Datenschutz in Europa und den USA -

Grenzüberschreitender Datenverkehr nach dem Safe Harbor Aus

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

1. Cyberraum als grenzüberschreitender Raum

Der Cyberstrategie-Bericht des Bundesinnenministeriums definiert den Cyberraum als einen Raum, der „alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen [umfasst].“[1] Dieser Raum birgt Chancen sowohl für die im Cyberraum agierenden Unternehmen als auch für die Verbraucher, welche die von den Unternehmen angebotenen Produkte und Dienste nutzen. Zugleich birgt der Cyberraum auch Risiken für die Verbraucher. Ein besonders hohes Risiko geht von dem Umstand aus, dass Verbraucher in unterschiedlichen Ländern unterschiedlich gut davor geschützt werden, durch den Umgang von Behörden und Unternehmen mit ihren personenbezogenen Daten[2] in ihren Persönlichkeitsrechten beeinträchtigt zu werden. Selbst wenn also das Rechtssystem des Landes, in dem ein/e Verbraucher/in lebt, einen hohes Datenschutzniveau gewährt, geht die Datenverarbeitung im Cyberraum über Landesgrenzen hinaus, wodurch das Aufrechterhalten eines hohen Datenschutzniveaus erschwert wird.

Vor diesem Hintergrund stellt dieser Beitrag zum einen die Unterschiede in der Entwicklung des Datenschutzrechts sowie zum anderen die Unterschiede in dem Schutzniveau der Datenschutzsysteme von Europa und den USA vor, um zu veranschaulichen, wie unterschiedlich das Datenschutzniveau im Cyberraum ausfallen kann und welche Schutzmechanismen sicherstellen sollen, dass die Verbraucher ein gleichwertig hohes Datenschutzniveau genießen können. Dieses wiederum ist essentiell wichtig, um den Verbrauchern im Cyberraum eine freie Entfaltung ihrer Persönlichkeit zu ermöglichen und zu verhindern, dass sich diese aus Angst vor Überwachungen gehemmt und angepasst verhalten.

2. Datenschutz in Europa und Deutschland

Innerhalb des Europäischen Binnenmarkts erkannte man bereits früh die ungleichen Datenschutzniveaus der einzelnen Europäischen Staaten als Handelshemmnis, weshalb 1995 die Europäische Datenschutzrichtlinie verabschiedet wurde, die wiederum in den einzelnen Staaten in nationales Recht umzusetzen war [DKWW13, Hahn94, TaGa10]. In Deutschland geschah dies durch eine Novellierung des Bundesdatenschutzgesetzes, der

Begriff des Datenschutzes etablierte sich in Deutschland jedoch nicht erst durch die Umsetzung der Europäischen Datenschutzrichtlinie, sondern bereits im Jahre 1970 durch das hessische Landesdatenschutzgesetz, welches als erstes allgemeines Datenschutzgesetz weltweit gilt [WoGe05]. Eine Besonderheit in Deutschland stellen zudem die zwei vom Bundesverfassungsgericht entwickelten datenschutzrechtlichen Grundrechte dar: Das Grundrecht auf informationelle Selbstbestimmung aus dem Jahr 1983, das den Betroffenen das Recht zugesteht, im größtmöglichen Umfang über ihre personenbezogenen Daten selbst zu entscheiden, sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem Jahr 2008, das sich auf den Schutz persönlicher Daten bezieht, welche in informationstechnischen Systemen gespeichert und verarbeitet werden [KüSS08, TaGa10].

Die Europäische Datenschutzrichtlinie gibt innerhalb des Europäischen Wirtschaftsraumes[3] (kurz:) strenge Datenschutzregelungen vor, die in den einzelnen Mitgliedsstaaten in nationales Recht umgesetzt wurden und somit ein vergleichbar hohes Datenschutzniveau in den einzelnen Mitgliedsstaaten garantieren. Hierzu gehören unter anderem die folgenden Datenschutzgrundsätze [DKWW13, KüSS08, TiBP12, TaGa10]:

- Das Verbot mit Erlaubnisvorbehalt regelt ein Verbot jeglicher Verarbeitung personenbezogener Daten. Eine Ausnahme dieses Verbots besteht dann, wenn eine Rechtsvorschrift dies erlaubt beziehungsweise die Betroffenen in die Verarbeitung ihrer personenbezogenen Daten einwilligen.
- Durch das Direkterhebungsprinzip ist die Erhebung personenbezogener Daten nur bei den Betroffenen selbst zulässig. Ausnahmen bestehen nur, wenn die Direkterhebung einen unverhältnismäßig großen Aufwand bedeuten würde.
- Das Zweckbindungs- und Erforderlichkeitsprinzip beschränkt die Verarbeitung personenbezogener Daten auf erforderliche Zwecke. Der Zweck ist vor der Verarbeitung festzulegen und darf nach der Erhebung nicht geändert werden.
- Das Datensparsamkeits- und Datenvermeidbarkeitsprinzip beschränkt die Verarbeitung personenbezogener Daten auf diejenigen Daten, die zur Erfüllung des Zwecks unbedingt notwendig sind. Werden gespeicherte Daten nicht mehr benötigt, so sind sie zu löschen oder zumindest zu anonymisieren.
- Die Pflicht, technische und organisatorische Maßnahmen zu ergreifen, sorgt dafür, dass u. a. unberechtigte Zugriffe auf personenbezogene Daten unterbunden werden sowie personenbezogene Daten vor zufälliger Zerstörung geschützt werden.
- Umfangreiche Betroffenenrechte sorgen u. a. dafür, dass Betroffene auf Anfrage Auskunft über die zu ihrer Person gespeicherten Daten erhalten müssen sowie falsch gespeicherte Daten korrigiert werden müssen.

Somit bedeutet der Begriff Datenschutz für die einzelnen Europäischen Bürger nunmehr den Schutz ihrer Persönlichkeitsrechte gegen unzulässigen Umgang mit ihren personenbezogenen Daten.

3. Datenschutz in den USA

Die Entwicklung des modernen Datenschutzrechts in den USA begann Anfang der Sechziger Jahre durch die Realisierung, dass die zunehmende Verwendung von Computern eine Gefahr für die Privatheit eines jeden Einzelnen darstellen könnte. Der Freedom of Information Act aus dem Jahr 1966 sowie der Privacy Act aus dem Jahr 1974 waren Versuche, den erkannten Gefahren zu begegnen, regelten jedoch primär Auskunftsrechte der Betroffenen sowie Verbote für Bundesbehörden, gespeicherte personenbezogene Daten zweckzuentfremden.

Problematisch ist, dass trotz vieler Bemühungen seitens der US-Regierung bis heute kein Datenschutzgesetz auf Bundesebene besteht, welches mit dem Datenschutzniveau des Europäischen Wirtschaftsraumes vergleichbar ist. Verschiedenste Regelwerke auf Staaten- und Bundesebene sowie Rechtsprechungen und unternehmensinterne Datenschutzregelungen machen es den Betroffenen nahezu unmöglich zu beurteilen, wie ihre personenbezogenen Daten geschützt sind [TiBP12, Blum03].

Nicht zuletzt wird ein hohes Datenschutzniveau durch die Reaktion auf die Terroranschläge des 11. September 2001 erschwert, in Folge derer der Patriot Act[4] verabschiedet wurde, der den US-amerikanischen Sicherheitsbehörden weitgehende Kontrollrechte zur Überwachung von über die USA gerouteten Daten einräumt [TiBP12].

Im Jahr 2013 veröffentlichte Edward Snowden, ein ehemaliger Mitarbeiter des US-Geheimdienstes NSA (National Security Agency), zudem Informationen über die weltweiten Überwachungspraktiken des US-Geheimdienstes. Im Mittelpunkt der Veröffentlichungen stand das System PRISM, durch welches die NSA einen Großteil der weltweiten Onlinekommunikation – zum Beispiel E-Mails, Bilder und Videos – überwacht. Durch die Informationen zu PRISM ist das Vertrauen in das Datenschutzsystem der USA weltweit erneut gesunken.

Festzustellen bleibt somit, dass sich der anfängliche Vorsprung der USA in Bezug auf das Datenschutzrecht mittlerweile in die gegensätzliche Richtung bewegt und ein mit dem Datenschutzsystem des EWR gleichwertiges Schutzniveau derzeit nicht absehbar ist.

4. Übermittlung personenbezogener Daten in die USA

Eine Übermittlung personenbezogener Daten von einem zum anderen Unternehmen ist innerhalb des EWR laut geltender Datenschutzvorschriften nur dann möglich, wenn ein Gesetz diesen Vorgang zweckgebunden erlaubt oder die Betroffenen in die Datenübermittlung einwilligen. An eine datenschutzkonforme Einwilligung sind wiederum gesetzlich festgeschriebene Bedingungen geknüpft: Demnach ist eine Einwilligung nur dann wirksam, wenn sie auf der freien Entscheidung der Betroffenen beruht und diese auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hingewiesen werden [KüSS08, TiBP12].

Dem Umstand, dass Datenschutzsysteme außerhalb des EWR nicht immer ein mit dem EWR vergleichbares Datenschutzniveau aufweisen, ist geschuldet, dass Übermittlungen personenbezogener Daten an Staaten außerhalb des EWR[5] an besonders strenge Voraussetzungen gebunden sind. Die Europäische Kommission hat jedoch das Recht inne, die Datenschutzsysteme von Drittstaaten zu bewerten und ein mit dem Schutzniveau des EWR gleichwertiges Schutzniveau zu bestätigen. In diese Staaten, zu denen etwa Kanada und Argentinien gehören, ist eine Übermittlung personenbezogener Daten aus dem EWR unter den gleichen Voraussetzungen wie Übermittlungen innerhalb des EWR möglich [DKWW13, KüSS08, TaGa10].
Bei einer Datenübermittlung in Drittstaaten, für welche die Europäische Kommission kein gleichwertiges Schutzniveau bestätigt hat, müssen zusätzlich zu den eben genannten Voraussetzungen weitere erfüllt werden, wobei zusammenfassend sichergestellt werden soll, dass in den Drittstaaten, in welche personenbezogene Daten übermittelt werden sollen, ein mit dem EWR gleichwertiges Schutzniveau z. B. durch den Abschluss von Verträgen hergestellt wird.

4.1 Safe Harbor

Um den Datenverkehr zwischen den USA und dem EWR nicht zum Erliegen zu bringen, erkannte die Europäische Kommission in ihrer Entscheidung 2000/520/EG vom 26.07.2000 an, dass US-Unternehmen immer dann ein ausreichendes Datenschutzniveau zusichern können, wenn diese die Safe Harbor Prinzipien anerkennen. Bei den Safe Harbor Prinzipien handelt es sich um Rahmenbedingungen zum Schutz der Betroffenen vor unberechtigten Umgängen mit deren personenbezogenen Daten. U. a. soll durch diese sichergestellt werden, dass die Betroffene Auskunft zu den über ihn verarbeiteten personenbezogenen Daten erhalten können und die verarbeiteten Daten durch angemessene technische und organisatorische Maßnahmen gesichert werden. In ihrer Gesamtheit sollen die Rahmenbedingungen dafür Sorge tragen, dass ein US-Unternehmen durch den freiwilligen Beitritt zu Safe Harbor ein mit dem EWR vergleichbares Datenschutzniveau herstellen kann und somit Übermittlungen von Daten aus dem EWR zu dem US-Unternehmen möglich werden [KüSS08, TiBP12].
Datenschutzexperten kritisieren bereits seit Längerem, dass der Beitritt zu Safe Harbor einer datenschutzrechtlichen Selbstzertifizierung der US-Unternehmen gleichkomme. Studienergebnissen im Rahmen des 10-Jährigen Jubiläums von Safe Harbor ergaben zudem, dass nur ca. 20% der zertifizierten Unternehmen den Kriterien des Abkommens tatsächlich entsprechen. Zudem gaben die Studienergebnisse Anlass, die gewissenhafte Überwachung der Safe Harbor Prinzipien durch die in den USA zuständige Federal Trade Commission anzuzweifeln [ErdR1O].
Mit dem Urteil vom 06.10.2015 erklärte der Gerichtshof der Europäischen Union (kurz: EuGH) die Entscheidung 2000/520/EG der Europäischen Kommission vom 26.07.2000 für ungültig. Der EuGH rügt u. a., dass die Europäische Kommission in ihrer

Entscheidung hätte feststellen müssen, dass die USA aufgrund ihrer innerstaatlichen Rechtsvorschriften ein Datenschutzniveau gewährleisten, das dem Datenschutzniveau des EWR gleichwertig ist. Eine derartige Feststellung habe die Europäische Kommission jedoch nicht getroffen, sie habe lediglich die Safe Harbor Rahmenbedingungen überprüft, die jedoch ausschließlich für beitretende US-Unternehmen – nicht aber für die US-Behörden – gelten. Zudem rügt der EuGH, dass u. a. die Erfordernisse der nationalen Sicherheit der USA Vorrang vor dem Safe Harbor Abkommen habe und 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 Privatslebens.
Aus diesen (und anderen[6]) Gründen erklärte der EuGH die Entscheidung 2000/520/EG der Europäischen Kommission für ungültig.[7]

4.2 Alternativen zu Safe Harbor

Ein gleichwertiges Datenschutzniveau kann u. a. durch die Unterzeichnung von EU-Standardvertragsklauseln sowie auf der Grundlage von rechtlich verbindlichen Unternehmensregelungen – so genannten Binding Corporate Rules – hergestellt werden.

EU-Standardvertragsklauseln sind von der Europäischen Kommission entwickelte Klauseln, durch deren Verwendung es möglich ist, die datenverarbeitende Stelle in einem Drittstaat datenschutzrechtlich umfangreich zu verpflichten, so dass diese im Umkehrschluss bei der Verarbeitung der personenbezogenen Daten ein mit dem EWR vergleichbares Datenschutzniveau einhält.

Binding Corporate Rules sind ein Regelungskomplex, durch den eine Gruppe von Unternehmen den Umgang mit personenbezogenen Daten regelt und sich diesen Regelungen unterwirft. Innerhalb dieser Gruppe von Unternehmen ist es sodann möglich, Datenübermittlungen durchzuführen, bei welchen die personenbezogenen Daten durch ein mit dem EWR vergleichbares Datenschutzniveau geschützt sind [DKWW13, TaGa10].

Wenngleich beide Alternativen eine höhere Rechtsverbindlichkeit – u. a. hinsichtlich der Möglichkeiten der Überwachung und Sanktionierung – als das vom EuGH als ungültig erklärte Safe Harbor Abkommen bieten, kann der Einsatz von EU-Standardvertragsklauseln und Binding Corporate Rules nicht die Bedenken der Unionsbürger hinsichtlich der massenhaften Überwachung durch US-Geheimdienste nehmen. Den Ursachen dieser Bedenken gilt es dementsprechend zukünftig entgegenzuwirken. Das Urteil des EuGH setzt diesbezüglich ein erstes wichtiges Zeichen, das hohe Datenschutzniveau für die Unionbürger zu erhalten.

5. Zusammenfassung

Zwar waren es in den sechziger Jahren die USA, die als Erste die Gefahren für die Privatheit auf Grund zunehmender Verwendung von Computern realisierten und Versuche unternahmen, diesen Gefahren mit Gesetzen entgegenzuwirken. Letztendlich scheint es jedoch, als würden sich die Versuche der USA, ihren Bürgern einen ausreichenden Datenschutz zuzusichern mittlerweile in das Gegenteil verlagern. Dies untermauert der EuGH mit seinem Urteil vom 06.10.2015. Zwar kann er die Unionsbürger durch das „Safe Harbor Aus“ nicht allumfassend vor den Überwachungspraktiken der elektronischen Kommunikation durch die USA schützen, jedoch setzt er ein klares Zeichen für den Europäischen Datenschutz und gegen generelle und anlasslose Massenüberwachungen durch die USA, den es in Zukunft weiter auszubauen gilt.

Die Chancen für ein hohes Europäisches Datenschutzniveau, welches versucht die Unionsbürger auch bei Verarbeitungen außerhalb des EWR vor Eingriffen in deren Datenschutzrechte zu schützen, stehen auch in Zukunft sehr gut, so dass die

Unionsbürger darauf hoffen dürfen, sich auch in Zukunft frei im Cyberraum verhalten zu können.
Weniger gut ist es demgegenüber um das Datenschutzniveau der US-Bürger gestellt, weshalb deren Risiko, sich auf Grund anlassloser Massenüberwachungen gehemmt und angepasst im Cyberraum zu verhalten, zu wachsen droht. Es ist daher wünschenswert, dass die USA in dem Urteil des EuGH auch Anlass dazu sehen, ihr eigenes Datenschutzsystem zu überdenken.

Literatur

[Blum03] Blumenwitz, Dieter: Einführung in das anglo-amerikanische Recht, C.H.Beck, 2003.

[DKWW13] Däubler, Wolfgang/ Klebe, Thomas/ Wedde, Peter/ Weichert, Thilo (Hrsg.): Bundesdatenschutzgesetz Kompaktkommentar zum BDSG, 4. Auflage, Bund Verlag, 2013.

[ErdR10] Erd, Rainer: Zehn Jahre Safe Harbor Abkommen - kein Grund zum Feiern, K&R 2010, S. 624-627.

[Hahn94] Hahn, Ulrich: Datenschutzrecht und grenzüberschreitender Datenverkehr-Regelungsbedarf, Rechtsvergleich und Rechtsfortbildung, 1994.

[KüSS08] Kühling, Jürgen / Seidel, Christian / Sivridis, Anastasios: Datenschutzrecht, Verlag Recht und Wirtschaft, 2008.

[Selz14] Selzer, Annika: Datenschutz bei internationalen Cloud Computing Services, DuD 2014, S. 470-474.

[SeWa12] Der Schutz personenbezogener Daten in Europa und den USA, 22. Smartcard-Workshop Tagungsband, Fraunhofer Verlag.

[TaGa10] Taeger, Jürgen/ Gabel, Detlev (Hrsg.): Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, Deutscher Fachverlag, 2010.

[TiBP12] Tinnefeld, Marie-Theres / Buchner, Benedigt / Petri, Thomas: Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht, Oldenbourg Verlag, 2012.

[WoGe05] Wohlgemuth, Hans/ Gerloff, Jürgen: Datenschutzrecht- Eine Einführung mit praktischen Fällen, Luchterhand, 2005.

---

1 Vgl. https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile, zuletzt besucht am 23.11.2015.

2 Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Beispiele für personenbezogene Daten sind u. a. Namen, Telefonnummern und Adressen.

3 Der Europäische Wirtschaftsraum wird durch die Staaten der Europäischen Union sowie Island, Liechtenstein und Norwegen gebildet.

4 Der Patriot Act wurde mittlerweile zum Teil durch den USA Freedom Act ersetzt.

5 Staaten, die sich außerhalb des EWRs befinden, werden im Europarechtlichen Kontext als Drittstaaten bezeichnet.

[6] U. a. führt der EuGH aus, „dass eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des Grundrechts auf wirksamen gerichtlichen Rechtsschutz verletzt. Eine solche Möglichkeit ist dem Wesen eines Rechtsstaats inhärent.“ Vgl. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117de.pdf, zuletzt besucht am 23.11.2015.

[7] Das Urteil ist abrufbar über http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:620 14CJ0362. Die zugehörige Pressemitteilung ist abrufbar über: http://curia.europa.eu/jcms/upload/docs/application/pdf/ 2015-10/cp150117de.pdf, beides zuletzt besucht am 23.11.2015.