DataGuard

Whitepaper

Zur Entscheidung des Europäischen Gerichtshofs (EuGH) am 16. Juli 2020 in der Sache „Schrems II"

EMPFEHLUNGEN ZUM INTERNATIONALEN DATENAUSTAUSCH

EINLEITUNG

Die Entscheidung des Europäischen Gerichtshofs (EuGH) am 16. Juli 2020 in der Sache „Schrems II“ hat mit seinen weitreichenden Auswirkungen auf den internationalen Datenaustausch auch außerhalb des Datenschutzes große Wellen geschlagen. Doch was sind die konkreten Konsequenzen der Schrems II-Entscheidung? Was müssen Unternehmen und Organisationen künftig bei Datentransfers in die USA aber auch in andere sogenannte Drittländer beachten? Und welche Maßnahmen sollte ich als datenverarbeitende Stelle konkret ergreifen?

Diesen Fragen widmen wir uns im vorliegenden Whitepaper, ohne dabei Anspruch auf Vollständigkeit oder abschließende Antworten zu erheben. Im Fokus stehen in erster Linie die erwartbaren praktischen Auswirkungen sowie praxisnahe Maßnahmen zur Minimierung von möglichen Risiken. Natürlich sind auch andere Auslegungen des Urteils und der damit einhergehenden Auswirkungen möglich – dies zeigen allein schon die teils unterschiedlichen Ansichten europäischer Datenschutzbehörden zu diesem Thema. Nichtsdestotrotz sind wir überzeugt, dass wir vorliegend einen vertretbaren und vor allem praxistauglichen Mittelweg beschreiten.

Viel Spaß bei der Lektüre!

Andreas Rübsam

Dipl.-Informatiker (FH),
Datenschutzbeauftragter (udisZert)
Head of Privacy (SMB)

Dr. Frank Schemmel

Dipl. iur. oec. univ.,
CIPP/E, Datenschutzbeauftragter (TÜV)
Head of Privacy (Corporate)

AUF EINEN BLICK – 11-PUNKTE-PLAN ZUR MINIMIERUNG VON RISIKEN

Folgende Maßnahmen kommen ggf. für Ihr Unternehmen oder Ihre Organisation zur Reduzierung möglicher Risiken in Verbindung mit der Schrems-II-Entscheidung in Betracht. Die einzelnen Maßnahmen werden weiter unten in einem eigenen Kapitel ausführlicher beschrieben.

01 Prüfung möglicher Einschränkung/ Beendigung der Drittlandübermittlung (insb. in die USA)

02 Wechsel von Privacy Shield zu Standarddatenschutzklauseln

03 Implementierung weiterer technischer Maßnahmen vor Drittlandübermittlung (insb. in die USA)

04 Weisungen und Aufforderungen an alle Datenimporteure (insb. Auftragsverarbeiter)

05 Weisungen und Aufforderungen speziell an Auftragsverarbeiter und Unterauftragsverarbeiter

06 Verwendung zusätzlicher Vertragsklauseln für Auftragsverarbeitungsverträge und SCC

07 Nutzung der Ausnahmeregeln in Art. 49 DS-GVO

08 Erwägung von Alternativanbietern

09 Prüfung und Anpassung von Binding Corporate Rules (BCR)

10 Prüfung und Anpassung der Datenschutzerklärungen (insb. auf Websites und Apps)

11 Aktualisierung der Verfahrensverzeichnisse

WARUM BETRIFFT DAS URTEIL MEIN UNTERNEHMEN?

Vielen ist nicht bewusst, dass das Urteil des EuGH aufgrund der Globalisierung und Digitalisierung Auswirkungen für fast jedes Unternehmen, jede Organisation oder jede Behörde hat. Selbst wenn aktiv keine personenbezogenen Daten in Länder außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraum (EWR) übermittelt werden (diese Länder werden im Datenschutz als „Drittland“ bezeichnet), setzen die meisten Unternehmen entweder Dienstleister ein, deren Server oder Sub-Unternehmer in Drittländern liegen, oder eine solche Übermittlung erfolgt passiv bzw. unbewusst.

WAS IST ÜBERHAUPT EINE DATENÜBERMITTLUNG?

Der Begriff der Übermittlung ist weder in der Datenschutz-Grundverordnung (DS-GVO) noch im Bundesdatenschutzgesetz (BDSG) definiert.

Gemeint ist in diesem Zusammenhang jeder Datenverarbeitungsvorgang, bei dem personenbezogene Daten außerhalb des Geltungsbereichs der DS-GVO gebracht werden und bei dem die Endbestimmung der Daten außerhalb der EU/des EWR liegt oder bei dem die Daten von außerhalb der EU/des EWR zugänglich sind.

Eine Datenübermittlung im Sinne einer solchen Offenlegung kann also z. B. in der (aktiven) Weitergabe, aber auch bereits in der Zugänglichmachung oder faktischen Abrufbarkeit von Daten aus dem Drittland vorliegen (z. B. bei Schnittstellen von Dienstleistern zu eigenen Systemen oder bei der Fernwartung). Letzteres ist vielen Praxisanwendern oft nicht bekannt. Es genügt auch ein einfaches Speichern von Daten auf Servern (z. B. Cloud-Diensten), die im Drittland liegen sowie eine sonstige Bereitstellung von Daten gegenüber Empfängern im Drittland.

Die Art und Weise der Übermittlung spielt hingegen keine Rolle, sodass die Übermittlung z. B. schriftlich, elektronisch, mündlich oder auch durch Übergabe eines Datenträgers erfolgen kann.

DARF ICH EINFACH SO DATEN INS AUSLAND ÜBERMITTELN?

Nein, hier gilt es datenschutzrechtlich besondere Anforderungen einzuhalten. Die DS-GVO sieht für die Übermittlung personenbezogener Daten in ein Land außerhalb der EU/des EWR besondere Regelungen (Art. 44–49) vor. Hier hat eine zweistufige Prüfung zu erfolgen:

Bei der Datenübermittlung in ein Drittland muss zunächst überprüft werden, ob unabhängig von den spezifischen Anforderungen an die Datenübermittlung in Drittländer auch alle übrigen Anforderungen der DS-GVO an die betreffende Datenverarbeitung eingehalten werden. Einfach gesagt: Zuerst muss geprüft werden, ob eine Rechtsgrundlage für die Verarbeitung (= Übermittlung) an sich vorliegt (1. Stufe). Wenn einer Verarbeitung nichts entgegensteht, müssen gemäß Art. 44 DS-GVO anschließend die in den Art. 45 ff. DS-GVO genannten spezifischen Anforderungen an die Übermittlung in Drittländer beachtet werden (2. Stufe). Eine Datenübermittlung in ein Drittland ist dann nur zulässig, wenn dort ein angemessenes, mit der DS-GVO vergleichbares Datenschutzniveau vorliegt bzw. wenn durch spezifische Maßnahmen ein solches Niveau erreicht werden kann.

Die DS-GVO sieht für Datentransfers in Drittländer dabei folgende Möglichkeiten vor:

- **Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Art. 45 DS-GVO) – z. B. das nunmehr durch den EuGH verworfene EU-US Privacy Shield; solche Angemessenheitsbeschlüsse existieren derzeit bspw. für Argentinien, Kanada, Japan, Neuseeland oder die Schweiz**
- **Vorliegen geeigneter Garantien (Art. 46 DS-GVO) – z. B. Standarddatenschutzklauseln (SCC) oder Binding Corporate Rules (BCR)**
- **Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO) – z. B. Einwilligung, Erforderlichkeit zur Vertragserfüllung oder Verfolgung von Rechtsansprüchen**

WAS HAT DER EUGH GENAU GEURTEILT?

Der EuGH hat sich in der Sache „Schrems II“ insbesondere zur Frage der Angemessenheit des Datenschutzniveaus in den USA geäußert. Dabei wurde der entsprechende Angemessenheitsbeschluss der EU-Kommission, das sogenannte EU-US Privacy Shield, überprüft und im Ergebnis für nichtig erklärt. Außerdem wurde die Frage nach der Gültigkeit von Standarddatenschutzklauseln (SCC) als geeignete Garantie in dieser Konstellation bewertet.

WARUM IST DAS PRIVACY SHIELD NUN UNWIRKSAM?

Seitens des EuGH wurde – wenig überraschend – festgestellt, dass aufgrund der gesetzlichen Zugriffsbefugnisse US-amerikanischer Sicherheitsbehörden auf übermittelte personenbezogene Daten in die USA kein der EU vergleichbares Schutzniveau vorliegt. Den betroffenen Personen stehen auch keine wirksamen Rechtsbehelfe gegen derlei Maßnahmen zur Verfügung. Aus diesem Grund hat der EuGH das Privacy Shield für nichtig erklärt. Diese Nichtigkeit gilt ohne Übergangsfrist ab sofort.

WAS SIND NACH DEM EUGH DIE ANFORDERUNGEN AN DATENÜBERMITTLUNGEN OHNE ANGEMESSENHEITSBESCHLUSS?

Bei fehlendem Angemessenheitsbeschluss dürfen entsprechend der Vorgaben in Art. 46 Abs. 1 DS-GVO nach Ansicht des EuGH personenbezogene Daten nur dann an ein Drittland übermittelt werden, wenn der Datenexporteur folgende drei Punkte gewährleistet:

01	02	03
Geeignete Garantien (diese können bspw. die SCC sein)	**Durchsetzbare Rechte** für betroffene Personen (z. B. Recht auf Auskunft oder Löschung)	**Wirksame Rechtsbehelfe** für betroffene Personen (z. B. Klage vor ordentlichen Gerichten)

Zusätzlich müssen Sie folgende Dinge berücksichtigen:

- Vertragliche Regelungen zwischen Datenexporteur (das in der EU/dem EWR ansässige Unternehmen) und Datenimporteur im Drittland (Empfänger der Daten)
- Ggf. Behördenzugriffe
- Elemente der Rechtsordnung im betreffenden Drittland

ERFÜLLEN DIE AKTUELLEN STANDARDDATENSCHUTZ-KLAUSELN (SCC) DIESE ANFORDERUNGEN?

Jein. Die SCC wurden durch den EuGH nicht grundsätzlich für unwirksam erklärt und können damit auch weiterhin in manchen Situationen ein wirksames Transferinstrument darstellen. Der EuGH differenziert hier im Ergebnis nach zwei Konstellationen:

Konstellation 1:

Das angemessene Datenschutzniveau kann **allein** aufgrund der SCC durch den Datenimporteur gewährleistet werden.

Konstellation 2:

Die in den SCC per se enthaltenen Bestimmungen sind alleine **nicht ausreichend**, um effektiv ein angemessenes Datenschutzniveau im jeweiligen Drittland zu gewährleisten, bspw. weil Gesetze im Drittland Behörden oder sonstigen Stellen unverhältnismäßige Eingriffe in die Rechte der betroffenen Personen erlauben.

WELCHE PFLICHTEN HAT DER EUGH DEM DATENEXPORTEUR UND DATENIMPORTEUR AUFERLEGT?

Nach Ansicht des EuGH kann es in der Konstellation 2 aufgrund der offenen und allgemeinen Formulierung der SCC je nach konkreter Lage im betreffenden Drittland erforderlich sein, über die SCC hinausgehende, zusätzliche Maßnahmen zu ergreifen, um die Einhaltung eines angemessenen Schutzniveaus zu gewährleisten.

Deswegen muss jeder Datenexporteur einzelfallbezogen und ggf. in Zusammenarbeit mit dem Datenimporteur prüfen:

- ob die SCC in unveränderter Form (Konstellation 1) zum Einsatz kommen können
- oder ob aufgrund der Rechtslage im betreffenden Drittland kein angemessenes Datenschutzniveau gewährleistet werden kann und deshalb über die SCC hinaus zusätzliche Garantien vereinbart werden müssen (Konstellation 2).

Konkret bedeutet dies:

01 **Prüfung ob die SCC unverändert verwendet werden können.**
Dabei sind folgende Fragen zu berücksichtigen:

a. Kann der Empfänger der Daten im Drittland alle SCC-Pflichten auch tatsächlich erfüllen und gewährleisten?
b. Sind Zugriffe durch Sicherheitsbehörden oder andere Stellen in dem betreffenden Drittland zumindest möglich?
c. Wenn ja: Sind diese Zugriffe tatsächlich grundsätzlich angemessen (insbesondere geeignet und erforderlich), um eines der in Art. 23 Abs. 1 DS-GVO aufgezählten Ziele zu erreichen?

02 **Vereinbarung/Umsetzung zusätzlicher Maßnahmen.**
Maßnahmen können dabei

a. vertraglicher
b. organisatorischer oder
c. technischer Art sein.

WAS SIND DIE KONKRETEN KONSEQUENZEN DES URTEILS FÜR MEINE ORGANISATION/ FÜR MEIN UNTERNEHMEN?

Die Folgen der Schrems-II-Entscheidung können sein, dass eventuelle Übermittlungen personenbezogener Daten in Länder außerhalb der EU/des EWR datenschutzrechtlich nicht mehr zulässig sind. Somit können Haftungs-, Sanktions- und Reputationsrisiken bestehen. Deswegen müssen folgende 5 Schritte durchgeführt werden:

1. IDENTIFIKATION UND AUFLISTUNG ALLER DATENFLÜSSE IN DRITTLÄNDER

Machen Sie eine gründliche Inventur Ihrer Prozesse und Verarbeitungsvorgänge und identifizieren Sie dabei alle Transfers personenbezogener Daten in Drittländer. Beschränken Sie sich dabei nicht nur auf die USA, sondern prüfen Sie auch andere Drittländer mit wahrscheinlich unzureichendem Datenschutzniveau und unzureichendem Schutz individueller Rechte betroffener Personen (z. B. China, Indien, Russland, Philippinen etc.).

2. IDENTIFIKATION VON DATENÜBERMITTLUNGEN AUF GRUNDLAGE DES PRIVACY SHIELDS

Prüfen Sie umgehend, welche Datenverarbeitungen mit Ihren Vertragspartnern eine auf dem Privacy Shield basierende Übermittlung personenbezogener Daten in die USA vorsehen, und erstellen Sie eine entsprechende Liste.

Sollten Sie bei der Prüfung Hilfe benötigen, senden Sie uns diese Verträge gern zur Prüfung zu.

3. IDENTIFIKATION VON DATENÜBERMITTLUNGEN AUF GRUNDLAGE VON STANDARDDATENSCHUTZKLAUSELN (SCC)

Prüfen Sie umgehend, welche Datenverarbeitungen mit Ihren Vertragspartnern eine auf SCC basierende Übermittlung personenbezogener Daten in Drittländer vorsehen, und erstellen Sie eine entsprechende Liste.

Sollten Sie bei der Prüfung Hilfe benötigen, senden Sie uns diese Verträge gern zur Prüfung zu.

4. IDENTIFIKATION VON DRITTLÄNDERN UND EMPFÄNGERN MIT KRITISCHEM DATENSCHUTZNIVEAU

Prüfen und dokumentieren Sie das grundsätzlich bestehende Datenschutzniveau im Empfängerstaat und insbesondere das Risiko und die Verhältnismäßigkeit behördlicher Zugriffsmöglichkeiten. Außerdem sollten Sie die Garantie eines funktionierenden und auf den jeweiligen Empfänger bzw. dessen Sektor bezogenen Rechtsschutzes beachten. Erstellen Sie eine abgestufte Liste der kritischen Länder und Empfänger.

5. IDENTIFIKATION ZUSÄTZLICHER VERTRAGLICHER, TECHNISCHER UND/ODER ORGANISATORISCHER MASSNAHMEN ZU SCC

Identifizieren und implementieren Sie basierend auf den vorhergehenden Risikobewertungen geeignete vertragliche, technische und/oder organisatorische Maßnahmen (siehe nachfolgender Abschnitt). So gewährleisten Sie die rechtskonforme Datenübermittlung und ein angemessenes Datenschutzniveau beim konkreten Empfänger im Drittland. Dokumentieren Sie diese Maßnahmen schriftlich und überprüfen Sie deren Einhaltung bzw. fordern Sie regelmäßig Nachweise dazu an. Dokumentieren Sie zudem ausführlich die Angemessenheit und Eignung der vertraglich vereinbarten Schutzmaßnahmen, die getroffenen technischen und organisatorischen Maßnahmen, die nationale Gesetzeslage im Drittland und warum diese Maßnahmen aus Ihrer Sicht ein angemessenes Datenschutzniveau gewährleisten.

Sollten Sie bei der Prüfung Hilfe benötigen, senden Sie uns diese Verträge gern zur Prüfung zu.

WELCHE MASSNAHMEN ZUR RISIKOMINIMIERUNG STEHEN DERZEIT ZUR VERFÜGUNG?

PRÜFUNG MÖGLICHER EINSCHRÄNKUNG/BEENDIGUNG DER DRITTLANDÜBERMITTLUNG (INSB. IN DIE USA)

Prüfen Sie umgehend, ob und in welchem Umfang Sie die Verarbeitung personenbezogener Daten auf die EU/den EWR oder andere Länder mit angemessenem Datenschutzniveau beschränken können bzw. ob Sie eine Übermittlung in die USA und/oder andere Drittländer zumindest für einen Teil der personenbezogenen Daten/Datensätze beenden können.

WECHSEL VON PRIVACY SHIELD ZU STANDARD-DATENSCHUTZKLAUSELN (SCC)

Wechseln Sie umgehend von Privacy Shield als Grundlage für die Datenübermittlung zu den SCC. Schließen Sie unverzüglich die entsprechenden SCC mit Ihren Vertragspartnern ab.

Ergänzen Sie die SCC um geeignete Garantien für ein angemessenes Datenschutzniveau.

Hierzu können Sie beispielsweise unsere unten aufgeführten Klauselvorschläge verwenden. Sollten Sie dabei Unterstützung benötigen, stehen wir Ihnen gern zur Verfügung.

IMPLEMENTIERUNG WEITERER TECHNISCHER MASSNAHMEN VOR DRITTLANDÜBERMITTLUNG (INSB. IN DIE USA)

Implementieren Sie weitere technische Maßnahmen, bevor personenbezogene Daten Empfängern in Drittländern zur Verfügung gestellt werden (insbesondere Auftragsverarbeitern wie US-amerikanische Cloud-Service- oder Zahlungsanbieter). Hierzu kommen insbesondere Maßnahmen wie Verschlüsselung, Pseudonymisierung oder Zugriffsbeschränkungen in Betracht. Im Fokus sollte stehen, dass die Übermittlung personenbezogener Daten organisatorisch oder technisch so stark wie möglich minimiert wird. Stellen Sie dabei unbedingt sicher, dass der Schlüssel zur Verschlüsselung allein bei Ihnen verbleibt. Asymmetrische Verschlüsselungsverfahren nach aktuellem Stand der Technik sind z. B. curve25519, curve448 oder ECC-Brainpool.
Prüfen Sie auch, ob Sie dafür sorgen können,

- dass nur telemetrische Daten oder Metadaten, aber keine personenbezogenen Daten in Drittländer gesendet bzw. auf Servern gespeichert werden, auf die aus Drittländern zugegriffen werden kann.
- dass lediglich Hashwerte der personenbezogenen Daten in ein Drittland gesendet werden (Hashverfahren nach aktuellem Stand der Technik sind z. B. SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384 oder SHA3-512).
- dass nur zwingend notwendige Website-Plugins verwendet werden. Unterbinden Sie z. B. einen Datenversand an Google durch Google Webfonts, indem Sie die gewünschte Schriftart direkt auf Ihrem Server ablegen.
- dass Daten auf solchen Servern nur während der Verarbeitung gespeichert und danach gelöscht werden. Achten Sie dabei besonders auf die Speicherung und Löschung technischer Daten und die Löschung von Buffern, Backups usw.

In diesem Zusammenhang sollten auch folgende Möglichkeiten der bekannten Cloud-Service-Anbieter in Betracht gezogen werden:

- **Microsoft** hat zwei neue Rechenzentren in Deutschland (Frankfurt am Main und Magdeburg) aufgebaut, auf die Sie zur Risikominimierung wechseln können. Diese sind seit Dezember 2019 produktiv und werden nicht von Microsoft selbst, sondern von T-Systems als „Data Trustee“ betrieben. Die beiden Rechenzentren spiegeln sich gegenseitig und bieten damit eine geeignete Sicherheit vor Systemausfällen.
  Folgende Regelungen charakterisieren das Modell:
  - Der Treuhändler T-Systems kontrolliert den Zugriff auf Kundendaten, sofern Zugriffsrechte nicht vom jeweiligen Kunden oder Endbenutzer gewährt werden.

- Microsoft wird der Zugriff auf Kundendaten nur in vertraglich festgelegten Fällen unter der Aufsicht des Datentreuhänders oder des Kunden gewährt.
- Microsoft verwaltet alle Aspekte des Betriebs und der Bereitstellung der Azure-Dienste, die keinen Zugang zu Kundendaten erfordern, und bleibt gegenüber seinen Kunden über Service Level Agreements (SLAs) verantwortlich.
- Es gibt keine Verbindung zu anderen globalen Cloud-Diensten von Microsoft.
- Azure Deutschland weist verschiedene Testate und Zertifikate vor, beispielsweise das C5-Testat des Bundesamtes für Sicherheit in der Informationstechnik, BSI („Cloud Computing Compliance Controls Catalogue“) und die Zertifizierung gemäß der Norm ISO/IEC 27001.

- **Amazon Web Services (AWS)** weist wie Microsoft eine ISO/IEC 27001-Zertifizierung auf, auch für die AWS-Rechenzentren in Berlin, Frankfurt und München. Es ist generell für AWS-Kunden möglich, die eigene Datenhoheit durch eine entsprechende Konfiguration im Kunden-Account zu verstärken und den Zugriff auf Daten nach geografischen Gesichtspunkten einzuschränken. Ebenso ist es möglich, die Verschlüsselung von Daten zu erzwingen. Kunden können dabei – wie als bewährte Praxis aus Sicht der Informationssicherheit ohnehin anzuraten – ihre eigenen Schlüssel clientseitig einsetzen und müssen nicht auf serverseitige Schlüssel von Amazon zurückgreifen. Natürlich setzt dies entsprechendes Vertrauen in die eigenen Schlüssel voraus. Ein Treuhänder-Prinzip wie bei Microsoft ist bei Amazon jedoch nicht verfügbar.

- **Google** hat die Funktion „Google Confidential Computing“ vorgestellt, welche eine Erweiterung von Verschlüsselungsmaßnahmen bei Google-Services bei ruhenden, versendeten und sich in Verarbeitung befindenden Daten darstellt. Google hat dabei nach eigenen Angaben keinen Zugriff auf die zur Verschlüsselung eingesetzten Schlüssel – diese sind allein im Besitz des Kunden. Eine ISO/IEC 27001-Zertifizierung weist die Google Cloud ebenfalls auf. Wir empfehlen Ihnen, die neue Funktion zu prüfen und ggf. zu implementieren.

WEISUNGEN UND AUFFORDERUNGEN AN ALLE DATENIMPORTEURE (INSB. AUFTRAGSVERARBEITER)

Fordern Sie umgehend alle Ihre Auftragsverarbeiter und/oder Vertragspartner, die personenbezogene Daten in die USA übermitteln, mit Fristsetzung auf, Ihnen unverzüglich:

a) mitzuteilen, ob der Auftragsverarbeiter und/oder Vertragspartner im Drittland gesetzlichen Anforderungen unterliegt, die die Erfüllung der von den abgeschlossenen Verträgen (AVVs, BCR, SCCs) geforderten Garantien voraussichtlich in erheblichem Maße beeinträchtigen könnten.
b) mitzuteilen, ob, inwieweit und auf welcher konkreten Grundlage (z. B. Freedom Act, Foreign Intelligence Surveillance Act (FISA) 702, US Executive Order 12333, Gramm–Leach–Bliley Act (GLBA), the Dept of Homeland Security Act of 2002, Public Law 110-53) diese Datenempfänger innerhalb oder außerhalb der USA Eingriffsbefugnissen von US-Behörden und/oder Geheimdiensten unterliegen.
c) zu bestätigen, dass die Datenempfänger die nach den SCC geforderten Maßnahmen und das entsprechende Datenschutzniveau einhalten.
d) angemessen dokumentierte Informationen und Nachweise für Punkt c. zuzusenden.

Oben genannte Maßnahmen sind leider in den meisten Fällen nur theoretische Möglichkeiten und aufgrund bestehender US-Gesetze höchstwahrscheinlich praktisch nicht vollständig umsetzbar. Sie tragen aber dazu bei, Ihr Haftungsrisiko im Innenverhältnis zum Auftragnehmer ggf. zu reduzieren, indem Sie einer Aufsichtsbehörde nachweisen können, dass Sie in Ihrer Hand liegende Schritte unternommen haben, um Verstöße gegen das Datenschutzrecht so weit wie möglich zu vermeiden.

WEISUNGEN UND AUFFORDERUNGEN AN AUFTRAGS-VERARBEITER UND UNTERAUFTRAGSVERARBEITER

a) Weisen Sie alle Auftragsverarbeiter, die personenbezogene Daten unter dem Privacy Shield in die USA übermitteln oder dort verarbeiten, umgehend schriftlich/per E-Mail (wie im entsprechenden Vertrag gefordert) an, 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.
b) Verlangen Sie von all Ihren Auftragsverarbeitern, die personenbezogene Daten unter dem Privacy Shield in die USA übermitteln, unverzüglich auf eigene Kosten alle notwendigen Schritte zu unternehmen, um so schnell so wie möglich geeignete Alternativmechanismen zu etablieren, die eine rechtmäßige Übermittlung personenbezogener Daten in die USA unterstützen.

Bevor Sie zur Aussetzung der Datenübermittlung in die USA auffordern, prüfen Sie unbedingt die entsprechenden Verträge: Berechtigen diese Ihre Vertragspartner ggf. zu Kündigungsrechten und/oder Schadensersatzansprüchen? Prüfen Sie zudem auch, welche Auswirkungen eine Aussetzung der Datenübermittlung/Datenverarbeitung auf Ihr Geschäft hätte. Lassen Sie sich zudem hinsichtlich der Konsequenzen einer Aussetzung unbedingt vorab von Ihrer eigenen Rechtsabteilung/externen Rechtsanwälten beraten.

VERWENDUNG ZUSÄTZLICHER VERTRAGSKLAUSELN FÜR AUFTRAGSVERARBEITUNGSVERTRÄGE UND STANDARDDATENSCHUTZKLAUSELN (SCC)

Stellen Sie sicher, dass in allen künftig abzuschließenden Auftragsverarbeitungsverträgen/SCC sowie aktuell genutzten SCC, die alleine nicht ausreichen, um im betreffenden Drittland ein angemessenes Datenschutzniveau zu gewährleisten, entsprechende zusätzliche vertraglichen Verpflichtungen und Garantien enthalten sind. Hierfür können Sie sich, je nach Einzelfall, an folgenden Formulierungen orientieren:

1. *Soweit sich der Auftraggeber oder der Auftragnehmer auf einen bestimmten gesetzlichen Transfermechanismus zur datenschutzkonformen internationalen Datenübermittlung berufen und dieser Transfermechanismus geändert, widerrufen oder von einem zuständigen Gericht für ganz oder teilweise ungültig erklärt wird, vereinbaren Auftraggeber und Auftragnehmer, in gutem Glauben zusammenzuarbeiten, um die Übermittlung unverzüglich auszusetzen oder einen geeigneten alternativen Transfermechanismus zu etablieren, der die rechtmäßige Übermittlung gewährleistet.*

2. *Falls der Auftragnehmer gesetzlich (z. B. gemäß Intelligence Surveillance Act (FISA) 702, US Executive Order 12.333, Freedom of Information Act, Gramm–Leach–Bliley Act (GLBA), the Dept of Homeland Security Act of 2002, Public Law 110-53) und/oder auf Anordnung eines Gerichts oder einer Strafvollzugsbehörde, Sicherheitsbehörde und/oder Regulierungsbehörde (insbesondere, aber nicht abschließend, National Security Agency, Homeland Security, Federal Trade Commission) – nachfolgend „Behörden“ – zur Offenlegung von diesem Vertrag erfasster personenbezogener Daten aufgefordert wird, ist der Auftragnehmer auf seine eigenen Kosten verpflichtet,*

a. dem Auftraggeber (sofern gesetzlich zulässig) unverzüglich, aber spätestens innerhalb von 24 Stunden nach Erhalt der entsprechenden Aufforderung schriftlich oder per E-Mail darüber zu informieren und zwar mit

Angabe der angefragten Daten, der ersuchenden Behörde sowie der Rechtsgrundlage für die geforderte Offenlegung; und

b. alle dem Auftragnehmer, seinen verbundenen Unternehmen sowie Unterauftragnehmern in dem entsprechenden Land zur Verfügung stehenden Rechtsmittel über alle Instanzen zur Vermeidung der Offenlegung der personenbezogenen Daten auszuschöpfen (insbesondere, aber nicht ausschließlich, entsprechende Verfahren vor U.S. District Courts, Circuit Courts, Federal Administrative Courts, Appelate Courts, Supreme Court), um die Rechte und Interessen der betroffenen Personen nach der DS-GVO zu schützen und eine DS-GVO konforme Datenverarbeitung zu gewährleisten; und

c. die Offenlegung der personenbezogenen Daten gegenüber oben genannten Behörden zu unterlassen, bis der Auftragnehmer nach Erfüllung seiner vorstehenden Verpflichtungen von einem zuständigen Gericht letztinstanzlich zur Offenlegung rechtskräftig verurteilt wurde.

3. *Der Auftragnehmer ist verpflichtet, regelmäßig, aber mindestens einmal im Kalenderjahr, dem Auftraggeber kostenfrei allgemeine Informationen über die erhaltenen Anfragen von Behörden zu unter diesem Vertrag verarbeiteten personenbezogenen Daten zur Verfügung zu stellen (z. B. Anzahl der Anträge um Offenlegung, Art der angefragten Daten, soweit möglich ersuchende Stelle usw.).*

4. *Der Auftragnehmer ist dabei für alle Handlungen und Unterlassungen seiner verbundenen Unternehmen, Mitarbeiter, Vertreter und Unterauftragnehmer verantwortlich, die gegen diesen Abschnitt verstoßen.*

Lassen Sie sich von Ihrer Rechtsabteilung/externen Rechtsanwälten beraten, ob und inwieweit Sie die vorstehenden Verpflichtungen oder eigene Formulierungen mit einer Vertragsstrafe zulasten des Auftragnehmers versehen können und sollten.

NUTZUNG DER AUSNAHMEREGELN IN ART. 49 DS-GVO

Prüfen Sie, ob die in Art. 49 DS-GVO genannten Ausnameregelungen als mögliche Rechtsgrundlage für die Drittlandübermittlung infrage kommen. Dabei ist zu beachten, dass Art. 49 DS-GVO von den europäischen Aufsichtsbehörden als Ultima-Ratio-Ausnahmeerlaubnis für Drittlandsübermittlungen grundsätzlich sehr eng ausgelegt wird und meist nicht auf regelmäßige und wiederkehrende Datentransfers (z. B. für klassische „Outsourcing“-Szenarien) anwendbar ist.

Grundsätzlich dürfte Art. 49 DS-GVO daher für die meisten Datenübermittlungen keine ausreichende Rechtsgrundlage bieten.

Es ist aber davon auszugehen, dass europäische Aufsichtsbehörden wegen der durch Schrems II verursachten Ausnahmesituation bei der Anwendung von Art. 49 DS-GVO für eine gewisse Übergangszeit Nachsicht walten lassen.
So wird verhindert, dass den elementar wichtigen Wirtschaftsbeziehungen zwischen der Europäischen Union und den USA nachhaltig geschadet wird. Es verbleibt aber ein Restrisiko bei diesen Alternativen.

Sollten Sie bei der Prüfung Unterstützung benötigen, stehen wir Ihnen gern zur Verfügung.

ERWÄGUNG VON ALTERNATIVANBIETERN

Überlegen und prüfen Sie, ob nicht Alternativen zu US-Anbietern in Betracht kommen. Es gibt vermehrt gute (und datenschutzfreundliche) Alternativen zu US-Produkten in allen datenintensiven Online-Bereichen.

Bei der Auswahl der Tools sollten neben den Business-Kriterien immer auch (datenschutz-) rechtliche Kriterien berücksichtigt werden. Dies ergibt sich aus Art. 24 und 25 DS-GVO. Bei den datenschutzrechtlichen Kriterien spielen die Datenströme und Auslandsbezüge eine wesentliche Rolle. Die nachfolgende Liste enthält lediglich Hinweise auf mögliche Alternativen, die aber nicht final als Empfehlung, sondern lediglich als Anregung dienen. Eine abschließende Prüfung ist nur unter Heranziehung des konkreten AVV (Auftragsverarbeitungsvertrages) und der TOM (technischen und organisatorischen Maßnahmen) sowie der konkreten Gegebenheiten/Einstellungen möglich. Gerne unterstützen wir Sie bei der Prüfung und Auswahl von Alternativen.

Als datenschutzfreundliche Alternativen kommen insbesondere folgende Vorschläge in Betracht:

Videokonferenzen: jitsi | sichere-videokonferenz.de | tixeo.com

Newsletter-Marketing: cleverreach | Newsletter2go | Klick-Tipp | rapidmail

Instant Messaging: Rocket.Chat | Threema | wire

Online-Umfragen: onlineumfragen.com | QuestionPro

PRÜFUNG UND ANPASSUNG VON BINDING CORPORATE RULES (BCR)

Der EuGH hat das Datenschutzniveau in den USA an sich in Frage gestellt. Da BCR genauso wie Standarddatenschutzklauseln (SCC) lediglich ein behördenseitig genehmigtes privatrechtliches Vertragskonstrukt sind, gilt für die Übermittlung personenbezogener Daten in die USA auf Basis von BCR deshalb grundsätzlich das Gleiche wie bei der Übermittlung auf Basis von SCC: Es muss im Einzelfall geprüft werden, ob die BCR an sich ausreichen, um ein adäquates Datenschutzniveau zu gewährleisten, und, falls nicht, müssen ggf. zusätzliche Maßnahmen ergriffen werden. Hierbei bietet es sich an, ähnliche Klauseln und Garantien wie für die SCC zu verwenden (siehe Ausführungen oben). Da es sich bei derlei Anpassungen üblicherweise um wesentliche Änderungen der BCR handelt, müssten diese der zuständigen Aufsichtsbehörde zur erneuten Genehmigung vorgelegt werden.

PRÜFUNG UND ANPASSUNG DER DATENSCHUTZ-ERKLÄRUNGEN (INSB. AUF WEBSITES UND APPS)

Die Datenschutzerklärung ist die „Visitenkarte des Unternehmens“ in Sachen Datenschutz und für jede betroffene Person zugänglich. Sowohl Aufsichtsbehörden, Verbraucherschutzverbände als auch mögliche Wettbewerber haben in der Vergangenheit unzureichende Datenschutzerklärungen dafür genutzt, um aufsichtsrechtliche Maßnahmen bzw. Abmahnungen nach dem Wettbewerbsrecht einzuleiten. Vermeiden Sie also potenzielle Haftungs- und Abmahnrisiken, indem sie keine Indizien für eine rechtwidrige Verarbeitung in der Datenschutzerklärung ausweisen.

Prüfen Sie deswegen in diesem Zusammenhang die Datenschutzerklärungen auf Ihren Websites, Apps, Webshops etc. Wird in diesen eine Übermittlung in Drittländer aufgeführt und werden dabei das Privacy Shield oder SCC als Transfermechanismus genannt, müssen die entsprechenden Passagen ggf. angepasst werden, da nach Art. 13 und 14 DS-GVO Datenschutzerklärungen den tatsächlichen Stand der Datenverarbeitung wiederzugeben haben.

Sollten Sie bei der Prüfung Unterstützung benötigen, stehen wir Ihnen gern zur Verfügung.

AKTUALISIERUNG DER VERFAHRENSVERZEICHNISSE

Neben den Datenschutzerklärungen müssen auch die Verzeichnisse der Verarbeitungstätigkeiten (VVT) entsprechend aktualisiert und angepasst werden. VVT werden üblicherweise von Aufsichtsbehörden im Rahmen von Überprüfungen angefordert. Zudem dienen VVT als entsprechende Quelle, um Betroffenenanfragen (z. B. das Recht auf Auskunft nach Art. 15 DS-GVO) zu erfüllen. Deswegen sollte die Datenschutzdokumentation immer aktuell gehalten werden.

WELCHE EMPFEHLUNGEN GEBEN DIE AUFSICHTSBEHÖRDEN?

Das Meinungsbild der europäischen Aufsichtsbehörden ist derzeit sehr ambivalent und teilweise sogar widersprüchlich. Während beispielweise die ICO (Aufsichtsbehörde des Vereinigten Königreichs) verarbeitenden Stellen im Vereinigten Königreich mitteilt, das Privacy Shield auch weiterhin zu benutzen, hat die Berliner Aufsichtsbehörde alle ihrem Verantwortungsbereich unterfallenden Unternehmen aufgefordert, Datenübermittlungen in die USA einzustellen und die Daten nach Europa oder andere Länder mit angemessenem Datenschutzniveau zurückzuholen. Diese gegenläufigen Empfehlungen sind für die Praxis unbefriedigend und widersprechen dem Harmonisierungsgedanken der DS-GVO. Die europäischen Datenschutzbehörden haben ein erstes FAQ veröffentlicht und arbeiten derzeit an einer gemeinsam abgestimmten Position hinsichtlich konkreter Maßnahmen und Handlungsempfehlungen.

Nachfolgend finden Sie eine Zusammenfassung ausgewählter Stellungnahmen europäischer Aufsichtsbehörden:

LEGENDE

Zurückhaltende, neutrale oder abgewogene Bewertung (kein unmittelbarer bzw. nur geringer Handlungsbedarf)

Strenge und strikte Auslegung (klare Handlungsempfehlungen bzw. Hinweise zu Risiken, Folgen oder Sanktionen)

Sehr strenge oder sehr restriktive Haltung (klare Aufforderung, Übermittlungen zu unterbinden bzw. Ankündigung von Prüfungen oder Sanktionen)

AUFSICHTSBEHÖRDE	BEWERTUNG	STELLUNGNAHME	QUELLE
Europäischer Datenschutzausschuss (EDSA)		- EU und USA sollten im Lichte der EuGH-Rechtsprechung abschließende und effektive Rahmenbedingungen schaffen, damit das Datenschutzniveau für personenbezogene Daten in den USA gleichwertig zum Schutzniveau in Europa ist. - SCC sind weiterhin gültig. Es wird auf die Wichtigkeit der Einhaltung der Verpflichtungen durch Datenexporteur und Datenimporteur aus den SCC verwiesen, insbesondere auf die Informationspflichten bzgl. einer Änderung der Rechtslage im Land des Datenimporteurs. - Datenexporteur und Datenimporteur müssen gemeinsam prüfen, ob im betreffenden Drittland ein angemessenes Datenschutzniveau vorliegt, und falls nicht, ggf. entsprechende zusätzliche Maßnahmen ergreifen. Der EDSA prüft noch, wie diese zusätzlichen Maßnahmen ausgestaltet sein können. - Datenschutzbehörden sind angehalten, datenschutzwidrige Übermittlungen zu untersagen. - Es gibt keine Übergangs-/Gandenfrist, sondern die Anforderungen aus Schrems II sind ab sofort umzusetzen.	Pressemitteilung FAQ

AUFSICHTSBEHÖRDE	BEWERTUNG	STELLUNGNAHME	QUELLE
Europäischer Datenschutzbeauftragter (EDPS)		- Es wird davon ausgegangen, dass die USA alles in ihrer Macht stehende tun wird, um umfassende rechtliche Rahmenbedingungen in Sachen Datenschutz zu schaffen, die den Anforderungen des EuGH entsprechen. - EDPS will entsprechende Verträge der EU-Institutionen (z. B. mit Microsoft) überprüfen.	Pressemitteilung
Dänemark (Datatilsynet)		- SCC sind grundsätzlich weiterhin gültig. - Weitere Maßnahmen und Handlungsempfehlungen werden derzeit erarbeitet.	Pressemitteilung
Deutschland – Bundesbeauftragter für Datenschutz und Informationsfreiheit (BfDI)		- Datenübermittlungen in die USA via SCC sind weiterhin möglich, bedürfen aber des Abschlusses zusätzlicher Maßnahmen. - Die Umstände von Datentransfers (auch in andere Länder) müssen von Fall zu Fall betrachtet und Verträge mit entsprechenden Dienstleistern überprüft werden. - Es gibt keine Gnadenfrist: Es muss sofort mit der Umstellung muss begonnen werden. - Datenschutzbehörden sollten ihre beaufsichtigten Stellen intensiv zu alternativen Grundlagen für den internationalen Datenaustausch beziehungsweise zu Umstellungen beraten.	Pressemitteilung (24. Juli) Pressemitteilung (16. Juli)

AUFSICHTSBEHÖRDE	BEWERTUNG	STELLUNGNAHME	QUELLE
Deutschland – Baden-Württemberg		- SCC sind weiterhin gültig. - Unternehmen und Aufsichtsbehörden müssen im Einzelfall prüfen, ob diese ausreichen. - Im Fall der USA liege das Ergebnis dieser Prüfung aber auf der Hand, denn praktisch kein amerikanisches Unternehmen könne glaubhaft garantieren, dass es vom Zugriff der dortigen Geheimdienste verschont bleiben wird. Somit sind durch das Urteil große Teile der amerikanischen Digitalwirtschaft für Europäer tabu. - Als zusätzliche Maßnahmen wird insbesondere die Verschlüsselung von Daten erwähnt. - Erwägungen des EuGH gelten entsprechend auch für Länder wie China oder Russland. - Die Aufsichtsbehörde in Baden Württemberg ist skeptisch, ob der EuGH nicht überschätzt, wie lang der europäische Hebel wirklich ist. Zudem sieht sie nicht, wie eine verträgliche praxistaugliche Lösung aussehen kann. - Ein Moratorium wie vormals bei Safe Harbour wird es folglich nicht mehr geben.	Interview in FAZ
Deutschland – Berlin		- Bis zu einer Änderung der Rechtslage dürfen personenbezogene Daten in aller Regel nicht mehr wie bisher in die USA übermittelt werden. Ausnahmen bestehen vor allem in den gesetzlich vorgesehenen Sonderfällen, etwa bei einer Hotelbuchung in den USA. - Sowohl die europäischen Datenexporteure als auch die Datenimporteure in Drittländern sind verpflichtet, vor der ersten Datenübermittlung zu prüfen, ob im Drittland staatliche Zugriffsmöglichkeiten auf die Daten bestehen, die über das nach europäischem Recht Zulässige hinausgehen. - Ist dies gegeben, müssen bereits ins Drittland übermittelte Daten zurückgeholt werden.	Pressemitteilung

- Sämtliche der Aufsichtsbehörde unterliegenden Verantwortlichen sind aufgefordert, die Entscheidung des EuGH zu beachten. 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.
- Das Urteil des EuGH betrifft laut Behörde nicht nur Übermittlungen in die USA, sondern insbesondere auch nach China, Russland oder Indien.
- Es wird zudem darauf verwiesen, dass betroffene Personen Schadensersatz für unzulässige Datenexporte verlangen können.

Deutschland – Hamburg

- EuGH urteile inkonsequent, wenn er SCC als angemessenes Instrument für die Übermittlung in die USA beibehalte. Vertragliche Vereinbarungen zwischen Datenexporteur und -importeur sind gleichermaßen ungeeignet, um Betroffene vor dem staatlichen Zugriff in den USA zu bewahren.
- Neben BCR und Einzelvereinbarungen sind es vor allem die SCC, die als Grundlage für Übermittlungen in andere Drittstaaten zukünftig genutzt werden können.
- Sowohl die Verhältnismäßigkeit behördlicher Zugriffsmöglichkeiten als auch die Garantie eines funktionierenden Rechtsschutzes hat der Exporteur seiner örtlich zuständigen Datenschutzbehörde auf Verlangen nachzuweisen. Diese sind bspw. für Länder wie China weit davon entfernt, ein angemessenes Niveau aufzuweisen.
- Eine Datenübermittlung in Staaten ohne angemessenes Datenschutzniveau wird es künftig nicht mehr geben dürfen.

Pressemitteilung

AUFSICHTSBEHÖRDE	BEWERTUNG	STELLUNGNAHME	QUELLE
Deutschland – Rheinland-Pfalz		- Als Konsequenz aus diesem Urteil wird der LfDI Rheinland-Pfalz zeitnah an Unternehmen herantreten, um festzustellen, ob sie in der Vergangenheit ihre Datenübermittlung in die USA auf das Privacy Shield gestützt haben. Da dies ab sofort nicht mehr möglich ist, müssen von den Verantwortlichen Maßnahmen getroffen und erläutert werden, wie künftig die entsprechenden Datenverarbeitungen gestaltet sein werden. Dazu müssen die Unternehmen aussagefähig sein. - Für Datenübermittlungen in die USA bedeutet dies, dass erhebliche Anstrengungen der Verantwortlichen erforderlich sind, die vermutlich nur in seltenen Fällen als ausreichend angesehen werden können. Dies ist aber eine Frage des Einzelfalles. - Die Datenübermittlung in die USA und sonstige Drittstaaten außerhalb der Europäischen Union auf der Grundlage von SCC ist und bleibt möglich. Die SCC müssen ggf. durch weitere Vereinbarungen oder Elemente ergänzt werden, um sicherzustellen, dass bei der Datenübermittlung in den Drittstaat das angemessene Schutzniveau erhalten ist. - Für Übermittlungen in andere Drittstaaten wie z. B. Indien, China oder Russland werden dringend Nachprüfungen angeraten. - Der LfDI Rheinland-Pfalz wird im Rahmen von Beschwerden oder ansonsten mittelfristig auf Unternehmen zukommen, um entsprechende Darlegungen zu erhalten. - Datenübermittlungen, die nicht den Anforderungen der DS-GVO und des EuGH entsprechen, müssen ausgesetzt werden. - Daten, die bisher auf Grundlage des Privacy Shield übermittelt wurden, sind entweder zurückzufordern oder zu vernichten und dies entsprechend zu dokumentieren. - Bei Untätigkeit durch Verantwortliche wird die Behörde entsprechende Maßnahmen ergreifen. Im Fall von anhaltenden und nachhaltigen Verstößen stehen auch Geldbußen im Raum.	Handlungsempfehlungen FAQ Pressemitteilung

AUFSICHTSBEHÖRDE	BEWERTUNG	STELLUNGNAHME	QUELLE
Deutschland – Thüringen		- Die Aufsichtsbehörde zweifelt, inwiefern SCC für Übermittlungen in die USA noch ein valides Instrument darstellen.	Pressemitteilung
Estland (Andmekaitse Inspektsioon)		- Datenexporteur und Datenimporteur müssen gemeinsam prüfen, ob im betreffenden Drittland ein angemessenes Datenschutzniveau vorliegt, und falls nicht, Übermittlung stoppen und erst wieder fortführen, soweit entsprechende zusätzliche Maßnahmen ergriffen wurden.	Pressemitteilung Zusätzliche Infos
Frankreich (CNIL)		- CNIL wird die Folgen des Urteils im Europäischen Datenschutzausschuss (EDSA) aufarbeiten.	Pressemitteilung
Irland (Data Protection Commission)		- Es ist fraglich, ob SCC Übermittlungen in die USA noch rechtfertigen können. - Unabhängig des gewählten Transfermechanismus, muss ein dem europäischen gleichwertiges Niveau erreicht werden. - Das Urteil und die Folgen sowie ggf. zu ergreifenden Maßnahmen werden seitens der Behörde nun sorgfältig geprüft.	Pressemitteilung
Liechtenstein (Datenschutzstelle)		- Daten können nach wie vor aufgrund anderer geeigneter Garantien nach Art. 46 ff. DS-GVO in die USA übermittelt werden, insbesondere auch aufgrund von SCC. - Zumindest mittelfristig, bis allenfalls durch die EU-Kommission ein neues Abkommen mit den USA zur Datenübermittlung geschlossen werden kann, müssen sich Verantwortliche nun auf solche Instrumente stützen.	Pressemitteilung

AUFSICHTSBEHÖRDE	BEWERTUNG	STELLUNGNAHME	QUELLE
Litauen (Valstybinė duomenų apsaugos inspekcija)		- Will die Folgen des Urteils im EDSA aufarbeiten.	Pressemitteilung
Niederlande (Autoriteit Persoonsgegevens)		- EU-Kommission sollte ein Nachfolgeabkommen für Privacy Shield in Erwägung ziehen. - Da in den USA kein gleichwertiges und angemessenes Datenschutzniveau vorliegt, sollten Unternehmen und Organisationen keine personenbezogenen Daten mehr in die USA übermitteln. - Die praktischen Konsequenzen und nächsten Schritte sollen im Europäischen Datenschutzausschuss (EDSA) aufgearbeitet werden.	Pressemitteilung
Norwegen (Datatilsynet)		- Datenexporteur und Datenimporteur müssen gemeinsam im Falle von SCC prüfen, ob im betreffenden Drittland ein angemessenes Datenschutzniveau vorliegt.	Pressemitteilung
Schweiz (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter)		- Laut Aufsichtsbehörde ist das Urteil für die Schweiz nicht anwendbar. - Das Urteil wird nun vertieft geprüft und zu gegebener Zeit eine weitere Stellungnahme veröffentlicht.	Pressemitteilung
Polen (Urząd Ochrony Danych Osobowych)		- Datenexporteur und Datenimporteur müssen gemeinsam im Falle von SCC prüfen, ob im betreffenden Drittland ein angemessenes Datenschutzniveau vorliegt. Liegt dieses nicht vor, müssen ggf. andere Maßnahmen getroffen werden.	Pressemitteilung

AUFSICHTSBEHÖRDE	BEWERTUNG	STELLUNGNAHME	QUELLE
Rumänien (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal)		- Alternativmechanismen für Übermittlungen in die USA sind BCR, SCC und Codes of Conduct.	Pressemitteilung
Slowenien (Informacijski Pooblaščenec)		- Alternativmechanismen für Übermittlungen in die USA sind BCR und SCC.	Pressemitteilung
Spanien (Agencia Española de Protección de Datos)		- SCC sind weiterhin gültig. - Ein abgestimmtes europäisches Vorgehen hinsichtlich der Anwendung und Folgen der Entscheidung ist nun erforderlich.	Pressemitteilung
Tschechische Republik (Úřad pro ochranu osobních ùdajů)		- Keine inhaltliche Bewertung, nur Hinweis auf das Urteil	Pressemitteilung
Vereinigtes Königreich (ICO)		- Das Privacy Shield kann für bisherige Übermittlungen zunächst weiterhin benutzt werden, bis neue Handlungsempfehlungen veröffentlicht werden. - Für neue Übermittlungen soll es aber nicht mehr genutzt werden.	Mitteilung

UND WAS UNTERNIMMT DER GESETZGEBER?

Die EU-Kommission hat angekündigt, eng mit den USA zusammenzuarbeiten, um sichere transatlantische Datenflüsse zu gewährleisten. Gleiches hat auch die US-amerikanische Seite verlautbart. Es ist also davon auszugehen, dass es ein Folgeabkommen zum Privacy Shield (eine Art Privacy Harbor) geben wird. Wann dies geschehen wird, kann derzeit jedoch noch nicht abgeschätzt werden. Nach der Ungültigkeitserklärung von Safe Harbor im Oktober 2015 hat es knapp ein dreiviertel Jahr benötigt, um das Privacy Shield zu verhandeln und abzuschließen. Dies kann als erste Indikation für den zeitlichen Maßstab fungieren.