Entscheidung C-311/18 vom 16.7.2020. CR: 522-529

[7] H.R.4943 - CLOUD Act. Zitiert 2020-09-03, Online unter https://www.congress.gov/bill/115th-congress/house-bill/4943 Weitergehende Informationen zum CLOUD Act z. B. unter https://www.justice.gov/dag/cloudact

Herausgabeverpflichtungen haben. Der Europäische Datenschutzausschuss sieht den CLOUD Act als nicht vereinbar mit den Vorgaben der DS-GVO an[8], gleiches findet sich auch in der Literatur[9].

Grundsätzlich muss daher seitens des europäischen (deutschen) Vertragspartners geprüft werden, ob der amerikanische Vertragspartner US-amerikanischem Recht unterliegt, welches einen vertraglichen Schutz personenbezogener Daten in den USA nicht erlauben.

In diesen Fällen können allenfalls technische Maßnahmen, welche sicher einen Zugriff der amerikanischen Dienstleister auf personenbezogene Daten ausschließen, ein entsprechendes Schutzniveau gewährleisten. Da somit die im Urteil als zwingend beschriebenen Rechtsbehelfe nicht existieren, kann in diesen Fällen mit vertraglichen Regelungen kein ausreichendes Schutzniveau erzielt werden.

3.2 Datenübermittlung entsprechend Privacy Shield

Auf dem Privacy Shield basierende Datenübermittlungen in die USA sind seit dem 16. Juli 2020 nicht mehr möglich. Wer seitdem basierend auf dem Privacy Shield Daten übermittelt, arbeitet rechtswidrig. Aufgrund der großen Medienberichterstattung zu dem Urteil muss davon ausgegangen werden, dass jeder Verantwortliche Kenntnis von dem Urteil erhielt und auf dem Privacy Shield nach dem Urteil basierende Übermittlungen personenbezogener Daten vorsätzlich rechtswidrig erfolgten.

Eine auf dem Privacy Shield basierende Übermittlung personenbezogener Daten ist daher unverzüglich zu beenden.

3.3 Standardvertragsklauseln

Die im Urteil angesprochenen Standardvertragsklauseln existieren in zwei Varianten:

1) EU Verantwortlicher und Verantwortlicher in einem Drittland[10]
2) EU Verantwortlicher und Auftragsverarbeiter in einem Drittland[11]

Relevanter sind insbesondere die Standardvertragsklauseln, welche das Verhältnis zwischen EU Verantwortlichen und Auftragsverarbeiter in einem Drittland regeln. Diese Verträge müssen grundsätzlich direkt zwischen Verantwortlichem in EU und Auftragsverarbeiter in Drittland abgeschlossen werden, d. h. diese Standardvertragsklauseln stellen keinen Vertrag zwischen Auftragsverarbeiter und Unter-Auftragsverarbeitern dar.

Klausel 4 enthält die Pflichten für Datenexporteur, d. h. des Verantwortlichen innerhalb der EU. Zu den aus den Standardvertragsklauseln resultierenden Pflichten gehören insbesondere, dass der Verantwortliche garantiert, dass er

- die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt,

[8] EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection. Zitiert 2020-09-03, Online unter https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_de

[9] So z. B. bei Schwartz P, Peifer KN. (2019) Data Localization Under the CLOUD Act and the GDPR. Cri: 1-10

[10] Klauseln der Kommission vom 15. Juni 2001 (Zitiert 2020-09-03, Online unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32001D0497) bzw. Klauseln der Kommission vom 27. Dezember 2004 (Zitiert 2020-09-03, Online unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32004D0915)

[11] Klauseln der Kommission vom 5. Februar 2010 (Zitiert 2020-09-03, Online unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087)

- für die Einhaltung der Sicherheitsmaßnahmen sorgt,
- betroffene Personen bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung von Drittstaatenverarbeitung informiert,
- betroffenen Person auf Anfrage Klauseln sowie eine Kopie des Vertrages über Datenverarbeitungsdienste zur Verfügung stellt.

Klausel 5 enthält die Pflichten für Datenimporteur, d. h. des Auftragsverarbeiters im Drittland. Zu den aus den Standardvertragsklauseln resultierenden Pflichten gehören insbesondere, dass der Auftragsverarbeiter garantiert, dass er

- seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen,
- eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält,
- den Datenexporteur unverzüglich über alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten informiert.

Somit ergibt sich schon aus den Standardvertragsklauseln selbst die Pflicht der Überprüfung, ob die rechtlichen Gegebenheiten in einem Drittland die Anwendung der Standardvertragsklauseln dahingehend erlauben, dass mit diesen einem dem EU-Recht entsprechendes Schutzniveau zu gewährleisten.

4 Bedeutung des Urteils für das Gesundheitswesen

Wie in allen anderen Branchen erfolgt auch im Gesundheitswesen eher regelhaft eine Verarbeitung personenbezogener Daten in Drittländern, sei es beispielsweise bei Wartung/Support informationstechnischer Systeme durch Unter-Auftragsverarbeitern von innerhalb der Europäischen Union ansässigen Auftragsverarbeitern oder im Rahmen von Forschungsvorhaben durch Kooperation mit im Drittland forschenden Akteuren wie beispielsweise dort ansässige Universitätskliniken.

Daher betrifft das Urteil sowie die sich daraus ergebenden Konsequenzen Versorgungseinrichtungen in Europa und insbesondere natürlich auch deutsche Krankenhäuser, Arztpraxen usw.

4.1 Patientenversorgung

In der heutigen Zeit kommt keine Einrichtung der Patientenversorgung ohne den Einsatz informationstechnischer Systeme (IT-Systeme) aus; allein schon zum Zweck der Abrechnung der erbrachten Leistungen ist ein elektronischer Datenaustausch entsprechend den Vorgaben des SGB V unerlässlich.

IT-Systeme müssen gewartet und aktualisiert, im Fehlerfall wird regelhaft die Unterstützung des Herstellers des IT-Systems benötigt. Daher müssen zwischen den jeweiligen medizinischen Leistungserbringern wie beispielsweise Arztpraxen, Krankenhäuser oder ambulante Pflegedienste Verträge zur Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitungs-Verträge, kurz AV-Verträge oder auch AVV) abgeschlossen werden.

Häufig kann der Hersteller die verkaufte und beschriebene Funktionalität seines IT-Systems nicht alleine gewährleisten, da der Hersteller selbst wiederum Produkte anderer Hersteller wie z. B. Datenbankmanagementsysteme von Oracle® oder Microsoft® einsetzt. Daher schließt der Hersteller

hier Verträge zur Unterauftragsverarbeitung mit den Herstellern ab, deren Unterstützung er für den Support des medizinischen Leistungserbringers benötigt. Hierfür benötigt er entsprechend den Vorgaben der DS-GVO die Zustimmung des Auftraggebers, also des medizinischen Leistungserbringers.

Erfolgt die Verarbeitung durch einen Unter-Auftragnehmer in den USA, so bestanden früher die zwei Möglichkeiten, dass der amerikanische Hersteller sich der Zertifizierung nach Privacy Shield anschloss oder das Standardvertragsklauseln abgeschlossen wurden.

a) Übermittlungen nach Privacy Shield sind spätestens seit dem Urteil rechtswidrig und müssen sofort eingestellt, die in den USA gespeicherten Daten gelöscht werden.
b) Standardvertragsklausen sind grundsätzlich zwischen dem Verantwortlichen in Europa und dem Dienstleister im Drittland abzuschließen. Regelhaft ließen sich Hersteller von IT-Systemen als Auftragsverarbeiter von ihren Auftraggebern das Recht aussprechen, dass die Hersteller in ihren Namen Standardvertragsklauseln abschließen dürfen. Ebenfalls regelhaft kennen die meisten medizinische Leistungserbringer die abgeschlossen Standardvertragsklausen nicht, den Verpflichtungen nach Klausel 4 wird sehr häufig nicht nachgekommen.

Medizinische Leistungserbringer müssen als Verantwortliche entsprechend dem EuGH-Urteil C-311/18 von ihren Herstellern die Standardvertragsklauseln anfordern und dahingehend prüfen, ob mit diesen Standardvertragsklauseln überhaupt ein dem EU-Recht genügendes Datenschutzniveau erzielt wird. Weiterhin müssen Prozesse etabliert werden, welche die Einhaltung der Anforderungen der Standardvertragsklausen an Datenexporteure (= die Verantwortlichen) bewirken.

4.2 Forschung

Medizinische Forschung erfolgt eher regelmäßig institutions- und häufig auch länderübergreifend statt. Gerade die aktuelle Situation um Covid-19 Pandemie zeigt, dass medizinische Forschung nicht auf ein Land, geschweige denn auf ein deutsches Bundesland begrenzt bleiben kann: Internationale Zusammenarbeit in der medizinischen Forschung ist unabdinglich, wenn Fortschritte in der medizinischen Behandlung von Erkrankungen.

Das EuGH-Urteil C-311/18 verbietet keine internationale Zusammenarbeit, jedoch zeigt es klar auf, dass auch hier europäische Verantwortliche für die Einhaltung des Datenschutzniveaus auch bei internationalen Forschungen achten müssen.

Auch eine Zusammenarbeit mit amerikanischen Universitäten/Kliniken ist im Rahmen der Forschung möglich, da diese in der Regel nicht unter die vom EuGH angesprochenen Überwachungsmaßnahmen fallen. Jedoch müssen die technischen Rahmenbedingungen genau betrachtet werden:

- Wird eine Cloud-Lösung eines amerikanischen Anbieters genutzt? Dieser fällt unter Section 702 FISA, d. h die Daten dürfen nur so verschlüsselt in der Cloud abgelegt werden, dass keine Möglichkeit der Entschlüsselung für den Cloud-Dienstleister besteht.
- Wie wird die Übertragung von Gesundheitsdaten geschützt? Hier ist der Stand der Technik eine Ende-zu-Ende-Verschlüsselung.
- Usw.

Entsprechend deutschem Recht müssen zur Forschung anonyme oder, wenn dies begründbar nicht möglich ist, pseudonyme Daten verwendet werden. Ist eine De-Pseudonymisierung nur demjenigen

möglich, bei dem die Patientendaten während der Behandlung anfielen, existiert hier ein sehr hochwertiger Schutz nicht nur, aber gerade auch bei der Kooperation mit Forschungspartnern in Drittstaaten.

Und natürlich müssen entsprechende Verträge den Schutz der Daten begleitend zu den technischen Maßnahmen absichern.

Für aktuelle Forschungsprojekte gilt:

1) Eine Datenübermittlung auf Grundlage des Privacy Shield ist rechtswidrig. Um das Forschungsprojekt nicht vorzeitig abbrechen zu müssen, sind hier Standardvertragsklauseln abzuschließen.
2) Bei vorhandenen Standardvertragsklauseln sind diese zu prüfen, ob sie den Vorgaben des EuGH-Urteils C-311/18 entsprechen oder ob weitergehende Maßnahmen zur Gewährleistung eines dem europäischen Recht entsprechendem Datenschutzniveaus zu vereinbaren und umzusetzen sind.

4.3 Sozialdaten

Entsprechend § 80 Abs. 3 SGB X dürfen Sozialdaten nur dann in einem Drittland verarbeitet werden, sofern für dieses Drittland ein Angemessenheitsbeschluss gemäß Art. 45 DS-GVO vorliegt.

Mit Aberkennung des Angemessenheitsbescheides der EU-Kommission hinsichtlich des Privacy Shields liegt für die USA kein Angemessenheitsbeschluss vor, sodass Sozialdaten in den USA nicht verarbeitet werden dürfen.

4.4 Digitale Gesundheitsanwendungen entsprechend § 33a SGB V

Mit Inkrafttreten des Digitale-Versorgung-Gesetzes (DVG) wurde insbesondere die „App auf Rezept“ für Patientinnen und Patienten in die Gesundheitsversorgung eingeführt (§§ 33a sowie 139 SGB V). Entsprechend § 139e Abs. 9 SGB V wurde das Bundesministerium für Gesundheit ermächtigt, insbesondere Anforderungen an den Datenschutz und die Datensicherheit nach dem Stand der Technik festzulegen. Dies erfolgte mit der Digitalen Gesundheitsanwendungen-Verordnung (DiGAV).

Entsprechend § 4 Abs. 3 DiGAV dürfen personenbezogenen Daten durch die digitale Gesundheitsanwendung nur dann in einem Drittland verarbeitet werden, sofern für dieses Drittland ein Angemessenheitsbeschluss gemäß Art. 45 DS-GVO vorliegt.

Mit Aberkennung des Angemessenheitsbescheides der EU-Kommission hinsichtlich des Privacy Shields liegt für die USA kein Angemessenheitsbeschluss vor, sodass Sozialdaten in den USA nicht verarbeitet werden dürfen. Somit dürfen §§ 33a, 139 SGB entsprechende digitale Anwendungen insbesondere von amerikanischen Dienstleistern angebotene Dienstleistungen wie z. B. Cloud-Speicherplatz oder Cloud-Services nicht nutzen.

5 Folgen einer rechtswidrigen Datenübermittlung in ein Drittland

Erfolgt eine widerrechtliche Übermittlung in ein Drittland, so stellt dies einen Bußgeldtatbestand nach Art. 83 Abs. 5 Buchst. c DS-GVO dar. Entsprechend können von den Aufsichtsbehörden Geldbußen von bis zu 20.000.000 Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (je nachdem, welcher der Beträge höher ist) verhängt werden.

Daneben hat gemäß Art. 82 DS-GVO jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz.

Weiterhin können die Strafvorschriften aus § 42 BDSG anwendbar sein, wenn von der rechtswidrigen Übermittlung in ein Drittland eine große Zahl von Personen betroffen sind.

6 Handlungsempfehlung

1) Unternehmen sollten untersuchen und dokumentieren, welche Drittlandtransfers in welche Länder auf welcher Rechtsgrundlage stattfinden. Dabei muss die vollständige Verarbeitung betrachtet werden, d. h.
   - inklusive aller Auftragsverarbeiter und
   - evtl. vorhandene Unter-Auftragsverarbeiter.

   Prüfen Sie auch Ihre Verträge zur Auftragsverarbeitung und sehen sie nach, wo die Verarbeitungsstandorte ihrer Auftragsverarbeiter liegen. Insbesondere bei älteren Verträgen: Fragen Sie Ihre Auftragsverarbeiter nach den konkreten Standorten der Verarbeitung ihrer Daten, lassen sie sich die bei der Verarbeitung ihrer Daten eingesetzten Unter-Auftragsverarbeiter inklusive der Verarbeitungsstandorte der Unter-Auftragsverarbeiter konkret benennen[12].
2) Erlaubten sie Dienstleistern, in ihrem Namen Standardvertragsklauseln abzuschließen, lassen sie sich unverzüglich die Verträge zur Prüfung übergeben,
3) Danach sollten Erkundungen zum Datenschutzniveau in diesen Drittländern durchgeführt werden; erster Ansprechpartner ist hier regelhaft der Vertragspartner im Drittland, welche bei Nutzung der Standardvertragsklauseln gemäß Klausel 5 hier zur Auskunft verpflichtet sind.
4) Datenempfänger im Drittland sollten insbesondere befragt werden zu
   - Datenschutzniveau im Drittland
   - inwieweit staatliche Behörden Zugriff auf die EU-Daten erhalten können
   - durch welche Maßnahmen ein der DS-GVO entsprechendes Datenschutzniveau gewährleistet wird bzw. welche etwaigen zusätzlichen Maßnahmen zur Herstellung eines den europäischen Vorgaben entsprechendes Datenschutzniveaus implementiert werden müssen
   - der Person des gemäß Art. 27 Abs. 1 DS-GVO erforderlichen Vertreters des Drittland-Unternehmens in der EU
5) Hinweis: Die unter der RL 95/46/EG „Datenschutzrichtlinie“) erlassenen Standardvertragsklauseln zur Auftragsverarbeitung gelten gemäß Art. 45 Abs. 9 DS-GVO auch unter der DSGVO fort. Allerdings erfüllen die Standardvertragsklauseln nicht alle der in Art. 28 Abs. 3 DS-GVO vorgegebenen Anforderungen, sodass hier Ergänzungen erforderlich sind. Hier sollte bei einer Überprüfung hinsichtlich der Erfüllung der sich aus dem Urteil C-311/18 ergebenden Anforderungen auch auf die Erfüllung der Anforderungen von Art. 28 DS-GVO geachtet werden. Dabei beachten:
   - Eine Änderung der Klauseln selbst führt wahrscheinlich zu einer Pflicht, die Klauseln vor Anwendung der für den Verantwortlichen zuständigen Aufsichtspflicht vorzulegen, die dann über die weitere Zulässigkeit für einen Drittstaatentransfer befinden.

[12] Hinweis: Die Organisation NYOB stellt Musterschreiben für Anfragen an DU-Datenimporteure zur Verfügung, die aber gut angepasst werden können. Zitiert 2020-09-03, Online unter https://noyb.eu/de/naechste-schritte-fuer-eu-unternehmen-faqs

- Günstiger für Ergänzungen entsprechend den Vorgaben aus Art. 28 DS-GVO ist Anhang 1 der Vertragsklauseln, da dies – sofern nicht den Vertragsklauseln selbst widersprochen wird - nicht zu einer Vorlagepflicht bei der Aufsichtsbehörde führt.

Grundsätzlich kann auch über die Aufnahme einer Regelung zur Zahlung einer Vertragsstrafe bei einem Verstoß gegen die Standardvertragsklauseln in den Anhang nachgedacht werden, welche dem aus den Regelungen der DS-GVO zu erwartendem Bußgeld für den Verstoß entspricht. Eine Weigerung des Vertragspartners zu entsprechenden Regelungen kann einen Hinweis darauf darstellen, dass im Drittland gesetzliche Regelungen existieren, welche dem Vertragspartner die Einhaltung der Klauseln nicht ermöglichen.

6) Alle Datenübermittlungen in die USA, die auf Grundlage des Privacy Shields erfolgten, müssen auf andere Übermittlungsmechanismen umgestellt werden. Möglichkeiten sind:
   - Abschluss von Standardvertragsklauseln
   - Binding Corporate Rules (BCR); können grundsätzlich weiter genutzt werden, sind aber überwiegend bei Verarbeitungen Konzern anwendbar. Entsprechend den aus dem EuGH-Urteil C-311/18 ergebenden Vorgaben müssen aber auch BCR daraufhin geprüft werden, ob mit ihnen ein dem europäischen Recht entsprechendes Datenschutzniveau gewährleistet werden kann.
   - Ausnahmeregelungen, insbesondere
     - Einwilligung (Art. 49 Abs. 1 Buchst. a DS-GVO)
     - Erforderlich zur Vertragserfüllung eines im Interesse der betroffenen Person abgeschlossenen Vertrages (Art. 49 Abs. 1 Buchst. b DS-GVO)

     Ausnahmeregelungen dürfen nach Ansicht des Europäischen Datenschutzausschusses auch nur in wirklichen Ausnahmefällen[13]. Insbesondere ist bei Art. 49 Abs. 1 Buchst. b, c, e DS-GVO nach ErwGr. 111 DS-GVO eine gelegentliche Übermittlung Voraussetzung zur Anwendung, können also nur sich nicht wiederholende Verarbeitungen legitimieren.

   In der Regel wird daher nur der Rückgriff auf Standardvertragsklauseln als Alternative zu dem Privacy Shield Abkommen möglich sein, wenn die Verarbeitung nicht eingestellt werden kann.
7) Kann die Übermittlung und Verarbeitung personenbezogener Daten in ein Drittland auf Basis der der Standardvertragsklauseln nicht mehr gerechtfertigt werden, so ist die Übermittlung und die Verarbeitung der Daten im Drittland zu beenden.
8) Es ist ein Prozess bzgl. der nach den Standvertragsklauseln erforderlichen Information der betroffenen Personen hinsichtlich der Drittland-Verarbeitung zu etablieren.
9) Ggf. sind die Datenschutzhinweise nach Artt. 13, 14 DS-GVO anzupassen.
10) Entsprechend Art. 5 Abs. 2 DS-GVO besteht eine Nachweispflicht insbesondere auch über die Rechtmäßigkeit bei der Verarbeitung. Zum Nachweis der Rechtmäßigkeit der Verarbeitung gehört selbstverständlich auch die Prüfung sowie das Prüfergebnis hinsichtlich der Rechtmäßigkeit einer Übermittlung in Drittstaaten. Daher muss der gesamte Prüfprozess sowie das Ergebnis dokumentiert und bei Bedarf den Aufsichtsbehörden vorgelegt werden.

[13] Europäischer Datenschutzausschuss (EDSA): Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679. Zitiert 2020-09-03, Online unter https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_en

7 Literatur

7.1 Online

- Urteil des Gerichtshofs (Große Kammer) vom 16. Juli 2020 in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems („Schrems II“). Zitiert 2020-09-03, Online unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62018CJ0311
- Europäischer Datenschutzausschuss (EDSA): Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18—Data Protection Commissioner gegen Facebook Ireland Ltd und Maximilian Schrems. Zitiert 2020-09-03, Online unter https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en
- Landesbeauftragte für den Datenschutz Baden-Württemberg: Orientierungshilfe des LfDI BW: Was jetzt in Sachen internationaler Datentransfer? Zitiert 2020-09-03, Online unter https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfe-des-lfdi-bw-was-jetzt-in-sachen-internationaler-datentransfer/
- Datenschutzkonferenz: Pressemitteilung zum Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II“) stärkt den Datenschutz für EU-Bürgerinnen und Bürger. Zitiert 2020-09-03, Online unter https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf

7.2 Zeitschriften

- Botta J. (2020) Eine Frage des Niveaus: Angemessenheit drittstaatlicher Datenschutzregime im Lichte der Schlussanträge in „Schrems II“. CR: 82-89
- Dralle T. (2020) Schrems II vor dem EuGH. BvD-News: 39-42
- Günther JP. (2020) EuGH-Urteil Schrems II - Ein Abgesang auf den internationalen Datenverkehr? PinG: 192-197
- Lejeune M. (2020) Datentransfer personenbezogener Daten in die USA vor dem Aus?! Kritische Anmerkungen zur EuGH Entscheidung C-311/18 vom 16.7.2020. CR: 522-529
- Müller-Peltzer P, Selz IL. (2020) EuGH, Urt. v. 16. 07. 2020 – Az. C-311/18 – EuGH kippt EU-US-Privacy-Shield und stellt erweiterte Prüfpflichten bei der Verwendung von Standardvertragsklauseln auf (Schrems II). PinG: 217-219
- Notta J. (2020) Zwischen Rechtsvereinheitlichung und Verantwortungsdiffusion: Die Prüfung grenzüberschreitender Datenübermittlungen nach „Schrems II“. CR: 505-513
- Rössel M. (2020) Unzulässige Datenübermittlung in die USA auf Grundlage des Privacy Shields. ITRB: 180-182
- Sellars C. 2020) EU: Schrems II and Standard Contractual Clauses – the Advocate-General’s Opinion. Cri: 29-30
- Tribess A. (2020) Der Privacy Shield ist ungültig, Übermittlung erfordert eine Einzelfallprüfung. GWR: 308
- Voigt P. (2020) Praxisprobleme im Zusammenhang mit den EU-Standardvertragsklauseln zur Auftragsverarbeitung – mehr als „nur“ Schrems II ... CR: 513-522