WIE GEHT ES NACH DEM SAFE-HARBOR-URTEIL DES EUGH WEITER?

Safe-Harbor-Alternativen und deren Tücken [1,2]

Was ist passiert?

Bisher haben sich deutsche Unternehmen, die personenbezogene Daten von US-Unternehmen weiterverarbeiten lassen wollten, zur Datenübermittlung an das entsprechende US-Unternehmen häufig auf das Safe-Harbor-Abkommen gestützt.[3] Das Abkommen sollte dafür Sorge tragen, dass Datenübermittlungen zwischen dem Europäischen Wirtschaftsraum (EWR) und den USA nicht auf Grund der unterschiedlichen Datenschutzniveaus innerhalb des EWR einerseits sowie den USA als sogenanntem Drittstaat andererseits zum Erliegen kommen. Die Europäische Kommission erkannte in ihrer Entscheidung 2000/520/EG an, dass US-Unternehmen immer dann ein ausreichendes Datenschutzniveau zusichern können, wenn diese die Safe-Harbor-Datenschutzprinzipien anerkennen. Bei diesen Prinzipien handelte es sich um Rahmenbedingungen zum Schutz der Betroffenen vor unberechtigtem Umgang mit deren Daten. In ihrer Gesamtheit sollten die Rahmenbedingungen dafür Sorge tragen, dass ein US-Unternehmen durch eine Erklärung gegenüber der Federal Trade Commission, die Safe-Harbor-Prinzipien einzuhalten, ein mit dem EWR vergleichbares Datenschutzniveau herstellen konnte und somit Übermittlungen von Daten aus dem EWR zu dem US-Unternehmen möglich wurden.[4]

Am 06. Oktober 2015 erklärte der Europäische Gerichtshof, kurz: EuGH, das Safe-Harbor-Abkommen jedoch für ungültig.[5] Der EuGH rügt u. a., dass die nationale Sicherheit der USA Vorrang vor dem Safe-Harbor-Abkommen habe und

[1] Hinweis: Die in diesem Artikel enthaltenen Arbeitsergebnisse sind sorgfältig und unter Zugrundelegung des bekannten Standes der Wissenschaft erstellt worden, stellen jedoch Forschungsansätze dar. Eine Haftung oder Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird aus diesem Grund nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

[2] Die Autoren danken SAP Deutschland SE & Co. KG für die freundliche Unterstützung dieses Artikels.

[3] Zur zweistufigen Prüfung für Datenübermittlungen an Drittstaaten vgl. §§ 4b, 4c BDSG sowie den Beschluss des Düsseldorfer Kreis vom 11. und 12.09.2013 zur Datenübermittlung in Drittstaaten.

[4] Erd, K und R 2010, S. 624 (624); Selzer, DuD 2014, S. 470 (473).

[5] Vgl. Pressemitteilung Nr. 117/15 vom 06.10.15 der Europäischen Union: *http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117de.pdf*.

dies zur Folge habe, dass US-Unternehmen verpflichtet sind, die Safe-Harbor-Prinzipien zu ignorieren, wenn diese im Widerspruch zu den Erfordernissen der nationalen Sicherheit der USA stehen. Der EuGH betont, dass es US-Behörden durch diesen Umstand möglich wäre, ohne Einschränkungen auf den Inhalt elektronischer Kommunikation zuzugreifen. Dies verletze den Wesensgehalt des europäischen, grundrechtlich verankerten Schutzes des Privatlebens. Darüber hinaus erklärt der EuGH, dass Regelungen, die Bürgern nicht erlauben, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden Daten zu erlangen sowie deren Löschung zu erwirken, »den Wesensgehalt des Grundrechts auf wirksamen gerichtlichen Rechtsschutz verletzt. Eine solche Möglichkeit ist dem Wesen eines Rechtsstaats inhärent.«[6] Konsequenterweise dürfen europäische Unternehmen, welche Daten ihrer Kunden und/oder Mitarbeiter an US-Unternehmen übermitteln wollen, die Datenübermittlung ab sofort nicht mehr auf das Safe-Harbor-Abkommen stützen.

Welche Alternativen gibt es?

International agierende Unternehmen müssen sich nun mit Alternativen zu Safe-Harbor befassen, um Datenübermittlungen an US-Unternehmen datenschutzkonform ausgestalten zu können.

a) EU-US-Datenschutzschild

Trotz teilweise heftiger Proteste von Datenschutzexperten trat am 12. Juli 2016 der EU-US-Datenschutzschild, auch »Privacy-Shield« genannt, als Nachfolger von Safe-Harbor in Kraft. Er besteht aus einem Beschluss der Europäischen Kommission, C (2016) 4176 final, sowie den Datenschutzgrundsätzen, welche die US-Unternehmen einzuhalten haben. US-Unternehmen werden durch den Eintrag in eine entsprechende Liste zur Einhaltung der Datenschutzgrundsätze des EU-US-Datenschutzschildes verpflichtet. Diese Selbstzertifizierung ist durch die US-Unternehmen jährlich zu erneuern.

Der EU-US-Datenschutzschild soll u. a. wie folgt Verbesserungen gegenüber dem Safe-Harbor-Abkommen herbeiführen:

- Klare Beschränkungen bezüglich der Überwachungsmechanismen der US-Regierung.
- Durchführung wirksamer Aufsichtsmaßnahmen sowie ggfs. Sanktionserteilung gegenüber den beigetretenen US-Unternehmen.
- Strengere Mitwirkungspflichten der US-Unternehmen im Beschwerdefall durch den/die Betroffenen sowie Etablieren eines Ombudsmanns.[7]

Datenschutzexperten monieren jedoch u. a., dass der EU-US-Datenschutzschild die europäischen Bürger nicht vor einer flächendeckenden und anlasslosen Überwachung schützen kann, da er nur für amerikanische Unternehmen, die sich ihm unterwerfen, gilt nicht aber für US-Behörden. Darüber hinaus bleiben wichtige Grundprinzipien des europäischen Datenschutzrechts, wie zum Beispiel Regelungen zu automatisierten Einzelfallentscheidungen, unberücksichtigt.[8]

b) Binding Corporate Rules

Binding Corporate Rules können, im Gegensatz zum Safe-Harbor-Abkommen, eine Übermittlung in jeden Drittstaat legitimieren. Ein angemessenes Datenschutzniveau wird bei Binding Corporate Rules dadurch erlangt, dass sich eine Gruppe von Unternehmen individuell ausgestaltete, rechtsverbindliche Datenschutzregeln, die von der zuständigen europäischen Aufsichtsbehörde genehmigt wurden, auferlegt. Innerhalb dieser Gruppe von Unternehmen ist es durch die Anerkennung und Befolgung der Binding Corporate Rules sodann möglich, Datenübermittlungen datenschutzkonform durchzuführen.[9]

c) EU- Standardvertragsklauseln

EU-Standardvertragsklauseln sind von der Europäischen Kommission entwickelte und durch die Entscheidung 2001/497/EG *anerkannte* Klauseln, die grundsätzlich - genau wie Binding Corporate Rules – die Übermittlung von Daten an jeden beliebigen Drittstaat ermöglichen. Durch die Verwendung der Klauseln ist es möglich, den Verarbeiter im Drittstaat datenschutzrechtlich umfangreich zu verpflichten, so dass dieser im Umkehrschluss bei der Benutzung und Verarbeitung der personenbezogenen Daten das Datenschutzniveau des EWRs einhält. Im Gegensatz

[7] Vgl. *http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf*.

[8] Vgl. u. a. Weichert, Privacy-Shield – Darstellung und rechtliche Bewertung, S. 5f.; Artikel-29-Datenschutzgruppe, WP 238 vom 13. April 2016, S. 3f.

[9] Selzer, DuD 2014, S. 470 (474).

zu Binding Corporate Rules handelt es sich bei den EU-Standardvertragsklauseln nicht um individuell ausgehandelte Verträge, sondern um Vertragsmuster, die unverändert übernommen werden müssen.

d) Export-Import-Standardvertrag

Das Netzwerk Datenschutzexpertise hat einen Export-Import-Standardvertrag vorgeschlagen, der zwischen Datenexporteur und -importeur abgeschlossen werden und künftig ermöglichen solle, Daten unter Einhaltung der Anforderungen des EuGHs in die USA zu übermitteln. »Der Vorschlag […] sieht materiell-rechtliche Garantien des Datenimporteurs wie auch bei Verstößen wirksame Sanktionen vor, die der Datenexporteur, die betroffenen Personen wie auch die für den Exporteur zuständige Datenschutzaufsichtsbehörde administrativ und gerichtlich durchsetzen können. Rechtlicher Anknüpfungspunkt ist nicht, wie bisher bei Safe-Harbor, ein reduzierter Datenschutz, sondern das für den Exporteur geltende Recht. Die Durchsetzung dieses Rechts ist im Land des Exporteurs möglich.«[10] Im Gegensatz zu den drei zuvor genannten Möglichkeiten handelt es sich bei dieser Alternative bisher noch nicht um eine offiziell anerkannte Möglichkeit der Datenübermittlung an Drittstaaten, sondern um einen zukunftsweisenden Vorschlag.

Kann Technik helfen?

In Zeiten, in denen es nahezu unmöglich scheint, Datenübermittlungen auf Grundlage internationaler Abkommen, Verträge u. ä. zu ermöglichen, wenn Länder rechtsstaatliche Grundsätze nicht einhalten, ist fraglich, ob Datenübermittlungen auf Grundlage technischer Lösungen datenschutzfreundlich gestaltet werden können.

a) Verschlüsselung

Der Einsatz von Verschlüsselungsverfahren vor der Datenübermittlung ist zur Wahrung der Privatsphäre von Kunden- und Mitarbeitern immer dann sinnvoll, wenn Daten am Zielort der Datenübermittlung lediglich gespeichert - und somit nicht inhaltlich bearbeitet – werden sollen. Dementsprechend ist für den Fall, dass Daten am Zielort der Übermittlung lediglich gespeichert werden sollen, dringend zu empfehlen, die Daten – neben vertraglichen Regelungen zur Datenübermittlung in Drittstaaten – vor der Übermittlung mit dem Stand der Technik entsprechenden Verschlüsselungsverfahren zu verschlüsseln.

Es ist umstritten, ob es sich bei verschlüsselten Daten um personenbezogene oder pseudonymisierte anonymisierte Daten handelt. Für die Abgrenzung ist primär die *Bestimmbarkeit* ausschlaggebend, für deren Auslegung es zwei Theorien gibt:

- Die relative Theorie besagt, dass es für die Bestimmbarkeit einer Person ausschließlich auf die Kenntnisse der datenverarbeitenden Stelle ankommt.
- Die absolute Theorie besagt hingegen, dass es für die Bestimmbarkeit einer Person nicht nur auf die Kenntnisse der datenverarbeitenden Stelle ankommt, sondern darauf, dass irgendein Dritter das Zusatzwissen zur Bestimmbarkeit der Person besitzt.[11]

Folgt man der relativen Theorie, so könnte eine Datenübermittlung an Drittstaaten bereits datenschutzkonform sein, wenn die verantwortliche Stelle die personenbezogenen Daten vor der Übermittlung der Daten an den Drittstaat verschlüsselt und den Entschlüsselungsschlüssel – auch bzw. vor allem gegenüber der datenempfangenden Stelle – geheim hält. Könnte das verwendete Verschlüsselungsverfahren langfristig als sicher gelten,[12] würden gemäß der relativen Theorie keine personenbezogenen Daten übermittelt, so dass Datenschutzvorschriften keine Anwendung fänden. Hierbei wäre jedoch auf ggfs. vorhandene Beziehungen zwischen der datenübermittelnden und der datenempfangenden Stelle zu achten: Würde z. B. ein deutsches Tochterunternehmen verschlüsselte Daten an das US-Mutterunternehmen übermitteln und wäre es absehbar, dass die US-Mutter die deutsche Tochter – ggfs. sogar unter Missachtung deutscher Gesetze – unter Druck setzen könnte, die Entschlüsselungsschlüssel herauszugeben, so ist dies bei der Diskussion um die *Bestimmbarkeit* durch die US-Mutter zu beachten.

Folgt man wiederum der absoluten Theorie wäre die Verschlüsselung lediglich eine technische Schutzmaßnahme für personenbezogene Daten, die neben vertraglichen bzw. sonstigen Garantien über ein angemessenes Datenschutz-

[10] Vgl. Schuler/Weichert, Nach Safe-Harbor: Vorschlag für Export-Import-Datenschutzvertrag mit den USA, S. 1 (Pressemitteilung Netzwerk)

[11] Vgl. u. a. Härting, NJW 2013, S. 2065 (2066); Meyerdierks, MMR 2013, S. 705, (706).

[12] Der verschlüsselnden Stelle muss das Risiko bewusst sein, dass Verschlüsselungsverfahren nicht dauerhaft sicher sind und dementsprechend heute sicher verschlüsselte Daten in Zukunft evtl. leicht entschlüsselbar werden. Dem kann dadurch entgegengewirkt werden, dass die Verschlüsselung bei Bedarf auf sichere Algorithmen und größere Schlüssellängen umgestellt wird (Vgl. den jährlich veröffentlichten Algorithmen Katalog, in dem das BSI Empfehlungen für sichere kryptographische Verfahren und Schlüssellängen jeweils nur für die nachfolgenden sieben Jahre macht).

niveau im Drittstaat immer dann angewendet werden sollte, wenn die Daten am Zielort lediglich gespeichert – und nicht inhaltlich bearbeitet – werden sollen.

b) Kontinuierliche Messung des Verarbeitungsstandortes

Im Falle des EU-US-Datenschutzschild und den anderen in Kapitel 2 genannten Alternativen ist die Datenverarbeitung an das datenempfangende Unternehmen gebunden. Es scheint empfehlenswert, die Datenverarbeitung auf datenempfangende Unternehmen zu beschränken, welche ihren Sitz und ihre Verarbeitungsstandorte in Ländern haben, in denen die rechtsstaatlichen Grundsätze beachtet werden. Ein technischer Lösungsansatz zur Überprüfung dieser geographischen Beschränkung besteht darin, dass im Namen der verantwortlichen Stelle kontinuierlich Messdaten über den Verarbeitungsstandort erhoben und ausgewertet werden, um zu kontrollieren, ob die datenverarbeitende Stelle die Daten ausschließlich an vertraglich vereinbarten geographischen Standorten verarbeitet. Wird durch eine Kontrolle die Datenverarbeitung an nicht vertraglich vereinbarten Standorten aufgedeckt, so muss zumindest vermutet werden, dass an diesen ggfs. anlasslose Massenüberwachungen durch Behörden stattfinden.

Werden Daten in der Cloud verarbeitet, kann u. A. untersucht werden, in welcher technischen Umgebung sich eine verarbeitende Virtuelle Maschine (VM) befindet. Dazu kann eine Software-Komponente mit entsprechender Sensorik in der VM der zu kontrollierenden Datenverarbeitung durch die verantwortliche Stelle installiert werden, wie in einer beispielhaften Lösung gezeigt wurde.[13] Darin erfasst die Sensorik charakteristische Merkmale der Umgebung und sendet die Messdaten an einen externen Dienst, der von der verantwortlichen Stelle oder einem unabhängigen Dritten betrieben wird. Darüber hinaus können auch außerhalb der Betreiberumgebung standortspezifische Parameter der Datenverarbeitung gemessen werden, beispielsweise charakteristische Routing-Parameter, öffentliche IP-Adressen, Informationen zur Erreichbarkeit der VM, Antwortzeiten und Merkmale von Proxy-Servern. Derartige Messdaten können als Indikatoren für den aktuellen Standort einer Datenverarbeitung dienen und beispielsweise auch einen Wechsel des Verarbeitungsstandorts aufdecken helfen.[14] Ob allerdings die personenbezogenen Daten an einen anderen Standort transportiert werden und welche Datenkopien an welchen Orten gespeichert sind, kann so nicht ermittelt werden. Zudem stehen nicht sämtliche technisch denkbaren Messmethoden zur Verfügung, da datenverarbeitende Stellen den verantwortlichen Stellen i. d. R. nur einen sehr eingeschränkten Zugriff auf die Ebene des VM-Monitoring gewähren. So bleiben wesentliche Details der Datenverarbeitung ausschließlich der datenverarbeitenden Stelle zugänglich. Werden für die Datenverarbeitung Infrastrukturdienste (IaaS) genutzt, können aber i. d. R. mehr betreiberunabhängige Messmethoden (beispielsweise in Form von dedizierten Mess-VMs) implementiert werden als bei der Nutzung reiner Softwaredienste (SaaS).

Auch wenn automatisierte Kontrollen des Verarbeitungsstandortes nicht allumfassenden Schutz vor unberechtigten Zugriffen gewährleisten können, können sie die verantwortliche Stelle dennoch dabei unterstützen, Verstöße gegen vertraglich zugesicherte/ausgeschlossene Verarbeitungsstandorte aufzudecken und somit zumindest implizit die Möglichkeit anlassloser Massenüberwachungen durch Behörden indizieren. Dies wiederum versetzt die verantwortliche Stelle in die Lage, auf einen kritischen Verstoß schnellstmöglich – z. B. durch Umzug zu einem datenschutzfreundlicheren Datenverarbeiter – zu reagieren.

Wie geht es weiter?

Der Vorschlag des Export-Import-Standardvertrages stellt einen sehr hilfreichen Ansatz in der Diskussion um die datenschutzkonforme Datenübermittlung an US-Unternehmen dar. Jedoch scheint sich das Hauptproblem, nämlich die anlasslosen Massenüberwachungen durch die NSA, durch den vorgeschlagenen Vertrag nicht beseitigen zu lassen: Zwar würde der amerikanische Datenimporteur dem europäischen Datenexporteur vertraglich zusichern, diesen über ggfs. stattfindende Überwachungen durch US-Behörden zu informieren. Jedoch kann bezweifelt werden, dass der amerikanische Datenimporteur dieser vertraglichen Pflicht in der Praxis nach-

[13] Vgl. den Lösungsansatz des BMBF-geförderten Projekts »VeriMetrix – Definition und Verifikation von Kennzahlen für den Datenschutz in Cloud-Anwendungen«, *www.verimetrix.de*.

[14] Vgl. Jaeger/Selzer/Waldmann, DuD 2015, S. 26–30.

kommen würde, wenn er sich zwischen der Beachtung von Gesetzen zur Erhaltung der nationalen Sicherheit der USA einerseits und der Beachtung eines Vertrages mit einem europäischen Unternehmen andererseits entscheiden müsste. Die Suche nach datenschutzkonformen Alternativen für die Datenübermittlung in Drittstaaten ist jedoch äußerst wichtig. Entsprechende Diskussionen und Entwicklungen sind daher unbedingt zu begrüßen und sollten unterstützt werden.

Obwohl sowohl der EU-US-Datenschutzschild, als auch Binding Corporate Rules und EU-Standardvertragsklauseln derzeit gültige Möglichkeiten zur Datenübermittlung darstellen, sollte vor der Verwendung dieser Möglichkeiten mit amerikanischen Unternehmen die Begründung des EuGH zur Ungültigkeit von Safe-Harbor berücksichtigt werden: Keine der drei Alternativen begründet Wirkung für amerikanische Behörden, so dass diese weiterhin in die Grundrechte der Betroffenen eingreifen können, ohne dass ausreichende Regeln zur Begrenzung der Eingriffe existieren. Dementsprechend bleibt zu vermuten, dass diese Alternativen zur Datenübermittlung in Zukunft durch den EuGH – zumindest für Datenübermittlungen an amerikanische Unternehmen – als unwirksam erklärt werden. Für Datenübermittlungen an amerikanische Unternehmen sind alle drei Alternativen als datenschutzunfreundlich einzustufen.[15] Es ist aus Datenschutzsicht derzeit dringend zu empfehlen, Datenübermittlungen an Staaten, deren Behörden sich an anlasslosen Massenüberwachungen beteiligen, zu überdenken. Zumindest aber sollte die Verwendung der oben genannten drei Alternativen um einen Vertrag analog § 11 Abs. 2 BDSG ergänzt werden und die übermittelten Daten wann immer möglich vor der Übermittlung verschlüsselt werden. Zur Kontrolle der Einhaltung vertraglich zugesicherter Verarbeitungsstandorte können in Zukunft darüber hinaus automatisierte Datenschutzkontrollen unterstützende Wirkung entfalten und die verantwortliche Stelle in die Lage versetzen, auf einen kritischen Verstoß schnellstmöglich zu reagieren.

Über die Autoren

Michael Herfert
Leiter der Abteilung Cloud Computing & Identity und Privacy am Fraunhofer SIT, Darmstadt
E-Mail: michael.herfert@sit.fraunhofer.de

Annika Selzer
Wissenschaftliche Mitarbeiterin am Fraunhofer SIT, Darmstadt
E-Mail: annika.selzer@sit.fraunhofer.de

Ulrich Waldmann
Wissenschaftlicher Mitarbeiter am Fraunhofer SIT, Darmstadt
E-Mail: ulrich.waldmann@sit.fraunhofer.de

Fraunhofer SIT

[15] Vgl. u. a. Roßnagel/Jandt/Richter, DuD 2014, S. 545 (545f.); Räther/Seitz, MMR 2002, S. 520 (527).