**Dr. Guido Brinkel:** Erstmal vielen Dank für die Unternehmensvorstellung und auch für den Hinweis, dass wir nicht nur Windows sind. Das ist richtig und die Zukunft liegt für uns, aber auch für viele andere Unternehmen tatsächlich in der Cloud. Es ist schwer nach so profunden Vorrednern noch einen Aspekt zu ergänzen, der noch nicht genannt wurde. Ich habe eben auch darüber nachdenken müssen, was ich vor 20 Jahren gemacht habe. Ich kann Ihnen garantieren, dass ich mit Datenschutz nichts am Hut hatte. Da habe ich mich gerade aufs Abitur vorbereitet. Insofern kann ich da auch nicht auf so ein langjähriges Knowhow zurückblicken wie meine Vorredner.

Ich würde gern zu Beginn meines Impulses nochmals die Debatte ein wenig weiten. In den Details ist ja schon gewühlt worden. Ich gehe auf einzelne Sachen, wie z.B. die Microsoft-Cloud für Deutschland auch gern detaillierter in der Diskussion ein. Aber ich glaube es ist jetzt interessant auch nochmals auf diesen industriepolitischen Aspekt einzugehen und genereller zu fragen: Was heißt eigentlich das, was wir hier sehen, insgesamt für Regulierung in einem globalen Medium? Ich glaube was sich heute schon herauskristallisiert hat, ist, dass man erstens sagen kann: Es geht hier nicht nur um Europa vs. Amerika. Es geht hier auch nicht nur um Safe Harbor, wenn man genau hinschaut. Und wenn man noch genauer hinschaut geht es auch nicht nur um Datenschutz.

Worum geht es dann? Was sind die Fragen, die, wenn die Wellen dieses akuten Zustandes, den wir im Moment gerade haben, verebbt sind? Ich glaube, dass die Debatte die wir heute über Safe Harbor führen, letztlich pars pro toto steht für eine etwas weiter gefasste fundamentale Herausforderung, die man vielleicht mit Global Internet Governance umschreiben könnte. Und ich meine das nicht in der Terminologie, wie man sie vielleicht kennt in Bezug auf Internet die sog. Internet Governance *Foren*, also Multi-Stakeholder-Prozesse, die damit versuchen gewisse Dinge festzulegen. Sondern in einem regulierungs-orientierterem Sinne, nämlich der Frage: Wie kann man überhaupt ein internationales Regulierungssystem für das Internet schaffen? Wie kommen wir zu einem noch stärker als heute harmonisierten Rechtssystem?

In der EU ist das relativ gut möglich, da gibt es das Instrument der Verordnung, aber wie sieht das eigentlich global aus? Wie gehe ich mit einem Konflikt von Jurisdiktionen um? Wo sich Jurisdiktionen in verschiedenen Ländern schlichtweg einfach widersprechen, Unternehmen aber in mehreren dieser Länder tätig sind? Wie sieht ein „level playing field“ aus, wenn es um die Durchsetzung von Rechten geht? Und wie können solche Individualrechte dann auch prozessual abgesichert werden? Das sind alles Fragen, die in der Safe Harbor Debatte angelegt sind.

Sie werden aber auch in ganz anderen Bereichen irgendwann relevant werden. Diese Frage ist nicht auf Datenschutz beschränkt, sondern das kann man fast auf jede Regulierungsmaterie, die relevant wird in Bezug auf digitale Dienste, herunter deklinieren. Wir haben ja noch an anderer Stelle eine sehr hitzige Debatte, die auch in der Transatlantikachse stattfindet, nämlich TTIP. Man wird vielleicht eines Tages auf die TTIP-Verhandlung zurückschauen und noch denken, das war die leichtere Übung. Denn die eigentlichen Probleme kamen dann erst, als es wirklich um das Regulierungssystem geht.

Wenn man es etwas längerfristig betrachtet, glaube ich, dass Safe Harbor nur ein Vorgeschmack ist, auf Dinge die da noch kommen werden in ganz anderen Gebieten, z.B. Persönlichkeitsrechten, Jugendschutz, Verbraucherschutz oder Urheberrecht. Dort haben wir heute schon auf völkerrechtlicher Ebene solche Versuche. Aber das ist eben nur Völkerrecht, die sog. WIPO-Treaties. Das wird noch überlagert von faktischen Entwicklungen, die heute auch schon fielen, weil sie im Datenschutzkontext auch relevant sind, z.B. das Thema Verschlüsselung.

Auch das kann man ja in eine Regulierungsfrage ummünzen und dann ist man bei dem Thema „Crypto Regulation“. Dies wird auch weltweit diskutiert, mit sehr unterschiedlichen Ansätzen, und ist am Ende aber eine ziemlich binäre Sache. Entweder habe ich eine saubere Verschlüsselung oder ich habe sie nicht. Und wenn die in dem einen Regulierungssystem verboten ist und in dem anderen wird sie gefordert, habe ich ein Problem. Insofern, hilft diese Diskussion auch, um aus den Scheuklappen der Safe Harbor Debatte herauszukommen und sich bewusst zu machen, dass diese Diskussion auch nicht die letzte sein wird, die wir in diesem globalen Maßstab führen, sondern es ist eher die erste von vielen.

Ich will auch noch auf ein anderes Problem, das sehr viel enger mit der Safe Harbor Debatte verbunden ist und das direkt mit Datenschutz im weiteren Sinne auch zu tun hat hinweisen, weil Microsoft hier eine besondere Rolle hat: Nämlich die Frage der extraterritorialen Anwendung von Recht. Das klingt sehr sperrig und ist nicht selbsterklärend, deswegen versuche ich es ganz kurz daran zu erläutern, was wir gerade in den USA durchfechten:

Es gibt in den USA, im Übrigen ähnlich wie auch in anderen Staaten, Auskunftspflichten für Unternehmen, entsprechend natürlich auch für Telekommunikationsunternehmen und Internetunternehmen, in Bezug auf öffentliche Sicherheit und Strafverfolgung. Wenn Gefahren drohen im strafrechtlichen Sinne, treten Behörden an die Unternehmen heran und fragen bestimmte Daten ab. Das gibt es auch in Deutschland. Wir haben so einen Fall 2013 in den USA auf den Tisch bekommen, der sog. „New York Search Warrant Case“.

Da ging es um eine strafrechtliche Ermittlung in Sachen Betäubungsmittel. Die US-Behörden wollten Zugriff auf E-Mails eines unserer E-Mail-Kunden und es stellte sich heraus, dass die Daten physisch in Irland liegen. Die US-Behörden und mittlerweile auch die Gerichte vertreten in diesem Verfahren die Auffassung, dass die Behörden Zugriff auf diese Daten haben, ohne dass sie sich auf das bestehende Rechtshilfeabkommen, die es zwischen Irland und der USA gibt, berufen müssen. Es wird uns also gesagt: „Wir müssen diese Daten intern bei uns aggregieren, auch wenn sie in Irland liegen und dann den Behörden zur Verfügung stellen“.

Das Interessante daran im Verhältnis zu Safe Harbor ist, dass ich hier praktisch umgekehrte Vorzeichen habe. Bei Safe Harbor geht es um den aktiven Transfer von Europa in die USA. Also um Daten, die Europa verlassen. Beim „warrant case“ geht es dagegen um Daten, die in Europa liegen; vermeintlich im Zugriff und in der Kontrolle der Regulierungsbehörden, die hier zuständig sind. Wir haben uns in den USA dagegen gewehrt, indem wir vor Gericht gegangen sind und das Verfahren läuft im Moment. Wir erwarten tatsächlich innerhalb der nächsten Wochen oder weniger Monate eine Entscheidung.

Es ist interessant, dass sich sehr viele Technologieunternehmen in den USA in Form von sogenannten Amicus-Briefen, in denen man beim Gericht deutlich machen kann, dass man das Interesse des entsprechenden Beschwerdeführers teilt, sich uns angeschlossen haben. Es haben sich auch sehr viele wissenschaftliche Institutionen unserem Vorgehen gegen diese Rechtsauffassung angeschlossen. Und nicht zuletzt hat sich auch die Regierung von Irland angeschlossen. In der ersten Instanz haben wir verloren. Die zweite Instanz steht jetzt aus und dann wird ggf. die Frage sein - das haben wir auch öffentlich angekündigt - wie das Verfahren vor dem Supreme Court ausgeht, wenn er sich dieser Sache annimmt. Das ist in den USA eine Spezialität, dass er das nicht muss.

Vielleicht noch ein Detail zu diesem Fall: das Interessante ist, dass auf dem Weg, den die Behörden hier gehen, bestimmte Sicherungen, die im Rahmen der Rechthilfeabkommen vorgesehen sind, nicht gelten würden. Also insbesondere wäre, wenn das so entschieden würde, die Regierung von Irland nicht zu informieren. Natürlich hat die mittlerweile von diesem Fall Kenntnis, aber in dem Standardverfahren wäre das nicht notwendig und der Betroffene wäre auch nicht zu informieren. Das sind auch Gründe, warum wir uns dagegen gewehrt haben. Und das steht jetzt zur Entscheidung an.

Ich habe eben diesen Konflikt der Rechtsordnung als ein Problem benannt, das praktisch deutlich breiter angelegt ist. Deshalb ist es interessant das Ganze rückzukoppeln mit der Datenschutzgrundverordnung, wie sie mit an Sicherheit grenzender Wahrscheinlichkeit beschlossen wird: Wenn wir davon ausgehen, dass die zweite Instanz genauso entscheidet wie die erste, nämlich gegen uns, dann haben wir also die Pflicht diese Daten herauszugeben, nach amerikanischem Recht. Und wir haben gleichzeitig dann spätestens ab 2018 - man kann sich auch fragen, ob das nicht heute schon letztlich Rechtslage ist - Artikel 43a Datenschutzgrundverordnung in Kraft, der uns genau das verbietet. Exakt diesen Fall. Es ist kein Zufall, dass dieses Thema in die Verordnung aufgenommen wurde. Artikel 43a sagt, dass Unternehmen keine Daten an Behörden von Drittstaaten herausgeben dürfen außerhalb von Rechtshilfeabkommen. Und das „Schöne“ daran ist, dass das mit 4% des weltweiten Konzernumsatzes maximal sanktioniert ist. Nicht nur bei uns, sondern das ist bei allen Unternehmen viel, zumal es pro Verstoß gilt. Diesen Konflikt kann man nicht auflösen. Das ist das Entscheidende. Ein Unternehmen, auch das willigste, kann diesen Widerspruch nicht auflösen.

Man hat bloß noch die Wahl, gegen welche Rechtsordnung man dann gegebenenfalls verstoßen würde. Und das führt dann auch zu Fragen, ob sich die Gesetzgeber künftig darin überbieten werden, durch die Erhöhung der entsprechenden Bußgelder den entsprechenden Delinquenten auf ihre Seite zu ziehen. Vor dem Hintergrund des neuen Sanktionssystems in der EU ist die Frage gar nicht so abwegig wie sie vielleicht klingt. Es sind praktisch die ökonomischen Erwägungen, die dann die einzige Leitplanke wären, die man als Unternehmen noch hätte, wenn man dann überhaupt eine Entscheidung treffen müsste.

Wichtig ist: Wir wehren uns dagegen sehr aktiv; wir sind auch in Europa unterwegs und wir brauchen Unterstützung von der Politik, wenn es z.B. zum Supreme Court gehen sollte, der zuerst darüber entscheiden muss, ob er das Verfahren überhaupt zur Entscheidung annimmt. Es wird interessant sein, ob die EU-Kommission dann sagt: Wir unterstützen das ebenfalls mit einem Amicus-Brief. Das Interessante am warrant case ist also, dass das auch akut ist. Genauso akut wie Safe Harbor, jedoch in Europa weniger diskutiert.

Was heißt das nun, wenn noch einen Schritt zurücktritt? Wie ist die Situation, die wir jetzt insgesamt haben? Unser Präsident und Chief Legal Officer Brad Smith hat letzte Woche in Brüssel bei einer Veranstaltung, die ein ähnliches Thema betraf, gesagt, dass die Verhandlungen, die wir im Moment führen zu Safe Harbor, aber letztlich auch in Bezug auf den Warrant Case, zu wichtig sind, um zu scheitern. „Too important to fail.“

Warum ist das der Fall? Da kommt die industriepolitische Dimension ins Spiel, die heute auch schon erwähnt worden ist. Wir hatten in 2015 ein Handelsvolumen zwischen Amerika und Europa von 240 Milliarden Dollar. China und Indien sind dabei gar nicht dabei. Das ist nicht das

Gesamthandelsvolumen, sondern das ist das digitale Handelsvolumen. Das ist die wirtschaftliche Kennzahl, wenn man wirklich nur auf den digitalen Bereich schaut.

US-Unternehmen beschäftigen insgesamt knapp 4 Millionen Menschen in der EU, das ist auch arbeitsmarktpolitisch interessant. Und wenn man sich anschaut, wie die Digitalisierung in Deutschland, in Brüssel, von Herrn Oettinger diskutiert wird, dann ist das die Zukunftshoffnung, auch für Europa. Die Politik redet sehr viel darüber, wie es Deutschland schafft, wie es Europa schafft, den Anschluss zu halten in digitalen Märkten. Wie kann die Industrie digitalisiert werden?

Das alles ist letztlich ohne Datentransfers nicht denkbar, denn wir haben in Europa 7% der Weltbevölkerung. In Plattformmärkten ist das nicht allzu viel. Wenn man die Industrie 4.0-Diskussionen anschaut, die auch eine Diskussion zur Plattformökonomie ist, wo es um sehr große globale Märkte geht - dann kann man das nur so denken. Und deswegen reicht insgesamt auch nicht der transatlantische Blick, sondern dann muss man wirklich überall schauen. Was ist mit Russland, was ist mit China? Das ist die industriepolitische Einrahmung des Ganzen. Und der Grund, warum es eine Lösung geben muss für alle Beteiligten.

Das ist kein Problem von amerikanischen Unternehmen, weil diese Frage gar nicht davon abhängt, wo man sitzt: Ein Mittelständler, der global sein Geschäft sucht, was ihm gerade durch die Digitalisierung ermöglicht wird; der Kunden in den USA oder in Indien sucht – der ist diese Datentransfers angewiesen. Es spielt keine Rolle, ob er in Deutschland, in Österreich oder in Indien seinen Hauptsitz hat, sondern er muss globale Datentransfers haben.

Es geht am Ende aber auch um das Grundvertrauen unserer Kunden in die Dienste. Das ist durch Snowden erschüttert worden und das kann natürlich durch solche Entwicklungen, wenn sie nicht einer Lösung zugeführt werden, weiter erschüttert werden. Wenn wir sagen, dass wir diese globalen Datentransfers brauchen, dann muss man natürlich auch dazu stehen, dass man auch verantwortlich sein muss in Bezug darauf, wie man damit umgeht. Und diese Verantwortlichkeit muss global funktionieren, für den Kunden, der sich betroffen sieht, aber trotzdem lokal zugänglich sein.

Da sind wir bei der Frage der Rechtsdurchsetzung und das ist sehr komplex. Es wird teilweise immer noch teilweise so getan, als sei der Datenschutz eine sehr deutsche und sehr europäische Angelegenheit. Ich glaube, das lässt sich spätestens nach Snowden so nicht mehr sagen. Datenschutz hat mittlerweile auch in den USA einen sehr viel höheren Stellenwert, vor allem auf der Nutzer-Seite. Da hat eine Angleichung stattgefunden. Hier haben sicher auch diese Debatten dazu beigetragen, die gerade geführt werden. Es gibt heute also eine Erwartungshaltung vom Kunden, in den USA genauso wie in Europa. Das ist auch der Grund warum letztlich Unternehmen gleichgelagertes Interesse haben.

Und damit sind wir im Grunde bei der Frage: Was bedeutet eigentlich Compliance? Compliance ist ja nicht nur ein rechtlicher Begriff, sondern auch ein ethisch-moralischer im Sinne von Unternehmensverantwortung. Und in der Welt in der wir uns bewegen, in der Cloud-Welt, in der digitalen Welt, heißt es letztendlich, dass wir uns global auf Standards einigen, auf die wir uns dann auch festlegen und an denen wir uns messen lassen. Die Frage, die jetzt entschieden wird, ist: Finden wir diese Standards oder finden wir sie nicht?

Also als ganz kurzes Fazit und dann Überleitung in die Diskussion, in der ich gerne auch nochmal auf einzelne Projekte von uns eingehe:

Es ist, wichtig zu sehen, dass Safe Harbor neben dieser sehr dringlichen operativen Komponente, die jetzt gerade in Brüssel und in USA diskutiert wird, eine fundamentalere Komponente hat, die man mitdenken sollte, weil uns das wiederbegegnen wird.

Weil wir vor der generellen Frage stehen, wie wir globale harmonisierte Regulierungssysteme im Cyberspace schaffen und wie wir diese Regulierungssysteme verbindlich machen. Für die Unternehmen verbindlich, weil das Rechtssicherheit bedeutet. Aber auch für die Nutzer verbindlich, um Verantwortung tatsächlich auch operativ wirksam zu machen.

Und am Ende, und das ist das ganz große Bild, geht es um das Primat der Politik. Safe Harbor wird mit darüber entscheiden, ob die Politik dieses Problem überhaupt noch lösen kann, oder ob hier auf politischer Ebene das Ganze scheitert, weil man sich nicht einigen kann, es den Behörden überlässt, die dann nur exekutieren können. Und es so am Ende dem Rechtsanwender überlässt. Und ich sage das bewusst so: Rechtsanwender sind sowohl Unternehmen wie auch die Kunden.

Soviel als Einleitung.