Peter Schaar: Nur informationshalber Hinweis: Der Judicial Redress Act ist ein Gesetz, ein Gesetzentwurf aus der Mitte des Kongresses, der es ermöglichen soll, dass das US-Justizministerium Bürgern von anderen Staaten ähnliche Rechte einräumt, in Sachen Datenschutz, wie US-amerikanischen Bürgern und Personen mit dauerndem Aufenthalt-Status, z.B. Auskunftsrechte gegenüber Sicherheitsbehörden. Vorgesehen ist ein gestuftes Verfahren. Es wird nicht durch das Gesetz selbst festgestellt, dass Europäer gleichgestellt werden. Sondern es vorgesehen, dass das US Justizministerium unter bestimmten Bedingungen eine entsprechende Entscheidung treffen kann, die aber auch widerrufbar ist. Dieses wurde vom US-Senat noch nicht abschließend gebilligt. Das Repräsentantenhaus hat aber schon zugestimmt. Alexander Dix ist nicht nur langjähriger Landesbeauftragter für den Datenschutz, zunächst in Brandenburg gewesen und jetzt in Berlin noch - bis zur morgigen Amtsübergabe an seine Nachfolgerin, sondern er ist auch in dieser Funktion noch Vorsitzender des Arbeitskreises für internationalen Datentransfer der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Insofern hätten wir hier keinen kompetenteren Referenten gewinnen können.

Alexander Dix:

Herzlichen Dank, meine Damen und Herren.

Die Datenschutzbehörden, Frau Kotthaus hat es schon angesprochen, haben einen klaren Auftrag vom Europäischen Gerichthof bekommen. Dem stellen sie sich jetzt. Sie sind gerade dabei. Heute hat eine entsprechende Sitzung stattgefunden in Frankfurt unter den deutschen Datenschutzbehörden und nächste Woche, am 02. Februar, treffen sich die europäischen Datenschutzbehörden um zu beraten, wie jetzt weiter vorgegangen werden soll.

Was ist der Auftrag des Europäischen Gerichtshofs? Der EUGH hat in der Sache Schrems in sehr klaren Worten gesagt, dass Daten von Unions-Bürgern nicht in Drittländer exportiert werden dürfen, in denen der Wesensgehalt der europäischen Grundrechte nicht geschützt ist. Und zwar der Wesensgehalt insbesondere der informationellen Selbstbestimmung, man könnte auch sagen des Telekommunikationsgeheimnisses auf der einen Seite und zum anderen der Wesensgehalt des Grundrechts auf richterliche Kontrolle, auf Rechtsschutz. Das sind die beiden Pfeiler, die der Gerichtshof sehr klar hervorgehoben hat. Ich sage das in so allgemeiner Form, weil ich deutlich machen will, wir unterhalten uns hier nicht nur oder nicht allein über den Transatlantischen Datenexport in die USA, sondern wir unterhalten uns über alle Wirtschaftsbeziehungen zwischen der europäischen Union und anderen Ländern. Ich nenne nur China, Indien und andere Länder. Japan ist erwähnt worden. Die sind alle betroffen. Natürlich ist es von der wirtschaftlichen Realität her so, dass die Vereinigten Staaten der wichtigste Handelspartner Europas sind. Insofern schlägt sich das hier nieder. Ironischerweise wissen wir auch über die Rechtslage in den USA verhältnismäßig viel. Wir wissen relativ wenig über die Rechtslage in China oder in Indien. Das aber entbindet die Datenschutzbehörden nicht von der Aufgabe, genau diesen klaren Auftrag, den der EuGH formuliert hat, jetzt umzusetzen und das ist eine sehr komplexe Aufgabe. Und es ist nicht realistisch anzunehmen - um gewissen Horrorszenarien, die in den USA an die Wand gemalt worden sind, die entgegenzutreten, - dass nächste Woche der gesamte Datenexport aus der Europäischen Union gestoppt wird. Das ist vollkommen unrealistisch. Aber was auch klar ist, die Datenschutzbehörden können jetzt nicht mehr erklären - wie sie es lange Zeit getan haben, schon seit der Mitteilung der Kommission vom Herbst 2013 - , sie würden prüfen, ob sie von den Aussetzungsmöglichkeiten Gebrauch machen sollten, die damals schon bestanden, sowohl bei den Standardvertragsklauseln, als auch bei anderen Transfermechanismen wie der Safe Harbor Entscheidung. Sie haben dann aber immer gesagt: wir warten bis wir ein Signal von der politischen Ebene bekommen, dass jetzt ein Nachfolgeabkommen, ein nachgebessertes Safe Harbor Abkommen, ausgehandelt ist mit der US-Seite. Diese Möglichkeit abzuwarten, haben die Datenschutzbehörden jetzt nicht mehr. Sie können nicht erneut eine weitere Frist setzen.

Das Moratorium, dass nach der EuGH-Entscheidung bekanntgegeben wurde, bis zum 31.01., also bis Ende dieser Woche, das galt schon nicht für Fälle, in denen sich Bürger an die Aufsichtsbehörden gewandt haben und sich etwa darüber beschwert haben, dass ihre Daten immer noch auf der Grundlage der Safe Harbor Entscheidung in die USA exportiert werden. Das ist nämlich seit der Entscheidung des EuGH eindeutig rechtswidrig und muss sofort unterbunden werden. Darüber kann es keinen Streit geben, sondern die Aufsichtsbehörden haben nur gesagt, wir warten jetzt bis Ende Januar um uns eine Strategie zu überlegen, wie gehen wir dann koordiniert vor. Das ist vom praktischen Gesichtspunkt her sicherlich sinnvoll, aber jetzt müssen die Datenschutzbehörden „springen“. Sie haben bisher nur den Mund gespitzt, jetzt müssen sie auch pfeifen.

Und ich will mal skizzieren, in welche Richtung das unter Umständen gehen könnte. Wir haben zunächst, immer noch, eine sehr unterschiedliche Rechtssituation in der Europäischen Union, was die Genehmigungspflicht z. B. von Datenexporten in Drittländer angeht. Es ist keineswegs so, dass in allen Ländern jeder Datenexport genehmigungspflichtig ist. Es gibt aber Länder, wo jeder einzelne tatsächlich genehmigt werden muss. Ich nenne nur Österreich und Luxemburg, die haben kritisch gesprochen relativ bürokratische Datenexport-Regimes und müssen jetzt darüber nachdenken, was sie mit allen diesen erteilten Exportgenehmigungen denn anfangen. Ob sie die widerrufen müssen. Sie stehen also vor erheblichen Problemen. In anderen Ländern gibt es keine Genehmigungspflichten, auch bei Safe Harbor gab es keine Genehmigungspflichten, teilweise noch nicht einmal Anzeigepflichten. Da muss überhaupt erst mal festgestellt werden, was existieren den aktuell jetzt für Datenflüsse hinsichtlich welcher Datenarten und auch welcher Rechtsgrundlage.

Also es besteht ein erheblicher Bedarf, dass sich die Datenschutzbehörden zunächst untereinander informieren, was passiert jetzt. Das ist auch deshalb wichtig, weil eine alte Gefahr wieder droht, die schon seit jeher angesichts der mangelhaften oder unzureichenden Harmonisierung des Datenschutzniveaus in Europa immer bestand, nämlich die Gefahr des Forum-Shopping. Wenn sich Datenexporteure in einem Land befinden, dessen Datenschutzbehörde relativ strikt und rigide vorgeht und sagt: wir prüfen, ob wir von der Ausnahmeregelung der Entscheidung zu den Standardvertragsklauseln Gebrauch machen und auch solche Datenflüsse im Einzelfall unter Umständen unterbinden, dann könnte das Unternehmen versucht sein, nach einem anderen Mitgliedsstaat Ausschau zu halten, wo die Aufsichtsbehörde das nicht so eng sieht. Solche Aufsichtsbehörden gibt es.

Wir befinden uns in einer Situation, wo die Datenschutzgrundverordnung noch nicht beschlossen ist. Wir rechnen damit, dass sie möglicherweise Mitte dieses Jahres endgültig in Kraft tritt. Der Rat will im April der Grundverordnung zustimmen, dann muss das Europäische Parlament noch zustimmen. Also Juni dieses Jahres ist wahrscheinlich realistisch und dann beginnt eine zweijährige Übergangsfrist. In dieser Frist haben wir noch kein funktionierendes Kohärenzverfahren, wir haben noch keinen wirklich funktionierenden europäischen Datenschutzausschuss. Aber trotzdem müssen die Aufsichtsbehörden schon in dieser Übergangsphase verhindern, dass erneut Datenflüsse so umgeleitet werden, dass man die Vorgaben des Europäischen Gerichtshofs leicht umgehen kann. Das ist ihre Hauptaufgabe im Moment.

Sie werden nicht von heute auf morgen sämtliche Datenflüsse unterbinden, das können sie praktisch gar nicht. Sie werden sich aber, denke ich, darauf verständigen, dass man zunächst mal eruiert, wo gibt es noch eine Datenübermittlung auf der Basis der Safe Harbor Entscheidung. Solche Übermittlungen darf es jetzt schon nicht mehr geben und es wird wahrscheinlich auch kein Unternehmen heutzutage noch offen sagen „Ja das machen wir nach wie vor auf der Grundlage von Safe Harbor“. Weil sie dann ins offene Messer rennen würden. Es wird kein Unternehmen zugeben, sondern man wird fragen müssen: was macht ihr stattdessen? Welche Rechtsgrundlage zieht ihr stattdessen heran? Wenn dann Bezug genommen wird auf Standardvertragsklauseln oder bindende und verbindliche Unternehmensregeln, ist zunächst festzuhalten, dass diese Transfermethoden nicht direkt vom Europäischen Gerichtshof behandelt wurden. Sie sind weiterhin gültig, aber zumindest die Entscheidungen der Kommission zu Standardvertragsklauseln enthalten alle einen Artikel 4, der sagt, dass die Aufsichtsbehörden das Recht und auch die Befugnis haben, im Einzelfall Datenflüsse in ein Land zu unterbinden, in denen staatliche Stellen auf die Daten der Unionsbürger in einem Maße Zugriff haben und Zugriff nehmen, wie es in einer demokratischen Gesellschaft nicht zwingend

erforderlich ist. Das ist genau der Standard, den die Europäische Grundrechtecharta und auch die Europäische Menschenrechtskonvention für die „National-Security“-Ausnahme vorsehen. Grundrechtseingriffe sind nur solange und in dem Ausmaß zulässig, wie es in der demokratischen Gesellschaft zwingend erforderlich ist.

Das ist ein Thema, welches nicht nur die USA betrifft. Es betrifft eine ganze Reihe außereuropäischer Länder gleichermaßen. Es betrifft auch europäische Länder, was die Amerikaner uns gerne entgegenhalten. Aber wir sprechen hier zunächst einmal über unsere Aufgabe als Aufsichtsbehörden, als Datenschutzbehörden - das ist im Moment zunächst nur die Kontrolle des Datenexports. Ich rechne damit, dass sich in diesem Jahr noch der Europäische Gerichtshof für Menschenrechte zu den Überwachungsgesetzen in Großbritannien äußern wird. Möglicherweise wird das sogar, wenn der Gerichtshof seiner bisherigen Rechtsprechung folgt, die in den letzten Monaten zu Fällen aus Russland und Ungarn ergangen ist, eine Rolle in der Brexit-Diskussion in Großbritannien spielen. Ich halte die Gesetze in Großbritannien für nicht vereinbar mit der Grundrechtecharta. Aber das ist ein Thema, welches man im Moment abkoppeln sollte von dieser Datenexport-Debatte. Hier geht es wirklich um die Frage, wie kann sichergestellt werden, dass die Daten von Unionsbürgern, wenn sie die Europäische Union verlassen, immer unter dem Schutzschirm eines im wesentlichen gleichwertigen Datenschutzes auch im Zielland ankommen und dort entsprechend behandelt werden. Das ist die zentrale Aufgabe. Die Unternehmen sollten nicht warten, bis die Datenschutzbehörden an der Tür stehen und klopfen und sagen “was macht ihr denn da eigentlich“. Sondern sie sollten selber einen Plan entwickeln und dieser Plan könnte so aussehen, dass man sich das Urteil des Europäischen Gerichtshofes anschaut und Konzepte dazu entwickelt, wie der unkontrollierte Zugriff von Nachrichtendiensten zumindest erschwert werden kann. Ganz ausgeschlossen werden kann er nie. Wie kann man Rechtsmittel ausschöpfen gegen staatliche Zugriffe? Wie kann man auch Verschwiegenheit als Anordnung, sogenannte gagging orders, wie sie in den USA üblich sind und Transparenz geradezu verhindern, zumindest einer gerichtlichen Überprüfung zuführen? Microsoft und andere Unternehmen haben das schon vorexerziert. Das würden die Europäischen Datenschutzbehörden mit Sicherheit erwarten, dass man zumindest alle rechtlichen Möglichkeiten ausschöpft, um sich solchen Überwachungsmaßnahmen entgegenzustellen. Auch wenn am Ende möglicherweise ein Gericht in den USA oder in einem anderen Drittstaat sagt, das sei alles in Ordnung.

Das nächste wichtige Thema sind auch technisch-organisatorische Maßnahmen, die die Sicherheit der Datenverarbeitung, die Zugriffsmöglichkeiten, erschweren, Stichwort Verschlüsselung. Und am Ende steht dann auch die Frage, in welchem Umfang ist ein jetzt als Datenexporteur auftretendes Unternehmen unter Umständen gehalten, die Datenverarbeitung nach Europa zu verlagern, wenn im Drittland gleichwertiger Datenschutz und Datensicherheit nicht sichergestellt werden können. Auch darüber muss gesprochen werden. Dazu wird Herr Brinkel möglicherweise nachher noch was sagen, weil Microsoft ja genau in diese Richtung denkt. Und andere amerikanische Unternehmen tun das auch. Also alle diese Konzepte liegen jetzt auf dem Tisch und die Datenschutzbehörden werden, das ist meine Prognose, jetzt Prioritäten setzen und sich geeignete Unternehmen aussuchen, die möglicherweise mit besonders sensitiven Daten, Stichwort Gesundheitsdaten, umgehen, mit Telekommunikationsdaten hantieren, die am ehesten der Gefahr unterliegen, dass Nachrichtendienste vor allem darauf zugreifen. Sie werden eine Prioritätenliste aufstellen, welche Unternehmen sie in erster Linie angehen werden und die Unternehmen, die sich Forderungen der Aufsichtsbehörden gegenüber sehen, sollten nicht den Fehler machen zu sagen, alle anderen machen

es aber auch so. Das ist ein schlechtes Argument. Die Aufsichtsbehörden sind unabhängig, sie können selbst entscheiden, wen sie sich zuerst vornehmen und es ist vollkommen logisch, dass sie ihre Ressourcen auch sinnvoll einsetzten müssen. Sie werden das in abgestimmter Form tun, um genau zu verhindern, dass das Problem des Forum-Shoppings jetzt auf einer anderen Ebene in der Folge der EuGH-Entscheidungen erneut auftritt.

Ich will noch abschließend einen Aspekt einbringen, der eher unjuristisch ist, den ich aber auch für wichtig halte, dies habe ich auch im Wirtschaftsministerium vor Kurzem betont. Das EuGH-Urteil hat auch einen industriepolitischen Effekt. Man könnte auch sagen einen wirtschaftspolitischen Effekt, den muss es haben, und manche Unternehmen haben das auch schon erkannt. Europa, europäische Unternehmen, Konzerne wie Telekom, BMW, Infineon haben eine gemeinsame Sicherheitsstrategie aufgelegt und dem Kommissar Oettinger vorgelegt. Genau so eine gemeinsame Datenschutzstrategie ist jetzt auch nötig. Europa muss seine Chance jetzt nutzen, um den Standort zu stärken und das ist etwas, was die Politik verstehen muss. Man kann jetzt fein ziselieren, darüber diskutieren muss man auch, das ist Aufgabe der Aufsichtsbehörden. Wie können die Standardvertragsklauseln jetzt überhaupt noch verwendet werden? Aber die Politik muss, abgesehen von den Bemühungen um ein Nachfolgeabkommen, auch die europäischen Daten-Verarbeiter, die IT-Industrie darin bestärken, europäische Lösungen voranzubringen. Auch mir ist vollkommen bewusst, dass es weltfremd wäre zu glauben, dass man sich von den Vereinigten Staaten vollkommen abkoppeln kann. Aber es besteht jetzt die Chance, auch mit diesen Aussagen des EuGH die europäische Position wirtschaftlich zu stärken. Das ist meine persönliche Auffassung.

Peter Schaar: Herzlichen Dank! Viele Fragen drängen sich auf, aber ich werde sie jetzt nicht stellen. Das Wort geht weiter an Herrn Professor Büllesbach, ich hatte vergessen zu erwähnen, dass er auch Vorstandsmitglied der EAID ist, schon lange, viel länger als ich, sogar Gründungsmitglied. Insofern haben wir eine geballte Kompetenz in Sachen Datenschutz hier und Erfahrung. Herr Prof. Büllesbach, Sie haben das Wort.

Peter Schaar: Es ist ja deutlich geworden, das Safe Harbor-Urteil des Europäischen Gerichtshofes betrifft nicht nur die amerikanischen Unternehmen, sondern auch die deutsche Wirtschaft. Und das ist, finde ich, eine ganz wichtige Botschaft, die noch nicht von allen so rezipiert worden ist. Wir befinden uns heutzutage in einer Welt, die stark durch Bewölkung geprägt ist, gerade in der Informationstechnologie. Wir haben Cloud-Services. Viele Services, die im kommerziellen Bereich undteilweise auch im privaten Bereich eifrig genutzt werden, sind Cloud-Services. Microsoft ist ja nicht nur ein Anbieter eines sehr erfolgreichen Betriebssystems für Personal Computer, auch vielfältige andere Produkte kommen aus dem Unternehmen und viele dieser Produkte sind heutzutage so strukturiert, dass sie eben auf der Cloud basieren, das heißt, dass Rechner, die über das Internet verbunden sind, mit Servern Leistungen abrufen können. Und das bedeutet natürlich, dass jetzt die Frage „Wo sind denn die Daten?“ für den Nutzer erstmal nicht so ohne Weiteres erkennbar ist und jedenfalls schwer zu beantworten ist, aber sie sind möglicherweise auch in den USA gespeichert und sie sind entsprechend grenzüberschreitend abrufbar. Nicht nur durch Stellen in den USA, sondern auch durch sonstige Stellen und andere sogenannten Drittstaaten, außerhalb der Europäischen Union. Insofern stellt sich für ein solches international aufgestelltes Unternehmen wie Microsoft die Frage in besonderem Maße, wie der Datenschutz im internationalen Maßstab garantiert werden kann. Ich freue mich sehr, dass Dr. Brinkel hier die Sichtweise seines Unternehmens und vielleicht auch einige Antworten, die Sie schon gefunden haben, uns hier präsentieren wollen. Sie haben das Wort.