audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Handlungsempfehlung nach EuGH Urteil zu EU-US Privacy-Shield

Zusammenfassung

Mit Urteil vom 16.07.2020 hat der EuGH den Beschluss der Europäischen Kommission (EU) 2016/1250 besser bekannt als der „EU-US Privacy Shield“, kurz Privacy Shield für ungültig erklärt. Das EuGH-Urteil gilt sinngemäß auch für das parallele Abkommen über den US-Swiss Privacy Shield.

Eine Übergangsfrist gibt es nicht. Sowohl die Übermittlung personenbezogener Daten aus der EU wie auch aus der Schweiz in die USA ist damit ab dem 16.07.2020 nicht mehr ohne weiteres zulässig und unterliegt damit auch hinsichtlich derjenigen Empfänger, die bislang unter Privacy Shield zertifiziert waren, besonderen Anforderungen. Der EuGH entschied zugleich, dass die Standardvertragsklauseln weiterhin grundsätzlich gültig sind. Es ist jedoch Sache des Unternehmens welches personenbezogene Daten in die USA übermittelt sowie des Empfängers der personenbezogenen Daten in den USA, zu ermitteln, ob die betroffenen Personen auf Grundlage der Standardvertragsklauseln ein „Schutzniveau genießen, das dem in der Union durch die DS-GVO […] gleichwertig ist.“ Sollte dies nicht der Fall sein, ist der Datentransfer auszusetzen, wenn der nach dem Unionsrecht erforderliche Schutz auch nicht mit anderen Mitteln gewährleistet werden kann. Den zuständigen Aufsichtsbehörden kommt hierbei eine maßgebliche Rolle zu. Diese können im beschriebenen Fall den Transfer verbieten, sollte dieser nicht ausgesetzt werden.

Über die Legitimierung der Übermittlung in die USA hinaus erwächst Unternehmen in der EU sowie in der Schweiz jedoch weiterer Handlungsbedarf. Dieser soll im Folgenden samt Optionen zur Reduzierung der durch die Entscheidung entstandenen Problematik aufgezeigt werden.

Problemstellung

Die Entscheidung des EuGH ist nur für wenige Unternehmen unproblematisch.

Unternehmensstandorte sowie der Betrieb kritischer Teile der IT-Infrastruktur des Unternehmens in den USA führen nach der Entscheidung des EuGH zu deutlich gestiegenen Compliance-Risiken. Zugleich kann eine Übermittlung personenbezogener Daten in die USA in den beschriebenen Fällen nicht ohne weiteres ausgesetzt werden, ohne dass sich hieraus Risiken für das laufende Geschäft ergeben.

Es besteht damit akuter und dringender Handlungsbedarf, sollen die Risikoauswirkungen der Entscheidung des EuGH zumindest kurz- bis mittelfristig bestmöglich reduziert werden ohne das die gegenwärtigen Geschäftstätigkeiten mit den USA durch die Aussetzung eines Transfers personenbezogener Daten ausgesetzt werden.

Lösungsansatz bei Datenübermittlung in die USA in 12 Schritten

Jedes Unternehmen sollte prüfen, ob im Rahmen der eigenen Geschäftstätigkeit personenbezogene Daten ins Drittland übermittelt werden. Aufgrund der Stellung der USA als einer der weltweit relevantesten Handelspartner außerhalb Europas wird dies auf zahlreiche Unternehmen zutreffen.

Ist die Übermittlung personenbezogener Daten in die USA bestätigt, ergibt sich folgender Handlungsbedarf in absteigender Priorität:

1. **Identifikation der konkreten Empfänger:**
   Es sollte geprüft werden, welche Empfänger personenbezogener Daten des Unternehmens ihren Sitz in den USA haben. Eine Liste der IT-Tools hilft hier rasch die kritischen Tools des Unternehmens zu identifizieren und dahingehend zu überprüfen. Typische

Empfänger sind AWS, Microsoft, Google, Hubspot oder Salesforce. Besondere Aufmerksamkeit sollten aufgrund der Sensibilität der mit ihnen verarbeiteten personenbezogenen Daten auch die durch das Unternehmen eingesetzten HR-Tools erfahren. Die Identifikation der Empfänger sollte jedoch nicht bei einer Überprüfung der durch externe Dienstleister bereitgestellten Tools verharren, sondern auch gruppeninterne Empfänger einbeziehen. US-Standorte, die auf Tools in der EU/Schweiz und darüber auf personenbezogene Daten zugreifen, die der DS-GVO unterliegen sollten, ebenfalls Berücksichtigung finden.

2. **Legitimierung der Übermittlung:**
   Die Rolle der Empfänger in den USA sollte daraufhin bewertet werden, ob es sich um weitere Verantwortliche oder Auftragsverarbeiter handelt. In Abhängigkeit der Rolle der Empfänger in den USA sollten mit diesen die entsprechenden Standardvertragsklauseln (Controller to Controller bei anderen Verantwortlichen bzw. Controller to Processor im Fall von Auftragsverarbeitern) abgeschlossen werden.

3. **Berücksichtigung bei Auswahl von Dienstleistern:**
   Soweit möglich sollten bis auf weiteres keine Auftragsverarbeiter mehr mit Sitz in den USA ausgewählt werden, damit die gegenwärtig bestehende Problematik für das Unternehmen nicht vergrößert wird.

4. **Anpassung der Informationsblätter:**
   Die Datenschutzinformationen des Unternehmens, hier insbesondere die Datenschutzerklärung auf der Webseite, sollten angepasst und Hinweise auf eine Legitimierung der Übermittlung via Privacy Shield entfernt werden.

5. **Anpassung der Vorlagen von Auskunftsverlangen:**
   Soweit Privacy Shield im Rahmen der Vorlagen zu Auskunftsverlangen Berücksichtigung findet, sollten die entsprechenden Vorlagen überprüft und der Hinweis auf Privacy Shield entfernt werden.

6. **Anpassung von Datenschutzfolgeabschätzungen:**
   Soweit Privacy Shield im Rahmen von Datenschutzfolgeabschätzungen (z.B. zum Thema Whistleblowing-Hotlines) Berücksichtigung gefunden hat, sollte die Datenschutzfolgeabschätzung überprüft, der Hinweis auf Privacy Shield entfernt und das Risiko neu bewertet werden.

7. **Anpassung von Verträgen:**
   Die Vertragswerke des Unternehmens sollten darauf geprüft werden, ob in Verträgen Bezug auf Privacy Shield genommen wird. Sollte dies der Fall sein, sollte kurzfristig in den entsprechenden Templates die Klausel angepasst werden, bei Neuabschlüssen/Neuverhandlungen sollte diese auch im Rahmen laufender Geschäftsbeziehungen entfallen.

8. **Anpassung von Richtlinien:**
   Richtlinien des Unternehmens, die Bezug auf Privacy Shield nehmen, sollten überarbeitet, die entsprechenden Hinweise entfernt und eine erneuerte Fassung der Richtlinie verabschiedet werden.

9. **Anpassung von Interessensabwägungen:**
   Soweit Privacy Shield im Rahmen von Interessensabwägungen zu Art. 6 Abs. 1 S. 1 lit. f) DS-GVO Berücksichtigung gefunden hat, sollten diese überprüft, der Hinweis auf Privacy Shield entfernt und die Interessensabwägung neu bewertet werden.

10. **Anpassung des Verzeichnisses der Verarbeitungstätigkeiten:**
    Im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten ist zu berücksichtigen, dass Privacy Shield nicht länger als Mechanismus der Legitimierung einer Übermittlung benannt werden kann.

11. **Anpassung der Risikobewertung von Dienstleistern:**
    Die Risikobewertung der gegenwärtig eingesetzten Dienstleister sollte nach dem Fall von Privacy Shield überprüft und unter Berücksichtigung der beschriebenen Problematik – einschließlich jener, die mit Verwendung der Standardvertragsklauseln verbunden ist- erhöht werden.

12. **Beobachtung der Rechtslage:**
    Nach ersten Stellungnahmen der deutschen Aufsichtsbehörden ist zeitnah ein Austausch zur Entscheidung des EuGH auf europäischer Ebene beabsichtigt. Zu erwarten ist insbesondere eine Empfehlung zur Überarbeitung der Standardvertragsklauseln durch die Europäische Kommission. Letztere arbeitet nach eigenem Bekunden bereits an alternativen Instrumenten für die internationale Übermittlung personenbezogener Daten.

    Die Entwicklung der Rechtslage sollte daher dringend beobachtet werden, um zeitnah auf relevante Änderungen reagieren zu können.

Hinweis auf unseren 90-minütigen Web-Workshop zum EuGH Urteil und den konkreten Handlungsempfehlungen, welcher am 05. August 2020 um 9:00 Uhr stattfindet:

https://www.audatis.de/trainings/veranstaltungen/details.php?vid=322

Autor und Ansprechpartner

Jannik Wallbaum
Senior Legal Consultant Datenschutz

Schwerpunkte: Internationaler Datenschutz, Datenschutzrecht, Compliance und Risikomanagement

Mail: j.wallbaum@audatis.de
Fon: 05221 87292-09

Haben Sie noch Fragen?

Wir haben versucht, alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Wir unterstützen Sie gerne bei der Umsetzung von internationalen Datenschutzvereinbarungen, der Betreuung von internationalen Unternehmensgruppen und der Beantwortung aller Fragen in Bezug auf die pragmatische Umsetzung der Anforderungen des EU-Datenschutzes und der Informationssicherheit.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de