Der unsichere Hafen

Die europäische Absage an das Safe Harbor Agreement und ihre Auswirkungen: Eigentlich sollte das Safe Harbor Agreement für einen ausreichenden Datenschutz sorgen und zugleich eine sichere Brücke zwischen zwei Kontinenten schlagen. Allerdings prallten hier von Beginn an zwei fundamental verschiedene Datenschutz-Systeme aufeinander.

Autor:
Jan Alexander Linxweiler,
Cassini Consulting

Bildquelle: Zerbor - fotolia.com

Datenschutz: die europäische Rechtsauffassung unterscheidet sich von der amerikanischen.

Dies führte zwangsläufig zu Umsetzungsschwierigkeiten, die nicht zuletzt durch die inhärenten Gefahrenpotenziale des Safe Harbor-Abkommens noch beflügelt wurden. Auch der Europäische Gerichtshof war dieser Ansicht. Er hielt das Schutzniveau des Abkommens für nicht ausreichend und warf Safe Harbor in seinem Urteil vom 06.10.2015 kurzerhand über Bord. Allerdings wurde dabei – ganz im Zeichen der Snowden-Enthüllungen – der Fokus insbesondere auf die Zugriffsmöglichkeiten der amerikanischen Behörden auf personenbezogene Daten gelegt. Wie kritisch man das gekippte Safe Harbor-Abkommen auch sehen mag – nun klafft eine Lücke, die erst noch zu schließen sein wird.

Systeme und Traditionen

Um das Safe Harbor Agreement und seine Auswirkungen zu verstehen, ist es wichtig, sich die darunterliegenden Datenschutzsysteme der USA und der EU zu vergegenwärtigen. Erste Ansätze zum Datenschutz reichen mehr als 100 Jahre zurück, und von den Datenschutzmodellen, die seither entstanden sind, lassen sich heute insbesondere vier hervorheben: der Schutz durch umfassende Gesetze, durch sektorale Gesetze, durch wirtschaftliche Selbstregulierung und der durch Technologien, die die Privatsphäre schützen. Schon die Begrifflichkeiten verdeutlichen, dass die Ansätze sich auf unterschiedliche Fundamente stützen.

a. Der Schutz durch umfassende Gesetze („comprehensive laws“) schafft einen Gesetzesrahmen für das Sammeln, Nutzen und Verarbeiten persönlicher Informationen, der durch offizielle Behörden überwacht und durchgesetzt werden soll. Dies ist ein sehr proaktiver Ansatz.

b. Demgegenüber ist der Schutz durch sektorale Gesetze („sectoral laws”) ein eher reaktiver Ansatz. Er befasst sich mit konkreten Einzelbereichen des Datenschutzes.

c. Der Schutz durch wirtschaftliche Selbstregulierung („industrial self-regulation“) ist der flexibelste Ansatz. Er verlässt sich lediglich auf Regeln, die sich die Wirtschaftsteilnehmer selbst auferlegen.

d. Zudem gibt es noch Technologien, die die Privatsphäre schützen („privacy-enhancing technologies“). Hierzu gehören vor allem Verschlüsselungs-

technologien, digitale Währungen und ähnliches.

Diese vier Ansätze sind hier natürlich als Idealtypen dargestellt. Auf der stürmischen See des Datenschutzes wird man sie kaum in genau dieser Form vorfinden. Die reale Umsetzung besteht meist in einer Kombination der Modelle und hängt davon ab, wie Datenschutz aufgefasst und bewertet wird.

USA – Datenschutz als Manifestation des Eigentumsrechts

Betrachtet man die Datenschutzphilosophie in den USA, tritt ein liberaler Datenschutz-Ansatz zutage: Im amerikanischen Selbstverständnis geht das Gefahrenpotenzial vom Staat aus. Eine Beobachtung, die im Lichte der Snowden-Affäre durchaus pointiert wirkt, jedoch keineswegs eines faktischen Fundaments entbehrt. Datenschutz wird in den USA als eine Manifestation des individuellen Eigentumsrechts begriffen. Diese starke Rechtsposition muss grundsätzlich in Einklang mit dem staatlichen Auftrag des Schutzes der öffentlichen Sicherheit gebracht werden. Entsprechend wird der Datenschutz, nach einer Entscheidung des Supreme Court, zugunsten staatlicher Überwachung beschränkt (bspw. Katz v. United States, 386 U.S. 954, 1967). Auch steht der Datenschutz in starkem Konflikt mit der Rede- und Pressefreiheit.

Vorstöße der Europäischen Union – vor allem zum „Recht auf Vergessenwerden“ („right to be forgotten”) – stehen der US-Rechtsprechung entgegen. Die USA verlassen sich in ihrem Datenschutzsystem auf staatliche und föderale Statuten und Doktrinen – mithin auf sektorale Gesetzgebung. Dazu gehören unter anderem: „Intelligence Surveillance Act”, „Children Online Privacy Protection Act”, „Protect IP Act”, „Health Insurance Portability and Accountability Act”. Der Datenschutz knüpft in den USA eher an Verbraucherschutz und Wettbewerbsrecht an. Vor allem fehlt auch eine überwachende Durchsetzungsbehörde, stattdessen soll ein selbstregulatorisches Element den Raum für Leistungspotenzial und Flexibilität sichern.

EU – Datenschutz im Zeichen der europäischen Gemeinschaft

Die Datenschutz-Tradition der Europäischen Union hat ihre Wurzel dagegen in der Idee der europäischen Gemeinschaft. Die Einheitlichkeit des Datenschutzes innerhalb Europas soll Barrieren zwischen den Mitgliedstaaten abbauen. Frei nach dem Motto: gemeinsamer Wirtschaftsraum – gemeinsame Grenzen – gemeinsamer Datenschutz. Zentrales Element ist es, dass die Staatengemeinschaft das Individuum gegenüber der Wirtschaft zu schützen hat. Letztlich ist von einem eher proaktiven Ansatz zu sprechen, der aber in Bezug auf außereuropäische Datenschutz-Systeme durch ein reaktives Element ergänzt wird: nämlich durch die Richtlinie über die Verarbeitung personenbezogener Daten (Richtlinie 95/46/EG).

Diese Richtlinie besagt grundsätzlich, dass die Verarbeitung von personenbezogenen Daten nur insoweit rechtmäßig ist, als dass eine Einwilligung der betroffenen Person vorliegt. Eine Übermittlung der personenbezogenen Daten in Drittländer gestattet diese Richtlinie in einer Standardklausel immer nur dann, wenn dort ein angemessenes Schutzniveau für personenbezogene Daten garantiert wird und die Europäische Kommission diesen Staaten eine entsprechende Bescheinigung ausgestellt hat.

Dieser Ansatz der EU verschärft natürlich das Konfliktpotenzial mit den USA – und wirft auch einen Streit über Zuständigkeitsbereiche auf. Nach klassischer Völkerrechtslehre wird die Zuständigkeit der Gerichtsbarkeit durch die Souveränität eines Staates festgestellt. Eigentlich sollen so Unabhängigkeit und Gleichheit der Staaten garantiert werden, hier führt es jedoch zu Reibungspunkten zwischen den USA und der EU: Die USA machen die Zuständigkeit je Einzelfall davon abhängig, ob tatsächlich eine wirtschaftliche Transaktion stattgefunden hat oder lediglich Informationen ausgetauscht wurden. Die EU sieht sich aber in allen Fällen zuständig, in denen Daten von EU-Bürgern gesammelt werden oder auf solche zugegriffen wird.

Sichere Häfen und ein neuer Goldstandard

Um diesen Konflikt zu lösen, wurde begrifflich tief in der romantischen Seefahrt-Phantasie gegraben: es entstand das Safe Harbor Agreement. Diese Datenschutzvereinbarung sollte den Datenverkehr zwischen der EU und den USA mit der Richtlinie 95/46/EG in Einklang bringen und so den europäischen Bürgern und Unternehmen nach der beschwerlichen, sekundenschnellen Überquerung des Datenozeans in die USA einen sicheren Hafen bieten. Ziel war es dabei, die Balance zu finden zwischen einem nach europäischer Ansicht adäquaten Datenschutz und der durch die USA bevorzugten Selbstregulation des Marktes.

Die Idee war, dass sich amerikanische Unternehmen den Vorgaben der „Safe Harbor Privacy Principles“ unterwerfen können – was jedoch vollkommen freiwillig geschah. Das Department of Commerce zertifizierte dabei jährlich die Einhaltung von selbstregulierenden Programmen. In diesem Zusammenhang erklärte es das Safe Harbor Agreement – auch der folgende Begriff lässt an Pira-

Wo kein Kläger, da kein Richter: dennoch bleibt die Rechtslage unsicher – die Frage der Territorialität wird an Bedeutung gewinnen Bildquelle: eyetronic - fotolia.com

tenerzählungen denken – als „Gold Standard for data protection“. Auf der europäischen Seite wurden diese „Principles” als ausreichend akzeptiert. Doch schon am Format der rechtlichen Ausgestaltung wird deutlich, dass nicht alles Gold ist, was glänzt: Das Safe Harbor Agreement stellte eben kein internationales Abkommen im legalistischen Sinne dar, sondern lediglich ein Agreement.

Auf beiden Seiten des Atlantiks konnte diese Vorgehensweise nicht überzeugen. Regelmäßige Überprüfungen ergaben gravierende Mängel. So waren im Jahre 2008 von 1.597 gelisteten Organisationen nur 1.109 noch zertifiziert oder überhaupt noch existent. Sogar nur 348 von ihnen erreichten den Mindeststandard der aufgeführten „Principles“. Die größten Defizite gab es im Bereich der Durchsetzung und bei den Konfliktlösungsmechanismen. Außerdem behaupteten 206 Organisationen fälschlicherweise, dass sie Mitglieder im Safe Harbor-Verbund seien – einige dieser „Piraten“ fälschten sogar Prüfzeichen.

Das Urteil des Europäischen Gerichtshofs

Zunächst waren es die faktischen datenschutzrechtlichen Defizite, die zur europäischen Kritik am Safe Harbor Agreement führten. Doch seit den Snowden-Enthüllungen im Jahre 2013 rückten die invasiven Vorstöße insbesondere von US-Behörden in den Fokus der Datenschutz-Gemeinde. Das Urteil des Europäischen Gerichtshofs befasst sich genau mit dieser Nuance des Safe Harbor Agreements. Anlass dafür war ein Rechtsstreit zwischen dem österreichischen Juristen Max Schrems und der irischen Datenschutzbehörde, der sich auf die datenschutzrechtlichen Regelungen bei der Facebook Ireland Inc. bezog. Diese europäische Facebook-Tochter nutzt ganz oder teilweise Server, die sich auf US-Territorium befinden. Hier wurde US-amerikanischen Behörden bei Überwachungen Zugriff auf personenbezogene Daten gewährt bzw. kein ausreichender Schutz gegen ebensolche Zugriffe sichergestellt. Unter Verweis auf das Safe Harbor Agreement hatte die irische Datenschutzbehörde die Beschwerde Schrems abgelehnt, die sich gegen diesen Umstand richtete. Mit dem Umweg über die Europäische Kommission, welche die USA als zulässiges Drittland eingestuft hatte, landete das Verfahren schließlich beim Europäischen Gerichtshof.

Der Europäische Gerichtshof betont in seinem Urteil, dass die Regelungen des Safe Harbor Agreements lediglich die amerikanischen Unternehmen erfassen. Weder nationalstaatliche noch bundesstaatliche Behörden seien durch das Abkommen verpflichtet worden. Vielmehr sei diesen ein durch die Unternehmen nicht einschränkbarer Zugriff auf die personenbezogenen Daten europäischer Bürger gewährt worden. Ansatz seien dabei stets Überlegungen der nationalen Sicherheit, des öffentlichen Interesses sowie der Vollzug nationaler oder bundesstaatlicher Gesetze gewesen. Gegen diesen Eingriff in die Grundrechte der Bürger der Europäischen Union könne in den USA im Zweifelsfall auch kein administratives oder gerichtliches Rechtsmittel eingelegt werden. Die durch den Eingriff belasteten Bürger könnten weder um Zugang zu den erhobenen Daten noch um Berichtigung oder Löschung ersuchen. Sie stehen gleichsam jeder Entermaßnahme der amerikanischen Behörden schutzlos gegenüber. Dieses Vorgehen stellt natürlich in sich eine Verletzung europäischer Grundrechte, nämlich auf gerichtlichen Rechtsschutz, dar. Ebenso sei bereits der Umfang der Datenerhebung grundrechtsgefährdend, denn es finde keine Beschränkung auf das Notwendige statt – wie sie beispielsweise als Zulässigkeitskriterium in Europa vorgesehen sei. Nach Ansicht des Europäischen Gerichtshofs werden aufgrund der invasiven Eingriffe bzw. der Eingriffsmöglichkeiten der US-Behörden die Grundrechte der EU-Bürger auf Ebene des Rechtschutzes, des Privatlebens sowie des Datenschutzes so massiv verletzt, dass die USA nicht als Land mit angemessenem Schutzniveau für personenbezogene Daten eingestuft werden kann. Infolgedessen erfülle auch das Safe Harbor Agreement nicht die Vorgaben der Richtlinie 95/46/EG. Es ist also tatsächlich nicht alles Gold, was glänzt.

Wie wirkt sich die Absage auf Unternehmen aus?

Nun fragt sich, welche Auswirkungen eine solche Absage an den Datenschutzansatz der USA und an das Safe Harbor Agreement für die europäische Wirtschaft und europäische Unternehmen hat. Grundsätzlich werden wohl keine unmittelbaren Auswirkungen zu spüren sein. Wahrscheinlich gilt das Prinzip: Wo kein Kläger, da kein Richter. Zunächst müssten den nationalen Datenschutzbehörden Unternehmen namentlich gemeldet werden, deren konkretes Vorgehen rechtswidrig oder zumindest nicht rechtskonform ist. Die nationale Behörde würde nach einer Prüfungspha-

se dann ein entsprechendes Statement abgeben. Auch wenn das Urteil gegen Safe Harbor keine unmittelbare Wirkung hat, dürfte es auf längere Sicht durchaus markante Änderungen auf dem europäischen bzw. transnationalen Markt geben. Größere Unternehmen wie Facebook, Google und ähnliche Giganten werden auf Serverlandschaften in der Europäischen Union angewiesen sein, um den Datenschutz-Vorgaben der EU gerecht zu werden. Dies bedeutet letztlich einen Ausbau der IT-Infrastruktur in Europa. Entsprechend würden auch verschiedenste branchenverwandte und branchennahe Dienstleister wachsende Auftragsvolumina verzeichnen. Grundsätzlich ließe sich aus dem Urteil also eine positive wirtschaftliche Entwicklung in Europa ableiten.

Allerdings haben einige Wirtschaftsexperten und -journalisten bereits angemerkt, dass kleinere Unternehmen, die ebenso auf den transatlantischen Handel angewiesen sind, bei dieser Ausgangslage in einen direkten Konkurrenzkampf mit den besagten Internet-Giganten treten würden: Start-Up-Unternehmen sowie kleinere, aber auch mittelständische Dienstleister müssten um den Zugang zu Servern bangen – ein starker Wettbewerbsdruck. Letztlich ist wohl von einer positiven wirtschaftlichen Entwicklung in unterschiedlichen Marktsegmenten auszugehen, wenngleich man das Risiko der Übervorteilung kleinerer und mittelständischer Unternehmen nicht vernachlässigen darf.

Das Datenschutzrahmenabkommen als Lösung?

Mit dem Ende des Safe Harbor Agreements stellt sich die Frage nach einer zukunftsfähigen politischen Lösung. Es wird eine neue Vereinbarung zwischen den USA und der EU geben müssen. Ist damit die Zeit für das Datenschutzrahmenabkommen angebrochen? Die Pläne zu diesem Vorhaben liegen schon länger auf Eis. Die jeweiligen Vorbehalte bewegen sich – schon beinahe symptomatisch – in den traditionell verwurzelten Argumentationsbahnen. Im Fokus der US-Kritik stand vor allem, dass der EU-Entwurf eines Datenschutzrahmenabkommens die kommerzielle Interoperabilität als behindernd und sogar als für Konsumenten kontraproduktiv ansah. Zudem wurden negative Auswirkungen auf die Redefreiheit und weitere Menschenrechte befürchtet. Dabei stand insbesondere das „Recht auf Vergessenwerden“ („the right to be forgotten“) im Mittelpunkt. Von den USA wurden sowohl dessen enge Ausgestaltung kritisiert als auch dessen technische Umsetzbarkeit in Frage gestellt. Zudem hielten die Kritiker die internationale Zusammenarbeit bei der Strafverfolgung und die Interoperabilität von Regulierungsbehörden für gefährdet. Maßnahmen bei europäischen Datenschutzbehörden erst anmelden und autorisieren lassen zu müssen, erschien den USA als zu umständlich – dies führe letztlich zu Ineffektivität.

Es zeigt sich, dass die traditionell verwurzelten Datenschutzansätze weiterhin die Entwicklung eines trans- oder gar international einheitlichen Datenschutzes hemmen. Auch das Urteil des Europäischen Gerichtshofs spiegelt letztlich nur die europäische Pfadgebundenheit wider. Ein Rahmenabkommen, so notwendig es nach dem Wegfall des Safe Harbor Agreements auch erscheint, dürfte vor diesem Hintergrund eher in noch weitere Ferne gerückt sein. Die Wellen, die das Urteil geschlagen hat, werden es zumindest in naher Zukunft nicht erleichtern, einen neuen sicheren Hafen zu finden.

Ein Meer ohne Hafen macht die Seefahrt nicht sicherer

Von Häfen, von Gold und von Piraten war hier die Rede – Datenschutz kann also durchaus aufregend sein. Aber all die romantisierende Begrifflichkeit kann auch nicht darüber hinwegtäuschen, dass das Urteil des Europäischen Gerichtshofs lediglich Fehler im Datenschutzsystem aufgedeckt hat. Die Absage an das Safe Harbor Agreement birgt langfristig das Potenzial, einen Wandel herbeizuführen – aber das bloße Ende von Safe Harbor stellt diesen Wandel noch nicht dar. Die Sicherheitslage für europäische Bürger und Unternehmen in den USA ist weiterhin als schwierig zu bezeichnen. Es käme jetzt darauf an, eine Lösung auf systemischer Ebene zu etablieren. Es ist die Aufgabe der Politik, den Wandel zu initiieren. Um es mit einer letzten Meeresmetapher zu sagen: Es bleibt zu hoffen, dass die Wellen des Safe Harbor-Urteils so hoch schlagen, dass sie nicht wirkungslos an den Felsenküsten der jeweiligen Datenschutztraditionen brechen.

Bildquelle: wayne_0216-fotolia.com