Privacy Shield – Keine Rechtsgrundlage mehr für transatlantische Datentransfers

Online-Seminar

13. Oktober 2020

AUDIT & ADVISORY • TAX • LEGAL • CONSULTING

Überblick

Ausgangspunkt

- EuGH: „Schrems I“- Urteil, 6. Oktober 2015, Aufhebung der bisherigen Datenübertragungsregelung „Safe Harbor“ für Datentransfer in die USA
- Abkommen zwischen der EU und den USA zur neuen Regelung der Datenübertragung, 12. Juli 2016, „EU-US Privacy Shield“
- Zusicherung der US-Regierung, dass das Datenschutzniveau dem der EU entspricht
- Grundlage für Datentransfers entweder direkt oder als Basis für Standardvertragsklauseln (SCCs)
- Bedenken gegen dieses Abkommen wegen eventueller Verstöße gegen Grundrechte-Charta der EU durch potentielle Zugriffe von US-Behörden
- Vorlage an den EuGH zur Überprüfung der Rechtmäßigkeit

„Schrems II“ Urteil des EuGH

- Erklärung des **„EU-US-Privacy Shield“** als **ungültig**
- **Datenschutzrecht in den USA nicht gleichwertig** zu dem durch die DSGVO im Licht der EU-Grundrechte Charta garantierten Niveau
- **Überwachungsprogramme** der US-Behörden, insbesondere §702 FISA und Executive Order 12 333 sind **nicht auf das zwingend erforderliche Maß beschränkt**
- **Rechtmäßige Übertragung bedarf zusätzlicher Maßnahmen**, um ein angemessenes Schutzniveau sicherzustellen
- **Untersagung der aktuellen Übertragungsvorgänge** nach dem Privacy Shield durch die zuständigen Aufsichtsbehörden erforderlich

Konsequenzen des Urteils

- **Privacy Shield** ist **keine Rechtsgrundlage** mehr – Datenübertragungen auf dieser Grundlage nicht mehr rechtmäßig
- **Keine Übergangsfrist!**
- **SCCs** und **Binding Corporate Rules** (BCRs) bleiben **grundsätzlich weiterhin als Rechtsgrundlage** für Datentransfers geeignet
- **ABER** es obliegt dem Datenexporteur, eine **eigene Risikoanalyse** durchzuführen und ein **adäquates Datenschutzniveau sicherzustellen**. Dazu sind ggf. **SCCs / BCRs nicht ausreichend –** Zusatzmaßnahmen können nötig sein, ggf. ist der Datentransfer einzustellen.
- Konsequenzen gelten nicht nur für Datentransfers in die USA, sondern in jedes Nicht-EU-Land, das kein von der Kommission als ausreichend zertifiziertes Datenschutzniveau hat
- **Risiken: Bußgelder und Schadensersatzansprüche** der Datensubjekte in potentiell erheblicher Höhe

Reaktionen der Datenschutz-behörden

Die Reaktionen der Datenschutzbehörden sind uneinheitlich:

Europäischer Datenschutzausschuss (EDSA)

- Einzelfallprüfung des Schutzniveaus durch Verantwortliche erforderlich
- Zusätzliche Schutzmaßnahmen müssen ergriffen werden
- Einstellen der Datenübermittlung nach Privacy Shield
- Notifizierung der EDSA bei Fortsetzung des Datentransfers trotz einer negativen Einzelfallprüfung
- Geltung auch für SCCs
- Weitere Untersuchung, welche zusätzlichen Maßnahmen möglich und notwendig sind

Reaktionen der Datenschutz-behörden

Europäischer Datenschutzbeauftragter (EDPS)

- Prüfung der Auswirkungen des Urteils, insbesondere auch hinsichtlich der von EU-Institutionen geschlossenen Verträge

Bundesbeauftragter für Datenschutz und Informationsfreiheit

- SCCs weiterhin mögliche Grundlagen des Datentransfers
- Internationaler Datenverkehr weiterhin möglich, für Übermittlungen in die USA zusätzliche Schutzmaßnahmen erforderlich

Deutsche Datenschutzkonferenz

- SCCs können für eine Übermittlung personenbezogener Daten in die USA und andere Drittländer grundsätzlich weiter verwendbar
- Zumindest für die USA allerdings nur mit zusätzlichen oder alternativen Schutzmaßnahmen denkbar

Reaktionen der Datenschutz-behörden

Datenschutzbehörden Baden-Württemberg, Berlin, Niedersachsen, Rheinland-Pfalz, Thüringen

- SCCs nicht prinzipiell unwirksam, aber reiner Abschluss genügt nicht, da u. A. keine Bindung von US-Behörden
- Ergänzung der SCCs notwendig – technisch, rechtlich oder organisatorisch – keine Einzelheiten bekannt
- Intensive Einzelfallprüfung der nationalen Gesetze der Drittländer notwendig, nicht nur USA
- Kein US-amerikanisches Unternehmen kann glaubhaft garantieren, nicht dem Zugriff der Geheimdienste ausgesetzt zu sein
- Datenexporte auf Basis des Privacy Shields umgehend einstellen
- Neue Lösungen erforderlich, beispielsweise Verschlüsselung der Daten nachweislich ohne Überwindungsmöglichkeit der Geheimdienste oder Alternativdienste außerhalb der USA nutzen
- „Zurückholung“ übermittelter Daten notwendig

Enforcement durch NOYB

- **Max Schrems NGO „None of Your Business“ (NOYB) hat Beschwerde gegen 101 Unternehmen bei diversen Datenschutzbehörden eingereicht.**
- **Vorwurf:** Websites werden immer noch unter Verwendung von Google Analytics und Facebook Connect betrieben (entgegen „Schrems II“).
- **Konsequenz:** Datenschutzbehörden werden tätig werden müssen
- **Risiko:**
  - Weitere Beschwerden zu erwarten
  - Schaffung von Präzedenzfällen
  - Möglicherweise uneinheitliches Vorgehen der Datenschutzbehörden und gesteigerte Rechtsunsicherheit

Zwischen-ergebnis

- Das **politische Problem** der Diskrepanz zwischen europäischem und US-amerikanischem (oder anderen, z.B. China) Verständnis zu Datenschutz ist **auf die Unternehmen abgewälzt**.
- **Es fehlen klare Vorgaben** oder Hinweise, wie praktisch mit den Konsequenzen des Urteils umzugehen ist / **Rechtsunsicherheit**
- Kurzfristig/mittelfristig ist **keine politische Lösung in Sicht**
- Aktuell bleibt unklar, wie sich Unternehmen absichern können – außer den Datentransfer aus der EU einzustellen
- Einstellen von Datentransfers ist vielfach praktisch nur schwer oder gar nicht möglich.
- Einzelfallbezogen sind folgende Schritte nötig:
  - Risiken nicht auszuschließen aber Maßnahmen zur **Risikominimierung** sind zwingend
  - **Strategien zur Verteidigung** gegen mögliche Bußgelder oder Schadensersatzansprüche sind zu entwickeln

Was ist zu tun?

Basis für Risikominimierung und Verteidigungsstrategie

- **Einzelfallbezogene Bestandsaufnahme**
  - Welche Daten werden wohin und an wen transferiert und zu welchem Zweck?
  - Wie häufig und regelmäßig geschehen solche Datentransfers?
  - Was ist die bisherige Rechtsgrundlage? (Privacy Shield, SCCs, BCRs)
  - Ist bekannt, ob bereits behördliche Zugriffe auf Daten erfolgt sind?
  - Welche zusätzlichen Schutzmaßnahmen gibt es aktuell?

- **Einzelfallbezogene Risikoanalyse**
  - Wie sensitiv sind die Daten?
  - Wie ist die Rechtslage im Empfängerstaat? Beispiel USA: Sec. 702 FISA, Executive Order 12 333, Hong Kong Security Law etc.
  - Ist eine Einschätzung möglich, ob die Daten für Behörden im Empfängerstaat von (gesteigertem) Interesse sind?
  - Einfluss zusätzlicher Schutzmaßnahmen auf Zugriffs-Risiko bzw. Schutzniveau

Was ist zu tun?

- **Rechtsgrundlage:**
  - SCCs oder BCRs
  - Art. 49 DSGVO, aber nur im Einzel- bzw. Ausnahmefall
- **Mögliche (Zusatz-)Maßnahmen?**
  - Verlagerung der Daten in die EU
  - Verschlüsselung der Daten
  - Anonymisierung der Daten
  - Zusatzvereinbarungen zu SCCs, z.B.
    - Freistellung
    - Mitteilungs- und Koordinationspflichten
- **Dokumentation und Transparenz**
  - Vollständig und nachvollziehbare Dokumentation aller Schritte
  - Information der Datensubjekte / Zustimmungen im Einzelfall

Was ist zu tun?

- **Rechtsgrundlage:**
  - SCCs oder BCRs
  - Art. 49 DSGVO, aber nur im Einzel- bzw. Ausnahmefall
- **Mögliche (Zusatz-)Maßnahmen?**
  - Verlagerung der Daten in die EU
  - Verschlüsselung der Daten
  - Anonymisierung der Daten
  - Zusatzvereinbarungen zu SCCs, z.B.
    - Freistellung
    - Mitteilungs- und Koordinationspflichten
- **Dokumentation und Transparenz**
  - Vollständig und nachvollziehbare Dokumentation aller Schritte
  - Information der Datensubjekte / Zustimmungen im Einzelfall
  - In Ausnahmefällen ggf. Information der Datenschutzbehörden

Fazit

- Derzeit keine Rechtssicherheit in Bezug auf Datentransfers aus der EU in die USA (und ggf. andere Drittstaaten)
- Rechtssicherheit kurz-/mittelfristig unwahrscheinlich
- Hohe Haftungsrisiken sind die Konsequenz
- Risikominimierung und vorausschauende Strategie zwingend erforderlich

Für Ihre Fragen stehen wir gerne zur Verfügung.

Dr. Christian Engelhardt

Rechtanwalt
Partner

Baker Tilly

Valentinskamp 88
20355 Hamburg

T: +49 40 600880-454
F: +49 40 600880-101

christian.engelhardt@bakertilly.de

bakertilly.de

Ihre Meinung ist uns wichtig

www.bakertilly.de/feedback