WilhelmGilliéron
AVOCATS

Auteur: Wilhelm Gilliéron Avocats | Le : 20 Juli 2020

Schrems II: Ist die Übermittlung von Personendaten in die USA noch erlaubt?

In einer lang erwarteten Entscheidung (C-311/18), die am 16. Juli 2020 verkündet und bereits weithin bekannt gemacht wurde, musste der Gerichtshof der Europäischen Union über die Gültigkeit der Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter mit Sitz in Drittländern entscheiden (Beschluss 2010/87, in der durch den Beschluss 2016/2297 geänderten Fassung, allgemein als „Modellklauseln“ bezeichnet) bzw. über den EU-US-Datenschutzschild (Beschluss 2016/1250, allgemein als „*Privacy Shield*“ bezeichnet).

Während die Modellklauseln knapp gerettet wurden, läutet dieses Urteil jedoch die Totenglocke für „*Privacy Shield*„.

I. Erinnerung an die Grundsätze, die der Übermittlung von Daten an einen Drittstaat zugrunde liegen

Einleitend sei daran erinnert, dass die Übermittlung von Daten aus einem EU-Mitgliedstaat in ein Drittland voraussetzt, dass entweder das Empfängerland von der Kommission als Land anerkannt worden ist, das ein als angemessenes Schutzniveau bietet (Artikel 45 DSGVO; eine Liste dieser Länder, zu denen die Schweiz derzeit gehört, finden Sie hier), oder dass der für die Verarbeitung Verantwortliche angemessene Garantien vorgesehen hat (Artikel 46 DSGVO).

Zusätzlich zu den Modellklauseln, die ausdrücklich als geeignete Garantieform für die Übertragung in die Vereinigten Staaten akzeptiert wurden (Art. 46 Abs. 2 lit. c) DSGVO), war bisher anerkannt worden, dass die Vereinigten Staaten ein angemessenes Schutzniveau für Unternehmen bieten, die sich entschlossen hatten, sich freiwillig dem „*Privacy Shield*“ zu unterwerfen (für eine Liste solcher Unternehmen siehe hier).

II. Erinnerung an die Fakten, die zu dem Streit geführt haben

Im Wesentlichen argumentierte Maximillian Schrems, ein österreichischer Staatsangehöriger, dass die Übermittlung seiner persönlichen Daten durch Facebook Irland an Facebook Inc. in den Vereinigten Staaten nicht die erforderlichen Versicherungsgarantien biete, da die US-amerikanische Überwachungsgesetzgebung gegen die Artikel 7 (Recht auf Achtung des Privat- und Familienlebens), 8 (Schutz personenbezogener Daten) und 47 (Recht auf einen wirksamen Rechtsbehelf und auf Zugang zu einem unparteiischen Gericht) der Charta der Grundrechte der Europäischen Union verstoße.

Dabei geht es vor allem um zwei Akte: erstens um Art. 702 FISA (*Foreign Intelligence Surveillance Act*), nach dem der Generalstaatsanwalt und der Direktor des Nationalen Nachrichtendienstes gemeinsam die Überwachung von Nicht-US-Bürgern außerhalb der Vereinigten Staaten genehmigen können, um „Informationen des Auslandsgeheimdienstes“ zu erhalten; Diese Bestimmung bildet die Grundlage für die Überwachungsprogramme PRISM (die Internet-Diensteanbieter anweist, der NSA und in gewissem Umfang auch dem FBI und der CIA alle von einer bestimmten Person gesendeten und empfangenen Mitteilungen zur Verfügung zu stellen) und UPSTREAM (die Telekommunikationsunternehmen, die das Internet-„Backbone“ betreiben, anweist, der NSA das Kopieren und Filtern von Internet-Verkehrsströmen zu gestatten, um Mitteilungen zu sammeln, die von den jeweiligen nicht-amerikanischen nationalen Behörden gesendet oder empfangen wurden). Zweitens die E.O. 12333, die es der NSA erlaubt, durch Zugang zu auf dem Atlantikboden verlegten Unterseekabeln auf Daten zuzugreifen, die sich „auf der Durchreise“ in die Vereinigten Staaten befinden, und ihre Daten zu sammeln und zu speichern, bevor sie in den Vereinigten Staaten ankommen und der FISA vorgelegt werden.

III. Gültigkeit von Modellklauseln

Zunächst hatte der Gerichtshof über die Frage zu entscheiden, ob die aus Sicherheitsgründen durchgeführte Datenverarbeitung nicht vom Anwendungsbereich der DSGVO ausgeschlossen ist, insbesondere im Lichte von Art. 2 Absatz 2 Buchstabe a), der bei seiner Auslegung die Anwendung der DSGVO ausschließt, wenn die Datenverarbeitung von Behörden aus Gründen der nationalen Sicherheit durchgeführt wird. Das Gericht verneint dies, da es hier nicht um die mögliche Verarbeitung durch die US-Behörden geht, sondern um den Transfer zwischen zwei Wirtschaftseinheiten (nämlich Facebook Irland einerseits und Facebook Inc. andererseits). Die Möglichkeit,

dass personenbezogene Daten, die zwischen zwei Wirtschaftsteilnehmern zu kommerziellen Zwecken übermittelt werden, während oder als Folge einer solchen Übermittlung für Zwecke der öffentlichen Sicherheit verarbeitet werden, hat jedoch nicht zur Folge, dass diese Übermittlung aus dem Anwendungsbereich des DSGVO herausfällt.

Nachdem diese Vorfrage geklärt ist, wendet sich der Gerichtshof der Frage zu, ob die Modellklauseln als „angemessenes Sicherungsrecht“ angesehen werden können, das eine Übertragung in die Vereinigten Staaten im Sinne von Art. 46 DDR erlaubt. Im Wesentlichen lautet ihre Argumentation wie folgt:

- Die Frage, ob es „geeignete Garantien“ sowie „durchsetzbare Rechte und wirksame Rechtsbehelfe“ gemäß Art. 46.1 DSGVO gibt, muss vor dem Hintergrund der durch die Charta garantierten Grundrechte betrachtet werden, die der grundlegende Maßstab für die Beurteilung der Angemessenheit eines Landes gemäß Art. 45 DSGVO ist.
- In diesem Rahmen muss der für die Verarbeitung Verantwortliche, wenn der Inhalt der Modelllauseln „geeignete Garantien“ darstellen kann, dennoch sicherstellen, dass die Möglichkeiten des Zugangs zu den Daten durch die Behörden des Empfängerlandes und die den betroffenen Personen zur Verfügung gestellten Mittel als annehmbar angesehen werden können, eine Frage, die im Lichte der in Art. 45 Abs. 2 DSGVO festgelegten Kriterien geprüft wird.
- Die Tatsache, dass die Kommission Modellklauseln im Sinne von Art. 46 Abs. 2 lit. c DSGVO angenommen hat, bedeutet nicht, dass die Prüfung dieser Klauseln durch die Aufsichtsbehörde und die Möglichkeit dieser Behörde, gegebenenfalls die in 58 Abs. 2 lit. f und j DSGVO vorgesehenen Maßnahmen zu ergreifen, nicht anwendbar sind. Allerdings muss dann unterschieden werden, ob der Empfängerland Gegenstand einer Angemessenheitsentscheidung im Sinne von Art. 45 Abs. 1 DSGVO war oder nicht:
- Ist das Empfängerland als ein Land anerkannt, das ein angemessenes Schutzniveau im Sinne von Art. 45 Abs. 1 DSGVO bietet (ein Fall, in dem ein Rückgriff auf die Modellklauseln nur schwer nachvollziehbar ist), so darf eine Aufsichtsbehörde von Amts wegen keine Massnahmen ergreifen, die einer solchen Angemessenheitsentscheidung zuwiderlaufen; eine solche Entscheidung hindert eine Person, deren Daten übermittelt wurden, jedoch nicht daran, bei der zuständigen nationalen Aufsichtsbehörde Beschwerde wegen Verletzung ihrer Grundrechte zu erheben, wie dies 77 DSGVO erlaubt.So muss die Aufsichtsbehörde, wenn sie von einer Einzelperson angerufen wird, in der Lage sein, selbständig zu prüfen, ob die durchgeführte Übertragung den in der DSGVO festgelegten Anforderungen entspricht, und gegebenenfalls bei den nationalen Gerichten eine Vorabentscheidungsklage zu erheben, damit diese gegebenenfalls den Gerichtshof anrufen, um die Gültigkeit der Übertragung zu prüfen. Erst wenn die Entscheidung vom Gericht für ungültig erklärt worden ist, kann die Aufsichtsbehörde die Datenübermittlung in das betreffende Land gemäss Art. 58 der DSGVO aussetzen oder verbieten.
- Wenn das Empfängerland nicht von einer solchen Angemessenheitsfeststellung profitiert, fällt die Antwort jedoch anders aus. Der Gerichtshof weist darauf hin, dass Modellklauseln sicherlich nur für die Parteien bindend sind, unter Ausschluss der Behörden des Bestimmungslandes, die offensichtlich nicht Vertragspartei sind. Die Tatsache, dass die Behörden nicht gebunden sind, bedeutet jedoch nicht, dass diese Klauseln ungültig sind. Solange der Inhalt dieser Klauseln jedoch Standard ist und als solcher nicht notwendigerweise die Gesetzgebung des Empfängerlandes, insbesondere hinsichtlich seiner Eingriffsmöglichkeiten, berücksichtigt, obliegt es dem für die Verarbeitung Verantwortlichen, eine Analyse der geltenden Vorschriften durchzuführen, um diese Modellklauseln gegebenenfalls in dem einen oder anderen Punkt zu ergänzen.

Mit anderen Worten, die Aufnahme einer Modellklausel reicht nicht aus, um sicherzustellen, dass der Transfer über angemessene Garantien verfügt. Die Gesetzgebung des Empfängerlandes muss auch wirksame Mittel vorsehen, damit sich Einzelpersonen über eine mögliche Verletzung ihrer Rechte nach Art. 47 der Charta beschweren können. Ist dies nicht der Fall, dann muss der Rückgriff auf die Modellklauseln ohne jegliche Ergänzung als unzureichend angesehen werden. In einem solchen Fall kann die Aufsichtsbehörde dann auf der Grundlage von Art. 58 der oben erwähnten DSGVO direkt eingreifen, um die Überstellung auszusetzen oder zu untersagen.

Art. 4 lit. a der Modellklausel verpflichtet der Verantwortliche nämlich dazu, sicherzustellen, dass die Gesetzgebung des Drittlandes es dem Auftragsverarbeiter erlaubt, den in der Modellklausel enthaltenen Verpflichtungen nachzukommen. Allerdings ist Art. 5 lit. a der Modellklausel in diesem Zusammenhang eine willkommene Hilfe für den für den Verantwortlichen, da der Auftragsverarbeiter ihn so schnell wie möglich über seine mögliche Unfähigkeit, seinen in der genannten Klausel enthaltenen Verpflichtungen nachzukommen, informieren muss, während Art. 5 lit. b diese Verpflichtung noch verstärkt, indem er vorsieht, dass der Auftragsverarbeiter auch bestätigen muss, dass er keinen Grund zu der Annahme hat, dass das anwendbare Recht ihn an der Erfüllung dieser Verpflichtungen hindert.

Ist der Auftragsverarbeiter hingegen nicht in der Lage, seinen Verpflichtungen nachzukommen, so ist der Gerichtshof der Auffassung, dass Art. 4 lit. a der Modellklausel den Verantwortlichen dann verpflichtet, jede Übermittlung auszusetzen oder zu untersagen, wobei präzisiert wird, dass Art. 12 zusätzlich verlangt, dass bereits übermittelte Daten zurückgegeben oder vernichtet werden. Im Falle einer Gesetzesänderung, über die der Auftragsverarbeiter den Verantwortlichen zu informieren hat, kann der Verantwortliche beschliessen, die Verarbeitung fortzusetzen, muss dann aber die Aufsichtsbehörde gemäss Art. 4 lit. g der Modellklausel informieren. Auch in diesem Fall steht es der Aufsichtsbehörde frei, die Verarbeitung gemäß Art. 58 DSGVO auszusetzen oder zu verbieten.

Im Hinblick auf das durch die Anwendung der Art, 4 und 5 der Modellklausel geschaffene System ist der Gerichtshof der Ansicht, dass die Klausel wirksame Mittel vorsieht, die den Anforderungen der Art. 7, 8 und 47 der Charta entsprechen. Damit bestätigt das Gericht die prinzipielle Gültigkeit der Modellklauseln.

IV. Mangelnde Angemessenheit des Datenschutzschildes

Während die Kombination von Art. 4 und 5 der Modellklausel ihre Gültigkeit behält, ist ein solcher Mechanismus im *Privacy Shield* nicht vorgesehen. Nach Ansicht des Gerichts bietet der *Privacy Shield* in zweierlei Hinsicht keine geeignete Garantien:

- Punkt 1.5 des Anhangs II stellt ausdrücklich fest, dass die Einhaltung der Grundsätze unter anderem durch „Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses und der Strafverfolgung“ eingeschränkt werden kann. Dieser Vorrang der staatlichen Einmischung vor den Grundrechten wird nicht durch Einschränkungen ausgeglichen, die in den Überwachungsprogrammen PRISM und UPSTREAM auf der Grundlage von FISA-Artikel 702 und E.O. 12333 enthalten sind. Damit verstößt das US-amerikanische Recht gegen die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit und im weiteren Sinne gegen die Art. 7, 8 und 52 der Charta, aus denen sich ergibt, dass jeder Eingriff in die Grundrechte einer Definition des Umfangs der Einschränkung der Ausübung des betreffenden Rechts unterliegen muss, klare und präzise Regeln für den Anwendungsbereich und die Anwendung der betreffenden Maßnahme enthalten und Mindestanforderungen auferlegen muss.
- Die Einsetzung eines Ombudsmannes, wie sie in Anhang III vorgesehen ist, kann nicht als wirksames Mittel der gerichtlichen Überprüfung im Sinne von Art. 47 der Charta angesehen werden, da der Ombudsmann direkt dem Außenminister untersteht und integraler Bestandteil des Außenministeriums der Vereinigten Staaten ist, ohne dass ein Rechtsbehelf bei einer Stelle eingelegt werden kann, die vergleichbare Garantien wie die in Art. 47 der Charta vorgesehenen bietet.

In Anbetracht der vorstehenden Ausführungen erklärt das Gericht den Beschluss 2016/1250 für ungültig.

V. Praktische Auswirkungen

Was ist über das Ergebnis dieses Urteils zu denken?

- Zunächst ist daran zu erinnern, dass Unternehmen, die dem *Privacy Shield* beigetreten sind, trotz der Ungültigkeitserklärung des Beschlusses 2016/1250 weiterhin dem *Privacy Shield* unterliegen und als solche ihren Verpflichtungen aus dem Beschluss weiterhin nachkommen müssen. Es ist jedoch zweifelhaft, ob es im Interesse dieser Unternehmen liegt, sich weiterhin dieser Regelung zu unterwerfen, da das Hauptziel dieses Beitritts nun irrelevant ist. Es ist daher wahrscheinlich, dass sie es vorziehen werden, einen Ausstiegsprozess zu beginnen. Die Zeit wird es zeigen.
- Zweitens beruht das ergangene Urteil im Wesentlichen auf einer Prüfung der Vereinbarkeit der angefochtenen Entscheidungen mit der Charta der Grundrechte der Europäischen Union, die auf die Schweiz nicht anwendbar ist. Es wäre jedoch naiv zu schliessen, dass das Urteil in der Schweiz keine Auswirkungen haben wird. Obwohl sich der Bundesbeauftragte noch nicht formell zu den Auswirkungen dieses Urteils auf die Gültigkeit des schweizerisch-amerikanischen *Privacy Shield* geäussert hat, ist es schwer vorstellbar, dass er in Bezug auf das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (besser bekannt als Übereinkommen 108) eine andere Position einnehmen würde. Schweizer Unternehmen, deren Aktivitäten eine Verarbeitung in den Vereinigten Staaten beinhalten, werden daher ein großes Interesse daran haben, die Situation in gleicher Weise zu betrachten wie jedes Unternehmen mit Sitz in der Europäischen Union.
- In dieser Hinsicht sind die folgenden Analysephasen zu beachten:
    1. Eine erste Reihe von Unternehmen, in der Regel bereits große Unternehmen, waren bereits dabei, ihre Einhaltung des *Privacy Shield* zu verdoppeln, als die Modellklauseln abgeschlossen wurden. Für diese Unternehmen scheint die Dringlichkeit geringer zu sein.
    2. Eine zweite Gruppe hatte, nachdem sie die mögliche Ungültigkeitserklärung des *Privacy Shield* vorweggenommen hatte, ausdrücklich vorgesehen, dass die Parteien in diesem Fall auf eine Modellklausel zurückgreifen würden. Für diese Unternehmen geht es nun darum, miteinander in Kontakt zu treten und eine solche Klausel zu unterzeichnen.
    3. Eine dritte Gruppe, die bereits Zweifel an der Gültigkeit des *Privacy Shield* hegte, hatte von Anfang an beschlossen, nur die Modellklauseln zu verwenden.
    4. Es reicht aber leider nicht mehr aus, von einer bestehenden oder künftigen Modellklausel zu profitieren. Jeder Verantwortliche muss mit Unterstützung des Auftragsverarbeiter dafür sorgen, dass die bestehenden Rechtsvorschriften es dem Auftragsverarbeiter ermöglichen, seinen Verpflichtungen nachzukommen, und den betroffenen Personen wirksame Mittel an die Hand geben, um sich über mögliche Verletzungen ihrer Grundrechte zu beschweren.

Was die Überstellung in die Vereinigten Staaten betrifft, so ist schwer vorstellbar, wie der Gesetzgeber im Lichte von Art. 47 der Charta wirksame Mittel vorsehen könnte, wenn der für die Verarbeitung Verantwortliche eine Modellklausel verwendet, während diese Bestimmung im Lichte des *Privacy Shield* verletzt würde. Solange die Daten nicht anonymisiert sind, dürfte der Datentransfer in die Vereinigten Staaten daher den Marktteilnehmern von nun an schwer fallen, es sei denn, sie sind bereit, das daraus resultierende Risiko zu akzeptieren. Daher wird hier eine sorgfältige Analyse erforderlich sein.

Dieser Ansatz gilt jedoch nicht nur für die Vereinigten Staaten, sondern für alle Länder, die kein angemessenes Schutzniveau bieten, d.h. für eine sehr große Mehrheit der Staaten. Der für die Datenverarbeitung Verantwortliche muss also die Risiken abschätzen, indem er sich insbesondere über : (i) den Umfang der Verarbeitung, (ii) die Art und Weise, in der die Daten verarbeitet werden, (iii) die Befugnisse der Behörden, die wahrscheinlich auf die Daten zugreifen wollen, und (iv) die Möglichkeit, sich einem solchen Ersuchen zu widersetzen (falls erforderlich vor Gericht).

Sollte diese Risikobeurteilung zu der Schlussfolgerung führen, dass die betreffenden Rechtsvorschriften keine ausreichenden Garantien bieten, sollte sich der für die Verarbeitung Verantwortliche dann bemühen, die Modellklauseln zu vervollständigen, um diese Mängel vor dem Gericht zu beheben.

Es muss jedoch eingeräumt werden, dass es schwer vorstellbar ist, wie durch Mängel in der Gesetzgebung mit vertraglichen Mitteln die Einmischung des Staates behoben werden könnte… Präzisere Klauseln und zusätzliche Verpflichtungen für den Auftragsverarbeiter dürften zumindest die Bemühungen des für die Verarbeitung Verantwortlichen widerspiegeln, Probleme zu erkennen und zu beheben und so die nachteiligen Folgen zu verringern, die eine fehlende Bewertung für ihn haben könnte. Es wird erwartet, dass das Europäische Datenschutzkomitee in naher Zukunft diesbezüglich einige Orientierungshilfen geben wird.

Letztendlich scheint es jedoch das Vorrecht der größten Marktteilnehmer zu sein, eine solche Risikobewertung vorzunehmen. In mancher verständlichen Hinsicht berücksichtigen die vorgebrachten Argumente jedoch nicht die wirtschaftliche Realität und die enormen Kosten, die eine systematische Risikobewertung für jedes Land, das kein angemessenes Schutzniveau bietet, für die überwiegende Mehrheit der Unternehmen nach sich ziehen wird. Werden Auftragsverarbeiter aus „Drittländern“ sich bereit erklären, die Kosten dieser Analyse zu schlucken, zu deren Durchführung die Verantwortlichen sie sehr oft auffordern werden, um ihnen die notwendigen Garantien zu bieten oder sie kommerziell in ihr Preismodell zu integrieren?

Geht man davon aus, dass eine solche Beurteilung systematisch notwendig ist, wie die Argumentation des Gerichtshofs vermuten lässt, verstößt eine solche Belastung nicht gegen den eigentlichen Zweck der Modellklausel und die angestrebte einfache Umsetzung, um auf die vorherige Zustimmung der Aufsichtsbehörde zu verzichten? Dann kann sich auch vorstellen, dass jede Risikoabschätzung auch eine Verpflichtung zur Dokumentation der Risiken bedeutet. Wäre es in diesem Fall nicht besser, eine vorherige Genehmigung durch die Aufsichtsbehörde zu bevorzugen, was genau das ist, was mit den Modellklauseln vermieden werden sollte?

Zugegeben, die Zeiten haben sich seit der Verabschiedung der Modellklauseln geändert, und der Eingriff in die nationale Sicherheit ist für viele Staaten ein Mittel zur übermäßigen Überwachung. In seinen Auswirkungen dürfte das Urteil des Gerichtshofs somit eine Neuaufteilung der Märkte fördern, eine Vision, die sicherlich möglich ist, die aber noch weit von der Realität einer Wirtschaft entfernt ist, die weitgehend globalisiert ist und sicherlich noch lange Zeit so bleiben wird. Bedeutet dies, dass dieses Urteil weitgehend undurchführbar bleiben wird, wenn die Modellklauseln nicht überarbeitet werden, um sie auf den neuesten Stand zu bringen? Das bleibt abzuwarten.

Wenn es nicht gelingt, die verarbeiteten Daten vollständig zu anonymisieren, was eine immer schwierigere Aufgabe ist, scheint es in Anbetracht der obigen Ausführungen jedenfalls vernünftig anzunehmen, dass die überwiegende Mehrheit der Marktteilnehmer es vorziehen würde, sich vorläufig ohne weitere Analyse an die Modellklauseln zu halten und die damit verbundenen Risiken einzugehen, anstatt sich systematisch auf eine solche Analyse einzulassen. Auf jeden Fall wird diese Position wahrscheinlich so lange Bestand haben, wie der Europäische Datenschutzausschuss und die Aufsichtsbehörden nicht zusammengearbeitet haben, um Richtlinien zu erlassen, wie dieses Urteil nun in der Praxis angewandt werden soll.

Wetten, dass die Haltung der Aufsichtsbehörden hier wie anderswo ein Vektor für die Haltung sein wird, die eingenommen werden soll: Wenn das ICO bereits bereit zu sein scheint, einen gewissen Pragmatismus zu zeigen, so ist es in Berlin nicht dasselbe, wo der Kommissar mitgeteilt hat, dass die Verantwortlichen sich nun an das Urteil halten müssen und insbesondere im Hinblick auf die Nutzung von Cloud-Providern nach Alternativen suchen müssen, die eine Rückführung der Daten nach Europa ermöglichen.

In einem zukünftigen Artikel werden

Source :
https://www.wg-avocats.ch/de/nachrichten/datenschutz/schrems-ii-ist-die-ubermittlung-von-personendaten-in-die-usa-noch-erlaubt/