

## **Privacy Shield Kundenberatung**

Ein Rechtsstreit zwischen einer Privatperson (Maximilian Schrems) und der irischen Aufsichtsbehörde über die Übermittlung seiner personenbezogenen Daten durch Facebook Irland zum Mutterkonzern von Facebook in die USA.

### Inhalt

<b>A.</b>	<b>Kernaussagen .....</b>	<b>2</b>
1.	<b>Die Datenschutz-Grundverordnung .....</b>	<b>2</b>
2.	<b>„Privacy Shield“ .....</b>	<b>2</b>
3.	<b>Die von der Kommission im Jahr 2010 beschlossenen Standardvertragsklauseln sind weiterhin gültig. ....</b>	<b>2</b>
<b>B.</b>	<b>Privacy Shield ist tot, es leben die Standardvertragsklauseln.....</b>	<b>4</b>
1.	<b>Was bedeutet das konkret? .....</b>	<b>4</b>
2.	<b>Wen trifft die Entscheidung? .....</b>	<b>4</b>
3.	<b>Die Ausnahmen des Artikel 49 DSGVO.....</b>	<b>5</b>
<b>C.</b>	<b>Was bedeutet die Entscheidung konkret? / Was ist zu tun? .....</b>	<b>6</b>
1.	<b>Wenn Sie Daten in die USA übermitteln oder sich eines Auftragsverarbeiters bedienen, der Daten in die USA übermittelt .....</b>	<b>6</b>
2.	<b>Wenn Sie Daten in ein anderes Drittland ohne angemessenes Datenschutzniveau übermitteln.....</b>	<b>7</b>
<b>D.</b>	<b>Checkliste .....</b>	<b>8</b>

## A. Kernaussagen

1. Die **Datenschutz-Grundverordnung (DS-GVO)** findet auf die Übermittlung personenbezogener Daten in ein Drittland auch in solchen Fällen **Anwendung**, in denen es aus Gründen der nationalen Sicherheit oder Verteidigung zu einem Zugriff durch Geheimdienste dieses Landes kommt. Die Ausnahmen des Art. 2 Abs. 2 a, b, d der DS-GVO gelten nur für die Mitgliedstaaten der EU.
2. Das **sog. „Privacy Shield“**, ein Angemessenheitsbeschluss der Kommission nach Art. 45 DS-GVO (2016/1250 vom 12.07.2016, noch zur Datenschutz-Richtlinie 95/46/EC), mit dem diese 2016 beschlossen hatte, dass die USA unter bestimmten Umständen ein angemessenes Schutzniveau für die Daten natürlicher Personen bieten und so die Übermittlung von Daten in die USA allgemein ermöglicht hatte, ist **ab sofort ungültig**.

Aufgrund der Befugnisse der US-Geheimdienste und der Rechtslage in den USA kann ein angemessenes staatliches Datenschutz-Niveau (Art. 45 DS-GVO) nicht sichergestellt werden:

- Section 702 des Foreign Intelligence Surveillance Act (FISA) sieht keine Beschränkungen der Überwachungsmaßnahmen der Geheimdienste und keine Garantien für Nicht-US-Bürger vor
- Presidential Policy Directive 28 (PPD-28) gibt Betroffenen keine wirksamen Rechtsbehelfe gegen Maßnahmen der US-Behörden und sieht keine Schranken für die Sicherstellung verhältnismäßiger Maßnahmen vor
- der im Privacy Shield vorgesehene Ombudsmann hat keine genügende Unabhängigkeit von der Exekutive; er kann keine bindenden Anordnungen gegenüber den Geheimdiensten treffen.

Maßstab der Feststellung des EuGHs, dass die staatlichen Überwachungsmaßnahmen der USA unverhältnismäßig sind, ist die EU-Grundrechte-Charta.

3. **Die von der Kommission im Jahr 2010 beschlossenen Standardvertragsklauseln sind weiterhin gültig.**

***Aber: Es muss ein Schutzniveau für die personenbezogenen Daten sichergestellt sein, das dem in der Europäischen Union entspricht.***

- Auszulegen im Lichte der EU-Grundrechte-Charta und im Hinblick auf Art. 46 Abs. 1 DS-GVO: geeignete Garantien des Verantwortlichen oder des Auftragsverarbeiters, durchsetzbare Rechte und wirksame Rechtsbehelfe für die betroffenen Personen,
- Hier sind nicht nur die vertraglichen Beziehungen zwischen Datenexporteur und Datenimporteur relevant, sondern auch die Zugriffsmöglichkeit auf die Daten durch Behörden des Drittlandes und das Rechtssystem dieses Landes insgesamt (Gesetzgebung und Rechtsprechung, Verwaltungspraxis von Behörden).

Die Standardvertragsklauseln können allerdings die Behörden des Drittlandes nicht binden und stellen daher in den Fällen, in denen die **Behörden** nach dem Recht des Drittlandes befugt sind, in die Rechte der betroffenen Personen **einzugreifen ohne zusätzliche Maßnahmen der Vertragspartner keinen angemessenen Schutz** dar.

**Der Verantwortliche muss für den Einzelfall prüfen, ob das Recht des Drittlandes ein angemessenes Schutzniveau bietet und entsprechende zusätzliche Maßnahmen treffen bzw. mit dem Datenimporteur vereinbaren.**

- Wo der Verantwortliche auch mit zusätzlichen Maßnahmen keinen geeigneten Schutz vorsehen kann, muss er den Transfer aussetzen/beenden.
  - Das gilt insbesondere, wenn das Recht des Drittlandes dem Datenimporteur Verpflichtungen auferlegt, die geeignet sind, vertraglichen Regeln, die einen geeigneten Schutz gegen den Zugriff durch staatliche Behörden vorsehen, zuwider zu laufen.
4. Ist ein solches angemessenes Schutzniveau nicht sichergestellt, **muss die Aufsichtsbehörde für den Datenschutz die Datenübermittlung aussetzen oder verbieten**, wenn der Schutz nicht durch andere Maßnahmen hergestellt werden kann.

## **B. Privacy Shield ist tot, es leben die Standardvertragsklauseln**

### **1. Was bedeutet das konkret?**

- bedeutet nicht, dass Unternehmen einfach Privacy Shield gegen Standardvertragsklauseln ersetzen können
- Standardvertragsklauseln müssen mit jedem Vertragspartner individuell abgeschlossen werden
- weiterer Faktor: manche Unternehmen haben aufgrund der bequemen Pauschalwirkung der nun vom EuGH verworfenen Regeln oftmals überhaupt keinen Überblick mehr darüber, welche Daten sie konkret in die USA übermitteln oder zu welchen Zwecken dies passiert
- Die dadurch zwingend notwendige interne Aufklärungsarbeit macht die Herausforderung oft umso schmerzvoller
- Angesichts der hohen potentiellen Bußgelder sollten Unternehmen aber Datenübertragungen in die USA sehr genau prüfen und im Zweifel eher aussetzen, bis die Datenschutzlücke durch den Wegfall von Privacy Shield geschlossen ist und individuelle Standardvertragsklauseln ausgehandelt worden sind

### **2. Wen trifft die Entscheidung?**

**Inter partes-Wirkung des Urteils:** erst einmal nur für das vorliegende irische Gericht bindend

- **Bindungswirkung für alle Behörden und Gerichte der Mitgliedstaaten**, die sich mit derselben Auslegungsfrage beschäftigen und die DS-GVO unter Berücksichtigung der Rechtsprechung des EuGHs auslegen und anwenden

- EuGH erklärt Gemeinschaftsrechtsakt für ungültig: alle Gerichte und Behörden in allen Mitgliedstaaten sind daran gebunden, ebenso **alle dem EU-Recht unterworfenen Unternehmen** (erga omnes-Wirkung)
- Urteil enthält allgemeine Aussagen zur Nutzung von Standardvertragsklauseln für Übermittlung von Daten in Drittländer: **alle öffentlichen Stellen oder Unternehmen, die Daten nicht in die USA, sondern in ein anderes Drittland übermitteln, sind von Entscheidung betroffen**

### 3. Die Ausnahmen des Artikel 49 DSGVO

Zulässigkeit des Datentransfers nach in Artikel 49 DSGVO explizit genannter und abschließender Fälle, wenn weder ein Angemessenheitsbeschluss der Europäischen Kommission noch geeignete Garantien vorliegen. Diese Ausnahmefälle umfassen u.a. folgende Situationen:

- wenn Einzelperson ausdrücklich in Übermittlung eingewilligt hat, nachdem sie alle erforderlichen Informationen über die mit der Übermittlung verbundenen Risiken erhalten hat
- wenn Übermittlung für Erfüllung oder den Abschluss eines Vertrags zwischen der Einzelperson und dem Verantwortlichen erforderlich ist, oder wenn der Vertrag im Interesse der Einzelperson geschlossen wird
- wenn die Datenübermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist
- wenn die Datenübermittlung für die Wahrung der zwingenden berechtigten Interessen der Organisation erforderlich ist.

Die Ausnahmen des Artikel 49 DSGVO sind **eng** auszulegen und dürfen nach den **Leitlinien des Europäischen Datenschutzausschusses** nicht für regelmäßige Datentransfers verwendet werden, die eine Vielzahl von Personen betreffen.

## C. Was bedeutet die Entscheidung konkret? / Was ist zu tun?

1. Wenn Sie Daten in die USA übermitteln oder sich eines Auftragsverarbeiters bedienen, der Daten in die USA übermittelt
  - **Privacy Shield** stellt **keine gültige Rechtsgrundlage** für die Übermittlung dar
  - **trotzdem durchgeführte Datentransfers sind rechtswidrig, sie können Bußgelder und Schadensersatzforderungen nach sich ziehen**
  - **Übermittlung auf Grundlage von Standardvertragsklauseln ist denkbar**, wird die Anforderungen **jedoch nur in seltenen Fällen erfüllen**: Der Verantwortliche muss **zusätzliche Garantien** bieten, die einen Zugriff durch die US-amerikanischen Geheimdienste effektiv verhindern, z.B. durch:
    - **Verschlüsselung**
    - **Anonymisierung**
  - **Eine Übermittlung nach Art. 49 DS-GVO ist denkbar; restriktive Charakter dieser Vorschrift ist zu beachten**
- Wortlaut des Titels „Ausnahmen für bestimmte Fälle“: **Ausnahmecharakter von Artikel 49** als Abweichung vom Regelverbot der Übermittlung in Drittstaaten bei Nichtvorliegen eines angemessenen Datenschutzniveaus
- für Art. 49 Abs. 1 UAbs. 1 b, c und e DS-GVO zusätzlich: **Wortlaut EG 111**: „**gelegentlich**“ erfolgende Datenübermittlungen, nicht systematisch wiederholend
- **noch restriktiver: Art. 49 Abs. 1 UAbs. 2** für Fälle, in denen keine Ausnahme für bestimmte Fälle vorliegt

- **für Behörden** gelten zudem gem. Art. 49 Abs. 3 DS-GVO die Art. 49 Abs. 1 UAbs. 1 a, b und c sowie UAbs. 2 nicht bei Ausübung ihrer hoheitlichen Befugnisse

## **2. Wenn Sie Daten in ein anderes Drittland ohne angemessenes Datenschutzniveau übermitteln**

- Rechtslage in dem genannten Land überprüfen, insbesondere hinsichtlich der Zugriffsmöglichkeiten des Geheimdienstes und
- der dem Betroffenen zustehenden Rechte und Rechtsschutzmöglichkeiten

## D. Checkliste

Sie sollten jetzt unverzüglich

- ✓ eine **Bestandsaufnahme** machen, in welchen Fällen Ihr Unternehmen/Ihre Behörde personenbezogene Daten in Drittländer exportiert
- ✓ sich mit Ihrem **Dienstleister/Vertragspartner** im Drittland in Verbindung setzen und ihn über die Entscheidung des EuGHs und deren Konsequenzen informieren
- ✓ Ihre **Datenschutzerklärungen** prüfen und anpassen, insbesondere im Hinblick auf Ihre Informationspflicht nach Art. 13 Abs. 1 f DS-GVO
- ✓ Ihre **Verzeichnisse der Verarbeitungstätigkeiten** entsprechend prüfen und anpassen
- ✓ alle Auftragsverarbeiter, die personenbezogene Daten unter dem Privacy Shield in die USA übermitteln oder dort verarbeiten, umgehend anweisen, die Übermittlung personenbezogener Daten in die USA mit sofortiger Wirkung auszusetzen, bis ihr Auftragsverarbeiter bzw. dessen Unterauftragnehmer dort im Einzelfall ein der DS-GVO entsprechendes Datenschutzniveau sichergestellt hat
- ✓ sich über die Rechtslage im Drittland informieren
- ✓ öffentliche Stellen wie die Datenschutz Aufsichtsbehörden, der Europäische Datenschutz-Ausschuss, die EU-Kommission oder das Auswärtige Amt sollten dazu jeweils Hilfestellungen geben können
- ✓ überlegen, ob Sie einen Transfer von Daten in Drittländer nicht dadurch vermeiden können, dass Sie
  - nur Dienste nutzen, die keine Daten in ein Drittland übertragen oder



- die vertragliche Vereinbarung treffen, dass keine Datenübertragung in ein Drittland vorgenommen wird
  - die Daten verschlüsseln und allein Zugriff auf den Schlüssel haben,
- ✓ überprüfen, ob es für das Drittland einen Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DS-GVO gibt
  - ✓ **überprüfen, ob Sie die von der Kommission beschlossenen Standardvertragsklauseln für das jeweilige Land nutzen können (Art. 46 Abs. 2c DS-GVO)**

**Eine Übermittlung von Daten mithilfe der Standardvertragsklauseln ist in die USA nur mithilfe zusätzlicher Garantien möglich.** Fehlt es an wirksamen zusätzlichen Garantien sollten Sie, um wenigstens Ihren Willen zu rechtskonformem Handeln zu demonstrieren und zu dokumentieren, **Kontakt mit dem jeweiligen Empfänger der Daten aufnehmen** und sich über folgende **Ergänzungen der Bestimmungen der Standardvertragsklauseln verständigen:**

- Ergänzung Anhang **Klausel 4f**: Information der betroffenen Person bei jeglicher Datenübermittlung, dass ihre Daten in ein Drittland übermittelt werden, das kein angemessenes Schutzniveau im Sinne der Verordnung (EU) 2016/679 bietet
- Ergänzung Anhang **Klausel 5d i**: Pflicht des Datenimporteurs, auch die betroffene Person unverzüglich zu informieren über alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten
- Aufnahme dieser Ergänzung in die Drittbegünstigung, ergänzend zu **Klausel 3 Abs. 2**
- Ergänzung von Anhang **Klausel 5 d** um die Verpflichtung des Datenimporteurs, 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

- Aufnahme dieser Ergänzung in die Drittbegünstigung, ergänzend zu Klausel 3 Abs. 2
- Ergänzung von Anhang **Klausel 5 h** um die Verpflichtung des Datenimporteurs, soweit dieser ihm bekannt ist auch den Betroffenen von der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zu benachrichtigen; Aufnahme dieser Ergänzung in die Drittbegünstigung, ergänzend zu Klausel 3 Abs. 2
- Ergänzung von **Klausel 6** um den Zusatz, dass die betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, nicht nur berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen, sondern auch vom Datenimporteur
- Aufnahme einer Verpflichtung des Datenimporteurs, den Betroffenen verschuldensunabhängig von allen Schäden freizustellen, die durch den Zugriff von Stellen seines Staates auf die Daten der Betroffenen entstehen.
- ✓ **überprüfen, ob Sie sich auf verbindliche interne Datenschutzvorschriften** gemäß Artikel 47 (Binding Corporate Rules BCRs) berufen können
- ✓ **überprüfen, ob als letztes Mittel die Übermittlung von Daten nach der Ausnahmevorschrift des Art. 49 DS-GVO in Betracht kommt**
- ✓ überprüfen, ob Sie alle Prüfungsschritte und Folgerungen dokumentiert haben und nachweisen können (Art. 5 Abs. 2 DS-GVO)

