Nach dem Ende von Safe Harbor: Whitepaper zu Datenexporten in die USA

I. Einleitung

Nicht erst seit dem Urteil des Europäischen Gerichtshofs (EuGH) zu Safe Harbor stehen die USA im besonderen Fokus des Datenschutzes. Über Jahre hinweg wurden Bemühungen auf politischer Ebene zur Gewährleistung eines angemessenen Datenschutzniveaus beim transatlantischen Handelspartner kritisiert, sei es in Gestalt des „sicheren Hafens“ oder im Zuge des gescheiterten „No-Spy-Abkommens“. Entsprechend sind hiesige verantwortliche Stellen verunsichert, ob personenbezogene Daten aus Europa noch zulässigerweise in die USA exportiert werden dürfen. Dieses Whitepaper des GDD-Arbeitskreises „Datenschutz International“ möchte einen Überblick über die gegenwärtige Sachlage geben, um Datenverarbeiter bei der Entscheidungsfindung zu unterstützen. Es stellt jedoch kein abschließendes Rechtsgutachten zur Zulässigkeit entsprechender Datenübermittlungen dar.

II. Management Summary

Die Rechtslage zur Zulässigkeit transatlantischer Datenströme ist weiterhin **nicht eindeutig geklärt**, insbesondere so lange sich die europäischen Aufsichtsbehörden bezüglich der alternativen Übermittlungswerkzeuge (EU-Standardvertragsklauseln und Binding Corporate Rules) nicht eindeutig positioniert haben und die Angemessenheitsentscheidung der EU-Kommission zum **EU-US Privacy Shield** noch nicht in Kraft getreten ist. Wann die Kommission die Angemessenheitsentscheidung zum Nachfolgeabkommen annehmen wird, ist derzeit noch ungewiss, wobei es Hinweise für eine Verabschiedung im Sommer 2016 gibt.

Nicht von der Hand zu weisen sind die politischen Bemühungen, um in den USA ein angemessenes Datenschutzniveau zu gewährleisten. Bis zu dem Zeitpunkt der endgültigen Positionierung der europäischen Aufsichtsbehörden bzw. der Verabschiedung der Angemessenheitsentscheidung zum EU-US Privacy Shield haben verantwortliche Stellen **abzuwägen**, ob sie weiterhin personenbezogene Daten in die USA übermitteln möchten. Sollten Stellen weiterhin auf Datenexporte in die USA setzen, sollte ein verstärktes Augenmerk auf die Aussagen der zuständigen Aufsicht zur Zulässigkeit der alternativen Übermittlungswerkzeuge gelegt werden. Ebenso sollte die Implementierung zusätzlicher **technisch-organisatorischer Maßnahmen** erwogen werden, um personenbezogene Daten zusätzlich zu schützen.

III. Das Safe Harbor Urteil und seine Folgen

Der EuGH hat mit seiner Entscheidung zu Safe Harbor am 6. Oktober 2015 hohe Wellen in die transatlantischen Datenströme geschlagen. Mit Verkündung des Urteils waren Datenexporte in die USA auf Basis der Angemessenheitsentscheidung der EU-Kommission zu Safe Harbor als rechtswidrig einzustufen, was an sich einen sofortigen Stopp diesbezüglicher Da-

tenexporte bedeutet hätte. Schnell waren die europäischen Aufsichtsbehörden versucht, weitere Rückschlüsse aus den Entscheidungsgründen des EuGH zu ziehen, was sich in einer Vielzahl behördlicher Stellungnahmen manifestierte. Erst die Artikel-29-Datenschutzgruppe auf europäischer Ebene sowie die Konferenz der Datenschutzbeauftragten von Bund und Länder auf nationaler Ebene vermochten Datenverarbeitern eine erste konsolidierte und praktikable Meinung zu den Folgen des Safe Harbor Urteils zu vermitteln.

Sowohl das Positionspapier der Konferenz der Datenschutzbeauftragten von Bund und Ländern[1] als auch die Artikel-29-Datenschutzgruppe[2] forderten die Mitgliedstaaten und die europäischen Institutionen nachdrücklich dazu auf, offene Gespräche mit den US-amerikanischen Behörden zu führen, um **politische, rechtliche und technische Lösungen für einen angemessenen Schutz der Grundrechte der EU-Bürger** zu finden. Gleichzeitig würde weiter untersucht werden, wie sich das EuGH-Urteil auf **andere Werkzeuge** zur Herstellung eines angemessenen Datenschutzniveaus in einem Drittland wie die **EU-Standardvertragsklauseln** oder **Binding Corporate Rules (BCRs)** auswirkt. Für die letztgenannten Werkzeuge wurde eine Frist bis Ende Januar 2016 gesetzt, bevor konsolidierte Durchsetzungsmaßnahmen der Aufsichtsbehörden – je nach Ausgang der Prüfung – verpflichtend umzusetzen wären. Die von der Artikel-29-Datenschutzgruppe und der Konferenz der Datenschutzbeauftragten von Bund und Ländern gesetzte Frist haben die Mitgliedstaaten und die europäischen Institutionen verstreichen lassen. Inzwischen drohen nationale Aufsichtsbehörden teilweise explizit Durchsetzungsmaßnahmen bezüglich der Datenexporte an, die noch auf Basis von Safe Harbor von statten gehen.[3]

Erst kurz nach Ablauf der gesetzten Frist veröffentlicht die EU-Kommission am 2. Februar 2016 eine Presseerklärung, in der eine Einigung zwischen der EU Kommission und den Vereinigten Staaten hinsichtlich einer Nachfolgeregelung von Safe Harbor, genannt **„EU-US Privacy Shield“,** verkündet wurde und bereits erste Eckpunkte vorgesehener Maßnahmen beinhaltete.[4] Detaillierte Informationen hinsichtlich der Umsetzung der Vorgaben des EuGH bezüglich der transatlantischen Datenströme waren der Erklärung noch nicht zu entnehmen, was die Artikel-29-Datenschutzgruppe zu der Aufforderung veranlasste, man möge ihr die entsprechenden Unterlagen über die Einzelheiten der Einigung bis Ende Februar 2016 zur Prüfung vorlegen.[5] Mittels der vorgelegten Unterlagen könne dann, neben der Bewertung des EU-US Privacy Shields, auch eine abschließende Einschätzung zu den alternativen Instrumenten für einen Datenexport in die USA, so auf Basis der EU-Standardvertragsklauseln oder der BCRs, erfolgen.

---

[1] https://www.datenschutz.rlp.de/de/grem_dsbkonferenz/sonstiges/20151021_Positionspapier_DSK_Safe_Harbor.pdf.

[2] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

[3] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Aktueller Sachstand zu Safe Harbor (Februar 2016), abrufbar unter. https://www.datenschutz-hamburg.de/news/detail/article/safe-harbor-aktueller-sachstand-im-februar-2016.html; Der Landesbeauftragte für Datenschutz und Informationsfreiheit Rheinland-Pfalz, Pressemitteilung vom 10. Februar 2016, abrufbar unter https://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2016021001.

[4] http://europa.eu/rapid/press-release_IP-16-216_en.htm.

[5] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf.

IV. EU-US Privacy Shield

Zum Ende der durch die Artikel-29-Datenschutzgruppe festgesetzten Frist veröffentlicht die EU-Kommission am 29. Februar 2016 verbindliche Inhalte des neuen **EU-US Privacy Shield** als Nachfolgeinstrument zu Safe Harbor. Ziel soll es sein – wie bereits im Rahmen von Safe Harbor – ein angemessenes Datenschutzniveau bei Datenempfängern in den USA zu gewährleisten, die sich nach den Vorgaben des EU-US Privacy Shield („**EU-US Privacy Shield Framework Principles**“[6]) zertifiziert haben. Hierbei wurden auf Basis der bereits in 2013 durch die Kommission selbst vorgeschlagenen 13 Empfehlungen zur Verbesserung von Safe Harbor[7] sowie den Entscheidungsgründen des EuGH die Anforderungen an zertifizierte Datenverarbeiter in den USA erhöht. Hinsichtlich des Anwendungsbereichs der Angemessenheitsentscheidung der Kommission tritt beim Privacy Shield aber zunächst keine Neuerung ein: Nur zertifizierte Unternehmen in den USA sollen in den Genuss europäischer Daten kommen. Welche erweiterten Vorgaben das „Datenschutzschild“ mit sich bringt, soll nachfolgend anhand ausgewählter Themen vorgestellt werden.

1. Transparenz

Eine Zertifizierung nach dem Privacy Shield erfolgt durch eine Erklärung gegenüber dem US-Handelsministerium und bedarf einer jährlichen Aktualisierung. Änderungen ergeben sich bei der Publizität von Zertifizierungen, die in der Vergangenheit nicht ausreichend gewährleistet war: Das US-Handelsministerium soll nunmehr ein Register führen, das neben bestehenden Zertifizierungen auch **unwirksame** bzw. **entzogene Zertifikate** sowie den diesbezüglichen **Grund** aufführt (Erwägungsgrund 24 und 39 der Angemessenheitsentscheidung im wurf[8]). **Anhängige Verfahren** bei der Federal Trade Commission (FTC), als einem Organ der Aufsicht über das Privacy Shield, so beispielsweise auf Grund eines Verstoßes gegen dessen Vorgaben, sollen über das Register nun ebenfalls kommuniziert werden.

Dauerhafte Verstöße gegen die Vorgaben des Privacy Shields resultieren nicht nur in der Entfernung aus dem Register aktueller Zertifizierungen, sondern münden in der Pflicht zur **Löschung aller unter dem Privacy Shield empfangenen Daten** (Erwägungsgrund 26). In anderen Fällen, die zu einem Entzug einer Zertifizierung führen, kann eine Stelle die empfangenen Daten zwar weiterhin verarbeiten. Das setzt aber voraus, dass sie gegenüber dem US-Handelsministerium erklärt, dass diese Daten weiterhin nach den Vorgaben der Privacy Shield Framework Principles oder mit Hilfe alternativer anerkannter Werkzeuge zur Herstellung eines angemessenen Datenschutzniveaus, so beispielsweise die EU-Standardvertragsklauseln, geschützt werden.

Die fälschliche Kommunikation einer gültigen Zertifizierung wird durch die Organe der Aufsicht verfolgt, wobei die Aufsicht im Wesentlichen der FTC, dem US-Handelsministerium bzw. dem US-Verkehrsministerium (Department of Transportation) obliegt. Um das Netz der Überwachung enger zu stricken, soll das Handelsministerium gar proaktiv kontrollieren, ob die Datenschutzerklärung des „ausgeschiedenen“ Unternehmens keinerlei Bezüge zum Privacy Shield mehr enthält (Erwägungsgrund 28). Verstöße sollen wiederum den Aufsichtsorganen mit Durchsetzungskompetenzen zugeleitet werden. Ebenso stellt das Handelsministe-

[6] Zu den Privacy Shield Framework Principles ausführlich, Angemessenheitsentscheidung der Kommission, Erwägungsgründe 16-23.
[7] http://europa.eu/rapid/press-release_MEMO-13-1059_de.htm.
[8] Im Weiteren wird auf den Zusatz „Angemessenheitsentscheidung im Entwurf“ verzichtet.

rium proaktiv sicher, so über das Versenden von **Fragebögen**, dass Unternehmen mit erloschener Privacy Shield Zertifizierung empfangene Daten gelöscht haben, bzw. freiwillig diese Daten nach den Vorgaben der Privacy Shield Principles oder alternativer anerkannter Angemessenheitswerkzeuge schützen (Erwägungsgrund 39).

2. Beschwerden und Abhilfemaßnahmen

Bereits unter Safe Harbor mussten US-Datenverarbeiter Beschwerdeverfahren zu Gunsten von Betroffenen einrichten und die eingerichtete Kontaktstelle zur Entgegennahme von Beschwerden über die Datenschutzerklärung kommunizieren. Um diese Verfahren zu beschleunigen, sind Beschwerden Betroffener nunmehr innerhalb einer Frist von **45 Tagen** durch den Datenverarbeiter zu beantworten. Auch die Streitschlichtung erfährt neue Blüte, indem eine unabhängige Stelle zu involvieren ist, die, neben kostenfreien Abhilfemaßnahmen zu Gunsten des Betroffenen, auch **einen jährlichen Bericht** hinsichtlich ihrer Aktivitäten mit Blick auf das Privacy Shield zu veröffentlichen hat, so unter anderem auch die Anzahl der Fälle, die Länge ihrer Bearbeitung sowie deren Ergebnis (Erwägungsgrund 31). Ebenso wird auf Seiten des Handelsministeriums sowie der FTC eine **Kontaktstelle** für **europäische Aufsichtsbehörden** eingerichtet, um Beschwerden Betroffener anzunehmen sowie beim US-Datenverarbeiter nachzuverfolgen. Die Kontaktstelle beim Handelsministerium hat innerhalb von höchstens **90 Tagen** über den Verlauf, bzw. Ausgang des Verfahrens zu informieren. Hierbei hat das Handelsministerium jährlich über eingegangene Beschwerden Bericht zu erstatten (Erwägungsgrund 36).

Im Zuge der Verbesserung von Safe Harbor wurde den europäischen Aufsichtsbehörden im EU-US Privacy Shield bei den Beschwerde- und Abhilfeverfahren eine besondere Rolle zugebilligt. Neben den erwähnten Kontaktstellen für aus Europa eingehende Beschwerden, soll die Meinung der europäischen Aufsicht zu bestimmten Streitfällen über ein eigenes, jedoch **informelles Gremium**, Gehör finden (s. Ergänzungsdokument zum EU-US Privacy Shield „The Role of the Data Protection Authorities). Für die Beschleunigung des Verfahrens sorgt wiederum eine Frist von **60 Tagen**, innerhalb derer die Aufsicht ihre Meinung gegenüber dem Handelsministerium, bzw. der FTC, kommuniziert haben muss. Sollte ein Unternehmen nicht innerhalb von **25 Tagen** den Rat der Aufsichtsbehörden umsetzen, werden wiederum die Aufsichtsorgane über das Privacy Shield informiert, was in Durchsetzungsmaßnahmen münden kann.

Sollte der Beschwerde eines Betroffenen über keines der verfügbaren Verfahren Abhilfe verschafft werden können, soll das **Privacy Shield Panel** als letzte Instanz durch den Betroffenen angerufen werden können (Erwägungsgrund 46). Dieses aus 20 ständigen Mitgliedern bestehende und vom Handelsministerium ernannte Expertengremium wird sich mittels einer Unterarbeitsgruppe Beschwerden von Betroffenen anhand festgelegter Verfahrensregeln zuwenden. Betroffene können den Verhandlungen über eine Video- oder Telefonkonferenz beiwohnen. Auf Basis einer nachvollziehbaren Begründung des Betroffenen kann ebenfalls eine **Übersetzung der Verhandlung** kostenfrei zur Verfügung gestellt werden. Für Vorbereitungsmaßnahmen des Betroffenen im Vorfeld der Verhandlung soll die zuständige nationale Aufsichtsbehörde unterstützend mitwirken. Sind Schlichtungs- oder Durchsetzungsmaßnahmen auch nach Einberufung des Privacy Shield Panels in den Augen eines Betroffenen immer noch nicht ausreichend erfolgt, um seiner Beschwerde Abhilfe zu verschaffen, besteht für den Betroffenen in letzter Instanz die Möglichkeit des Anrufens einer **Schiedsgerichtsbarkeit in den USA** nach dem **Federal Arbitration Act** (Erwägungsgrund 47).

3. Audits

Die Pflicht zur Überprüfung der Einhaltung der Privacy Shield Principles obliegt weiterhin jedem Datenverarbeiter selbst, indem er interne Audits durchführt oder Dritte mit der Überprüfung beauftragt. Daneben soll jedoch das Handelsministerium eine zusätzliche Kontrolle der Einhaltung durch die Versendung entsprechender **Fragebögen** durchführen. Dies kann anlassunabhängig erfolgen oder beispielsweise auf Basis der Eingabe eines Betroffenen, bzw. im Falle einer nicht erfolgten Streitschlichtung (Erwägungsgrund 35). Im Falle aufsichtsbehördlicher Ermittlungen sind Nachweise für die Implementierung der Privacy Shield Framework Principles vorzuhalten (Erwägungsgrund 30).

4. Onward Transfers

Die Verantwortlichkeit für die Weitergabe von Daten an weitere Stellen („Onward Transfers“) wird erweitert. Im Unterschied zu Safe Harbor, das eine Weitergabe an ebenfalls zertifizierte Stellen ohne Einschränkungen zugelassen hatte, knüpft der Privacy Shield die Weitergabe an eine konkrete Zweckbindung und vertragliche bzw. vergleichbare Regelungen innerhalb von Unternehmensgruppen, die die Umsetzung der Vorgaben des Privacy Shields garantieren (Erwägungsgrund 22). Bei Datenschutzverstößen in einer Verarbeitungskette ist die für die Verarbeitung der Daten verantwortliche Stelle (Controller) uneingeschränkt haftbar, sofern sie sich nicht exkulpieren kann.

5. Verwendung von Daten des Privacy Shield für die nationale Sicherheit

Die Angemessenheitsentscheidung der Kommission enthält eine ausführliche Analyse bestehender Beschränkungen des US-Rechts hinsichtlich der Verwendung personenbezogener Daten des Privacy Shields durch Geheimdienste, bestehende Rechtschutzmöglichkeiten sowie der Überwachung solcher Dienste (Erwägungsgrund 52 ff.). Diese Rahmenbedingungen seien nach Auffassung der Kommission in Folge der von ihr ausgesprochenen Empfehlungen von 2013 nochmals verschärft worden (Erwägungsgrund 55). Was zunächst als Klarstellung gegenüber verunsicherten EU-Bürgern bzw. Datenverarbeitern zu verstehen ist, wird jedoch auch mit Ergänzungen versehen, die im Zuge der Verhandlungen zwischen der Kommission und Vertretern der US-Regierung entstanden sind.[9] Hervorzuheben ist die Einrichtung einer unabhängigen Ombudsperson für Datenschutz („**Privacy Shield Ombudsperson“**). Diese Ombudsperson soll nicht nur auf Anfrage einer ausländischen Regierung hin Datenverarbeitungen der US-Geheimdienste auf ihre Zulässigkeit hin prüfen, sondern ebenfalls Beschwerden von Betroffenen zum Anlass für Prüfungen nehmen. Eine direkte Anlaufstelle für Betroffene stellt die Ombudsperson jedoch nicht dar. Vielmehr müssen sich Betroffene zunächst an die jeweilige nationale Aufsicht in der EU bezüglich vermuteter Geheimdienstaktivitäten wenden, bevor diese eine Beschwerde weiterleitet. Hierbei brauchen Betroffene jedoch nicht zu beweisen, dass ihre Daten tatsächlich durch Geheimdienste unzulässig verwendet wurden.

[9] Ausführlich hierzu Erwägungsgründe 56 ff.

6. Stellungnahme der Artikel-29-Datenschutzgruppe

Die Artikel-29-Datenschutzgruppe hat im Sinne ihrer beratenden Funktion am 13. April 2016 eine Stellungnahme zu den Inhalten des EU-US Privacy Shield abgegeben.[10] Darin begrüßt sie die erheblichen Verbesserungen durch das Privacy Shield im Vergleich zum vorherigen Safe-Harbor-Framework. Gleichwohl identifiziert sie im Rahmen der inhaltlichen Auseinandersetzung eine Reihe von Aspekten, bei denen sie Nachbesserungsbedarf sieht. Neben sprachlichen Ungereimtheiten bestünden u.a. Bedenken hinsichtlich einer fehlenden Regelung zur Datenlöschung, der weiterhin bestehenden Möglichkeit von massenhaften und willkürlichen Datensammlungen sowie einer unklaren Kompetenz und Stellung der Ombudsperson.

7. Angemessenes Datenschutzniveau

Unter den verbindlichen Dokumenten zum Privacy Shield findet sich auch ein Entwurf für eine Angemessenheitsentscheidung der Kommission zur Gewährleistung eines angemessenen Datenschutzniveaus hinsichtlich zertifizierter Stellen nach dem EU-US Privacy Shield. Gem. Art. 25 Abs. 6 der EU-Datenschutzrichtlinie 95/46/EG kann die Kommission in einem Ausschußverfahren feststellen, dass ein Drittland auf Grund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein **angemessenes Schutzniveau für personenbezogene Daten** gewährleisten. Ziel der Kommission ist es, allen Stellen in den USA, die sich den Vorgaben des Privacy Shield einer Zertifizierung unterwerfen, ein angemessenes Datenschutzniveau zu attestieren. Eine Genehmigung der Aufsichtsbehörde für den einzelnen Datenexport an den nach dem Privacy Shield zertifizierten Empfänger wäre dann - wie bereits im früheren Verfahren bei Safe Harbor - nicht mehr erforderlich.

In den Augen der Kommission bieten die USA durch die neuen Vorgaben des EU-US Privacy Shield sowie den rechtlichen Rahmenbedingungen für die Verwendung personenbezogener Daten von EU-Bürgern durch US-Geheimdienste ein **angemessenes Datenschutzniveau** im Sinne der EU-Datenschutzrichtlinie. Um Veränderungen rechtlicher oder tatsächlicher Art Rechnung zu tragen, soll die Angemessenheitsentscheidung mit Blick auf die Wirksamkeit der darin vereinbarten Maßnahmen zum Privacy Shield eine **jährliche Überprüfung** zusammen mit dem Handelsministerium, der FTC sowie weiteren US-Behörden (falls erforderlich) durchlaufen (Erwägungsgrund 122). Sowohl die europäischen Aufsichtsbehörden als auch die Artikel-29-Datenschutzgruppe können dieser Überprüfung beiwohnen. Begründen Tatsachen die Annahme, dass die getroffenen Vereinbarungen rund um das EU-US Privacy Shield nicht eingehalten werden oder die Rahmengesetzgebung der USA bezüglich Datenerhebungen und Verwendungen der Geheimdienste kein ausreichendes Schutzniveau mehr gewährleistet, soll die Angemessenheitsentscheidung **widerrufen** werden können (Erwägungsgrund 125 f.).

Da diese Angemessenheitsentscheidung auf Basis der Stellungnahme der Artikel-29-Datenschutzgruppe und einem Ausschußverfahren nach Art. 31 Abs. 2 der EU-Datenschutzrichtlinie erst noch verabschiedet werden muss, können Datenübermittlungen in die USA auf Basis des EU-US Privacy Shield derzeit noch nicht erfolgen.

[10] Abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

V. EU-Standardvertragsklauseln/Binding Corporate Rules

Entgegen der Ankündigung der Artikel-29-Datenschutzgruppe wurden die alternativen Instrumente zur Herstellung eines angemessenen Datenschutzniveaus im Drittland keiner abschließenden Prüfung unterzogen. Durch die Veröffentlichung der Dokumente zum EU-US Privacy Shield ist die Artikel-29-Datenschutzgruppe dazu aufgefordert, hier eine abschließende Meinung abzugeben. In der Zwischenzeit hat jede verantwortliche Stelle zu prüfen, ob sie weiterhin von den alternativen Instrumenten Gebrauch machen möchte oder von einem Datenexport in die USA Abstand nimmt. Im Unterschied zu Datenexporten auf der Grundlage von Safe Harbor gewähren die nationalen Aufsichtsbehörden teilweise eine Schonfrist[11], bzw. verweisen auf die ausstehende Prüfung der Artikel-29-Datenschutzgruppe.[12] Ferner werden keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen erteilt.[13] Anzumerken ist, dass derzeit lediglich 10 von insgesamt 17 Datenschutzaufsichtsbehörden in Deutschland sich die Genehmigung von Datenübermittlungen auf Grundlage von BCRs vorbehalten haben.[14] Darüber hinaus kann nicht ausgeschlossen werden, dass Bürger gegen Datenübermittlungen in die USA auf der Grundlage von Standardvertragsklauseln klagen, und die Frage der Zulässigkeit letztlich beim EuGH beurteilt werden wird.

VI. Weitere Maßnahmen zur Stärkung des Datenschutzes

1. Datenschutz-Rahmenabkommen

Seit 2010 verhandelt die EU-Kommission über das erste Datenschutz-Rahmenabkommen mit den USA („**Data Protection Umbrella Agreement**“). Hintergrund waren die Auseinandersetzungen um transatlantische Abkommen zur Übermittlung personenbezogener Daten in die USA, so beispielsweise bei Bankdaten (SWIFT) und Flugreisedaten bei den Passenger Name Records („PNR“). Statt bei jeder neuen Datenübermittlung erneut über Datenschutzbestimmungen zu verhandeln, sollen datenschutzrechtliche Grundsätze erarbeitet werden, die dann für alle Abkommen im Bereich der **Verhütung, Aufdeckung, Untersuchung und Verfolgung von Straftaten, einschließlich des Terrorismus** gelten. Vorgesehen ist hierbei, EU-Bürgern den gleichen gerichtlichen Rechtschutz wie US-Bürgern zu gewähren, sollte es zu einem Datenschutzverstoß gekommen sein.[15] In den Augen der Kommission soll das Rahmenabkommen jedoch weder eine Rechtsgrundlage für den transatlantischen Datenaustausch darstellen noch ein angemessenes Datenschutzniveau im Sinne des Art. 25 Abs. 6

[11] Vgl. Pressemitteilung des LfD Rheinland-Pfalz vom 10.02.2016.

[12] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Safe Harbor - aktueller Sachstand im Februar 2016, abrufbar unter https://www.datenschutz-hamburg.de/news/detail/article/safe-harbor-aktueller-sachstand-im-februar-2016.html.

[13] Konferenz der Datenschutzbehörden des Bundes und der Länder, Positionspapier zu Safe Harbor vom 26.10.2015, abrufbar unter https://www.datenschutz.hessen.de/ft-europa.htm#entry4521.

[14] Vgl. Liste “National filing requirements for controller BCR (“BCR-C”)”, abrufbar unter http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf.

[15] Hierzu wurde der US Privacy Act durch den Judicial Redress Bill am 24.02.2016 novelliert; kritisch zu den Rechtschutzmöglichkeiten von lediglich EU-Bürgern, Juristischer Dienst des Europäischen Parlaments, Stellungnahme zum Rahmenabkommen vom 14.01.2016, abrufbar unter http://statewatch.org/news/2016/feb/ep-legal-opinion-umbrella.pdf.

der Richtlinie 95/46/EC bieten. Eine Einigung hinsichtlich des Datenschutz-Rahmenabkommens ist bis zum heutigen Tag jedoch noch nicht erfolgt.

2. Privacy Council

Im Zuge verstärkter Aktivitäten rund um die Cybersicherheit hat Präsident Obama am 9. Februar 2016 per Exekutiverlass[16] die Einrichtung eines permanenten Datenschutzgremiums auf Bundesebene (**„Federal Privacy Council“**) angekündigt, das die Datenschutzkoordinatoren in den jeweiligen Behörden („**Senior Agency Officials for Privacy**“) im Rahmen ihrer Tätigkeiten bei der Wahrung des Datenschutzes und seiner Durchsetzung unterstützen soll. Zu den Kernaufgaben des Datenschutzgremiums gehört sowohl die **Entwicklung und Koordinierung von Datenschutz-Vorgaben** bzw. **Best Practices** als auch die Analyse des Weiterentwicklungsbedarfs auf Regierungsebene. Die neuen Anforderungen an die Datenschutzkoordinatoren in den Behörden sollen innerhalb von 120 Tagen kommuniziert werden. Dann ist auch mit der Aufnahme der praktischen Arbeit des Datenschutzgremiums zu rechnen.

VII. Fazit

Die Rechtslage zur Zulässigkeit transatlantischer Datenströme in die USA ist weiterhin **nicht eindeutig erklärt**, insbesondere so lange sich die europäischen Aufsichtsbehörden bezüglich der alternativen Übermittlungswerkzeuge noch nicht eindeutig positioniert haben und die Angemessenheitsentscheidung der EU-Kommission zum **EU-US Privacy Shield** noch nicht in Kraft getreten ist. Die von der Artikel-29-Datenschutzgruppe und der Konferenz der Datenschutzbeauftragten von Bund und Ländern gesetzte Frist zur Umstellung von Datenexporten auf Basis von Safe Harbor ist am 31.01.2016 verstrichen. Unternehmen, die gehofft hatten, ihre auf Safe Harbor gestützten Datenübermittlungen an verantwortliche Stellen in den USA nahtlos auf ein Nachfolgeabkommen überführen zu können, sind enttäuscht worden. Für diese Unternehmen besteht nun dringender Handlungsbedarf, um aufsichtsbehördliche Sanktionen zu vermeiden, insbesondere wenn die Datenexporte aus einem Bundesland erfolgen, in dem die zuständige Aufsichtsbehörde bereits mit der Verhängung von Sanktionen begonnen hat.

Zwar sind die politischen Bemühungen, um in den USA ein angemessenes Datenschutzniveau zu gewährleisten, nicht von der Hand zu weisen. Die Verhandlungen zum EU-US Privacy Shield sind jedoch noch nicht abgeschlossen. Wann die Kommission die Angemessenheitsentscheidung zum Nachfolgeabkommen annehmen wird, ist derzeit noch ungewiss, wobei Hinweise hinsichtlich einer Verabschiedung im Sommer 2016 bestehen.

Bis zu dem Zeitpunkt der endgültigen Positionierung der europäischen Aufsichtsbehörden bzw. der Verabschiedung der Angemessenheitsentscheidung zum EU-US Privacy Shield haben verantwortliche Stellen **abzuwägen**, ob sie weiterhin personenbezogene Daten in die USA übermitteln möchten oder nicht doch alternative Möglichkeiten in Betracht ziehen. Festzuhalten ist allerdings, dass Datenübermittlungen zumindest auf der Grundlage der EU-Standardvertragsklauseln bis auf Weiteres gesetzeskonform sind.

[16] https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council.

Sollten oder müssen Stellen weiterhin auf Datenexporte in die USA setzen, sollte ein verstärktes Augenmerk auf die **Aussagen der zuständigen Aufsicht** zur Zulässigkeit der alternativen Übermittlungswerkzeuge gelegt werden. Praktisch kommen dabei derzeit ausschließlich die EU-Standardvertragsklauseln in Betracht, da die Aufsichtsbehörden mit dem Beschluss der Konferenz der Datenschutzbeauftragten von Bund und Ländern angekündigt haben, bis zur Vorlage der noch ausstehenden finalen Stellungnahme der Artikel-29-Datenschutzgruppe keine neuen Genehmigungen für Datenexporte in die USA zu erteilen. Von dieser Entscheidung sind grundsätzlich alle laufenden bzw. neu beginnenden Genehmigungsverfahren für Binding Corporate Rules oder Einzelgenehmigungen auf Grundlage einer Entscheidung nach § 4c Abs. 2 BDSG („ad-hoc“-Datenexportverträge) betroffen.

Unabhängig vom aktuellen Stand der Verhandlungen sollte für Datenexporte in die USA die Implementierung zusätzlicher **technisch-organisatorischer Maßnahmen** erwogen werden (zum Beispiel Verschlüsselung), um personenbezogene Daten zusätzlich zu schützen (Anhaltspunkte dazu finden sich u.a. in der Orientierungshilfe „Cloud Computing“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises[17]).

Wenn an Unternehmen in die USA exportierte Daten an weitere Stellen weitergegeben werden (Onward Transfers), sollte auf Grund des zu erwartenden Aufwands bereits jetzt mit der **Dokumentation der Unterauftragnehmerbeziehungen** begonnen werden, da für Datenexporte auf Grundlage des EU-US Privacy Shields zukünftig vergleichbar strenge Anforderungen gelten werden, wie dies bereits jetzt bei den EU-Standardvertragsklauseln der Fall ist.

Unabhängig davon, wie sich die EU-Kommission bzw. die Artikel-29-Gruppe hinsichtlich der Datenübermittlungen in die USA positionieren: Ein nicht kalkulierbares Risiko besteht darin, dass durch initiierte Klagen gegen die Rechtsgültigkeit von Datenexporten in die USA eine negative Entscheidung des EuGH auch in Bezug auf die alternativen Instrumente nicht ausgeschlossen werden kann.

Bonn, 20. April 2016

[17] https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf