JACQUES DELORS INSTITUT
BERLIN

BLOG POST 26.02.2016

Datenschutz: Wird „Privacy Shield“ ein sicherer Hafen?

Paul-Jasper Dittrich
Wissenschaftler beim Jacques Delors Institut – Berlin

Am 06. Oktober 2015 kippte EuGH das Safe Harbor Abkommen zwischen der EU und den USA. Am 2. Februar 2016 verkündete die Kommission, dass ein Nachfolgeabkommen, welches den Namen “Privacy Shield” tragen wird, in Grundzügen ausgehandelt wurde. Dieser Blogpost erklärt die Hintergründe zu Safe Harbor und argumentiert, dass die EU in punc-to Datenschutz in nächster Zeit vor allem einen sicheren Rechtsrahmen schaffen und eine Balance zwischen Innovation und europäischen Grundrechten finden muss.

Pariser Platz 6
D – 10117 Berlin
Tel.: +49 (0)30 467 26 09 – 01

Online: delorsinstitut.de
E-Mail: office@delorsinstitut.de
Twitter: @delorsinstitut

1 Datenübertragung in die USA: Eine rechtliche Grauzone?

Am 09. Februar 2016 erklärte die französische Datenschutzbehörde CNIL, dass sie das soziale Netzwerk Facebook bereits im Januar dazu aufgerufen hat, innerhalb von drei Monaten Verstöße gegen das französische Datenschutzrecht abzustellen, die die CNIL festgestellt hat. Anderenfalls könne es zu Sanktionen kommen. Einer der Gründe für die Rüge war der Umstand, dass Facebook weiterhin europäische Daten auf Basis von Safe Harbor in die USA überträgt.

Der Fall wirft ein Schlaglicht auf die komplizierte Rechtslage, in der sich viele Unternehmen nach dem Urteil des EuGH vom 06. Oktober 2015 befinden. Denn seit dem Urteil ist es für Unternehmen unzulässig, Daten von europäischen Bürgern in die USA zu übertragen und sich dabei auf Safe Harbor zu berufen.

In Reaktion auf das EuGH-Urteil stellte die Art. 29-Datenschutzgruppe, ein Zusammenschluss der europäischen Datenschutzbehörden, der EU-Kommission und den USA ein Ultimatum: Wenn sie bis Ende Januar 2016 kein neues Abkommen oder eine Vereinbarung vorweisen könnten, würden die europäischen Datenschutzbehörden damit beginnen, die Datenschutzstandards amerikanischer Unternehmen zu überprüfen und im Zweifelsfall Sanktionen zu verhängen. Solange hatten auch die Unternehmen Zeit, auf rechtliche Alternativen zu Safe Harbor auszuweichen. Dass die CNIL jetzt ausgerechnet gegen Facebook einen Vorstoß gemacht hat, ist durchaus auch als Warnung an andere Unternehmen zu verstehen, sich zukünftig an die geltende Rechtslage in der EU zu halten. Um die Brisanz dieser Vorgänge einzuordnen, lohnt es sich, noch einmal kurz die „Akte“ Safe Harbor zu rekapitulieren.

2 Worum ging es bei Safe Harbor?

Der nun verhandelte Nachfolger „Privacy Shield“ soll die Auflagen des EuGH nun erfüllen und Unternehmen ermöglichen, ihre Daten ohne Rechtsbedenken in die USA zu übertragen. Safe Harbor war aber nie die einzige Möglichkeit, mit der sich Unternehmen verpflichten konnten, den EU-Datenschutz einzuhalten. Mit sogenannten Standardvertragsklauseln und “corporate binding rules” können Unternehmen sich ebenfalls verpflichten, einen dem europäischen Recht angemessenen Schutz von Daten zu gewährleisten. In der Praxis schließen dann zum Beispiel europäische Tochterfirmen von amerikanischen Konzernen solche Verträge mit der Muttergesellschaft.

Unternehmen können zurzeit solche Standardvertragsklauseln abschließen, um mehr Rechtssicherheit zu erlangen, bis “Privacy Shield” offiziell wird, also vorrausichtlich im Juli 2016. Die Entscheidung des EuGH vom 06. Oktober wird aber von den meisten Juristen so interpretiert, dass sie auch für Standardvertragsklauseln und corporate binding rules gelten könnte, was den Datentransfer in die USA für Unternehmen noch unsicherer macht. „Privacy Shield“ wird also vermutlich auch eine Änderung bestehender Verträge nötig machen. Diese im Moment schwelende Rechtsunsicherheit ruft bei immer mehr Unternehmen zunehmende Frustration hervor.

Denn Möglichkeiten dazu, Daten nur in der EU zu belassen gibt es zwar, Unternehmen bieten dafür spezielle Cloud-Lösungen an. Die Frage ist allerdings, wie sinnvoll solche Speicher sind, wenn viele Unternehmen, gerade deutsche Mittelständler, aber auch Start-Ups, ihre Märkte zum Großteil außerhalb der EU haben und daher darauf angewiesen sind, Daten ohne rechtliche Bedenken global übertragen zu können. Dazu kommt, dass sich größere Unternehmen solche spezialisierten Dienste leisten können, kleinere Startups aber zum Beispiel oft den populären Amazon Cloud-Dienst nutzen, dessen Server hauptsächlich in den USA stehen. Das Internet ermöglicht darüber hinaus viele Geschäftsmodelle, bei denen auch kleine Startups schnell skalieren und Märkte auf der ganzen Welt erschließen können. Diese Unternehmen leiden am meisten unter Rechtsunsicherheit, auch weil sie sich keine teure Zwischenlösungen oder Anwälte leisten können. „Privacy Shield“ muss also an allererster Stelle die Rechtssicherheit wiederherstellen. Genau daran bestehen aber viele Zweifel, was allerdings auch an den gemachten Zugeständnissen der Amerikaner liegt. Das zeigen die Verhandlungsergebnisse.

3 Privacy Shield: Was sind die Details des neuen Abkommens?

Das neue Abkommen beinhaltet durchaus Verbesserungen gegenüber Safe Harbor, soweit die Details inzwischen bekannt sind. So werden sich die USA schriftlich verpflichten, keine Massenabschöpfung von Daten mehr zu betreiben (was freilich auch unter „Safe Harbor“ schon nicht legal war), sondern nur noch unter außergewöhnlichen Umständen, zum Beispiel bei Bedrohung der nationalen Sicherheit, auf einzelne Daten zuzugreifen. Das amerikanische Wirtschaftsministerium soll zukünftig die Einhaltung der Datenschutzgesetze durch die Unternehmen überwachen. Dazu wird die Stelle eines unabhängigen Ombudsmanns eingerichtet, der beim amerikanischen Außenministerium angesiedelt sein wird und über Fälle von Datenmissbrauch urteilen soll, wobei seine genauen Befugnisse noch nicht klar sind.

3.1 Oberste Priorität: ein sicherer Rechtsrahmen

Die EU-Kommission weist besonders auf ein Detail des neuen Abkommens hin: Einmal im Jahr soll in einem Überarbeitungs-Prozess die Umsetzung der neuen Regeln unter Einbeziehung der Datenschutzbehörden überprüft werden. Sollte sich herausstellen, dass die amerikanische Regierung, beziehungsweise ihre Sicherheitsbehörden sich nicht an die neuen Regelungen halten, kann das Abkommen suspendiert werden. Mit dieser Regelung erhält die EU ein Druckmittel, um die europäischen Grundsätze zum Schutz von Daten in Zukunft effektiver durchzusetzen. Die Frage ist allerdings, ob diese Regelungen genügen, um die Auflagen des EuGH zu erfüllen und es nicht in naher Zukunft wieder zu einer Phase der Rechtsunsicherheit kommt. Bei allen weiteren Konsultationen und Verhandlungen sollte ein sicherer Rechtsrahmen für Unternehmen die Zielsetzung der Kommission sein.

3.2 Die EU als Datenschutz-Union

Die Verhandlungen zeigen ein grundsätzliches Dilemma zwischen Macht und Ohnmacht der EU in puncto Datenschutz, auf. In der EU gilt der strengste Datenschutz der Welt, der zudem ab 2018 mit der Datenschutz-Grundverordnung weitgehend vereinheitlicht wird. Als größter Binnenmarkt der Welt gilt der Anspruch, entscheidender Player beim Entwickeln von globalen Standards zu sein und sie gegenüber den USA zu behaupten. Ein erster Erfolg in dieser Hinsicht ist, dass die USA sich verpflichten, Transparenz über das Ausmaß der Datenabfragen von Unternehmen zu schaffen und die entsprechenden Daten jährlich zu veröffentlichen. Auch dass bei den „Privacy-Shield“-Verhandlungen die NSA überhaupt mit am Tisch saß, gilt in der Kommission schon als Indiz für die gestiegene Bedeutung der EU beim Durchsetzen von Standards.

Exemplarisch für die grundsätzlich wichtiger werdende Rolle von Datenschutz ist auch ein Gerichtsprozess, den Microsoft grade gegen die USA austrägt und der bis zum Obersten Gerichtshof gelangen könnte. Die amerikanische Regierung hatte Microsoft schon 2014 gezwungen, Emaildaten herauszugeben, die der Konzern lediglich in Europa gespeichert hatte und sich dabei auf den Patriot Act berufen. Große amerikanische Unternehmen sind sich der Bedeutung von Datenschutz für ihre (europäischen) Kunden zunehmend bewusst.

4 Datenschutz und Innovation sollte kein Nullsummenspiel werden

Fest steht allerdings auch, dass der Export dieser Standards langfristig nur funktioniert, wenn die USA ihre eigenen Gesetze weit mehr als bisher verschärfen. Solche Änderungen haben die Amerikaner aber ausgeschlossen und damit die heftige Kritik vieler Datenschützer an „Privacy Shield“ befeuert. Es besteht die vage Hoffnung, dass Datenschutz in den USA auf Druck der Zivilgesellschaft oder von großen Unternehmen, die in der EU Marktanteile haben, in Zukunft eine größere Rolle spielen könnte. Niemand geht aber davon aus, dass in den USA bald ähnliche strenge Vorschriften wie in der EU gelten könnten. Das neue Abkommen zeigt also gleichzeitig die (Verhandlungs-)Macht der EU und deren Grenzen.

Aus ökonomischer Perspektive hat die EU-Datenschutz-Politik ebenfalls Licht- und Schattenseiten. Die Zahl der Datenspeicherzentren auf europäischem Boden steigt und Sicherheitstechnik aus der EU erfreut sich weltweit immer größerer Beliebtheit. Für viele Unternehmen ist höchster Datenschutz mithilfe von europäischen Cloud- und Verschlüsselungstechnologien selbstverständlich. Ökonomische Zugewinne durch einheitlichen Datenschutz und Sicherheitstechnologie zahlen sich langfristig aber nur dann aus, wenn es der EU gelingt, ihre Standards zu exportieren und für innovative Unternehmen der Datenökonomie attraktiv zu bleiben. Startups schaffen deutlich mehr Arbeitsplätze als Server-Farmen. Die EU sollte daher mit öffentlichen Investitionen Forschung zu Anonymisierung und Pseudonymisierung vorantreiben, um bei datengetriebenen Geschäftsmodellen nicht an Boden gegenüber Amerikanern und Asiaten zu verlieren. Datenschutz und Innovation darf kein Nullsummenspiel werden.

5 Bis spätestens 2016 müssen alle Fragen geklärt sein

In den nächsten Monaten werden die europäischen Datenschutzbehörden den Text der Kommission genau studieren und kommentieren. Die Kommission kann dann unter den neu verhandelten Bedingungen eine neue Entscheidung über die Gewährleistung eines angemessenen Schutzniveaus in den USA treffen. Letztlich – und das ist ebenfalls eine Erkenntnis des Schrems-Urteils – hindert das aber nicht die nationalen Datenschutzbehörden daran, die Einhaltung des Datenschutzes bei Beschwerden im Einzelfall zu überprüfen.

Ein einheitlicher Schutz für Europa ist ein großer Fortschritt, kann aber seine Vorteile für den Binnenmarkt und global nur entfalten, wenn er durch klare rechtliche Vorgaben nach außen und innovationsfördernde Regulierung nach innen unterstützt wird. Dabei ist Eile geboten. Ab 2018 wird die EU dank der Datenschutz-Grundverordnung zu einer echten Datenschutz-Union. Bis dahin sollte es keine ungeklärten Rechtsfragen mehr geben. Auch bei der Verordnung sind nämlich noch viele Punkte in Bezug auf Datentransfer mit Drittstaaten unklar. Außerdem sollte die EU bis dahin einen Plan entwickelt haben, um höchsten Datenschutz und datengetriebene Innovation in Einklang zu bringen.

Gefördert durch:
Bundeskanzleramt

Herausgeber: Prof. Dr. Henrik Enderlein. Die Publikation gibt ausschließlich die persönliche Auffassung der Autoren wieder. Alle Rechte vorbehalten.

Nachdruck und sonstige Verbreitung – auch auszugsweise – nur mit Quellenangabe zulässig.

Originalfassung © Jacques Delors Institut – Berlin, 2015.

NOTRE EUROPE JACQUES DELORS INSTITUTE
Hertie School of Governance