„Und nun?“? ist derzeit eine vielfach aufgeworfene Frage der Datenschützer in ganz Europa nach dem Ergehen des EuGH Urteils in der Rechtssache C-311/18 (Schrems II) vom 16.07.2020. Hier finden Sie das Urteil: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=3294920.

Hierauf versucht der folgende Artikel eine Antwort zu geben.

Aber beginnen wir am Anfang.

Es war einmal ein datenschutzbegeisterter Mann namens Schrems. Dieser setzte sich sehr für die Durchsetzung des Datenschutzes ein. Vor allem eine Übermittlung personenbezogener Daten in die USA war ihm ein Dorn im Auge. Die Übermittlungen erfolgten zuerst auf der Rechtsgrundlage des Safe-Habour-Abkommens und später auf dem EU-US Privacy Shield Abkommen. Als erstes nahm er sich das Safe-Habour-Abkommen vor und brachte es zu Fall. Nun nahm er sich das EU-US Privacy Shield Abkommen vor und brachte auch diese zu Fall. Beide Abkommen sollten die notwendige Rechtsgrundlage für die Übermittlung von personenbezogenen Daten in die USA sein. Folglich sind allen Datenübermittlungen von personenbezogenen Daten in die USA, die als Rechtsgrundlage das EU-US Privacy Shield Abkommen benennen, die Rechtsgrundlage entzogen worden und benötigen nun eine neue Rechtsgrundlage.

Aber gehen wir noch einen Schritt zurück. Wie konnte es dazu kommen? Dafür muss die Frage beantwortet werden, welche Voraussetzungen benötigt werden, um personenbezogene Daten zu übermitteln. Die Voraussetzungen sind in einem zweistufigen Prüfverfahren zusammengefasst. Als erstes wird ein Erlaubnistatbestand in Form der Einwilligung oder einer Rechtsgrundlage benötigt. Zusätzlich, und hier setzt nun das Urteil an, muss beim Datenempfänger ein angemessenes Datenschutzniveau sichergestellt sein. Herr Schrems hat in seiner Klage behauptet, das Datenschutzniveau in den USA, würde nicht den Vorgaben der DSGVO entsprechen und daran ändere auch das EU-US Privacy Shield Abkommen (weitere Informationen unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_de abrufbar) nichts. Im Ergebnis stimmte der EuGH Herrn Schrems zu. Aber nicht nur das. Der EuGH legte zusätzlich fest, welche Voraussetzungen gegeben sein müssen, damit ein angemessenes Datenschutzniveau angenommen werden kann und infolgedessen personenbezogene Daten in ein Drittland übermittelt werden dürfen.

Schon Erwägungsgrund 104 der DSGVO gibt einen Hinweis, wie ein angemessenes Datenschutzniveau zu gewährleisten ist. Denn hierin lautet es:

Das Drittland sollte insbesondere eine wirksame unabhängige Überwachung des Datenschutzes gewährleisten und Mechanismen für eine Zusammenarbeit mit den Datenschutzbehörden der Mitgliedstaaten vorsehen, und den betroffenen Personen sollten wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe eingeräumt werden.

An diesen Voraussetzungen scheitert das EU-US Privacy Shield Abkommen. Denn der EuGH stellt fest, dass keine unabhängige Überwachung des Datenschutzes gegeben ist. Die eingerichtete Stelle in den USA unterliegt der Weisung des Außenministeriums. Auch ein Rechtsweg kann vom Betroffenen nicht im gleichen Maß beschritten werden.

Und einen weiteren Punkt hat der EuGH angesprochen: Es darf keine anlasslose Abschöpfung der persönlichen Daten staatlicherseits geben. Aber gerade dies ist durch den Section 702 des Foreign Intelligence Surveillance Act (FISA) und Executive Order 12333 möglich. Der Geheimdienst darf anlasslos Daten abgreifen und muss hierüber noch nicht einmal das betroffene Unternehmen informieren und schon gar nicht den Betroffenen.

Folglich fällt das EU-US Privacy Shield als Rechtsgrundlage zur Übermittlung von Daten aus. Dabei muss der Kommission die Rechtslage bekannt gewesen sein. Das EU-US-Privacy-Shield kann daher lediglich als Feigenblatt fungiert haben.

Aber was nun?

Vielfach ist zu lesen, dass einfach EU-Standartvertragsklauseln als neuer Rechtsgrund mit den jeweiligen Unternehmen abzuschließen sind. Das würde ausreichend sein. Oder aber diese EU-Standartvertragsklauseln sollten um einige Passagen erweitert werden (vgl. Orientierungspapier LfDI BW https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/LfDI-BW-Orientierungshilfe-zu-Schrems-II.pdf). Doch hilft dies tatsächlich weiter?

Eine Antwort finden wir in den Grundsätzen der Juristerei. Privatwirtschaftliche Verträge, und die Standardvertragsklauseln sind solche, binden immer nur den Vertragspartner. Und damit nicht die Executive der USA. Durch einen solchen Vertrag kann weder ein der DSGVO gleichwertiger Rechtsweg noch eine unabhängige Datenschutzbehörde geschaffen noch ein

Verbot des staatlichen Zugriffs auf die übermittelten Daten durchgesetzt werden. Vertragspartner hierfür müsste die Exekutive der USA sein. Ist sie aber nicht.

Daher ist es zwar nicht verkehrt die Standardvertragsklauseln abzuschließen, aber auf der sicheren Seite ist man damit keineswegs. Auch, wenn dies vielfach suggeriert wird.

Immer wieder kommt in diesem Zusammenhang die Frage auf, ob eine Änderung der Standardvertragsklauseln überhaupt zulässig ist, denn eigentlich ist dies nicht erlaubt. In dem vorliegenden Fall jedoch, spricht m.E. nichts dagegen. Denn durch die Abänderung der Klauseln wird ein höheres Schutzniveau vereinbart, welches eher den Gedanken der DSGVO entspricht.

Der EuGH stellt in seinem Urteil deutlich heraus, dass selbst wenn Standardvertragsklauseln gegeben sind, der Verantwortliche immer im Einzelfall zu prüfen hat, ob das Recht des Drittlandes ein angemessenes Schutzniveau bietet, er entwickelt demnach eine Prüfpflicht, um ggf. entsprechende zusätzliche Maßnahmen zu treffen bzw. mit dem Datenimporteur vereinbaren, falls das Schutzniveau geringer ausfällt. Folglich reicht lediglich der Verweis auf eine Vereinbarung in Form der Standardvertragsklauseln nicht aus.

Dieses Minus an Schutzniveau könnte durch zusätzliche Garantien ausgeglichen werden. Zumeist stellen diese die sogenannten technisch organisatorischen Maßnahmen dar. Diese müssten jedoch zum einen den Zugriff durch die US-amerikanischen Geheimdienste effektiv verhindern und so die Rechte der Betroffenen schützen. Dies wäre ggf. denkbar, falls eine Verschlüsselung vorliegt, die nur der Datenexporteur entschlüsseln kann. An dieser Stelle sei darauf verwiesen, dass dies immer unter Mitarbeit des Vertragspartners zu erfolgen hat, der wiederum ggf. staatlicherseits verpflichtet ist Daten weiterzugeben und somit diese Möglichkeit ausscheidet. Eine weitere Möglichkeit wäre die Übermittlung lediglich anonymisierter oder pseudonymisierter Daten, bei denen die Zuordnung nur durch den Exporteur erfolgen kann. Weiterhin müsste auch eine unabhängige Aufsicht gegeben sein und die Bestreitung des Rechtsweges für betroffene Personen. Beide letztgenannten Voraussetzungen können jedoch, wie oben bereits ausgeführt, mit dem Vertragspartner nicht rechtskräftig vereinbart werden.

Wer den Text bis hier hin aufmerksam gelesen hat, wird feststellen, dass der EuGH die Grundsätze der DSGVO in seinem Urteil deutlich herausgearbeitet hat. Und gerade, weil es sich um Grundsätzliches handelt, hat das Urteil eine viel breitere Wirkung als auf den ersten Blick angenommen. Denn die Grundsätze finden bei allen Datenübermittlungen in ein Drittland Anwendung. Aus diesem Grunde sollten nun nicht nur die Datenübermittlungen in

die USA einer Überprüfung unterzogen werden, sondern alle Datenübermittlungen, die in ein Drittland erfolgen.

Wie geht es nun weiter?

Der EU-Datenschutzausschuss arbeitet derzeit an Vorschlägen für konkrete Garantiemaßnahmen. Diese sollen bis Ende des Jahres vorliegen. Die deutschen Datenschutzaufsichtsbehörden arbeiten momentan auch mit Nachdruck an einer einheitlichen Meinungsfindung und an Lösungen. Die LDI NRW arbeitet in diesen Arbeitsgruppen mit. Eine harmonisierte Veröffentlichung von Auffassungen ist ab Mitte bis Ende November 2020 zu erwarten. Doch, wie zuvor ausgeführt, können diese Garantien die USA nicht binden. Und Sie kennen doch das Sprichwort:

„Alle guten Dinge sind drei!“ Sollte Herr Schrems davon überzeugt sein, dass die Garantien kein gleichwertiges Schutzniveau bieten, wird er wieder vor den EuGH ziehen und wieder wird das Recht auf seiner Seite stehen. Daher werden auch die Garantien lediglich einen Aufschub geben und sich daraufhin wahrscheinlich viele Unternehmen in falscher Sicherheit wiegen.

Ein alleiniges Abwarten kann an dieser Stelle nicht empfohlen werden.

Daher sollten folgende Maßnahmen getroffen werden:

1. Überblick schaffen, bei welchen Verarbeitungstätigkeiten ein Drittlands Bezug gegeben ist (falls kein gutes Verzeichnis von Verarbeitungstätigkeiten vorliegt: unter www.kcd-nrw.de können Sie eines herunterladen). Bitte beachten Sie hier, dass nicht nur ein Datenexport unter das Urteil fällt, sondern auch ein Zugriff von privaten oder öffentlichen Stellen aus dem Drittland.
2. Analyse des Schutzniveaus anhand der getroffenen vertraglichen und vor allem technisch-organisatorischen Maßnahmen, sowie der Rechtslage im Drittland. Anschließendes kategorisieren der Datenexporte in „rechtskonform“ und „nicht rechtskonform“. Liegen nur rechtskonforme Datenexporte vor, so sind Sie an dieser Stelle auf der sicheren Seite und können das Weiterlesen stoppen. Ansonsten geht es mit den folgenden Punkten weiter:
3. Prüfen, ob ein Angemessenheitsbeschluss gem. Art. 45 DSGVO gegeben ist (einsehbar unter: https://ec.europa.eu/info/law/lawtopic/data-protection/international-dimension-data-protection/adequacydecisions_en).

4. Prüfen, ob Standardvertragsklauseln gem. Art. 46 DSGVO gegeben sind (einsehbar unter: https://eurlex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087). Aber Achtung! Auch, wenn ein Angemessenheitsbeschluss vorliegt, muss ein gleichwertiges Schutzniveau gegeben sein! Im Zweifel lieber noch einmal nachprüfen und zusätzliche Garantien (s.o. v.a. technisch organisatorische Maßnahmen wie Verschlüsselung, Anonymisierung, Pseudonymisierung, etc.) vereinbaren und die Standardvertragsklauseln um die Passagen des Orientierungspapiers des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg erweitern (abzurufen unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/Orientierungshilfe-Was-jetzt-in-Sachen-internationaler-Datentransfer.pdf).
5. Kontakt zu Vertragspartnern des Drittlandes aufnehmen und über Lösungsmöglichkeiten sprechen.
6. Nach Möglichkeit eine Vereinbarung treffen, dass die Daten innerhalb des Geltungsbereichs der DSGVO gehostet werden und keine Datenübertragung in die USA oder ein Drittland mit geringerem Schutzniveau vorgenommen wird.
7. Kommen Sie zu dem Schluss, dass kein ausreichendes Schutzniveau gewährleistet werden kann, müssen Sie den Datenexport einstellen. Wollen Sie dies nicht, so müssen Sie dies Ihrer Aufsichtsbehörde melden.
8. Prüfen, ob zumutbare Alternativangebote ohne Datenexport in ein problematisches Drittland existieren. Dies vor dem Hintergrund einer Bewertung auf einer kurz- und mittel- sowie langfristigen Betrachtungsweise. Denn es ist zu erwarten, dass die Aufsichtsbehörden im Rahmen ihrer Kontrollaktivitäten beurteilen werden, inwieweit ein Wechsel eines Vertragspartners oder Dienstleisters und eine Verlagerung der Datenverarbeitung in die EU für den Datenexporteur zumutbar ist, insbesondere wenn keine zusätzlichen Garantien für Betroffene geschaffen oder vereinbart werden können.
9. Empfehlungen und Handlungen der Datenschutzbehörden beobachten.

Diese Maßnahmen sollten dokumentiert werden, um sie der Aufsichtsbehörde bei einer Prüfung vorlegen zu können.

Dies alles ist mit einem enormen Aufwand verbunden und stellt Unternehmen vor große Herausforderungen. Der Datenschützer im Unternehmen wird sich immer wieder die Frage gefallen lassen müssen, was denn passiert, wenn nichts unternommen wird, sondern einfach

alles beim Altbewährten gelassen wird. Es kommt damit die Frage nach den Risiken auf. Diese sind kurz aufzählbar:

1. Verhängung von Bußgeldern seitens der Aufsichtsbehörde.
2. Schadensersatzzahlungen an die betroffene Person.
3. Untersagung der Übermittlung personenbezogener Daten und damit der Nutzung des entsprechenden IT-Systems bzw. Programmes durch die Aufsichtsbehörde.

Letztendlich wäre es sinnvoll alle Daten im Geltungsbereich der DSGVO zu behalten und keinen Datenexport in ein Drittland zuzulassen. Da der Markt für Programme jedoch unübersichtlich ist, würde ich mich freuen, wenn Sie mir europäische Programme nennen könnten, die keinen Datenexport in ein Drittland zulassen, damit diese Ihren Kollegen in dem Newsletter vorgestellt werden können.

Bitte senden Sie mir Ihre Vorschläge und gerne auch die Erfahrungen an: teheesen@vrr.de

Und was lernen wir aus der Geschicht?

Nichts Genaues weiß man nicht.

Oder:

Ein Feigenblatt ist nur ein Feigenblatt.