Internationaler Datenverkehr

Am 16. Juli 2020 sprach der Europäische Gerichtshof (EuGH) ein bedeutendes Urteil - das sogenannte Schrems II (16.07.2020, C-311/18). Mit dieser Entscheidung hat der EuGH festgestellt, dass Daten von EU-Bürgern nur an Drittländer außerhalb des Europäischen Wirtschaftraumes übermittelt werden dürfen, wenn die Daten in diesem Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU.

Der EuGH hat weiters das Privacy Shield Abkommen (dies regelte den Datentransfer von personenbezogenen Daten von der EU in die USA) für ungültig erklärt.

Was bedeutet das nun für Unternehmen der Hotellerie und Gastronomie als Verantwortliche für die Datenverarbeitung? Ganz klar, es herrscht Handlungsbedarf.

Wo und wie nun anfangen - unsere Empfehlungen:

Schritt 1

Prüfen Sie, wo die Systemanbieter (z.B. für PMS, Tischreservierung- und Onlinebuchungssysteme auf der Webseite, Newslettertools, CRM, etc.) und/oder Hoster (z.B. Amazon AWS) ihren Sitz haben bzw. Ihre Unternehmensdaten weiterleiten, verarbeiten oder auch lediglich eine Zugriffsmöglichkeit darauf haben.

Werden personenbezogene Daten in einen Staat innerhalb der EU / EWR transferiert, so ist ein einheitliches Schutzniveau der Daten vorhanden und es ist zunächst nichts weiter zu tun.

Schritt 2

Stellen Sie bei der Prüfung fest, dass personenbezogene Daten in einen Drittstaat übermittelt werden, prüfen Sie zuerst, ob es für diesen einen sogenannten Angemessenheitsbeschluss nach Art. 45 DSGVO gibt. In diesem Beschluss sind die Länder taxativ angeführt, für die die Europäische Kommission bestätigt, dass ein angemessenes Schutzniveau für die Verarbeitung von personenbezogenen Daten vorliegt. Wenn ja, dann ist keine weitere Voraussetzung für den Datentransfer erforderlich. (Abgesehen von einem Auftragsdatenverarbeitungsvertrag – den Sie ja generell mit all ihren Dienstleistern auch schon längst haben sollten. 😊)

TIPP: Die Europäische Kommission hat am 04. Juni 2021 zusätzlich Standardvertragsklauseln als Ersatz für die klassischen Vereinbarungen zur Datenverarbeitung im Auftrag nach Art. 28 DSGVO veröffentlicht, welche insbesondere für Vertragspartnern aus unterschiedlichen Herkunftsländern innerhalb der EU / EWR oder Länder mit einem Angemessenheitsbeschluss genutzt werden könne. Wir empfehlen diesen Entwurf zu nutzen, da inhaltlich der Text nicht verändert werden darf und somit von dem Vorliegen eines rechtskonformen Vertrags ausgegangen werden darf. Die Prüfung auf Vollständigkeit entfällt.

H3 Hotel Training & Beratung e.U. | Mag. (FH) Annemarie Maurer
Obere Straße 26 | 3553 Schiltern | +43 664 504 68 28 | office@h3training.at | www.h3training.at
FN 445044 b | AT54 3242 6000 0030 7090

Schritt 3

Sofern Daten in einem unsicheren Drittland verarbeitet werden, suchen Sie das Gespräch zum Dienstleister. Führen Sie rasch eine **Risikobewertung** bzw. **TIA** (Transfer Impact Assessment), welche sich aus Klausel 14 der neu abzuschließenden Standardvertragsklauseln (SCC) ergibt, durch.

Es müssen alle Risiken und Maßnahmen bewertet werden, die es „verhindern", dass Behörden des Drittlandes Zugriff auf Daten europäischer Bürger erhalten. Zusätzliche Sicherheiten, wie Verschlüsselung der Datenbanken oder ein Datenumzug in den EU/EWR Raum müssen garantiert werden, um eine weitere Nutzung rechtskonform zu ermöglichen. Dies ist nicht immer leicht – je mehr allerdings hier auf den Dienstleister zugehen, desto eher werden diese ihre Datenverarbeitungen überdenken.

Schritt 4

Sollten Ihre Gespräche und Bemühungen zu keinem Konsens führen und Sie partout nicht auf den Dienstleister verzichten möchten, prüfen Sie, ob Sie Standardvertragsklauseln für das jeweilige Land und Dienstanbieter nutzen können. Bis Ende 2022 sind alle bestehenden Standardvertragsklauseln (SCC Version 2010) zu ersetzen. Aktuell zu vereinbarende SCC sind ausnahmslos in der Version vom 04. Juni 2021 abzuschließen. Mehr dazu finden sie hier.

WICHTIG: Standardvertragsklauseln können nur dann verwendet werden, wenn Behörden oder sonstige Stellen des Drittlandes nicht in unverhältnismäßiger Art und Weise in die Rechte der betroffenen Personen eingreifen können (z.B. ein massenhafter Abruf von Daten ohne Information der Betroffenen und ohne verfahrensrechtliche Sicherungen wie einen Richtervorbehalt) und es einen wirksamen Rechtsschutz für die Betroffenen gibt. Für die USA wurde dies eben vom EuGH verneint, da der Rechtsschutz für EU-Bürger auf Grund der umfangreichen sicherheitsbehördlichen und geheimdienstlichen Befugnisse mangelhaft ist!

Schritt 5

Liegt für den Datentransfer in einen Drittstaat kein Angemessenheitsbeschluss vor und die Verwendung von Standardvertragsklauseln alleine bietet nicht genug Schutz, wie es z.B. im Fall eines Datentransfers in die USA ist, so sind zusätzliche Garantien wie z.B. eine Verschlüsselung der personenbezogenen Daten zu verwenden. Hier sollte die verantwortliche Stelle über den alleinigen Zugriff auf den Schlüssel verfügen.

H3 Hotel Training & Beratung e.U. | Mag. (FH) Annemarie Maurer
Obere Straße 26 | 3553 Schiltern | +43 664 504 68 28 | office@h3training.at | www.h3training.at
FN 445044 b | AT54 3242 6000 0030 7090

Schritt 6

Führt auch dies zu keinem gangbaren Weg mit Ihrem Dienstleister, so ist im letzten Schritt zu prüfen, ob eine Ausnahme für bestimmte Fälle für einen Datentransfer vorliegt. Dies wird wohl nur dann der Fall sein, wenn die betroffene Person in die vorgeschlagene Datenübermittlung ausdrücklich einwilligt (Art. 49 (1) a DSGVO, nachdem sie über die für sie bevorstehenden möglichen Risiken derartiger Datenübermittlung unterrichtet wurde.

Und hier stellen sich nun die Fragen:

Wie werden Gäste reagieren, wenn Sie von einem Datentransfer in einen unsicheren Drittstaat erfahren? Beschweren sie sich bei der Datenschutzaufsichtsbehörde?

Wo holen wir uns elegant und in der Guest Journey sinnvoll integriert die ausdrückliche Einwilligung für die Datenverarbeitung? Wie kann diese rechtssicher dokumentiert werden?

Wie kann ein Widerruf der betroffenen Person im Nachhinein abgewickelt werden? Eine Einwilligung kann ja jederzeit vom Betroffenen widerrufen werden. Ein Widerruf ist natürlich umgehend an den Dienstleister weiterzugeben und zu monitoren, ob die Daten entsprechend gelöscht werden. Wie kann diese rechtssicher dokumentiert werden?

Und was macht der Hotelier, wenn wesentliche Systeme, z.B. PMS/CRM oder Newslettertool, personenbezogene Daten in die USA oder ein anderes unsicheres Drittland übermitteln, der Gast aber nicht in die Datenverarbeitung einwilligt hat? Den Gast nicht beherbergen???

Wir empfehlen Ihnen daher, wenn Sie feststellen, dass Sie mit Dienstleistern zusammenarbeiten, die personenbezogenen Daten in einem unsicheren Drittland verarbeiten, zu prüfen, ob es für diese Leistung andere Dienstleister im EU/EWR Raum mit einem adäquaten Produkt (Qualität und Leistung) gibt. Führen Sie rasch einen Wechsel durch.

Gibt es Ihrer Ansicht nach kein vergleichbares Produkt, das ein Dienstleister im EU/EWR Raum anbietet, so bleibt als weitere Möglichkeit der Abschluss von Standardvertragsklauseln in Kombination mit weiteren Garantien (wie z.B. Verschlüsselung).

Kann auch diese Möglichkeit wie z.B. integrierte Dienste auf der Webseite wie bei der Verwendung von Trackingdiensten (z.B. Google Analytics, Facebook Pixel, …) oder Advertisingdienste (z.B. Google Ads, Google DoubleClick, …) nicht wahrgenommen werden, so ist die ausdrückliche Einwilligung des Betroffenen

H3 Hotel Training & Beratung e.U. | Mag. (FH) Annemarie Maurer
Obere Straße 26 | 3553 Schiltern | +43 664 504 68 28 | office@h3training.at | www.h3training.at
FN 445044 b | AT54 3242 6000 0030 7090

einzuholen. Alternativ kann der Dienst auch von der Webseite genommen werden, wenn eine Auswertung o.ä. nicht stattfindet.

Ausschließlich Sie als Datenverantwortlicher haften für die Datenverarbeitung. Es ist daher Ihre Pflicht, eine rechtskonforme Datenverarbeitung zu gewährleisten.

Autorin: Annemarie Maurer
H3 Hotel Training & Beratung, über 20 Jahre Berufserfahrung in so gut wie allen Detailbereichen der Hotellerie.
Für Hotels und Kurhotels der Garant für punktgenaue Lösungen, umsetzbare Strategien und treffsichere Maßnahmen im Bereich Datenschutz.

H3 Hotel Training & Beratung e.U. | Mag. (FH) Annemarie Maurer
Obere Straße 26 | 3553 Schiltern | +43 664 504 68 28 | office@h3training.at | www.h3training.at
FN 445044 b | AT54 3242 6000 0030 7090