Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

„Der Einsatz von Cloudlösungen und weiteren Diensten im Kontext von Schrems II/ CLOUD Act“

bei der Bitkom Privacy Conference

28.09.2022

Online

Es gilt das gesprochene Wort

Sehr geehrte Damen und Herren,

I. Einleitung

ich freue mich, heute Teil dieser Veranstaltung zu sein und zu sehen, dass eine so große Zahl an fachkundigen Datenschutzexpertinnen und Datenschutzexperten aus Deutschland, Europa und der ganzen Welt zusammenkommt, um wichtige Privacy Themen zu diskutieren.

Dem Programm haben Sie bereits das Thema meiner Keynote entnommen, mit der ich heute zur Diskussion beitragen werde: „Der Einsatz von Cloudlösungen und weiteren Diensten im Kontext von Schrems II/ CLOUD Act“. Und ich behaupte dieser Titel enthält allein mit den Begriffen „Cloudlösungen“, „Schrems II“ und „CLOUD Act“ schon eine ganze Reihe an Begriffen, die gleich zu Beginn dazu geeignet sind, eine Vielzahl der Zuhörer zu triggern und damit hoffentlich das Ziel einer lebendigen und konstruktiven Auseinandersetzung mit diesem Thema zu fördern.

Wir alle hier wissen: Datentransfers kennen keine Grenzen. Infolge der Digitalisierung aller wirtschaftlichen und gesellschaftlichen Lebensbereiche werden personenbezogene Daten im Rahmen digitaler Dienste und Geschäftsmodelle zunehmend global übertragen und verarbeitet. Da dies aus Datenschutzsicht ganz erhebliche Auswirkungen hat, stellt sich die Frage, wie wir mit diesen Herausforderungen umgehen können. Und auch das wissen Sie alle, diese Frage stelle nicht ich heute

zum ersten Mal, sie wurde in den letzten Jahren und Jahrzehnten aus vielen Blickwinkeln gestellt und zuletzt eben besonders im Rahmen des titelgebenden Schrems II Urteils und im Kontext des CLOUD Act behandelt.

Dabei stellt sich natürlich zuvorderst die Frage, ob überhaupt und wenn ja wie denn nun die aktuellen datenschutzrechtlichen Herausforderungen nach den Urteilen des Europäischen Gerichtshofs (EuGH) die Zusammenarbeit mit US-Cloud-Providern weiter möglich machen. Das ist ohne Zweifel zum jetzigen Zeitpunkt nicht einfach zu beantworten und, um das Fazit vorwegzunehmen, nein – es gibt keine Patentlösung, die ich Ihnen heute hier präsentieren könnte.

Was ich aber sehr wohl kann, ist Ihnen die aktuellen Entwicklungen im Umgang mit Clouddiensten aufzuzeigen und die Anforderungen zu benennen, die dabei aus Datenschutzsicht zwingend erforderlich sind. Die bestehenden Unsicherheiten können uns alle nicht zufrieden stellen – da sind wir uns einig. Und die Sorgen und Nöte, die sich für die Wirtschaft aus dieser Unsicherheit ergeben, sind mir durchaus bewusst. Ich nehme diese Sorgen sehr ernst, gleichzeitig sehe ich es aber auch als Chance, dass wir durch die jüngsten Urteile dazu gezwungen werden, den Rechtsrahmen noch klarer und sauberer auszugestalten und damit gezielt Einfluss zu nehmen, um datenschutzkonforme Lösungen zu schaffen, die für alle Beteiligten eine sichere und vertrauensvolle Datenübermittlung ermöglichen.

Die Entwicklungen der letzten Jahre haben gezeigt, dass sich Datenschutz „Made in Europe“ durchaus zu einem Wettbewerbsvorteil entwickeln kann und das gilt auch und vielleicht sogar ganz besonders für den Bereich von Cloudlösungen.

Lassen Sie mich ausführen, was ich damit konkret meine und warum es in unser aller Interesse liegt und liegen muss, dass wir hier gemeinsam eine rechtssichere und vertrauensvolle Basis für einen sicheren Datentransfer schaffen.

II. Schrems II als Herausforderung

Die Auswirkungen von Schrems II sind definitiv nicht zu unterschätzen. Internationale Datentransfers stehen jetzt wieder ganz besonders im Fokus – auch der Aufsichtsbehörden. Das Problem beim Einsatz von Cloudlösungen liegt darin, dass in Drittländer (wie etwa, aber nicht ausschließlich, die USA) übermittelte personenbezogene Daten unter rechtlichen Voraussetzungen behandelt werden, die nicht dem europäischen Verständnis von einem angemessenen Datenschutzniveau entsprechen, dem wir uns mit der Einführung der DSGVO verpflichtet haben. So einfach kann man die Misere im Grunde zusammenfassen.

Der EuGH hat am 16. Juli 2020 mit dem Urteil in der Rechtssache Schrems II den EU-US-Privacy-Shield-Beschluss der EU-Kommission für ungültig erklärt. Zuvor galt die Annahme, dass die Vorgaben des

Datenschutzschilds dem Datenschutzniveau der Europäischen Union weitestgehend entsprechen und damit eine Übermittlung personenbezogener Daten in die USA möglich war. In seinem Urteil hat der EuGH diese Annahme zurückgewiesen.

Als Ergebnis der Schrems II Entscheidung können sich datenschutzrechtlich Verantwortliche nun bei Datentransfers in die Vereinigten Staaten nicht mehr auf die Angemessenheit des Datenschutzniveaus berufen. Die Voraussetzungen für die Übermittlung von personenbezogenen Daten haben sich damit fundamental geändert. Auch wenn sich durch das am 25. März 2022 angekündigte Privacy Shield 2.0 (Trans-Atlantic Data Privacy Framework) eine Lösung für Datentransfers in die USA abzeichnet, müssen Verantwortliche derzeit weiterhin insbesondere auf Standardvertragsklauseln setzen. Für den Datentransfer in die USA sowie in andere Drittländer kommt deshalb nun diesen Standard Contractual Clauses (SCC), als neuer Rechtsgrundlage eine gesteigerte Bedeutung zu. Sie enthalten Vorgaben und vertragliche Verpflichtungen, die die Datenverarbeitung in Drittstaaten absichern und auf ein Schutzniveau heben sollen, das dem in der EU in gewissen Umfang entspricht. Aber auch zu den SCCs hat sich der EuGH in seinem Urteil bereits geäußert. Ohne zusätzliche technische und organisatorische Maßnahmen sind sie in der Regel nicht ausreichend, um Daten auf dieser Basis in die USA zu übermitteln.

SCCs können so zwar zunächst weiter für Datenübertragungen genutzt werden, der bloße Vertragsschluss reicht hierfür aber noch nicht aus. In der Konsequenz müssen Unternehmen bei Datenübermittlungen in Drittländer letztlich für jeden Einzelfall prüfen, ob ein der DSGVO entsprechendes Schutzniveau im Drittland gewährleistet ist. Sollte das nicht der Fall sein, müssen sie zusätzliche Schutzmaßnahmen umsetzen und deren Einhaltung sicherstellen. Dass dies mit einem hohen Aufwand und damit auch mit erhöhten Kosten für Unternehmen einhergeht, steht außer Frage. Aber, und das darf man nicht aus den Augen verlieren, hier geht es um den Grundrechtsschutz der Bürgerinnen und Bürger in der EU.

Der Europäische Datenschutzausschuss (EDPB) hat im Juni 2021 neue Empfehlungen veröffentlicht, mit denen er den Unternehmen bei der „komplexen Aufgabe, Drittländer zu bewerten und geeignete zusätzliche Maßnahmen zu ermitteln“, helfen will. Diese Empfehlungen beschreiben eine Vorgehensweise, wie Datenexporteure – also Verantwortliche oder Auftragsverarbeiter – bei der Verarbeitung personenbezogener Daten prüfen können, ob etwaige Datenübermittlungen an Drittstaaten den Anforderungen der DSGVO genügen, wenn für die betreffenden Drittstaaten kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt. Wenn das nicht Fall ist, geben sie Hinweise, wie geeignete Maßnahmen ergriffen werden können.

Ein Anhang zu diesen Empfehlungen beschreibt Anwendungsfälle, bei denen die Aufsichtsbehörden Möglichkeiten sehen, durch zusätzliche technische Maßnahmen die Datenübermittlung so abzusichern, dass sie den Anforderungen des Datenschutzes nach Schrems II genügen. Außerdem werden zwei Konstellationen dargestellt, bei denen aus Sicht der Aufsichtsbehörden keine entsprechenden Maßnahmen möglich erscheinen. Dies bedeutet nun andererseits nicht, dass nicht auch in diesen Fällen ein Transfer datenschutzkonform abgesichert werden könnte – es wird aber wahrscheinlich durchaus eine extreme Herausforderung darstellen.

Zusammenfassend gilt also: Vor der Übermittlung von personenbezogenen Daten in einen Drittstaat muss der Datenexporteur bewerten, ob ein angemessenes Datenschutzniveau im Empfängerland gewährleistet werden kann. Und dies gilt nicht nur für das allgemeine Datenschutzniveau im Empfängerland, sondern ganz konkret für die zu übertragenden Daten. Auch Risiken durch die Speicherung der Daten und mögliche zumutbare Alternativen müssen geprüft werden. Verläuft diese Bewertung negativ, ist also das Schutzniveau nicht mit dem europäischen vergleichbar, muss der Datenexporteur vor dem Transfer zusätzliche Maßnahmen ergreifen, um den Schutz der Daten zu garantieren.

Zu den empfohlenen Maßnahmen gehören etwa Pseudonymisierung, eine wirksame Verschlüsselung oder die Wahl eines Empfängers, der durch das Recht des Ziellandes vor Zugriffen geschützt ist.

Bei Anbietern, die auf Daten im Klartext zugreifen müssen (z. B. bei Cloud Processing) und gegenüber denen öffentliche Stellen über das für eine demokratische Gesellschaft notwendige Maß hinaus Zugriffsbefugnisse haben, wird demnach meist keine datenschutzkonforme Übermittlung möglich sein.

An dieser Stelle sei noch einmal als Nebenbemerkung darauf hingewiesen, dass die hier dargestellte Problematik der Drittstaatenübermittlung und die Verantwortung des Verantwortlichen auf die Wahl geeigneter Auftragsverarbeiter keineswegs nur die USA betrifft, sondern jedes Land ohne gültigen Angemessenheitsbeschluss der EU-Kommission.

Der Titel meiner Keynote nimmt auch Bezug auf den 2018 in den USA erlassenen Cloud Act, auf den ich an dieser Stelle nur kurz eingehen will, um die Problematik solcher Datenübermittlungen plastischer werden zu lassen. Anbieter von elektronischen Kommunikations- oder Cloud-Diensten, die US-amerikanischem Recht unterliegen, können gemäß Cloud Act zur Herausgabe von Daten verpflichtet werden – und zwar unabhängig davon, wo diese Daten gespeichert sind. Sollte also ein US-Konzern in Besitz von Daten sein oder Kontrolle über diese haben, die bspw. ein Tochterunternehmen mit Sitz in Europa in der EU verarbeitet, dann unterliegen diese Daten einer potentiellen Pflicht zur Herausgabe. Das macht deutlich, dass auch europäische Anbieter, die unter den beschriebenen Umständen unter den Cloud Act fallen können, einer besonderen Prüfung zu unterziehen sind.

Selbstverständlich gibt es Interessen, die es rechtfertigen, dass staatliche Stellen im Rahmen ihrer Arbeit auch Kenntnis von personenbezogenen Daten erhalten, die von privaten Unternehmen und möglicherweise auch in anderen Ländern verarbeitet werden. Die Bekämpfung von internationalem Terrorismus oder organisierter Kriminalität sind Beispiele dafür. Entscheidend bleibt aber immer, unter welchen Voraussetzungen dies erfolgt, welche Schranken gegen ein uferloses Datenzugriffsregime bestehen, welche rechtsstaatlichen Verfahren hierfür vorgesehen, wie die Rechte der Betroffenen ausgestaltet sind und durchgesetzt werden können. Datenschutz als Grundrecht bedeutet eben auch, dass jeder Grundrechtsträger – jede Person im Geltungsbereich der DSGVO – die Möglichkeit haben muss, ihr Grundrecht gerichtlich durchzusetzen.

Die Datenschutz-Anforderungen mit Blick auf Drittlandtransfers sind damit weiter herausfordernd – gerade im Bereich von Cloudlösungen.

Also ja, es ist kompliziert. Aber eben dieses Beispiel zeigt doch, was wir damit schützen. Warum wir diesen Aufwand betreiben: Um die Privatsphäre zu sichern, um Grundpfeiler unserer demokratischen Wertvorstellungen nicht zu opfern, um wirtschaftlichen Erfolg, Fortschritt und Datenschutz in Einklang zu bringen und so unsere digitale Souveränität zu stärken.

III. Dunkle Wolken über der Wirtschaft?

Clouddienste sind das erste, was uns in den Sinn kommt, wenn wir über Schrems II reden, es gibt aber durchaus auch Auswirkungen auf Dienste, die man damit nicht direkt in Verbindung bringt, wie z. B. im Bereich der Infrastruktur.

Der Cloud-Markt ist breit gefächert und zu einem Milliardengeschäft geworden, von dem für die Wirtschaft mittlerweile viel abhängt. Dass sich durch die engen Pflöcke, die Schrems II gesetzt hat, hier besondere Zwänge für die wirtschaftlichen Akteure ergeben haben, das ist mir bewusst. Mit den erwähnten Empfehlungen des EDPB haben sich die Aufsichtsbehörden dazu verständigt und erste Schritte auf den Weg gebracht, um Datenexporteure bei der rechtmäßigen Übertragung von personenbezogenen Daten in Drittländer zu unterstützen. Bei der Erarbeitung dieser Empfehlungen wurden Zweifel und Kritik von Interessenvertretern berücksichtigt. Und das planen wir auch weiter zu tun. Die Sorgen der Wirtschaft ernst zu nehmen, Kritikpunkte aufzunehmen und die bestmögliche Lösung für alle Stakeholder zu entwickeln, das ist auch unser Anliegen. Und deshalb möchte ich Sie alle dazu auffordern, sich weiterhin rege in diese Diskussion einzubringen. Lassen Sie uns nicht nur auf die schwierigen Ausgangsbedingungen fokussieren. Lassen Sie uns stattdessen die Möglichkeiten begreifen, die uns die aktuelle Situation bringt, um diese auch als Interessenvertreter mitzugestalten. Wir sind offen für Anregungen aus der Wirtschaft.

Die Rahmenbedingungen für internationale Datentransfers werden jetzt neu geordnet – das kann eine große Chance sein.

IV. Ein Licht am Horizont? Wie geht es weiter?

Um nicht falsch verstanden zu werden: Es geht nicht darum, Drittlandübermittlungen zu vermeiden oder gar zu verbieten. Es müssen gute Lösungen für die damit einhergehenden Herausforderungen gefunden werden, gleichzeitig können und sollten aber auch europäische Alternativlösungen in Betracht gezogen werden. Dies erweist sich in der Praxis noch als schwierig, da es im Augenblick oft keine wirklichen Alternativen zu den marktgängigen amerikanischen Cloud-Providern gibt. Es wäre aber wünschenswert, dass Ansätze entwickelt werden, um Lock-in-Effekte bei außereuropäischen Anbietern zu vermeiden. Doch ein flächendeckender Einsatz von entsprechenden Lösungen zeichnet sich aktuell noch nicht ab.

Es ist essenziell, dass wir nicht nur innerhalb Europas, sondern auch darüber hinaus an einem einheitlichen Verständnis des Datenschutzes arbeiten. Die DSGVO ist das beste Beispiel dafür, dass unsere Bemühungen hier fruchten. Die Entwicklungen in Japan oder auch in Brasilien, wo wichtige neue Datenschutzgesetze verabschiedet wurden, die sich an der DSGVO orientieren, zeigen doch, dass es möglich ist weltweit guten Datenschutz umzusetzen, ohne dass Wirtschaftsbeziehungen darunter leiden.

Bei dieser Gelegenheit grüße ich ganz herzlich meine Kollegin Miriam Wimmer, Chefin der brasilianischen Datenschutzaufsichtsbehörde, die morgen über die spannenden Entwicklungen in Brasilien berichten wird. Auch in den USA wird inzwischen ein Privacy Act auf föderaler Ebene im Parlament diskutiert, genauso in Indien, Argentinien und Mexiko, alles mit Anlehnung an die DSGVO – es ist einiges in Bewegung.

V. Ein gemeinsamer Datenraum ist möglich

Das alles zeigt, dass Datenschutzstandards nicht nur auf einzelne Länder oder Staatengemeinschaften beschränkt bleiben sollten, sondern ein globales Anliegen sein müssen. Einerseits für die Grundregeln staatlichen Zugriffs, andererseits auch für die allgemeinen Datenschutzregelungen.

Ein breites gemeinsames Verständnis für den Schutz der Grundrechte und damit eben auch für den Datenschutz muss über die Grenzen Europas hinaus erreicht werden, damit wir Instrumente wie Cloudlösungen sinnvoll und sicher anwenden können. Das erfordert eine internationale Zusammenarbeit und kooperative Regulierungsansätze. Um einen gemeinsamen Datenraum auf der Grundlage geteilter Werte schaffen zu können, der den freien Datenverkehr auf einem hohen Schutzniveau vor staatlichem Zugriff ermöglicht und in dem dann auch noch verschiedenste Datenschutzregelungen für den privaten Sektor wirken können, müssen alle beteiligten Akteure einen Beitrag leisten.

Ein gemeinsamer Datenraum, der digitale Innovation, wirtschaftlichen Wohlstand und einen demokratischen Wertekontext fördert, wäre am Ende des Tages ein Gewinn für alle Stakeholder.

Und in der Tat sind wir als internationale Datenschutzaufsichtsbehörden in verschiedenen Formaten bereits sehr aktiv, um zu gemeinsamen Lösungen zu kommen. Erst Anfang September haben wir in Bonn im Kreise der Datenschutzbehörden der G7-Staaten auf meine Einladung hin intensiv über grenzüberschreitenden Datenschutz und Datentransfer diskutiert.

Eine derartige Entwicklung würde uns auch deshalb zu weltweit hohen Datenschutzstandards für private Geschäftsmodelle führen, weil global agierende Unternehmen von vereinheitlichten Regelungen immens profitieren. Der gemeinsame Datenraum würde einen Markt schaffen, der sich mit datenschutzfreundlichen Lösungen von anderen absetzt und der hohe Datenschutzstandards zu einem zentralen Qualitätsmerkmal werden lässt.

Wichtig zu sagen ist, dass es sich dabei nicht um eine exklusive Gruppe handeln soll, sondern um eine Einladung an Staaten aus allen Teilen der Welt. Und hier komme ich gerne noch einmal auf das Beispiel Brasiliens zurück. Zeigt nicht gerade die dortige Entwicklung, dass dieser Gedanke eines gemeinsamen Datenraums keine Utopie sein muss? Dass wir gemeinsame Grundlagen für vertrauensvolle Datentransfers bei

Cloudlösungen schaffen und damit auch zu wirtschaftlicher Prosperität beitragen können. Bei allem Aufwand – eine Win-Win Situation für die beteiligten Akteure.

VI. Cloud und Datenschutz

Der EuGH hat in seinem Urteil sehr deutlich gemacht, dass die Beurteilung einer datenschutzkonformen Übermittlung an Drittländer von den konkreten Umständen des Einzelfalls abhängig ist. Wie bereits zu Beginn angekündigt: Es gibt keine Patentlösung, die ich Ihnen heute hier präsentieren könnte

Wir – und damit meine ich tatsächlich uns alle – Aufsichtsbehörden und Politik, Wirtschaft und Zivilgesellschaft müssen es als unsere gemeinsame Aufgabe verstehen, dass wir in einer global vernetzen Welt einen freien, sicheren und vertrauenswürdigen Datenverkehr gewährleisten können. Klare Strukturen, die es uns erlauben die Privatsphäre und demokratische Wertvorstellungen bestmöglich zu schützen und dabei wirtschaftlichen Erfolg, digitalen Fortschritt und Datenschutz miteinander zu verbinden und die digitale Souveränität zu stärken. Auch wenn es weh tut, auch wenn es keine einfachen Lösungen gibt.

Schaffen wir das nicht, dann gefährden wir das, worauf wir so dringend angewiesen sind: Vertrauen.

Wenn Vertrauen in die digitale Transformation, in digitale Dienste und Geschäftsmodelle verloren geht, dann kostet uns das am Ende sehr viel mehr als die Anstrengungen und Mühen, die wir jetzt aufbringen müssen, um diese Gestaltungsaufgabe auszufüllen. Dann sinkt der Innovationsdruck, Verbraucherinnen und Verbraucher haben weniger Auswahlmöglichkeiten, Unternehmen verlieren im internationalen Wettbewerb an Boden.

Und genau deshalb arbeiten wir mit so vielen Akteuren über die europäischen Grenzen hinaus so intensiv an einem hohen Datenschutzniveau. Die erforderlichen Rechtsgrundlagen zu schaffen, das ist vor allem Aufgabe der Politik. Alles was darüber hinaus geht, etwa Alternativen zu marktgängigen Anbietern und Anwendungen zu schaffen, technische Lösungen und vielleicht in mancherlei Hinsicht auch einmal unkonventionelle Ideen zu denken, daran können wir alle mitwirken. Datenschutz ist kein Selbstzweck, sondern Grundrechts-schutz. Datenschutz ist kein Verhinderer, sondern, wenn wir ihn richtig gestalten, ein Wettbewerbsvorteil. Lassen Sie uns daran gemeinsam arbeiten.

Ich danke Ihnen für Ihre Aufmerksamkeit.