Datenübermittlung in die USA – Standard-Datenschutz-Klauseln und zusätzliche Maßnahmen – Was kann eine Organisation nun tun?

EU-US-Privacy-Shield ist seit 16.7.2020 Geschichte.

Die Standard-Datenschutzklauseln haben weiterhin Gültigkeit, können aber ohne „zusätzliche Maßnahmen“ des Verantwortlichen für Übermittlungen in ein Drittland nicht verwendet werden.

Datenübermittlungen in ein Drittland

Mit der Entscheidung **Schrems II** des EuGH (C-311/18 vom 16.07.2020) ist klargestellt, dass die USA als „Drittland“ anzusehen sind, und keine Privilegierung mehr für die Übermittlung von personenbezogenen Daten genießen. Daher ist auf die „allgemeinen Bestimmungen“ der Art 45 ff DSGVO für die Datenübermittlung in Drittländer abzustellen.

Privacy-Shield ist seit 16.7.2020 nicht mehr als Grundlage tauglich. Zu den **Standarddatenschutzklauseln**, die als Vertragswerk zwischen dem **Datenexporteur** (Verantwortlicher / Auftragsverarbeiter in der EU) und **Datenimporteur** (Auftragsverarbeiter oder Verantwortlicher im Drittland) zu vereinbaren sind, und dann eine taugliche (formelle) Grundlage für die Übermittlung.

Standarddatenschutzklauseln

Der EuGH hat dazu ausgesprochen (Hervorhebungen durch den Verfasser):

132 Da **Standarddatenschutzklauseln**, wie aus Rn. 125 des vorliegenden Urteils hervorgeht**, aufgrund ihres Vertragscharakters naturgemäß keine drittstaatlichen Behörden binden können**, […] das durch die **DSGVO verbürgte Schutzniveau für natürliche Personen nicht beeinträchtigt wird**, kann es sich als **notwendig** erweisen, die in den **Standarddatenschutzklauseln enthaltenen Garantien zu ergänzen**. Dazu heißt es im 109. Erwägungsgrund […] **weitere Klauseln oder zusätzliche Garantien hinzuzufügen**", und dass der Verantwortliche insbesondere „ermutigt werden [sollte], [durch Ergänzung der Standarddatenschutzklauseln] zusätzliche Garantien zu bieten".

Zusätzliche Maßnahmen iSd Schrems II Entscheidung

Folgende Voraussetzungen könnten daher uU ausreichend sein, um Datenübermittlungen in Drittländer (und die USA) auf eine taugliche Grundlage zu stellen:

- Abschluss von Standarddatenschutzklauseln mit den Empfängern

- Zusätzliche Maßnahmen im Sinne von „geeigneten Garantien", um das Schutzniveau zu erhöhen bzw. ein angemessenes Schutzniveau zu erreichen, wobei dies insbes. auch von der Art der Daten, die übermittelt werden, abhängig sein wird, und zB bei Art 9 DSGVO-Daten strengere Anforderungen zu stellen sind, als bei der IP-Adresse oder MAC-Adresse sowie Standort oder Gerätedaten, die auf einer Website von einer betroffenen Person an den Social-Media-Dienst übertragen wird:

    - Strengere Pflichten für die Datenempfänger(importeure), könnten sein:

        - Strenge Informationspflichten für den Datenempfänger bei Zugriff oder auch nur konkret angedrohtem Zugriff durch staatliche Stellen

        - Das Recht für den Datenexporteur, den Vertrag ohne Frist und Termin aufzulösen, sofern es zu einem Zugriff staatlicher Stellen kommt, oder ein derartiger befürchtet wird, damit es zu keinen weiteren Datenübermittlungen kommt

        - Verpflichtung zur Datenverschlüsselung auf Seiten des Datenimporteurs

Wechsel des Dienstleisters als Datenempfänger:

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit empfiehlt den Organisationen:

„Verantwortliche, die – insbesondere bei der Nutzung von Cloud-Diensten – personenbezogene Daten in die USA übermitteln, sind nun angehalten, umgehend zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln."

Stimmen aus anderen EU-Staaten:

Großbritannien:

Das Information Commissioners Office empfiehlt sich weiterhin auf das EU-US-Privacy-Shield zu stützen, aber keine neuen Übermittlungen auf dieser Basis vorzunehmen.

"We are currently reviewing our Privacy Shield guidance after the judgment issued by the European Court of Justice on Thursday 16 July 2020.

If you are currently using Privacy Shield please continue to do so until new guidance becomes available.

Please do not start to use Privacy Shield during this period."

Rheinland-Pfalz:

„Der Ball liegt nun im Feld der Verantwortlichen. Sie kommen nicht umhin, sich mit den nationalen Gesetzen des Drittlandes, in welche sie Daten übermitteln möchten, intensiv auseinanderzusetzen. Unterliegen die Datenempfänger gesetzlichen Regeln ihres Heimatlandes, die gegen das europäische Datenschutzrecht verstoßen, können sie die vertraglichen Regelungen der Standardvertragsklauseln ggf. nicht einhalten. In diesem Fall muss der Verantwortliche in der EU die Datenübermittlung dorthin aussetzen, da er sonst einen Datenschutzverstoß begeht."

Dort gibt es auch eine Rubrik „FAQ" zur Datenübermittlung in Drittländer

Thüringen:

„Fraglich bleibt für Dr. Hasse aber, wie die weiterhin anwendbaren Standardvertragsklauseln der EU künftig mit „Leben erfüllt“ werden sollen. Diese Klauseln sollen die Garantien dafür bieten, dass es bei der Daten-Übermittlung aus der EU ins Ausland angemessenen Schutz für die personenbezogenen Daten von EUBürgern gibt.“

Frankreich:

„Über die Zusammenfassung hinaus, die der EuGH in seiner Pressemitteilung geteilt hat, führt die CNIL derzeit zusammen mit ihren im Europäischen Ausschuss für Datenschutz versammelten europäischen Kollegen eine genaue Analyse des Urteils durch. Diese gemeinsame Arbeit wird es ermöglichen, so bald wie möglich die Konsequenzen für die Datenübertragung von der Europäischen Union in die Vereinigten Staaten zu ziehen.“

Niederlande:

„Im Anschluss an dieses Urteil wird die Europäische Kommission eingesetzt, um ein neues System für die Übermittlung von Daten aus der EU in die USA einzurichten.

Die niederländische Datenschutzbehörde (AP) prüft nun die praktischen Folgen des Urteils innerhalb des Europäischen Datenschutzausschusses (EDPB). Und was für die nächsten Schritte sein könnte.“

Europäischer Datenschutzausschuss

„Während die SCCs weiterhin gültig sind, unterstreicht der EuGH die Notwendigkeit, sicherzustellen, dass diese in der Praxis ein Schutzniveau aufrechterhalten, das im Wesentlichen dem entspricht, das die DSGVO im Lichte der EU-Charta garantiert.

Die Beurteilung, ob die Länder, in die Daten gesendet werden, einen angemessenen Schutz bieten, liegt in erster Linie in der Verantwortung des Exporteurs und des Importeurs, wenn überlegt wird, ob SCCs geschlossen werden sollen.

Bei der Durchführung einer solchen vorherigen Bewertung berücksichtigt der Ausführer (erforderlichenfalls mit Unterstützung des Einführers) den Inhalt der SCC, die besonderen Umstände der Überstellung sowie die im Land des Einführers geltenden Rechtsordnung. Die Prüfung der letzteren erfolgt unter Berücksichtigung der nicht erschöpfenden Faktoren gemäß Artikel 45 Absatz 2 DSGVO.

Was kann weiterhelfen?

NOYB, die von **Max Schrems** gegründete Organisation hat sich dazu Gedanken gemacht, und hat auch bereits auf der Website unter „nächste Schritte für Unternehmer“ einige „**Tools**“ zur Verfügung gestellt.

Besonders hervorheben möchte ich die „**Fragenkataloge**“, die für Verantwortliche (aber auch Auftragsverarbeiter), die Daten in die USA übermitteln, verwenden kann, um das „Datenschutzniveau“ im Zielland zu definieren.

Hier die **Information** und die **Links**, wobei angekündigt wurde, weitere Muster zur Verfügung zu stellen.

Musterantrag an US-Datenimporteure, wenn Sie noch SCCs verwenden ("Einzelfallanalyse")

Version ohne Noyb-Deckblatt

Word-Version (editierbar)

Musterantrag an Anbieter, die Daten in der EU/EWR verarbeiten, aber US-Beziehungen haben ("Einzelfall"-Analyse)

Version ohne Noyb-Deckblatt

Word-Version (editierbar)