Verarbeitung personenbezogener Daten durch EU-Tochtergesellschaften von US-Anbietern –Kritisch?

[25.08.2021]

Von: **Dr. Axel-Michael Wagner**

Vielen europäischen Verantwortlichen, die personenbezogene Daten von Mitarbeitern, Kunden bzw. deren Ansprechpartnern, Lieferanten bzw. deren Ansprechpartnern oder Dritten verarbeiten, ist nicht klar, wie viel davon tatsächlich unter der „Oberherrschaft" von US-Unternehmen verarbeitet wird. Solange der Verantwortliche nicht selbst Lösungen insbesondere der drei großen Cloud-Anbieter Google, Amazon und Microsoft nutzt, geschieht dies doch in aller Regel durch Auftragsverarbeiter, denen man Daten zur Verarbeitung überlässt, oder deren Unter-Auftragsverarbeiter. Irgendwo in der Kette taucht unweigerlich zumindest einer der drei Namen wieder auf. Der Hauptsitz dieser Unternehmensgruppen liegt in den USA, auch wenn die eigentlichen Vertragsbeziehungen mit einer irländischen oder luxemburgischen Tochtergesellschaft abgeschlossen worden sein mögen. Ist das unproblematisch?

Zulässigkeit des Transfers von personenbezogenen Daten im „Klartext" in die USA

Auf den ersten Blick drehen sich viele Veröffentlichungen einschließlich des „Schrems II"-Urteils des EuGH, Verlautbarungen des Europäischen Datenschutzausschusses und der deutschen Datenschutzbehörden um personenbezogene Daten, die in die USA übermittelt werden. Man wähnt sich dann sicher, wenn die personenbezogenen Daten „europäischen Boden nicht verlassen", etwa, wenn die Dienste der großen Cloud-Anbieter so konfiguriert werden, dass europäische (oder deutsche) Rechenzentrumsstandorte für die Daten vereinbart werden. Ob dies tatsächlich dann auch nicht geschieht, ist offen.

Für den Bereich des Windows-Betriebssystems und der dort erhobenen, überwiegend personenbezogenen „Telemetriedaten", die ständig an US-Server von Microsoft gesandt werden, wurde beispielsweise von verschiedenen Stellen in geradezu detektivischer Feinarbeit ermittelt, unter welchen Bedingungen solche Transfers wirksam unterbunden werden können. Microsoft hat eine solche Unterbindung nach neueren Erkenntnissen der Datenschutzbehörden anscheinend – verschlüsselt übertragene Daten sind natürlich kaum richtig untersuchbar und Microsoft besitzt auch die Möglichkeit, die übertragenen Telemetriedaten per Fernzugriff umzukonfigurieren – in der „Enterprise"-Version von Windows ermöglicht. Das war wohl zumindest auch das Ergebnis des auf die Erkenntnisse der Datenübertragungen hin ausgeübten Drucks. Nur wie viele Unternehmen benutzen

diese Version nicht oder wenden nicht die richtigen Einstellungen in ihrer „Enterprise"-Version an?

Für die großen (Cloud-) Dienste kann die Einhaltung der Zusage, die Daten nicht aus einem bestimmten geografischen Bereich bzw. Rechenzentrum heraus zu transferieren, letztlich überhaupt nicht durch den Auftraggeber verifiziert werden. Einerseits kann man im (beabsichtigten) Dickicht der vielen Leistungsdefinitionen und Nebenbedingungen oft nicht mit völliger Sicherheit ausschließen, dass für einzelne (z. B. Such- oder KI-) Dienste die Daten dann doch vertragsgemäß in die USA übertragen werden dürfen, andererseits kann der (interne) Datenfluss zwischen beispielsweise einem europäischen Google-Rechenzentrum und einem US-Google-Rechenzentrum vom „kleinen" Verantwortlichen gar nicht geprüft werden. In letzter Konsequenz sind europäische Verantwortliche also auf die vertraglichen Zusagen bzw. auf – teils schwer zugängliche und ihrerseits unter verschiedensten Prämissen stehende – Prüfberichte Dritter angewiesen.

In den „Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data / Version 2.0 / Adopted on 18 June 2021" des Europäischen Datenschutzausschusses EDPB werden die praktischen Konsequenzen der „Schrems II"-Entscheidung des EuGH aus Sicht der Datenschutzbehörden skizziert. Da in den USA ein behördlicher Zugriff auf bei einem Cloud-Anbieter gehostete personenbezogene Daten von Europäern ohne Einhaltung von aus EU-Sicht rechtsstaatlicher Verfahren möglich ist, darf ein Transfer solcher Daten nur erfolgen, wenn zusätzlich „effektive technische Maßnahmen" ergriffen werden. Solche Maßnahmen können Verschlüsselung und Pseudonymisierung sein. Die meisten Fälle eines Einsatzes von Cloud-Diensten, insbesondere also SaaS-Angeboten (die mit den Daten inhaltlich operieren müssen), bedingen aber, dass die Daten auf dem US-Server vollständig und im Klartext vorliegen müssen. Eine Verschlüsselung oder Pseudonymisierung über die gesamte „Drittlands-Verarbeitungskette" hinweg scheiden aus, wenn die Daten sinnvoll inhaltlich in der Cloud – also durch SaaS-Anwendungen, die auf den Servern in der Cloud laufen – verarbeitet werden sollen. Auch wenn die Daten im „ruhenden" Zustand, also außerhalb der inhaltlichen Verarbeitung, verschlüsselt werden, müssen sie doch während der Verarbeitung selbst (inhaltliche Operationen, Filterung, Aufbereitung für die Darstellung etc.) unverschlüsselt verfügbar sein. Es bleiben ansonsten, vereinfacht gesagt, nur Cloud-Speicherdienste übrig, bei denen die Ver- und Entschlüsselung bzw. die Pseudonymisierung und Re-Pseudonymisierung ausschließlich lokal in der EU erfolgen können.

Den skizzierten Hauptanwendungsfall einer inhaltlichen Verarbeitung von Daten in der Cloud beschreibt das EDPB als „Transfer to cloud services providers or other processors which require access to data in the clear" und schließt dann folgende Wertung an:

„Then the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on the data subject's fundamental rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear."

Der EDPB bringt also hier die Auswirkungen der Schrems II-Entscheidung auf den Punkt: Ein Transfer personenbezogener Daten „als solcher", also (zu irgendeinem Zeitpunkt) unverschlüsselt und mit vollem Personenbezug zur inhaltlichen Verarbeitung in den USA, ist unzulässig. Dies kann auch nicht durch Standard-Vertragsklauseln oder „binding corporate rules" behoben werden, denn auch diese können – als Vertragswerke – das Risiko des Datenabzugs durch US-Behörden natürlich nicht wirksam ausschließen.

Datenabzug von in der EU liegenden Daten aus den USA heraus

Bis hierher werden sich – ggf. mit den skizzierten Restunsicherheiten bei der Konfiguration der „Datenlokation" in der EU behaftet – viele Verantwortliche sicher wähnen, weil sie ihre Daten nicht in die USA transferieren. Nun liegt das eigentliche Problem aber woanders: Die Daten könnten dort, wo „sie sich in Sicherheit wähnen", einfach abgezogen werden. So ordnete es das FBI 2013 gegenüber Microsoft USA an für personenbezogene Daten, die physisch in Irland (mutmaßlich in Servern der irischen Microsoft-Gesellschaft) lagen. Microsoft erklärt nicht, dass dies rechtlich oder faktisch nicht möglich sei, sondern, dass das damalige US-Recht aus dem Jahr 1986 keine taugliche Rechtsgrundlage für eine behördliche Anordnung zur Vorlage von „Nicht-US-Daten" sei. Der Fall ging zum Obersten Gerichtshof der USA und wurde dort 2018 „links überholt" vom „CLOUD Act", der nun mit Section 702 des „Foreign Intelligence Surveillance Acts" (FISA) eine ausdrückliche Rechtsgrundlage für die behördliche Anforderung von personenbezogenen Daten schuf, die außerhalb der USA liegen. Damit war die Bewertung des ursprünglichen Falles nicht mehr notwendig und es musste in den USA keine abschließende gerichtliche Entscheidung mehr getroffen werden. Section 702 FISA war dann aber 2020 Beurteilungsgrundlage des EuGH in der Schrems-II-Entscheidung. Dass der EuGH seine Kritik auch auf die „Executive Order 12333" gestützt hat, soll hier nicht zusätzlich behandelt werden.

Der Kritikpunkt des EuGH am amerikanischen Recht bezieht sich darauf, dass nach Section 702 des US-„Foreign Intelligence Surveillance Acts" (FISA) ein „electronic communication service provider" durch US-Behörden angewiesen werden kann, personenbezogene Daten eines Nicht-US-Bürgers vorzulegen, ohne dass dagegen in einem rechtsstaatlichen Verfahren vorgegangen werden kann, welches EU-Vorgaben entspricht. Ein solcher „electronic communication service provider" ist namentlich auch

ein „provider of a remote computing service" (Sec. 701 (b) (4) (C) FISA), d. h. ein Cloud- oder SaaS-Dienst. Die das US-Unternehmen treffende Verpflichtung wird mit „immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition [of foreign intelligence information]" umschrieben (Sec. 702 (h) (1) (A) FISA), was – nach deutschem Rechtsverständnis – auch die Anweisung eines in den USA ansässigen (Mutter-) Unternehmens an sein in der EU ansässiges 100%-Tochterunternehmen umfassen kann. Unter US-Recht werden solche Gesellschaftsgrenzen innerhalb einer Unternehmensgruppe eher selten thematisiert. Im Folgenden soll es nun nicht darum gehen, inwieweit diese Wertung des EuGH aus US-Perspektive nachvollziehbar ist, sondern, was sich aus dieser Wertung für in der EU liegende Daten mit Personenbezug ergibt.

Aus Section 702 FISA lässt sich entnehmen, dass alleine der Umstand, dass ein europäischer Verantwortlicher mit einer EU-Tochtergesellschaft eines US-Cloudanbieters – und nicht mit diesem selbst – ein Vertragsverhältnis eingeht und in diesem Vertragsverhältnis vereinbart oder konfiguriert wird, dass die Daten in EU-Rechenzentren liegen, nicht weiterhilft. Denn im Falle einer behördlichen Anordnung muss aus US-Perspektive die US-Muttergesellschaft die EU-Tochtergesellschaft anweisen, die relevanten Daten „still" an die US-Muttergesellschaft bzw. an die US-Behörde herauszugeben. Natürlich befinden sich die Organe der EU-Tochtergesellschaft dabei im Konflikt, eine nach EU-Recht auf eine rechtswidrige Datenverarbeitung gerichtete Gesellschafterweisung auszuführen, und sind deshalb sowohl nach EU-Recht (Art. 48 DSGVO) als auch ggf. nach dem national anwendbaren Recht des EU-Mitgliedsstaates nicht verpflichtet, diese Weisung umzusetzen. In Deutschland muss etwa ein GmbH-Geschäftsführer das Zumutbare unternehmen, um die Ausführung von rechtswidrigen Gesellschafterbeschlüssen zu verhindern. Ggf. ist dieser „Umweg" aber auch gar nicht notwendig und die US-Muttergesellschaft bzw. deren IT-Abteilung kann sich die Daten selbsttätig beschaffen. Zwar ist aus datenschutzrechtlicher Perspektive die US-Muttergesellschaft ein „Dritter", und die EU-Tochtergesellschaft müsste einen solchen „Durchgriff" bzw. eine solche „Selbsthilfe" aktiv verhindern, um die Vertraulichkeit der Daten zu gewährleisten. Aber wenn die Muttergesellschaft die Cloud-Technologie selbst (weiter-) entwickelt hat und z. B. Updates für die Infrastruktursysteme von der Muttergesellschaft aus ausgerollt werden, dürfte kaum eine Möglichkeit bestehen, Datenabzugsfunktionen effektiv zu verhindern (oder überhaupt zu bemerken). Man muss sich bei all diesen Verästelungen auch immer wieder vor Augen halten, dass es bei der rechtlichen Sichtweise um die Einschätzung von Risiken bzw. Möglichkeiten geht und nicht um die Frage, ob derartige Fälle in der Praxis tatsächlich nachweisbar sind.
Es ist unbekannt, wie viele derartige behördliche Anordnungen, im Ausland belegene Daten abzuziehen – so wie im Microsoft-Sachverhalt von 2013 (s. o.) –, bislang gegenüber den großen US-Cloud-Providern erlassen wurden.

Bedeutet dies, dass dieselben Erwägungen, die oben dazu geführt haben, dass EU-Daten nicht „offen“ (also unverschlüsselt und nicht pseudonymisiert) in die USA transferiert werden dürfen, auch dann Anwendung finden müssen, wenn EU-Daten „offen“ in EU-Rechenzentren transferiert werden, die von einem US-Anbieter „beherrscht“ werden? Immerhin sind die Regelungen der DSGVO zur Drittlandsübermittlung durch den Verantwortlichen in diesem Fall nicht einschlägig. Die Antwort auf diese Frage ist relativ einfach: Nach Art. 28 Abs. 1 DSGVO darf ein in der EU ansässiger Auftragsverarbeiter nur dann beauftragt werden, wenn er „hinreichend Garantien“ dafür bietet, „dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Bearbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet“. Und dies ist natürlich gefährdet, wenn das Risiko besteht, dass der Auftragsverarbeiter die Daten „abzieht“ und an US-Behörden weitergibt bzw. die US-Muttergesellschaft des Auftragsverarbeiters diese Daten – direkt oder indirekt – abzieht. Dieses Risiko ist im Vorfeld des Abschlusses einer Auftragsverarbeitungsvereinbarung vom Verantwortlichen zu evaluieren und die Evaluierung im Kontext von Art. 5 Abs. 2 DSGVO zu dokumentieren.

Die Existenz eines solchen Risikos könnte dann ausgeschlossen werden, wenn die EU-Tochtergesellschaft nachweisen kann, dass ein Zugriff der US-Muttergesellschaft nicht möglich ist – und zwar aus rechtlicher und (!) faktischer Sicht. Soweit ersichtlich, hat sich bislang kein US-Cloudanbieter (bzw. dessen EU-Tochtergesellschaft) an einem solchen Beweis versucht. Auch eine Selbstverpflichtung der US-Muttergesellschaft, bei etwaigen Behördenaufforderungen nach Section 702 FISA in jedem Fall den (US-) Rechtsweg einzuschlagen bzw. solchen Aufforderungen nicht nachzukommen, zumindest wenn sie sich auf in der EU liegende Daten beziehen, dürfte in diesem Zusammenhang keine effektive ergänzende Maßnahme aus EU-Sicht sein. „Effektiv“ kann diese Erklärung nichts verhindern, zumal wenn man beispielhaft folgende Formulierung zum generellen Umgang mit dieser Problematik in den Microsoft-Bestimmungen für Kundendaten im B2BBereich („Professional Services Daten“) liest:

„Microsoft wird keine verarbeiteten Daten offenlegen oder Zugang zu ihnen gewähren, außer: [...] (3) wie gesetzlich vorgeschrieben. [...] Microsoft wird verarbeitete Daten gegenüber Strafverfolgungsbehörden nur offenlegen bzw. den Zugriff darauf ermöglichen, wenn dies gesetzlich vorgeschrieben ist. Wenn sich eine Strafverfolgungsbehörde mit Microsoft in Verbindung setzt und verarbeitete Daten anfordert, wird Microsoft versuchen, die Strafverfolgungsbehörde an den Kunden zu verweisen, damit sie diese Daten direkt beim Kunden anfordert. Wenn Microsoft gezwungen wird, verarbeitete Daten an die Strafverfolgungsbehörden weiterzugeben oder diesen den Zugriff darauf einzuräumen, benachrichtigt Microsoft den Kunden unverzüglich und übermittelt eine Kopie der

Anforderung, sofern dies nicht gesetzlich verboten ist. Nach Erhalt einer sonstigen Anfrage von Dritten zur Weitergabe verarbeiteter Daten benachrichtigt Microsoft den Kunden unverzüglich; es sei denn, dies ist gesetzlich untersagt. Microsoft wird die Anfrage ablehnen, sofern nicht gesetzlich vorgeschrieben. Wenn die Anfrage zulässig ist, wird Microsoft versuchen, den Dritten zu verweisen, um die Daten direkt beim Kunden anzufordern."

Dieses Addendum bezieht sich übrigens seinem Wortlaut nach nur auf den Datentransfer in die USA und wird im Rahmen einer Auftragsverarbeitungsvereinbarung (neben den Standardvertragsklauseln) zwischen der US-Muttergesellschaft und dem europäischen Kunden abgeschlossen. Für eine Beziehung zu einer EU-Tochtergesellschaft sind solche Vereinbarungen nicht notwendig, weil die DSGVO direkt Anwendung findet und damit auch das Verbot der Weitergabe der Daten an US-Behörden. Im Mai 2021 hat Microsoft zusätzlich verlauten lassen, dass ab Ende 2022 eine „EU-Datengrenze" gezogen werde, die es unmöglich mache, Daten aus der EU heraus zu transferieren. Microsoft erklärt: „Wir werden technische Schutzmaßnahmen wie Lockboxen oder vom Kunden verwaltete Verschlüsselungen für Kundendaten auf die zentralen Cloud-Dienste von Microsoft ausweiten." Das könnte zunächst im Umkehrschluss bedeuten, dass es die bisherige Situation (und auch die Situation bis zur Implementierung Ende 2022) durchaus technisch zulässt, Daten aus der EU heraus in die USA zu transferieren. In den FAQ zu diesen Plänen der „absoluten Lokalisierung" von Daten („data residency") heißt es zur Rechtsauffassung von Microsoft über den Konflikt zwischen US- und EU-Recht:

„We also believe that data residency may bolster our ability to make legal challenges to some non-EU government demands for access to data. At the same time, it's important to note that any technology provider with sufficient presence in the U.S. – even if it's based in Europe – is subject to U.S. legal process."

Dies zeigt, dass auch Microsoft davon ausgeht, dass sich der Fall von 2013 unter Section 702 FISA wiederholen kann – mit offenem Ausgang und auch bei (noch) stärkerer Lokalisierung der Daten in der EU. Unter US-Recht wird im Übrigen auch bereits diskutiert, ob eine selbstständige Verschlüsselung von EU-Daten durch die EU-Tochtergesellschaft eines US-Konzerns (nicht durch den Verantwortlichen wie vom EDPB gefordert), sodass diese Daten für die US-Muttergesellschaft nicht mehr zum Abzug zur Verfügung stehen, überhaupt zulässig wäre oder eine Umgehung von Section 702 FISA darstellt.

Zusammengefasst besteht demnach auch in den Fällen, in denen die personenbezogenen Daten physisch in der EU verbleiben und eine Auftragsverarbeitungsvereinbarung mit einer EU-Tochtergesellschaft eines US-Cloud-Unternehmens abgeschlossen wird, das

Risiko eines Zugriffs durch US-Behörden. Vertragliche Zusicherungen, dass gegen behördliche Anordnungen vorgegangen wird, können dieses Risiko nicht ausschließen. Auch eine Zusicherung, dass die US-Muttergesellschaft auf die in der EU von der Tochtergesellschaft gehaltenen Daten faktisch keinen Zugriff hat, wäre mit Vorsicht zu genießen, da diese letztlich in der komplexen und ständig weiterentwickelten Cloud-Infrastruktur gar nicht nachprüfbar ist. Wenn, dann müsste diese fehlende Zugriffsmöglichkeit durch eine unabhängige Stelle bestätigt werden, und auch dann besteht natürlich jederzeit die Möglichkeit, dass sich die Infrastruktur ändert oder im Rahmen eines solchen Audits Möglichkeiten des Datenabzugs übersehen werden. Die Frage ist nun, wie sich dieses Risiko in der rechtlichen Bewertung der Zulässigkeit der Auftragsverarbeitung durch ein EU-Tochterunternehmen eines US-Konzerns auswirkt.

Gerichtliche Beurteilung durch das französische Oberste Verwaltungsgericht

Die Thematik wurde, soweit ersichtlich, bislang von den Gerichten nur in zwei Fällen vor dem französischen Obersten Verwaltungsgericht (Conseil d'État) aufgegriffen. Das eine Verfahren betraf ein Hosting von Gesundheitsdaten französischer Bürger durch die von der französischen Regierung ins Leben gerufene Plattform „Health Data Hub", dessen Daten bei Microsoft in den Niederlanden bzw. in Frankreich gehostet werden sollten, das andere Verfahren die Plattform des privaten Anbieters „Doctolib", die zur Verwaltung von Impfterminen im Rahmen des COVID-Impfprogramms in Europa bei Amazon (AWS) gehostet werden sollte. In beiden Fällen war das Anliegen der Antragsteller, die jeweilige Datenverarbeitung über die Plattform im Wege des einstweiligen (vorbeugenden) Rechtsschutzes einzustellen. Es handelte sich also jeweils um ein summarisches (Eil-) Verfahren, bei dem die Sache „nicht bis zum Ende durchdekliniert" wurde – dies würde nach deutschem Rechtsverständnis einem Hauptsacheverfahren vorbehalten bleiben.

Das Gericht folgte in beiden Fällen im Grundsatz der Argumentation auch der französischen Datenschutzbehörde CNIL, dass das „US-Risiko" auch in Bezug auf eine EU-Tochtergesellschaft bestehe. Allerdings wurde dieses Risiko nicht für absolut gehalten, sondern eine allgemeine Risikoabwägung vorgenommen. Im „Doctolib"-Fall beispielsweise wurde das US-Durchgriffsrisiko dadurch „abgemildert", dass keine Gesundheitsdaten übermittelt werden sollten (etwa über den Anlass einer Terminpriorisierung für die Impfung), dass die Daten nach drei Monaten wieder gelöscht würden und die Löschung auch vorher durch den Betroffenen angestoßen werden konnte, sowie dass sich AWS vertragsgemäß gegen eine US-Vorlageaufforderung wehren würde. Letztlich war all dies aber, wenn man den Maßstab des EDPB anlegt, bedeutungslos: Die Daten lagen nach den Feststellungen im summarischen Verfahren bei AWS nur verschlüsselt vor und der Schlüssel selbst wurde von einer vertrauenswürdigen dritten

Partei in Frankreich und nicht von AWS gehalten. Damit war das Risiko eines Abzugs der Klardaten eigentlich ausgeschlossen.

Im „Health Data Hub"-Fall wurden die Daten nur in pseudonymer Form gehostet, d. h. eine US-Behörde hätte diese Daten (so der Aufsatzpunkt des Gerichts) den Betroffenen nicht einzeln zuordnen können.

Wie sind diese Entscheidungen im Kontext der DSGVO einzuordnen? In der „Health Data Hub"-Entscheidung, die ausführlicher begründet wurde, hat sich das Gericht im Rahmen der Prüfung der Voraussetzungen von Art. 28 Abs. 1 DSGVO auf die Auftragsverarbeitungsvereinbarung mit Microsoft bezogen. Diese – sinngemäß vor allem die Zusage „Microsoft wird die Daten an Dritte nur herausgeben, wenn Microsoft dazu verpflichtet ist" – wurde (lediglich) so interpretiert, dass es dabei um europäische Behörden bzw. europäische Verpflichtungen geht. Ein Vorbehalt des Datenabzugs aus den USA heraus wurde demnach in den vertraglichen Regelungen nicht gesehen. Vielmehr wurde die Möglichkeit eines Datenabzugs als zusätzliches, faktisches Risiko eingeordnet, welches, worauf das Gericht besonders hinwies, nicht Gegenstand der Schrems II-Entscheidung des EuGH war. Dieses „US-Risiko" wurde dann als im Verhältnis zum Nutzen (Bekämpfung der COVID-Pandemie) nachrangig bewertet und die handelnden Parteien (Auftraggeber und Auftragsverarbeiter) „aufgefordert", weitere Maßnahmen zu ergreifen. Solche Maßnahmen wurden aufgeteilt in vorläufige Maßnahmen als auch in weitere Maßnahmen, „um jegliches Risiko auszuschalten, wie die Wahl eines neuen Auftragsverarbeiters". Ergänzend erklärte das Gericht aber auch, dass eine „harte" Anordnung von Maßnahmen zur Beseitigung des Risikos im Wege des einstweiligen Rechtsschutzes im gesetzlich vorgesehenen Falle einer schwerwiegenden und offenkundig rechtswidrigen Verletzung einer Grundfreiheit durch den französischen Staat (Art. L. 521-2 des „Code du Justice Administrative") in den vorliegenden Fällen rechtlich gar nicht möglich sei.

Dies wirft die Folgefrage auf, wie eine Entscheidung ausfallen würde, wenn – ggf. nach genauerer technischer Analyse – personenbezogene Daten ganz oder teilweise doch irgendwann bei der EU-Tochtergesellschaft eines US-Konzerns unverschlüsselt „im Klartext" und ohne Pseudonymisierung zugänglich sind, wie dies in der Praxis häufig der Fall ist. Immerhin benötigt ja z. B. ein Cloud-Dienst eine Adresse (E-Mail, Mobilfunknummer, IP-Adresse etc.), um mit einem Endgerät überhaupt kommunizieren zu können; die für die Kommunikation notwendigen, personenbezogenen (Meta-) Daten können nicht Gegenstand einer Ende-zu-Ende-Verschlüsselung sein. Vom Technologieanbieter „Tanker", von dem Doctolib seine Verschlüsselungstechnologie bezieht, werden als Anwendungsfälle für diese Technologie vertrauliche Chats, Dokumentenspeicherung und Patientenakten genannt. Diese Inhaltsdaten lassen sich auf

dem sendenden Endgerät verschlüsseln und auf dem empfangenden Endgerät entschlüsseln; inhaltliche Operationen mit diesen Daten sind dann in der Cloud nicht möglich und der Cloud-Betreiber hält nur verschlüsselte Daten. Aber bei Vereinbarung eines Termins bei einem Arzt oder einem Impfzentrum über die Plattform könnte das für die zu erhebenden Stammdaten schon wieder anders aussehen.

Das Wort „hinreichend“, dessen Maßstab im Detail natürlich unklar ist, in Art. 28 Abs. 1 DSGVO legt die Möglichkeit einer Risikoabwägung nicht nur im prozessualen Rahmen einer summarischen Entscheidung im vorbeugenden Rechtsschutz (Eilverfahren) nahe. Theoretisch kann eine solche Risikobewertung bzw. Abwägung selbst ohne vollständige Verschlüsselung positiv (d. h. zugunsten einer zulässigen Verarbeitung unter der Ägide eines US-Anbieters) ausgehen. Wann das aber genau der Fall wäre, ohne dass öffentliche Interessen wie die Pandemiebekämpfung mit in die Waagschale zu werfen sind, darüber enthalten die französischen Entscheidungen keine genaueren Angaben oder „Guidance“.

Wichtig ist noch einmal der Hinweis, dass im Gegensatz dazu die Schrems II-Entscheidung des EuGH in einem anderen materiellrechtlichen Kontext stand, nämlich im Kontext der Drittlandsübermittlung, in deren Rahmen sichergestellt werden muss, „dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird“ (Art. 44 S. 2 DSGVO). Eine Abwägung in dem Sinne, dass das US-Zugriffsrisiko nur dann besteht, wenn die personenbezogenen Daten besonders sensibel sind, kann der Schrems II-Entscheidung im Kontext dieser Rechtsgrundlage nicht entnommen werden. Im Gegenteil: Um welche (inhaltlichen) Facebook-Daten von Herrn Schrems es beim Transfer in die USA überhaupt konkret ging, war überhaupt nicht Gegenstand der Gerichtsentscheidung. Vielmehr dürfte die Schrems-II-Entscheidung als ja/neinEntscheidung zu interpretieren sein, d. h. entweder kann das US-Zugriffsrisiko durch effektive zusätzliche Maßnahmen „gebannt“ werden (dann ist der Transfer bzw. die Verarbeitung unter der Ägide eines US-Anbieters zulässig) oder eben nicht (dann ist der Transfer bzw. die Verarbeitung unzulässig). Das wäre wohl ein anderer Maßstab als im Rahmen einer Risikobewertung nach Art. 28 Abs. 1 DSGVO.

Eine solche Abwägung nimmt auch das Landgericht München I in einer Entscheidung aus dem Januar 2022 nicht vor. Im zugrundeliegenden Sachverhalt wehrte sich ein Betroffener gegen den Umstand, dass seine dynamische IP-Adresse infolge der (nicht lokalen) Einbindung des Dienstes „Google Fonts“ von einem Website-Betreiber an die Server des Diensteanbieters (Google) in die USA übermittelt worden war. Dabei ist daran zu erinnern, dass eine dynamische IP-Adresse nur deshalb ein (wenn auch im Grundsatz „weniger sensibles“) personenbezogenes Datum i. S. d. DSGVO ist, weil der Bundesgerichtshof im Anschluss an eine Entscheidung des Europäischen Gerichtshofs (Breyer-Entscheidung) der Ansicht war, es stelle eine (selbst bei massenhafter Erhebung

derartiger Daten) realistische Möglichkeit dar, dass ein Website-Betreiber den Betroffenen einer Straftat bezichtigt und dann Akteneinsicht in die von der Staatsanwaltschaft (durch Anfrage beim Access-Provider) erlangte Zuordnung zum Klarnamen des Betroffenen nehmen könnte. Nach dem Landgericht München I stellt die Übermittlung der dynamischen IP-Adresse durch den Website-Betreiber an Google im Zuge des Seitenaufbaus einen Datenschutzverstoß durch ungerechtfertigte Drittlandsübermittlung dar. Google sammle, so das Landgericht, „bekanntermaßen Daten über seine Nutzer". Das vom Betroffenen danach „empfundene individuelle Unwohlsein" sei so erheblich, dass dies ein Schadensersatzanspruch gerechtfertigt ist. Ob die besuchte Internet-Seite eine gesteigerte Aussagekraft hinsichtlich des Betroffenen zugelassen hätte – etwa eine politisch, sexuell oder religiös geprägte Seite –, wurde vom Landgericht München I nicht überliefert. Man mag den hier ausgeurteilten Schadensersatzbetrag (100 Euro) für nicht wesentlich halten, aber es geht natürlich auch um den Breiteneffekt über viele Besucher hinweg.

Der Gesichtspunkt der fehlenden Abwägung hinsichtlich der Sensibilität der Daten ist auch deshalb so wichtig, weil große Mengen personenbezogener Daten im B2B-Bereich „nur" Niedrigrisikodaten sind – nämlich betriebsbezogene Kontaktdaten wie Name, Betriebszugehörigkeit, betriebliche E-Mail und Telefonnummer –, über deren Schutz (bzw. Schutzbedürftigkeit) sich in der Praxis kaum jemand Gedanken macht. Auch für diese Daten gilt aber grundsätzlich der „one size fits all"-Ansatz der DSGVO, und auch mit diesen Daten können durch Unbefugte verschiedene Formen des Identitätsdiebstahls begangen werden. Selbst wenn hier der Soll-Maßstab für die Absicherung der DSGVO-konformen Verarbeitung nach Art. 24, 32 DSGVO risikobedingt niedrig sein mag, gibt es zumindest in der EuGH-Rechtsprechung im Kontext der Drittlandsübermittlung bislang keinen Hinweis, dass man es deshalb mit dem Transfer in die USA nicht so eng nehmen muss. Es mag sein, ist aber letztlich spekulativ, dass die Abwägung im Rahmen von Art. 28 Abs. 1 DSGVO hier mehr Spielraum ermöglicht, was das Gewicht der Gefahr des Datenabzugs aus den USA heraus betrifft.

Abhilfe durch Zertifizierung?

Die derzeit im Zulassungsverfahren befindliche AUDITOR-Zertifizierung von Cloud-Diensten, u. a. vom Bundesministerium für Wirtschaft und Energie gefördert, sieht einen ausführlichen Kriterienkatalog vor, der sich natürlich auch mit Datensicherheit, Vertraulichkeit und Verschlüsselung befasst. Beim Thema Verschlüsselung beispielsweise geht es aber nur um die „ruhenden" Daten, d. h. die Daten außerhalb der „aktiven" Verarbeitung (innerhalb der Cloud-Umgebung). Der Cloud-Anbieter muss hier den Einsatz wirksamer und aktueller Verschlüsselungstechniken sowie entsprechender Berechtigungskonzepte bzw. Zugangsrechte hinsichtlich der Schlüssel nachweisen, und

für die höchste Schutzklasse heißt es: „Zusätzlich werden unberechtigte Zugriffe auf den Schlüssel hinreichend sicher durch geeignete TOM ausgeschlossen." Solche und ähnliche Vorgaben können jedoch die technische Möglichkeit (!) des „Abwanderns" von Daten an eine die gesamte Infrastruktur steuernde und vorgebende US-Muttergesellschaft trotz entsprechender Prüfungshandlungen im Rahmen von Zertifizierungsprüfungen nicht effektiv verhindern. Dazu muss man nicht erst die Pressemeldungen über nachträglich aufgespürte Hintertüren und „Datenabzüge" im Nachgang zu den Snowden-Enthüllungen zurate ziehen, die selbst nur eine zufällige Auswahl der identifizierten Fälle und damit die Spitze des Eisbergs ausmachen dürften. Es wird interessant sein zu sehen, wie eine Zertifizierungsstelle in diesem Kontext beispielsweise die obige Klausel von Microsoft einordnen wird.

Auswege für den Verantwortlichen

Man kann das Problem ganz einfach dadurch lösen, dass man das Risiko eines US-„Durchgriffs" auf personenbezogene Daten, die unter der Ägide eines US-Cloud-Konzerns in der EU liegen, für datenschutzrechtlich irrelevant hält. Immerhin gibt es bislang keine allgemeinzugänglich dokumentierten Fälle, dass sich der „irische Microsoft-Fall" aus dem Jahr 2013 (s. o.) unter der Geltung von Sec. 702 FISA wiederholt hat. Man könnte also darauf vertrauen, dass „es nicht passieren wird" und wenn doch, dann zumindest darauf, dass die EU-Gesellschaft von Microsoft als Auftragsverarbeiter „schon das Richtige tun", sprich sich an EU-Datenschutzrecht und vertragliche Zusagen halten und keine personenbezogenen Daten herausgeben wird, schon gar nicht ohne dass die US-Muttergesellschaft den Fall vor den US-Gerichten maximal eskaliert hat. Das führt im Ergebnis dazu, ein im Grunde mangels Datenbasis nicht messbares (Rechts-) Risiko als nicht maßgeblich anzusehen.

Da das Risiko dadurch zwar als existent angesehen, aber letztlich pauschal mangels Messbarkeit „unter den Tisch gekehrt" würde, liegt es näher, das Risiko des US-„Durchgriffs" im Rahmen der Bewertung der Zuverlässigkeit des (EU-) Auftragsverarbeiters nach Art. 28 Abs. 1 DSGVO – und in diesem Kontext auch bei einer generellen Risikoabwägung (vgl. Kurzpapier 18 der DSK) oder einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) – einfließen zu lassen, ähnlich wie im Rahmen der Entscheidung des französischen Obersten Verwaltungsgerichts. Man würde also davon ausgehen, dass das verbleibende Restrisiko – das US-Unternehmen hält sich nicht an seine Zusagen oder erhält eine behördliche Anordnung, über die es die Betroffenen und den Kunden nicht in Kenntnis setzen darf und die es aufgrund einer gerichtlichen Bestätigung der Anordnung ausführen muss – verhältnismäßig klein ist, und setzt dies ins Verhältnis zum möglichen Schaden. Der Schaden liegt zunächst „nur" im Verlust der Kontrolle über die Daten – sowohl seitens des Verantwortlichen als auch seitens des Betroffenen –, aber es sind auch

Folgeschäden bis hin zur Weitergabe an Behörden anderer (Dritt-) Staaten und zur strafrechtlichen Verfolgung denkbar. Erscheint das Risiko hiernach im Ergebnis „niedrig“ oder „normal“ und bestehen keine weiteren Risikominimierungsmöglichkeiten, kann es sein, dass der Verantwortliche das verbleibende Risiko im Rahmen seiner Risikoabwägung als akzeptables Restrisiko ansehen darf. Wann genau dieses Niveau erreicht ist, ist allerdings unklar.

Auch dieser zweite, besser begründbare Lösungsweg müsste natürlich vom Verantwortlichen sorgfältig evaluiert, vor dem Hintergrund der konkreten Umstände begründet und dokumentiert werden. Sicher – sieht man einmal von sonstigen geheimdienstlichen Möglichkeiten ab – kann der unbefugte Abzug der in der EU liegenden Daten nur durch die Wahl eines anderen Auftragsverarbeiters mit anderer „Risikostruktur“ verhindert werden. Dies deutet auch das französische Oberste Verwaltungsgericht an (s. o.). Geschieht ein Datenabzug durch den Auftragsverarbeiter in der EU auf Geheiß von dessen US-Muttergesellschaft, so liegt ein Fall des „Exzesses“ vor (Art. 28 Abs. 10 DSGVO), für den die EU-Tochtergesellschaft die datenschutzrechtliche Verantwortlichenrolle einnehmen würde, der aber auch den ursprünglichen Verantwortlichen treffen kann (Art. 82 Abs. 1 DSGVO). Geschieht dieser direkt durch die US-Muttergesellschaft an der EU-Tochtergesellschaft vorbei, so könnte man dies schon beinahe mit einem Hackerangriff auf die Daten – natürlich dadurch erleichtert, dass der Verantwortliche die Daten in die „Sphäre des US-Konzerns“ eingebracht hat – gleichsetzen. Eine Entscheidung des EuGH, dass beide Risiken nicht akzeptabel sind und daher eine Auftragsverarbeitung durch einen solchen Cloud-Dienstleister ausscheidet, würde faktisch einem „Berufsverbot“ der (EU-Ableger der) US-Cloud-Konzerne gleichkommen. Ob der EuGH so weit gehen würde, ist offen. Es blieben dann nur noch Lösungen wie das letztlich mangels Kundeninteresse 2018 eingestampfte „Daten-Treuhand-Modell“ („Microsoft Cloud Deutschland“) von Microsoft und Telekom.

Fazit

Für den Moment kann man festhalten, dass Billionen personenbezogener Daten – mehr oder weniger sensiblen Inhalts – in einem datenschutzrechtlich als „Grauzone“ zu bezeichnenden Rechtszustand verarbeitet werden, an die sich im Moment niemand so richtig heranwagt. Im englischen Sprachraum würde man es wohl „the elephant in the room“ nennen. Die europäischen Datenschutzbehörden haben das Dilemma der in der EU liegenden Daten unter US-Ägide erkannt, sich dazu aber bislang nicht positioniert. Lediglich was den direkten Anwendungsfall der Schrems II-Entscheidung angeht, den physischen Datentransfer in die USA (oder die willkürliche Einräumung von Zugriffsrechten an europäischen Daten z. B. für Konzerngesellschaften in den USA), wird der Druck zunehmend durch Fragebögen und Sachverhaltsermittlungen seitens der

Aufsichtsbehörden erhöht. Hier macht aber die Aussage „Wir konfigurieren die von uns genutzten Cloud-Dienste so, dass die Daten ausschließlich in der EU liegen und nicht in ein Drittland transferiert werden und räumen Dritten keine Zugriffsrechte daran ein“ die Beantwortung weiterer Fragen bislang (vordergründig) obsolet. Das Problem selbst und die damit verbundene Rechtsunsicherheit verschwindet so natürlich nicht. Klare Guidance fehlt demnach.

Nun wird man allerdings den US-Gesetzgeber nicht ohne Weiteres „auf EU-Spur bringen“ können, zumal insbesondere in der Diskussion um den Angemessenheitsbeschluss für Großbritannien nach dem Brexit schon immer kritisiert wird, dass behördliche bzw. geheimdienstliche Eingriffsgrundlagen auch innerhalb der EU existieren. Deshalb kursiert auch der Vorwurf, dass hier mit zweierlei Maß gemessen wird: Derartige Möglichkeiten in den USA werden als Generalangriff auf personenbezogene EU-Daten gewertet, in der EU oder Großbritannien werden hingegen die entsprechen-den Risiken eines Datenabzugs negiert. Wenn Daten zunehmend auch von EU-Tochtergesellschaften von Anbietern in anderen Jurisdiktionen gehostet werden – Indien, China etc. –, kann das Problem auch dort zu diskutieren sein. Eine Änderung der DSGVO dürfte in der derzeitigen politischen Situation ebenfalls ausscheiden. Ohnehin „denkt“ die DSGVO nicht auf solcher Detailebene; eine punktuelle Regelung im Rahmen der Bewertung spezifischer Risiken ist der zumeist hoch abstrakten DSGVO fremd.

Die Kräfte des Marktes tun ihr Übriges: Schon mehren sich Stimmen, dass man als europäisches SaaS-Unternehmen Schwierigkeiten hat, seinen Kunden zu erklären, warum man unter der Ägide eines US-Unternehmens personenbezogene Daten seiner Kunden hosten will. Mit der technischen Überlegenheit der US-Anbieter – ironischerweise auch im Bereich der Datensicherheit – kann man in dieser Situation nicht mehr zwangsläufig überzeugen. Man muss demnach konzedieren: Wenn es das (politische) Ziel der DSGVO war, im B2B-Bereich nicht nur die großen US-Anbieter, sondern auch deren EU-Ausläufer zurückzudrängen, könnte der EuGH auch dem mit der Schrems II-Entscheidung Flügel (oder besser Zähne) verliehen haben, schon allein wegen der dadurch ausgelösten Rechtsunsicherheit in Bezug auf Daten unter der Ägide der US-Konzerne. Diese Rechtsunsicherheit betrifft ein gigantisches Marktvolumen und wird letztlich auf dem Rücken der vielen kleinen Software-Anbieter und Start-ups ausgetragen, die ihre Software, ihre Datenbanken und ihre Daten „irgendwo“ zu vernünftigen wirtschaftlichen und technischen Konditionen rechtssicher betreiben wollen. Die europäischen und deutschen Cloud-Anbieter stehen zwar in den Startlöchern, können aber das – durch größte Investitionen und teils immer noch defizitäre Cloud-Geschäftsmodelle erkaufte – Niveau der US-Anbieter noch nicht bieten. Ob sie es in absehbarer Zeit können werden, ist ungewiss.