www.compliance-berater.de

Compliance Berater

11 / 2020

Betriebs-Berater Compliance

28.10.2020 | 8.Jg
Seiten 405–448

Schwerpunktheft Banken-Compliance

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

CB-BEITRAG

Dr. Jan Dörrwächter, RA, und Johannes Brinkkötter, RA

Europäische Daten in den USA: Weder sicherer Hafen noch sicheres Schild

Nach einem aktuellen Urteil des EuGH dürfen ab sofort personenbezogene Daten nicht mehr auf Basis des sogenannten Privacy Shields in die USA übermittelt werden. Die Entscheidung betrifft potenziell alle Unternehmen mit Geschäftsaktivitäten im EU-Wirtschaftsraum, deren personenbezogene Daten an Mutter- oder Tochtergesellschaften oder an Dienstleister in den USA übermittelt werden. Als Folge sehen sich Unternehmen erheblichen Reputations- und Rechtsrisiken bis hin zu empfindlichen Bußgeldern und Schadensersatzansprüchen ausgesetzt. Zudem berühren Verstöße auch unternehmensinterne Compliance-Vorschriften.

I. Einleitung

Mit einer Klage gegen Facebook Ireland Ltd. hatte ein österreichischer Datenschutzaktivist die langjährige Praxis zum Austausch personenbezogener Daten mit den USA durch Soziale Netzwerke und andere Unternehmen unterbinden wollen. Seiner Auffassung nach waren personenbezogene Daten nicht ausreichend vor dem Zugriff von US-Sicherheitsbehörden geschützt. Daran ändere auch das zu diesem Zweck verabschiedete Abkommen (Safe-Harbour) zwischen der EU und den USA nichts. Der Europäische Gerichtshof (EuGH) folgte dieser Argumentation und erklärte es 2015 für ungültig.[1]

Seitdem wurden personenbezogene Daten auf der Grundlage des als Nachfolgeregelung genutzten „Privacy Shield" sowie sogenannter Standarddatenschutz-Klauseln in die USA übermittelt. Hiergegen klagte der Aktivist erneut, und einmal mehr gab ihm die höchste juristische Instanz der EU Recht. Laut EuGH-Urteil[2] müsse bei Übertragung personenbezogener Daten in ein Drittland ein Schutzniveau gewahrt werden, das dem der EU-Datenschutzgrundverordnung (DSGVO) entspricht. Davon könne angesichts der Rechtslage in den USA nicht ausgegangen werden, weswegen auch der Privacy Shield ungültig sei.

II. Detailbetrachtung im Kontext der DSGVO

Nach Art 44. DSGVO ist jede Übermittlung personenbezogener Daten, die bereits verarbeitet wurden oder nach ihrer Übermittlung an ein Drittland verarbeitet werden sollen, nur zulässig, wenn der Verantwortliche oder der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen und auch die sonstigen Bestimmungen der DSGVO einhalten.

Laut DSGVO darf eine Übermittlung personenbezogener Daten an ein Drittland ohne besondere Genehmigung vorgenommen werden, wenn die EU-Kommission diesen ein angemessenes Schutzniveau bescheinigt. Insoweit kann die Kommission nach Art. 45 Abs. 3 DSGVO feststellen, dass ein Drittland ein angemessenes Schutzniveau bietet. Einen entsprechenden Beschluss hatte die EU-Kommission mit Blick auf den vom Privacy Shield gewährten Schutz gefasst[3]. Sie war hierbei davon ausgegangen, dass die USA einen angemessenen Rechtsschutz für personenbezogene Daten gewährleisten, die im Rahmen des EU-US-Datenschutzschilds aus der EU an Organisationen in den USA übermittelt werden.

Falls kein (wirksamer) Beschluss nach Art. 45 Abs. 3 DSGVO vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (Art. 46 Abs. 1 DSGVO). Diese Garantien können unter anderem in sogenannten Standarddatenschutzklauseln bestehen, die von der EU-Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 DSGVO erlassen werden. Des Weiteren kann die Übermittlung personenbezogener Daten in ein Drittland nach Art. 47 DSGVO auf sogenannte Verbindliche Interne Datenschutzvorschriften (Corporate Binding Rules) gestützt werden, sofern die zuständige Aufsichtsbehörde diese genehmigt hat. Hierbei handelt es sich ihrer Rechtsnatur nach ebenfalls um vertragliche Garantien im Sinne von Art. 46 DSGVO. Ist keine der genannten Voraussetzungen erfüllt, ist eine Datenübermittlung nur in Ausnahmefällen gemäß Art. 49 DSGVO möglich. Hier kommt vor allem die Einwilligung des Betroffenen nach Abs. 1 Satz 1 lit. a in Betracht.

Der EUGH hat in seinem Urteil vom 16.7.2020 den Beschluss der EU-Kommission, in dem die Kommission festgestellt hatte, dass das EU-US-Datenschutzschild (Privacy Shield) ein angemessenes Schutzniveau bietet, für ungültig erklärt. Dabei stützt sich der EuGH vor allem auf die weitreichenden Eingriffsbefugnisse für Sicherheitsbehörden in den USA, die nach seiner Ansicht nicht auf das zwingend erforderliche Maß beschränkt seien. Außerdem kommt der EuGH zu dem Schluss, dass in den USA kein ausreichend effektiver Rechtsschutz vor Eingriffen

1 EuGH, Urt. v. 6.10.2015 – C-362/14, EuZW 2015, 881.
2 EuGH, Urt. v. 16.7.2020 – C-311/18, CB 2020, 437.
3 Durchführungsbeschuss (EU) 2016/1250 der Kommission vom 12.7.2016.

gewährleistet sei. Insbesondere eröffne der implementierte Ombuds-Mechanismus keine ausreichenden Rechtsschutzgarantien.

III. Wirksamkeit von Standarddatenschutzklauseln sehr zweifelhaft

Als alternative Lösung kommen Standarddatenschutzklauseln in Betracht, die auch der EuGH grundsätzlich als geeignetes Instrument ansieht, die Vorgaben der DSGVO zu wahren. Da diese jedoch ihrer Natur nach keine Garantien bieten, die über eine vertragliche Verpflichtung zur Einhaltung des unionsrechtlich verlangten Schutzniveaus hinausgehen, kann es, wie der EuGH betont, je nach Lage in einem Drittland erforderlich sein, zusätzliche Schutzmaßnahmen zu ergreifen.
Damit obliegt es dem Verantwortlichen bzw. seinem Auftragsverarbeiter, in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung – zu prüfen, ob das Recht des Bestimmungsdrittlands einen nach Maßgabe des Unionsrechts angemessenen Schutz der auf Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet, und ob erforderlichenfalls weitere Garantien vorzusehen sind.
Angesichts der weitreichenden hoheitlichen Befugnisse der US-Sicherheitsbehörden erscheint das jedoch höchst zweifelhaft, können doch diese Eingriffsbefugnisse gegenüber in den USA ansässigen Unternehmen wohl kaum durch zivilrechtliche Vereinbarungen im transatlantischen Datenaustausch wirksam beschränkt werden.[4]
Beredt schweigt hierzu der EuGH und deutet in seinem Urteil nicht einmal an, wie die von ihm geforderten zusätzlichen Schutzmaßnahmen aussehen könnten. In technischer Hinsicht wird erwogen, ob End-to-End-Verschlüsselungen als zusätzliche Schutzmaßnahmen in Frage kommen. Und ohne Zweifel sind solche Verfahren dringend anzuraten, um Eingriffe Dritter in den Datenübermittlungsprozess abzuwehren. Werden jedoch etwa Daten von einer EU-Tochter an ihre Mutter in den USA zur Speicherung und/oder Verarbeitung übermittelt, nützt auch diese Verschlüsselungstechnik nichts, weil die entsprechenden Daten ja bei der Empfängerin im Regelfall wieder entschlüsselt werden, um sie dort verarbeiten zu können.
Kann jedoch kein angemessenes Schutzniveau garantiert werden, muss die Übermittlung personenbezogener Daten in die USA unverzüglich ausgesetzt bzw. beendet werden. Dies hat beispielsweise der Berliner Datenschutzbeauftragte bereits gefordert.[5]

IV. Gültigkeit auch für Verbindliche Interne Datenschutzvorschriften

Ohne dass der EuGH sich hierzu explizit geäußert hat, gilt Ähnliches wohl auch für die Verbindlichen Internen Datenschutzvorschriften. Denn auch diese dürften sich gegenüber hoheitlichen Zugriffsrechten von US-Sicherheitsbehörden als untaugliches Schutzschild erweisen, weil sie diese per se gar nicht binden können.
Fraglich ist daher auch, ob etwa sogenannte „Chinese Walls", also interne Regelungen, wonach beispielsweise der Konzernmutter in den USA der Zugriff auf personenbezogene Daten ihrer EU-Tochter untersagt ist, einen ausreichenden Schutz bieten. Denn im Konflikt zwischen unternehmensinternen Vorgaben einerseits und dem – in der Regel mit entsprechenden Zwangsmitteln durchsetzbaren – hoheitlichen Auskunftsbegehren einer US-Behörde andererseits dürften sich die Verantwortlichen in den USA klar zugunsten des letzteren entscheiden. Damit lässt sich ein angemessenes Schutzniveau nur durch technische Vorkehrungen erreichen, vor allem durch IT-technische Zugriffsbeschränkungen der Konzernmutter in den USA.
Ob solche internen Firewalls zum Schutz europäischer Daten in Drittländern technisch überhaupt realisierbar sind, bleibt dahingestellt. Denn es erscheint unwahrscheinlich, dass sich amerikanische Unternehmen entsprechenden behördlichen Anordnungen zur Weitergabe von Daten hinter internen Firewalls – unter Verweis darauf, dass die Türen in der Firewall nur von Tochterunternehmen in der EU zu öffnen sind – erfolgreich widersetzen können. Damit ist es mehr als zweifelhaft, ob solche Schutzmaßnahmen überhaupt mit der vom EuGH geforderten Zuverlässigkeit vereinbar sind.
Da sich aber die Verantwortliche in Unternehmen genau der Wirksamkeit solcher technischen Schutzmaßnahmen versichern müssen, bevor personenbezogene Daten an ein Unternehmen mit einer Konzernmutter oder ein Tochterunternehmen in den USA übermittelt werden, ist festzustellen, dass kurzfristig verfügbare technische Maßnahmen nicht in Sicht sind, um die vom EuGH geforderten zusätzlichen Garantien für ein DSGVO-konformes Schutzniveau abzubilden.

V. Konsequenzen für die Unternehmenspraxis

Die Entscheidung des EUGH bedeutet daher in der Konsequenz:

1. Eine Übermittlung personenbezogener Daten in die USA kann sich nicht mehr auf das Privacy Shield stützen – Daten müssen zurückgeholt werden

Eine Datenübermittlung auf Grundlage des *Privacy Shield* ist ab sofort und ohne Übergangsfrist unzulässig. Laut Bundesverband IT-Sicherheit TeleTrusT e. V. betrifft dies mehr als 5.000 Firmen und Dienstanbieter in den USA.[6]
Betroffen ist nicht nur die zukünftige Datenübermittlung. Auch bereits übermittelte Daten müssen unverzüglich zurückgeholt werden. Findet eine Datenübermittlung weiterhin statt, könnten betroffene Personen Schadensersatz für den erlittenen immateriellen Schaden verlangen und Aufsichtsbehörden gegen den Verantwortlichen nach EU-Recht ein Bußgeld in „abschreckender" Höhe verhängen. Rein vorsorglich sei darauf hingewiesen, dass es wenig erfolgversprechend erscheint, für eventuelle Bußgelder oder Schadensersatzforderungen amerikanische Vertragspartner in Regress nehmen zu wollen.

2. Standarddatenschutzklauseln und Verbindliche Interne Datenschutzvorschriften sind keine rechtsichere Grundlage

Der EuGH hat die Nutzung von Standarddatenschutzklauseln nicht untersagt. Er knüpft diese aber an überaus strenge Voraussetzungen. Zunächst sind der Verantwortliche bzw. sein Auftragsverarbeiter künftig verpflichtet, in jedem Einzelfall zu prüfen, ob das Recht des Bestimmungsdrittlands einen angemessenen Schutz nach Maßgabe EU-Recht gewährleistet, und sofern dies nicht der Fall ist, weitere erforderliche Schutzmaßnahmen zu ergreifen.
Legt man an den vom EuGH nahegelegten Anspruch an, die aus Sicht des höchsten EU-Gerichts exzessiven Zugriffsrechte amerikanischer

4 Ebenso *Schröder*, DB 2020, 1945, 1947.
5 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf.
6 Siehe: https://www.privacyshield.gov/list.

Sicherheitsbehörden wirksam einzuschränken, dürfte das in der Praxis durch zwischen privaten Unternehmen vereinbarte Garantien kaum leistbar sein. Damit bietet aber auch die Verwendung von Standarddatenschutzklauseln – und ebenso von Verbindlichen Internen Datenschutzvorschriften – selbst mit weiteren Schutzmaßnahmen keine rechtsichere Garantie für die Zulässigkeit einer Datenübermittlung in die USA.

3. Ausnahmetatbestände nach Art. 49 DSGVO gelten nur für Einzelfälle und taugen nicht als allgemeine Grundlage für eine Datenübermittlung

Eine Datenübermittlung ist weiterhin zulässig, wenn ein Ausnahmetatbestand des Art. 49 DSGVO greift, vor allem wenn eine (wirksame) Einwilligung der betroffenen Person vorliegt. Die Hürden für eine solche Einwilligung sind aber hoch: Denn die betroffene Person muss in die vorgeschlagene Datenübermittlung ausdrücklich einwilligen, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde (Art. 49 Abs. 1 S. 1 lit. a DSGVO). Dies impliziert, dass eine derartige Einwilligung nicht pauschal, sondern nur für konkrete Datenübermittlungen erteilt werden kann. Wird die Einwilligung gleichzeitig mit anderen (standardisierten) Vereinbarungen erteilt, sind zudem AGB-rechtliche Wirksamkeitsrisiken, insbesondere mit Blick auf das Verbot überraschender Klauseln (§ 305c Abs. 1 BGB) sowie das Transparenzgebot (§ 307 Abs. 1 S. 2 BGB) zu beachten.

Insgesamt hat der Europäische Datenschutzausschuss die Ausnahmetatbestände so eng ausgelegt, dass sie praktisch nicht als Basis für regelmäßige Datenübermittlungen herangezogen werden können.[7]

4. Vollständige Rechtssicherheit lässt sich nur durch eine ausschließliche Verarbeitung personenbezogener Daten innerhalb der EU gewährleisten

Demnach müssen derzeit für eine in jedem Falle rechtssichere Datenverarbeitung Daten auf Servern in einem Mitgliedstaat der EU vorgehalten werden, ohne dass US-Behörden zum Beispiel über in den USA ansässige Konzernzentralen oder Tochterunternehmen Zugang dazu haben, beispielsweise durch Weisungsrechte, Daten- oder IT-Zugriffsmöglichkeiten.

VI. Einordnung in den HR-Management-Kontext

Das jüngste EuGH-Urteil spiegelt das höchst unterschiedliche Verständnis von Datenschutz in der EU und den USA wider. Es ist zugleich Beleg für die stark zunehmende Bedeutung des Datenschutzes als Wettbewerbskriterium und die erheblichen Rechtsrisiken, die mit der Übermittlung personenbezogener Daten verbunden sind.

Das Urteil betrifft ganz grundsätzlich die alltägliche Arbeit in Personalabteilungen von Unternehmen, etwa Informationen über die Mitarbeiter im Arbeitsvertrag, über die Gehaltsabrechnung, über das Management von Vergütungsdaten bis hin zur betrieblichen Altersversorgung.

Ein typisches Beispiel für das Speichern und Verarbeiten hochsensibler Daten ist der Umgang mit Vergütungsinformationen. Unternehmen überlassen diese Daten oft externen Spezialisten für Gehaltsabrechnungen oder anderen Dienstleistern. Gerade bei Vergütungsinformationen von Top Executives ist zwischenzeitlich unstrittig, dass diese – selbst wenn vermeintlich anonymisiert – in der Regel personenbezogene Daten darstellen.

In den letzten Jahren haben Unternehmen wie Dienstleister ihre HR-Management-Prozesse oft global vereinheitlicht und umfassende cloudbasierte HR-Systeme eingeführt. Dabei wurden teilweise auch Speicherung und Verarbeitung personenbezogener Daten ins außereuropäische Ausland ausgelagert bzw. werden solche Systeme aus Drittstaaten betreut. Die erweiterten Prüfpflichten vor der Übermittlung von Daten beispielsweise an Dienstleister lösen potenziell nicht nur erhebliche Reputations- und Rechtsrisiken – bis hin zu empfindlichen Bußgeldern und Schadensersatzansprüchen Betroffener – aus, sondern berühren bei Verstößen auch unternehmensinterne Compliance-Vorgaben. Denn diese sehen oftmals auch die Einhaltung der datenschutzrechtlichen Vorschriften vor.

Darüber hinaus ist in vielen Dienstverträgen von Führungskräften inzwischen die explizite Verpflichtung enthalten, die Bestimmungen der DSGVO zu beachten. Damit wird aus dem Datenschutz- auch ein arbeitsrechtliches Risiko für die Betroffenen. Und im Rahmen der Vorstandsvergütung börsennotierter Unternehmen werden zunehmend sogenannte Clawback-Klauseln vereinbart, welche die Rückforderung ausgezahlter variabler Vergütung bei Compliance-Verstößen erlauben.[8]

An diesen Beispielen wird deutlich, dass die Auswirkungen des jüngsten Urteils des EuGH zu Privacy Shield weit über den engeren datenschutzrechtlichen Kontext hinaus reichen. Auch aus diesem Grund sind getroffene strategische Entscheidungen zur Speicherung und Verarbeitung personenbezogener Daten neu zu bewerten und gegebenenfalls unverzüglich zu revidieren. Am sichersten fahren Unternehmen, wenn sie personenbezogene Daten europäischer Mitarbeiter und Kunden nur in Europa speichern und verarbeiten (lassen). Sie sind dabei gut beraten, an dauerhaft rechtssicheren Lösungen zur Übertragung von Daten in die USA zu arbeiten, wenngleich verlässliche Lösungen momentan nicht in Sicht scheinen.

AUTOR

Dr. Jan Dörrwächter *ist Rechtsanwalt und seit April 2017 Senior Partner und Mitglied der Geschäftsleitung der hkp/// group. Er berät Unternehmen unter anderem in allen Fragen der Vorstandsvergütung, aber auch zur Vergütung von Führungskräften und sonstigen Mitarbeitern einschließlich des Tarifbereichs.*

Johannes Brinkkötter *ist Rechtsanwalt und seit Juli 2018 Partner und Mitglied der Geschäftsleitung der hkp/// group. Er zählt zu den führenden Shared Service Beratern in Deutschland und blickt auf eine themenspezifisch geprägte Laufbahn im BASF- und EON-Konzern zurück.*

7 *Schröder*, DB 2020, 1945, 1948.

8 Dazu näher *Dörrwächter/Wolff*, AG 2020, 233.