0800 400 510 1

AKTUELLE INFORMATION DATENTRANSFER IN DIE USA ERMÖGLICHEN

Datenschutz - Nr. 06/2021

Datenschutz

Wir entlasten Führungskräfte und schützen Mitarbeiter. Seit 1997.

Datentransfer in die USA ermöglichen

Als der Europäische Gerichtshof (EuGH) Datentransfers in die USA auf Grundlage des Privacy Shield für unzulässig erklärt hat, nahm er Kollateralschäden bei den europäischen Unternehmen in Kauf. Als Opfer der Datenschutzpolitik müssen diese nun praktisch die Aufgaben der EU-Kommission übernehmen und ihre US-Datentransfers selbst prüfen. Bereits angekündigt ist, dass die Landesdatenschutzbehörden den US-Datentransfer, sowie US-Dienstleister mit Hilfe von Fragebögen überprüft werden sollen.
Zeit also, Ihren US-Datentransfer verstärkt zu überprüfen und zu bewerten.

Mit unserem heutigen Newsletter möchten wir Ihnen daher helfen eine Prüfung von Datentransfers in die USA (bzw. den Einsatz von US-Diensten/ -Anbietern) durchzuführen und verbleibende Risiken einzuschätzen. Zwar hat der Newsletter heute deutlich mehr Text, sollte Ihnen aber zukünftig zur eigenständigen Überprüfung und Durchführung von TransferImpactAssessments dienen können.

Weshalb ist eine Prüfung erforderlich?

- Laut der DSGVO dürfen personenbezogene Daten nur dann außerhalb der EU übermittelt werden (in sogenannte Drittländer), wenn in dem Zielland ein adäquates Datenschutzniveau besteht (Art. 44 DSGVO).
- Für die USA hatte die EU-Kommission ein adäquates Datenschutzniveau für Unternehmen festgestellt, die bestätigten, eine Reihe von Vorgaben zu beachten (dieses System wurde als der "Privacy Shield" bezeichnet).
- Der Vorteil des Privacy Shield bestand darin, dass man bei den Privacy-Shield-(selbst)zertifizierten Unternehmen ein adäquates Datenschutzniveau ohne eine weitere Prüfung annehmen durfte.
- Der Privacy Shield wurde vom EuGH im Juli 2020 für unwirksam erklärt (EuGH, 16.7.2020 – C-311/18 "Schrems II"). Der EuGH entschied, dass die Befugnisse der US-Behörden, die es sogar erlauben auf personenbezogenen Daten der EU-Bürger heimlich und ohne effektive Rechtsbehelfsmöglichkeiten zuzugreifen, gegen ein adäquates Datenschutzniveau in den USA sprechen.

Ohne den Privacy Shield bedarf es nunmehr anderer Mittel, um ein adäquates Datenschutzniveau annehmen zu dürfen. Ein solches Mittel sind die so genannten „Standardvertragsklauseln" (auch als "Standardschutzklauseln" oder auf Englisch als "Standard Contractual Clauses", SCC, bezeichnet).

Leistungsangebot Datenschutz

AKTUELL & WICHTIG!

Datenschutzrechtliche Beratung Krisenmanagement

Externer Datenschutzbeauftragter gemäß DSGVO

Sicher zum Verarbeitungsverzeichnis

Betroffenenrechte & Mitteilungspflichten steuern

Webseiten rechtskonform gestalten

Audits & Bestandsaufnahmen durchführen

Informationspflichten praktikabel umsetzen

WIE KÖNNEN WIR IHNEN HELFEN?

FKC CONSULT GmbH
Eschenburgstr. 5
23568 Lübeck
www.fkc-gmbh.de

datenschutzanfrage@fkc-gmbh.de

0800 400 510 1

AKTUELLE INFORMATION DATENTRANSFER IN DIE USA ERMÖGLICHEN

Datenschutz - Nr. 06/2021

Datenschutz

Risikominderung durch eigene Prüfung von Datentransfers

Basierend auf den Empfehlungen von Datenschutzbehörden sollten Sie Ihre Datentransfers in die USA überprüfen, dann sollten Sie zumindest nachweisen können, entsprechend den behördlichen Ratschlägen gehandelt zu haben. Im Fazit ermöglichen Sie es mit der Beachtung der folgenden Maßnahmen den Behörden daher einfacher, keine Maßnahmen gegen Sie zu ergreifen.

Prüfung von Standardvertragsklauseln

Achtung: **Zu den am 04.06.2021 geänderten Standardvertragsklauseln werden wir Sie außerordentlich in den kommenden Tagen Informieren.**

Da Standardvertragsklauseln nach Wegfall des Privacy Shield zu der wichtigsten Rechtsgrundlage für US-Transfers werden, stehen Sie im Zentrum der folgenden Ratschläge.
Bei den Standardvertragsklauseln handelt es sich um Musterverträge, die zwischen dem Verantwortlichen und dem Empfänger der Daten abgeschlossen werden (also z. B. beim Einsatz von US-Anbietern und US-Diensten). Der Abschluss der Standardvertragsklauseln allein ist jedoch nicht ausreichend.

Sie müssen zusätzlich die folgenden Punkte prüfen:

- Ob die Standardvertragsklauseln nicht verändert wurden und falls ja, die Änderung zulässig war.
- Ob die Zusagen das adäquate Datenschutzniveau einzuhalten, auch tatsächlich eingehalten werden. Das heißt Sie müssen überprüfen, ob das vom EuGH beschriebene Risiko des Zugriffes auf die Daten durch US-Behörden verhindert wird.
  In der Praxis erfolgt die Prüfung zunächst anhand von Fragen an die US-Verarbeiter, doch zuerst sollten Sie wissen, welche Verarbeitungen Sie prüfen müssen.

Großbritannien und andere Drittländer: Hauptsächlich geht es um die Prüfung von US-Datentransfers. Allerdings muss die Prüfung für alle Drittländer erfolgen, bei denen die EU-Kommission kein angemessenes Datenschutzniveau festgestellt hat. Dazu gehört ab Ende des Jahres neben den USA und z. B. Indien, China oder Russland, mit aller Wahrscheinlichkeit auch Großbritannien.“.

Step 1: Datentransfers in die USA erkennen

- Überprüfen aller Dienstleister und Verarbeitungsverfahren auf mögliche US-Transfers oder den Einsatz von US-Dienstleistern
  - Auf Subunternehmer von deutschen Dienstleistern achten und wo Daten verarbeitet werden,
  - Oft europäische Tochterunternehmen trotzdem zu beachtendes US-Recht

Daher müssen Sie auch die Angaben zu Subunternehmern bei Ihren Auftragsverarbeitern (sowie genau genommen auch bei anderen Dienstleistern) prüfen und auch bei diesen eine Prüfung durchführen. Im Ergebnis sollten Sie alle von Ihnen eingesetzten Dienste und Dienstleister auf eine Verarbeitung von personenbezogenen Daten in den USA oder mögliche Zugriffe von US-Behörden prüfen und im Zweifel die folgende Anfrage auch an sie versenden.

Firma Unterauftragnehmer	Anschrift
Amazon Europe Core SARL	5 Rue Plaetis, L-2338 Luxembourg, Luxembourg
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Irland
Microsoft Ireland Operations, Ltd.	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland
Telekom Deutschland GmbH	Landgrabenweg 151, D-53227 Bonn
Xandr Inc.	28 W. 23rd Street, New York, NY 10010, USA

Es geht nicht nur um den Fall der Auftragsverarbeitung:
Standardvertragsklauseln werden vor allem im Zusammenhang mit der Auftragsverarbeitung verwendet, also wenn die Beauftragung eine Verarbeitung von Daten zum Kern hat (zum Beispiel bei einer Plattform für Bewerber, eine Cloud-Software mit der Kundenbestellungen verwaltet oder Newsletter verschickt werden). Standardvertragsklauseln umfassen sogar Regelungen zur Auftragsverarbeitung, so dass ein zusätzlicher Auftragsverarbeitungsvertrag nicht erforderlich wird (Art. 28 Abs. 7 DSGVO). Allerdings müssen US-Transfers auch im Rahmen des Einsatzes von Drittanbietern (die selbst verantwortlich und keine Auftragsverarbeiter sind) berücksichtigt werden (Art. 25 Abs. 1 DSGVO).

Step 2: Alternativen prüfen

Bevor Sie eine Prüfung des Datenschutzniveaus durchführen, sollten Sie prüfen, ob alternative Verarbeitungsmöglichkeiten in der EU/EWR oder in Staaten mit anerkanntem Datenschutzniveau bestehen (z. B. Schweiz, Kanada, Israel, Japan).

Die Alternativen müssen aber gleichwertig sein, wobei Sie die folgenden (nicht abschließenden) Faktoren berücksichtigen können:

- **Usability** – Können die Alternativen z. B. genauso einfach bedient werden oder müssten Mitarbeiter neu geschult oder Kunden neu an eine Software gewöhnt werden?

0800 400 510 1

AKTUELLE INFORMATION DATENTRANSFER IN DIE USA ERMÖGLICHEN

Datenschutz - Nr. 06/2021

Datenschutz

- **Funktionalität und Funktionsumfang** – Lassen sich die beabsichtigten Verarbeitungen mit der Alternative genauso effektiv durchführen?
- **Kosten** – Sind die Alternative und Kosten ihrer Einführung wesentlich teurer und ist die Mehrbelastung wirtschaftlich bedeutend.
- **Sicherheitsrisiko** – Bietet die Alternative faktisch dasselbe Sicherheitsniveau? Behörden weisen z.B. darauf hin, dass man z. B. Videokonferenzdienste selbst betreiben kann. Allerdings erscheint es häufig fraglich, ob dabei dasselbe Sicherheitsniveau, wie auf den Konferenzservern großer Unternehmen, geboten werden kann.

Step 3: Ermittlung der Rechtsgrundlagen

Da die Rechtsgrundlage „Privacy Shield“ weggefallen ist, sollten sie die jeweiligen rechtliche Grundlagen prüfen.

Folgende kommen hierfür in Frage:

- **Abschluss von Standardvertragsklauseln (SCC)** – Diese von der EU-Kommission gestellten Musterverträge, müssen um den Gegenstand der Verarbeitung und Hinweise auf Schutzmaßnahmen ergänzt werden, bevor sie in Schriftform oder elektronischer Form abgeschlossen werden können. Die folgende Prüfung berücksichtigt die Standardvertragsklauseln, da sie das Mittel der Wahl nach Wegfall des Privacy Shield sein werden.
- **Binding Corporate Rules (BCR)** – Selbstverpflichtende Datenschutzregeln der Unternehmen. Diese Alternative ist eher selten, zumal auch eine externe Zertifizierung oder eigene Prüfung erforderlich wäre, um auf deren Grundlage Daten in Drittländer zu transferieren. Die Prüfung kann auch auf Binding Corporate Rules übertragen werden.
- **Erforderliche Datentransfers** – Wenn die Übermittlung oder sonstige Verarbeitung der Daten in Drittländern erforderlich und für die Betroffenen erkennbar ist, darf die Übermittlung erfolgen (z. B. wenn eine Reise in den USA gebucht oder eine E-Mail in die USA verschickt wird). Erforderliche Datentransfers werden in jedem Fall eine Aufklärung den Kunden oder sonstigen Betroffenen über die Verarbeitung ihrer Daten in den USA erfordern.
- **Einwilligungen** – Als letzte Möglichkeit bleiben praktisch nur die Einwilligungen der betroffenen Personen. Diese sind jedoch zum einen kompliziert und können schnell an fehlender Transparenz, ausdrücklicher Abgabe oder an fehlender Freiwilligkeit (z. B. bei Arbeitnehmern, Art. 26 DSGVO) oder fehlender Einwilligungsfähigkeit (in Deutschland ab 16 Jahren, s. Art. 8 Abs. 3 DSGVO) scheitern.
- **Weitere Ausnahmen** – Weitere Ausnahmen können Sie Art. 49 DSGVO entnehmen (die jedoch eher selten zutreffend werden).

Step 4: Anfragen

Bevor Sie mit der Prüfung beginnen, müssen Sie die erforderlichen Informationen einholen. In den meisten Fällen werden Sie auf Ihre Anfrage eher allgemeine Antworten erhalten und müssen die relevanten Informationen aus dem Text herausfiltern.

Erinnern und rückfragen – Trotz der detaillierten Fragen, sollten Sie nicht damit rechnen, ebenso detaillierte Informationen zu erhalten. Die meisten Dienstleister oder Anbieter werden mit eher standardisierten Informationen antworten, die häufig auf

0800 400 510 1

AKTUELLE INFORMATION DATENTRANSFER IN DIE USA ERMÖGLICHEN

Datenschutz - Nr. 06/2021

Datenschutz

noch laufende Prüfungen verweisen werden. In diesem Fall sollten Sie nachfragen, wann mit einem Ergebnis zu rechnen ist oder nach Ablauf einer angemessenen Zeit (zwei bis vier Wochen), an die Anfrage erinnern. Sollte die Antwort weder auf laufende Prüfungen verweisen noch auf Ihre Fragen eingehen, sollten Sie mit erneuter Frist die Anfrage wiederholen (oder ansonsten zum nächsten Schritt der Prüfung schreiten).

Step 5: Bestimmung des Risikos für Betroffene Personen

Um zu prüfen, ob das Datenschutzniveau in den USA angemessen ist, müssen Sie wissen wie hoch die Anforderungen an das Datenschutzniveau sind. Der EuGH hat das Datenschutzniveau in den USA pauschal beurteilt und musste dabei auch potenziell sensible Sachverhalte beurteilen (z. B. Angaben zu politischen Aktivitäten, sexuelle Ansichten, vermögensbezogene Angaben, etc.).

Sie nehmen jedoch eine individuelle Prüfung vor und müssen beurteilen, welche möglichen Folgen für die Betroffenen beim Zugriff durch US-Behörden eintreten können Dabei können Sie davon ausgehen, dass je sensibler die verarbeiteten Daten sind, desto höher das Risiko sein wird. **Beispiele:**

- **Verarbeitung einer Personalakte in den USA** – Eine Personalakte kann Angaben zur Gesundheit, Gewerkschaftszugehörigkeit, Leistungsbewertungen oder weitere sensible Informationen enthalten. Wenn diese bekannt werden würden, dann könnten diese Informationen z. B. zur Verweigerung einer Einreise aufgrund Vorerkrankungen oder für ein politisches Profiling verwendet werden. In diesem Fall müssten die Schutzmaßnahmen hoch sein und z. B. eine Verschlüsselung voraussetzen, bei der nur das EU-Unternehmen, aber nicht der US-Anbieter Zugriff auf die Daten erhält.
- **Nutzung von Videokonferenzdiensten** – Ein weitaus geringeres Risiko liegt dagegen vor, wenn Mitarbeiter mit ihrer beruflichen E-Mailadresse an einer Videokonferenz teilnehmen und dort berufliche Inhalte austauschen. In einem solchen Fall wäre m. E. die Verschlüsselung der Kommunikationsinhalte ausreichend und die mögliche Kenntnis, wann Mitarbeiter mit wem gesprochen haben, für die Mitarbeiter kaum vom Nachteil.
- N**utzung von US-Newsletterplattformen** – Die Tatsache, dass jemand einen Newsletter bezieht, sehe ich zunächst eher als unverfänglich an. Daher wäre das Risiko E-Mailadressen bei einem US-Anbieter zu speichern gering. Anders wäre es, wenn es sich um einen Newsletter zu politisch brisanten oder sexuellen Themen handeln würde (und zudem auch gespeichert werden würde, welche Inhalte die Nutzer gelesen oder welche Links im Newsletter sie geklickt haben). Hier wäre das Risiko höher und eine Speicherung auf EU-Servern oder Aufklärung der Nutzer wäre zu empfehlen.

Information der Beschäftigten, Kunden oder Nutzer: Es ist zwar nicht direkt eine Schutzmaßnahme der Anbieter, aber die Information der Betroffenen über die Verarbeitung ihrer Daten in den USA senkt das Risiko (auch wenn man sich natürlich darüber streiten, inwieweit).

0800 400 510 1

AKTUELLE INFORMATION DATENTRANSFER IN DIE USA ERMÖGLICHEN

Datenschutz - Nr. 06/2021

Datenschutz

Step 6: Schutzmaßnahmen bewerten

In diesem Beispiel wurde das Datenschutzniveau für Microsoft Teams Videokonferenzen geprüft. Selbstverständlich können Sie die Auflistung anders aufbauen, um weitere Angaben zu ergänzen oder gleich in ein vorhandenes Verzeichnis Ihrer Verarbeitungstätigkeiten zu integrieren:

Dienst/Zweck	Microsoft Teams Videokonferenzen
Anbieter	Microsoft
Arten von Daten	Vornamen, Namen, Arbeitgeber, berufliche Funktion, E-Mailadressen (je nach Teilnahmeart auch Telefonnummern) von Mitarbeitern und Kommunikationspartnern, Audio-, Video- und textliche Inhalte der Kommunikationen, Zeitpunkt, Dauer und Ort der Teilnahmen, IP-Adressen und Hardwareinformationen der Teilnehmer.
Rechtsgrundlage im Fall der Drittlandübermittlung	Standvertragsklauseln.
Risikograd für Betroffene	Gering, überwiegend betriebliche Informationen.
Anfrage/ Antwort vom	18.08.2020 / 25.08.2020
Alternativen (EU/Anerkanntes Datenschutzniveau)	Diverse Videoanbieter, die jedoch nicht gleich geeignet sind: Geringere Verbreitung/Akzeptanz und Kunden, Notwendigkeit der Instruktion von Mitarbeitern, Aufwand er Implementation und zusätzliche Kosten, zusätzlicher Zeitaufwand für technische und datenschutzrechtliche Wartung/Pflege.
Sicherheitsmaßnahmen	EU-Server, Verschlüsselung der Kommunikationsinhalte, Zusage Erforderlichkeitsprüfung (Gerichtliche Abwehr erfolgte bereits in Vergangenheit), Zusage Information im Fall der Abfrage durch US-Behörden, Information der Teilnehmer.
Hinreichendes Datenschutzniveau	ja
Nächste Prüfung	01.02.2021

Das Schwierigste ist die Auswertung der Rückläufe und die Beurteilung, ob das Datenschutzniveau bei den jeweiligen Anbietern hinreichend ist. Aufgrund fehlender Muster ist hier eine Einzelfallbeurteilung notwendig. Dabei können Sie auf die folgenden Kriterien zurückgreifen:

- **Verarbeitung auf EU-Servern** – Der sog "Cloud Act" erlaubt den US-Behörden in bestimmten Fällen die Herausgabe von Daten auf EU-Servern zu verlangen. Allerdings ist das Risiko einer physischen Beschlagnahme der Datenträger im Fall der Weigerung der Anbieter geringer.
- **Verschlüsselung** – Auch eine Verschlüsselung der verarbeiteten Daten steigert das Datenschutzniveau. Allerdings kommt es auf die Art der Verschlüsselung an. Am sichersten ist eine Verschlüsselung, bei der nur Sie die Daten entschlüsseln können oder von Ihnen bestimmte Dritte (sog. Ende-zu-Ende-Verschlüsselung). Ein geringeres Schutzniveau besteht, wenn der US-Verarbeiter Ihre Daten entschlüsseln kann (was bei SaaS-Anwendungen zur weiteren Verarbeitung der Daten in der Regel notwendig ist). Zudem muss auch bedacht werden, dass häufig Inhalte verschlüsselt werden, aber nicht die Metadaten (d. h. z. B. Angaben, wer mit wem, wann und wo kommuniziert hat).
- **Kein Vorhandensein von Backdoors** – Um auch gegen behördliche Zugriffe geschützt zu sein, sollten Verschlüsselungsverfahren keine Möglichkeiten einer Hintertür für Behörden bieten (zumal solche Hintertüren, dann auch eine Gefahr für unerlaubte Zugriffe anderer Akteure bieten).

- **Zusicherung der Prüfung und Abwehr von Anfragen der US-Behörden** – Auch die Maßnahmen der US-Behörden müssen für sich beurteilt werden. So ist eine Anfrage im Fall schwerer Kriminalität, die sich auf evidente Tatsachen stützt und auf einen Einzelfall bezieht anders zu bewerten als eine unbegründete und verdachtslose Abfrage einer Vielzahl von Daten. Die Zusicherung diese Prüfung zu hinterfragen und sich gerichtlich gegen nicht erforderliche Abfragen zu wehren, steigert daher das Datenschutzniveau.
- **Zusicherung der Information über Behördenanfragen** – Eine gesonderte Zusicherung der Information im Fall behördlicher Anfragen (außer diese sind strafrechtlich untersagt) erhöht das Datenschutzniveau, da so z. B. eigene Abwehrmaßnahmen ergriffen werden können.
- **Art der Zusicherungen** – Zusicherungen der US-Verarbeiter wiegen je mehr, je verbindlicher sie erfolgen. So wäre eine vertragliche Verpflichtung keine Daten ohne Vorprüfung herauszugeben höher zu werten als ein einseitiges "Commitment".
- **Nachweis durch Audits** – Viele der technischen und organisatorischen Maßnahmen basieren letztendlich auf Vertrauen in den Anbieter. Dieses Vertrauen kann durch positive und unabhängige Prüfberichte bestätigt werden.
- **Verpflichtung zur Zahlung einer Vertragsstrafe** – Ein Indiz dafür, dass ein Anbieter seine Zusagen ernst meint, ist die explizite Verpflichtung eine Vertragsstrafe an betroffene Personen bei Verstößen zu zahlen. Allerdings wird dies aufgrund der unsicheren Rechtslage eher selten der Fall sein.
- **Keine Änderung der Standardvertragsklauseln** – Standardvertragsklauseln dürfen grundsätzlich nur unverändert genutzt werden. Ansonsten müssen die Datenschutzbehörden die Änderungen freigeben. Aus diesem Grund sollten Zusicherungen am besten in gesonderte Vereinbarungen aufgenommen werden.

Diese Liste ist nicht abschließend und kann um weitere Maßnahmen zur Erhöhung er Sicherheit ergänzt werden.

Step 7: Prüfung „Negatives Ergebnis"

Falls Ihre Prüfung negativ ausfallen sollen, müssen Sie entweder doch eine Alternative suchen, das Risiko eines bewussten Rechtsverstoßes eingehen oder zuerst eine Meldung an die Datenschutzbehörde erstatten und darauf hoffen, dass ihre Fallbearbeitung länger dauert als die Errichtung eines neuen "Privacy Shield 2". Wann dieser kommt, kann derzeit jedoch niemand vorhersagen. Bei dem aufgehobenen Privacy Shield dauerten die Verhandlungen 6 Monate, wobei das politische Klima zwischen der EU und den USA weitaus weniger angespannt war als es derzeit ist.

Wenn Sie mit Ihrer Abwägung zu dem Ergebnis kommen, dass ein angemessenes Datenschutzniveau besteht, dann können Sie die Nutzung der Dienste oder sonstige US-Transfers aufrechterhalten (sollten jedoch nach ca. 6-12 Monaten evaluieren, ob keine Änderungen eingetreten sind).

Sollten Sie im Ergebnis dazu gelangen, dass das Datenschutzniveau nicht aufrecht gehalten werden kann, stehen Ihnen die folgenden Optionen zur Verfügung:

- **Verarbeitung einstellen und eine Alternative wählen** – Damit wären Sie wieder beim Schritt 2 und müssten die dort genannten Nachteile der Alternativen in Kauf nehmen.

0800 400 510 1

AKTUELLE INFORMATION DATENTRANSFER IN DIE USA ERMÖGLICHEN

Datenschutz - Nr. 06/2021

Datenschutz

- **Anfrage bei der Datenschutzaufsichtsbehörde stellen** – Laut dem Europäischen Datenschutzausschuss und laut den Datenschutzbehörden sollen Sie Verarbeitungen, die nicht dem Datenschutzniveau genügen, den Datenschutzbehörden melden. Allerdings kann ich mir kaum vorstellen, dass die Behörden zu einem anderen Ergebnis gelangen werden als Sie.
- **Risiko eingehen** – Zumindest bisher scheint es nicht so, als ob Aufsichtsbehörden konkrete Schritte ergreifen und diese vor allem über die Untersagung reichen werden. Denn dies könnte einen wirtschaftlich und politisch unerwünschten Dominoeffekt auslösen, wenn die US-Transfers blockiert werden. Daher gehe ich auch nicht von der Verhängung von Bußgeldern aus. Insoweit erscheint das Risiko doch ein positives Ergebnis anzunehmen, aber weiter zu evaluieren sowie die Sach- und Rechtslage (bis ein neuer "Privacy Shield" beschlossen wird) zu beobachten als vertretbar. Das zumindest, wenn das Datenschutz niveau nicht offensichtlich unterschritten wird (Hinweis: Weder rate ich allgemein zu der Alternative, noch heiße ich sie gut).

Beispiele für die Fragebögen der Datenschutzbehörden:
Beispiele für die Fragebögen der Datenschutzbehörden finden Sie bei der Landesdatenschutzaufsicht Brandenburg z.B. für eingesetzte Webhoster, Mailhoster, Trackinganbieter, Bewerberportale und weitere
Für die Umsetzung in der Praxis hier eine Checkliste als Zusammenfassung

Checkliste SCC

1. **Schritt: Datentransfers in die USA erkennen**
   - In den US ansässige Unternehmen.
   - Unternehmen, die Subunternehmer aus den USA einsetzen (wenn unbekannt, nachfragen).

2. **Schritt: (EU-)Alternativen prüfen**
   - Kriterien: Gleiche Eignung, Funktionen, Usability, Kosten.

3. **Schritt: Rechtsgrundlagen prüfen**
   - Abschluss von Standardvertragsklauseln (Regelfall)
   - Binding Corporate Rules
   - Erforderliche Datentransfers
   - Einwilligungen
   - Weitere Ausnahmen

4. **Schritt: Anfragen stellen**

5. **Schritt: Bestimmung des Risikos für Betroffene**

0800 400 510 1

AKTUELLE INFORMATION DATENTRANSFER IN DIE USA ERMÖGLICHEN

Datenschutz - Nr. 06/2021

Datenschutz

6. **Schritt: Bewertung der Schutzmaßnahmen**
   - Verarbeitung auf EU-Servern.
   - Verschlüsselung.
   - Kein Vorhandensein von Backdoors.
   - Zusicherung der Prüfung und Abwehr von Anfragen der US-Behörden.
   - Zusicherung der Information über Behördenanfragen.
   - Nachweis durch Audits und Zertifikate.
   - Art der Zusicherungen (einseitig/ vertraglich).
   - Keine Änderung der Standardvertragsklauseln.
   - Information der Betroffenen über Risiken der US-Verarbeitung.

7. **Schritt: (Negatives) Ergebnis**
   - Verarbeitung einstellen und eine Alternative wählen
   - Anfrage bei der Datenschutzaufsichtsbehörde stellen
   - Risiko eingehen

Sehen Sie die in diesem Beitrag vorgestellten Maßnahmen als Hilfe an. So sind Sie in der Lage die Zulässigkeit von Datentransfers in die USA, bzw. den Einsatz von US-Dienstleistern und Diensten zu prüfen.

Die Durchführung senkt bereits das Risiko, selbst wenn Ihr Ergebnis noch ungewiss sein sollte. Denn anders als die Auswertung der Antworten, lassen sich die Anfragen nicht so schnell nachholen, sollte dies z. B. auf Nachfrage der Behörden hin notwendig werden (auch hier rate ich Ihnen die Prüfung dennoch vollständig und möglichst zeitnah durchzuführen).

Haben Sie noch Fragen oder benötigen Unterstützung? Gerne helfen wir Ihnen bei der Umsetzung.

datenschutzanfrage@fkc-gmbh.de