



SONDERAUSGABE

Das Schrems II-Urteil – und was nun?

Newsletter September 2020

Datenschutz

Liebe Leserinnen und Leser,

mit dem Kippen des Privacy Shields sind Unternehmen europaweit vor große Probleme gestellt worden, da die bisherige Grundlage für einen rechtssicheren Datenaustausch mit Drittländern damit wegfällt.

Standardvertragsklauseln werden als möglicher Ersatz zum Privacy Shield weiterhin gern aufgeführt. Die Sicherstellung des Datenschutzniveaus bei einer Datenübermittlung in Drittländer - insbesondere in die USA - ist damit dennoch nicht gesichert. Die uneingeschränkte Zugriffsmöglichkeit auf die personenbezogenen Daten durch staatliche Überwachungsbehörden stellt hier das größte Problem dar. Dies kann bedauerlicherweise durch Standardvertragsklauseln nicht gelöst werden, weil diese für die Behörden nicht bindend sind.

Auch wenn die Lösung dieser neuen rechtlichen Herausforderung auf den ersten Blick nicht ohne Weiteres möglich ist, besteht dennoch akuter und zeitnaher Handlungsbedarf. Diverse Datenschutzbehörden haben bereits Kontrollen mit entsprechenden Maßnahmen angekündigt.

Was ist zu tun?

Nach unseren Erfahrungen ist es sinnvoll, sich an den Empfehlungen von Datenschutzbehörden zu orientieren. Die Datenschutzbehörde in Baden-Württemberg sagt dazu beispielsweise folgendes:

- Nehmen Sie unverzüglich eine Bestandsaufnahme vor. Ermitteln Sie, in welchen Fällen Ihr Unternehmen personenbezogene Daten in Drittländer exportiert. Darunter können auch Zugriffsmöglichkeiten von privaten oder öffentlichen Stellen in Drittstaaten auf bei Ihnen vorgehaltene Daten zählen.
- Setzen Sie sich mit Ihrem Dienstleister bzw. Vertragspartner im Drittland in Verbindung und informieren ihn über die Entscheidung des EuGH und deren Konsequenzen.
- Informieren Sie sich über die Rechtslage im Drittland. Hier können Sie z.B. öffentliche Stellen, wie die Datenschutz-Aufsichtsbehörden, der Europäische Datenschutz-Ausschuss (EDSA), die EU-Kommission oder das Auswärtige Amt um Hilfestellung bitten.

Fortsetzung von Seite 1

- Überprüfen Sie, ob es für das Drittland einen Angemessenheitsbeschluss nach Art. 45 DS-GVO gibt. Für die USA wurde dieser nun für ungültig erklärt, aber für Argentinien, Kanada, Japan, Neuseeland oder die Schweiz besteht diese Möglichkeit noch. Eine ausführliche Liste finden Sie unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Gegebenenfalls können Sie sich auch auf verbindliche, interne Datenschutzvorschriften gemäß Artikel 47 (BCRs) berufen.
- Überprüfen Sie, ob Sie die von der Kommission beschlossenen Standardvertragsklauseln für das jeweilige Land nutzen können (Art.46 Abs. 2c DS-GVO). Diese sind abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087>.
- Sollten - wie im Falle der USA - Behörden oder sonstige Stellen des Drittlandes in unverhältnismäßiger Art und Weise in die Rechte der betroffenen Personen eingreifen können (z.B. ein massenhafter Abruf von Daten ohne Information der Betroffenen und ohne verfahrensrechtliche Sicherungen wie einen Richtervorbehalt), so sind die Klauseln keine Alternative. Ausnahme wäre, das Vorliegen einer zusätzlichen Garantie durch z.B. Verschlüsselungen oder einem Hosting der Daten im Geltungsbereich der DS-GVO.
- Um Ihren Willen zu einem rechtskonformen Handeln zu demonstrieren und zu dokumentieren, sollten Sie zudem Kontakt mit dem jeweiligen Empfänger der Daten aufnehmen und sich über Änderungen in den Bestimmungen der Standardvertragsklauseln verständigen. Vorschläge hierzu finden Sie im Anhang.
- Wenn nach Überprüfung aller Vorgaben eine Datenübermittlung nicht zulässig wäre, bleibt als letztes Mittel ggf. die Übermittlung von Daten nach der Ausnahmenvorschrift des Art. 49 DS-GVO.

Entscheidend bei der Bewertung durch die Datenschutzaufsichtsbehörden scheint die Frage zu sein, ob es neben dem gewählten Dienstleister bzw. Vertragspartner zumutbare Alternativangebote ohne Transferproblematik gibt. Kann man die Datenschutzbehörde nicht davon überzeugen, dass der eingesetzte Dienstleister bzw. Vertragspartner kurz- und mittelfristig für das Unternehmen und dessen Geschäftsfähigkeit unersetzlich ist, muss man davon ausgehen, dass der Datentransfer untersagt und mit einem Bußgeld belegt wird.

Unser Fazit

Handeln Sie proaktiv und dokumentieren Sie gut. Auch wenn die Kommunikation mit Anbietern wie Google etc. aussichtslos erscheint, demonstrieren Sie damit, dass Sie sich mit dem Thema ernsthaft auseinandersetzen. Bitten Sie gegebenenfalls die Datenschutzbehörde auch einfach einmal um Unterstützung bzw. Einschätzung.

Zudem gilt: „Hand aufs Herz“.... Welcher Datentransfer ist für Sie unternehmerisch wirklich relevant, sodass der nicht unerhebliche Aufwand und das damit verbundene Risiko bei einer Überprüfung gerechtfertigt ist.

Wenn Sie Fragen haben, wenden Sie sich gern an Ihren Datenschutzbeauftragten der ANMATHO AG.

Anhang

Änderungsvorschläge für die Standardvertragsklauseln

- Abänderung der Anhang Klausel 4f:
Die Information der betroffenen Person darüber, dass ihre Daten in ein Drittland übermittelt werden, das kein angemessenes Schutzniveau im Sinne der Verordnung (EU) 2016/679 bietet, erfolgt nicht nur bei der Übermittlung besonderer Datenkategorien, sondern kurzfristig bei jeglicher Datenübermittlung.
- Abänderung der Anhang Klausel 5d i:
Der Datenimporteuer hat die Pflicht nicht nur den Datenexporteur, sondern auch die betroffene Person unverzüglich zu informieren, sobald eine Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten aufgefordert hat. Sollte diese Informationsweitergabe durch zum Beispiel ein strafrechtliches Verbot oder ähnlichem untersagt sein, muss das weitere Vorgehen mit der Aufsichtsbehörde abgeklärt werden.
- Ergänzung der Anhang Klausel 5 d:
Der Datenimporteuer ist verpflichtet, den Rechtsweg gegen eine Weitergabe von personenbezogenen Daten zu beschreiten und die Offenlegung der personenbezogenen Daten gegenüber den jeweiligen Behörden zu unterlassen, bis er von einem zuständigen Gericht letztinstanzlich zur Offenlegung rechtskräftig verurteilt wurde.
- Abänderung von Anhang Klausel 7 Abs. 1, nur Aufnahme von b):
Sollte eine betroffene Person gegenüber dem Datenimporteuer Rechte als Drittbegünstigte und/oder Schadenersatzansprüche aufgrund der Vertragsklauseln geltend machen, ist das Gericht des Mitgliedstaates zuständig, in dem der Datenexporteur sich niedergelassen hat.
- Aufnahme des in Anhang 2 genannten Beispiels für eine Entschädigungsklausel (Haftung):
Die Parteien erklären sich damit einverstanden, dass, wenn eine Partei für einen Verstoß gegen die Klauseln haftbar gemacht wird, den die andere Partei begangen hat, die zweite Partei der ersten Partei alle Kosten, Schäden, Ausgaben und Verluste, die der ersten Partei entstanden sind, in dem Umfang ersetzt, in dem die zweite Partei haftbar ist. Die Entschädigung ist abhängig davon, dass a) der Datenexporteur den Datenimporteuer unverzüglich von einem Schadenersatzanspruch in Kenntnis setzt und b) der Datenimporteuer die Möglichkeit hat, mit dem Datenexporteur bei der Verteidigung in der Schadenersatzsache bzw. der Einigung über die Höhe des Schadenersatzes zusammenzuarbeiten.