

## **EuGH: Privacy Shield-Beschluss ungültig, aber EU-Standardklauseln gültig: Was das nun bedeutet!**

Mit Urteil vom 06.10.2020 hatte der Gerichtshof der Europäischen Union (EuGH) bereits die „Vorgängerregelung“ - die Safe-Harbour-Principles - für unwirksam erklärt, und nun mit Urteil vom 16.07.2020 (Rechtssache C-311/18) auch das sogenannte Nachfolgekonzept – den EU-US-Privacy-Shield (EU-Kommission Beschluss 2016/1250). Der EuGH hat sich aber auch mit dem Beschluss 2010/87 der EU-Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern befasst. Er hat diesen Beschluss zwar nicht für unwirksam erklärt. Aber die Begründung der Ungültigkeit des Privacy Shields wirkt sich – jedenfalls in Bezug auf den Datentransfer in die USA – auch hier aus.

### **Ungültigkeit des Privacy Shields**

Das EU-US-Privacy-Shield ist keine Grundlage mehr für den Datentransfer in die USA. Das hat Auswirkungen auf den Datentransfer in Unternehmen, Online-Anwendungen, Social Media, Cloud-Diensten usw.

### **Warum ist das so brisant?**

Nach Artt. 13, 14 DS-GVO muss jede betroffene Person pro aktiv auch auf die Datenübermittlung in Drittländer hingewiesen werden. Damit ist – anders als noch zur Rechtslage bei der Safe-Harbor-Entscheidung – das Thema für jeden „auf dem Präsentierteller“. Auch ist die allgemeine Aufmerksamkeit infolge der DS-GVO und vor allem die Sanktionen größer. Hier ist sowohl an Bußgelder als auch an Schadensersatzansprüche zu denken.

### **Warum ist die Reaktion jetzt komplizierter als 2015 bei der Safe-Harbor-Entscheidung des EuGH?**

In der Vorgängerentscheidung „Schrems I“ vom 05.10.2020 hat sich der EuGH für die Begründung der Unwirksamkeit darauf beschränkt, dass die EU-Kommission die Angemessenheit des Schutzniveaus – insbesondere mit Blick auf Zugriffsbefugnisse der US-Sicherheitsbehörden - nicht ausreichend geprüft habe. Das genügte seinerzeit für die Unwirksamkeit.

Im Urteil vom 16.07.2020 befasst sich der EuGH nunmehr – auf der Grundlage der Feststellungen der EU-Kommission im Beschluss 2016/1250 – mit dem Rechtsrahmen und sieht - vereinfacht gesagt – ein ausreichendes Schutzniveau in den USA als nicht gegeben an. Dieser Unterschied zwischen den beiden Entscheidungen ist entscheidend und wirkt sich auch auf die Bewertung von Alternativen zum Datentransfer in die USA aus. Denn diese Wertung des EuGH ist auch bei der Bewertung anderer Rechtsgrundlagen für den Datentransfer in die USA zu berücksichtigen.

Mit Erklärung der Ungültigkeit des EU-US-Privacy Shields stellt der EuGH fest, dass die USA aufgrund der fehlenden gerichtlichen Rechtsschutz-Möglichkeiten für Unionsbürger gerade mit Blick auf die weitreichenden Zugriffsmöglichkeiten der US-Behörden kein angemessenes Schutzniveau der betroffenen Personen bieten. Für den Datentransfer in die USA müssen daher besondere Schutzmaßnahmen ergriffen werden.

### **Generelle Wirksamkeit der Standardvertragsklauseln für Drittland-Transfer**

Der EuGH stellt klar, dass der Beschluss der EU-Kommission zu den Standardvertragsklauseln nicht unwirksam ist. Die Standardvertragsklauseln kommen damit weiterhin für eine Übermittlung personenbezogener Daten in ein Drittland in Betracht.

Zum Hintergrund: Die Standardvertragsklauseln gelten als Rechtsgrundlage für jede Datenübermittlung in ein Drittland, wohingegen das EU-US-Privacy Shield nur für den Datentransfer in die USA greift.

ABER: Der EuGH stellt in diesem Zusammenhang klar, dass bei dem Einsatz von EU-Standardklauseln im Sinne des Art. 46 Abs. 1 und 2 DS-GVO zu überprüfen ist, ob in dem betreffenden Drittland tatsächlich angemessen durchsetzbare Rechte und wirksame Rechtsbehelfe bestehen. Sollte dies nicht der Fall sein, dürfen – und müssen – die zuständigen Aufsichtsbehörden entsprechende Datenübermittlungen aussetzen oder verbieten.

Der EuGH stärkt damit die europäischen Datenschutzprinzipien und die Rolle der Datenschutzaufsichtsbehörden. Er macht zudem deutlich, dass internationaler Datenverkehr weiter möglich ist, jedoch müssen die Grundrechte der europäischen Bürgerinnen und Bürger beachtet werden.

### **Bedeutung nicht nur für die Datenübermittlung in die USA**

Die Anforderung der Prüfung einer Drittlandübermittlung als Aufgabe des Verantwortlichen als Datenexporteur und des Empfängers als Datenimporteur ist nicht auf die USA beschränkt.

Die durch den EuGH geforderte Prüfung gilt für jeden Datentransfer in ein Drittland, sofern die EU-Kommission nicht ein angemessenes Datenschutzniveau in dem Drittland per Beschluss anerkannt hat.

Mit anderen Worten: Der bloße Abschluss eines EU-Standardvertrags allein genügt auch bei anderen Drittländern nicht mehr.

### **Konkret: Was bedeutet das nun für eine Datenübermittlung in die USA?**

Das EU-US-Privacy Shield ist keine Rechtsgrundlage mehr für eine Datenübermittlung in die USA. Die Datenübermittlung muss daher auf eine andere Grundlage im Sinne der Artt. 44 ff. DS-GVO gestützt werden. Hierbei müssen die Ausführungen des EuGH zu Privacy Shield wieder berücksichtigt werden.

Sofern ein Drittland – wie die USA - kein angemessenes Datenschutzniveau aufgrund eines fehlenden Angemessenheitsbeschlusses der EU-Kommission bietet, ist eine Datenübermittlung nach Art. 46 DS-GVO vorbehaltlich geeigneter Garantien zulässig. Art. 46 DS-GVO regelt eine der Möglichkeiten, mit denen sichergestellt werden kann, dass bei der Datenübermittlung an Drittländer und internationale Organisationen das durch die DS-GVO vorgegebene Schutzniveau gewährleistet wird. Hierzu zählen insbesondere

- verbindliche interne Datenschutzvorschriften, sog. Binding Corporate Rules, diese müssen jedoch von der zuständigen Datenschutzaufsichtsbehörde genehmigt werden und scheiden demnach als schnelle Alternative aus,
- genehmigte Verhaltensregeln und Zertifizierungen; diese Möglichkeit ist mit Inkrafttreten der DS-GVO neu hinzugekommen und bisher kaum genutzt bzw. genehmigt worden,
- oder die EU-Standardvertragsklauseln.

Der EuGH stellte fest, dass die USA aufgrund der fehlenden gerichtlichen Rechtsschutz-Möglichkeiten für Unionsbürger gerade mit Blick auf die weitreichenden Zugriffsmöglichkeiten der US-Behörden kein angemessenes Schutzniveau der betroffenen Personen bieten.

Das bedeutet: Auch bei den alternativen Rechtsgrundlagen muss nun bewertet werden, ob und wie ein ausreichender Schutz so sichergestellt werden kann, dass bei Datenempfängern in den USA ein angemessenes Datenschutzniveau sichergestellt ist. Dies erscheint – jedenfalls aktuell - nur schwer darstellbar.

### **Was ist nach Maßgabe des EuGH zu tun, wenn eine Rechtsgrundlage nicht eingreift?**

Als Folge ist der Verantwortliche zur Aussetzung der Datenübermittlung und/oder zum Rücktritt vom Vertrag verpflichtet. Kommt er seiner Verpflichtung nicht nach, ist wiederum die Aufsichtsbehörde

nach Art. 58 Abs. 2 Buchst. f und j der DS-GVO verpflichtet, eine Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten. Hierauf stellt der Europäische Datenschutzausschuss in seinen FAQ vom 23.07.2020 (dort Ziffer 1) ab.

### **Welche Zulässigkeit bleibt noch?**

Die scheinbar einzige Möglichkeit der datenschutzkonformen Datenübermittlung in die USA ist derzeit wohl nur über Art. 49 DS-GVO herbeizuführen. Eine Datenübermittlung in die USA kann bei fehlendem Angemessenheitsbeschluss und fehlender geeigneter Garantien daher nur erfolgen, wenn ein Ausnahmefall nach Art. 49 DS-GVO vorliegt. Dies ist insbesondere dann der Fall, wenn

- die betroffene Person über die vorgeschlagene Datenübermittlung ausdrücklich in die Datenübermittlung eingewilligt hat, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,
- die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist,
- die Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist oder
- die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

### **Die Einwilligung der betroffenen Person als Lösung?!**

Die Einwilligung nach Art. 49 DS-GVO kommt ebenfalls als Grundlage für die Drittlandübermittlung in Betracht. Hierauf weist sowohl der Europäische Datenschutzausschuss in seinen FAQ vom 23.07.2020 als auch die deutschen Datenschutzaufsichtsbehörden in ihrer Pressemitteilung hin.

Die deutschen Datenschutzaufsichtsbehörden verweisen hierfür auf die Leitlinien des Europäischen Datenschutzausschusses zu Art. 49 DS-GVO. Der Europäische Datenschutzausschuss stellt in seinen FAQ vom 23.07.2020 (dort Ziffer 8) bestimmte Anforderungen an eine solche Einwilligung heraus.

Die Wirksamkeit einer solchen Einwilligung hängt von ihrer Transparenz und Vollständigkeit ab. Diese will daher gut beraten und sorgfältig gestaltet sein.

### **Was ist zu tun?**

**Der Europäische Datenschutzausschuss spricht in seinen FAQ vom 23.07.2020 explizit an, dass es keine Übergangszeit gibt. Daher muss sofort gehandelt werden. Auch wenn sich der Datentransfer in die USA aufgrund der Entscheidung aufdrängt, besteht der Handlungsbedarf für jedes Drittland!**

***Sprechen Sie uns an! Wir unterstützen Sie!***

<b>So können Sie vorgehen: Checkliste von <i>dmp Derra, Meyer &amp; Partner Rechtsanwälte PartGmbB 2020</i></b>			
<b>Reihenfolge</b>		<b>Fragestellung</b>	<b>Checkbox</b>
<b>1.</b>		<b>Identifikation aller Übermittlungen personenbezogener Daten in Länder außerhalb der EU</b>	<input type="checkbox"/>

	1.1		Unterscheiden Sie zwischen Datenübermittlung in die USA und andere Drittländer.	<input type="checkbox"/>
	1.2		Prüfen Sie auch, ob Ihre Dienstleister als Subunternehmer (weitere) Unternehmen in Drittländern einbinden.	<input type="checkbox"/>
2.			Prüfen Sie, ob personenbezogene Daten übertragen werden.	<input type="checkbox"/>
	2.1		Werden personenbezogene Daten an Unternehmen in Drittländer übertragen?	<input type="checkbox"/>
	2.2		Haben Unternehmen aus Drittländern Zugriff auf personenbezogene Daten bei Ihnen?	<input type="checkbox"/>
	2.3		Kann eine Übertragung bzw. ein Zugriff durch bspw. Verschlüsselung verhindert werden?	<input type="checkbox"/>
3.			Identifizieren Sie die Rechtsgrundlage für die Datenübertragung.	<input type="checkbox"/>
	3.1		Wird die Übertragung auf das EU-US-Privacy Shield gestützt?	<input type="checkbox"/>
		3.1.1	Identifizieren Sie die entsprechenden Unternehmen.	<input type="checkbox"/>
		3.1.2	Fordern Sie die entsprechenden Unternehmen zur Abstimmung alternativer Gestaltungen auf.	<input type="checkbox"/>
		3.1.3	Prüfen Sie die alternativen Gestaltungen (siehe Ziffer 3.3).	<input type="checkbox"/>
	3.2		Wird die Übertragung auf die EU-Standardvertragsklauseln oder auf Binding Corporate Rules (BCR) gestützt?	<input type="checkbox"/>
		3.2.1	Sofern eine Übermittlung in die USA erfolgt, sind die Ausführungen des EuGH zum angemessenen Datenschutzniveau auch auf EU-Standardvertragsklauseln bzw. BCR zu beachten.	<input type="checkbox"/>
		3.2.2.	Erfolgt eine Übermittlung in ein anderes Drittland, dann ist ebenfalls zusätzlich die Angemessenheit des dortigen Datenschutzniveaus zu hinterfragen.	<input type="checkbox"/>
		3.2.3.	Fragen Sie zur Bewertung auch beim Datenempfänger im Drittland an. Auch dieser ist in der Pflicht.	<input type="checkbox"/>
	3.3		Wird die Übertragung auf eine der Zulässigkeitsregelungen des Art. 49 DS-GVO gestützt?	<input type="checkbox"/>
		3.3.1	Prüfen Sie die Voraussetzungen der zulässigen Datenübertragung.	<input type="checkbox"/>
		3.3.2	Insbesondere bei Einwilligungen: Prüfen Sie die rechtlichen Anforderungen an eine wirksame Einwilligung.	<input type="checkbox"/>

4.			Prüfen und korrigieren Sie erforderlichenfalls die Datenschutzhinweise nach Artt. 13, 14 DS-GVO.	<input type="checkbox"/>
<b>© Dr. Jens Eckhardt, dmp Derra, Meyer &amp; Partner Rechtsanwälte PartGmbH 2020</b>				