

Brexit: UK wird „unsicheres Drittland“

Mit Ausscheiden von Großbritannien aus der EU sind auch Konsequenzen bei grenzüberschreitenden Verarbeitungstätigkeiten verbunden. Wie können Sie sich jetzt noch vorbereiten?

Auch der [Europäische Datenschutz Ausschuss](#) (EDPD) hat sich mit der Frage des Brexit beschäftigt, und dazu [Stellung](#) genommen.

UK wird „unsicheres Drittland“ – für Sie von Bedeutung?

Der Brexit ist datenschutzrechtlich für alle Organisationen als Verantwortlicher iSd DSGVO von Bedeutung, die

- über eine **Niederlassung** und/oder **Tochtergesellschaft** und/oder ein sonstiges **konzernverbundenes Unternehmen** in **GB** verfügen, dessen Daten in der EU verarbeitet werden, oder das Daten des Verantwortlichen verarbeitet
- **Dienstleister** (Auftragsverarbeiter, zB im Bereich Marketing, Clouddienstleistungen, Online-Tools etc..) mit Sitz in **GB** beauftragen
- zur Ausführung von eigenen **Leistungen Auftragnehmer in GB einsetzen** (zB Transportunternehmen für Warenlieferungen, Sub-Auftragnehmer zur Erbringung von Dienstleistungen)

Welche Datenkategorien können betroffen sein?

Grundsätzlich ist davon auszugehen, dass (zB bei einem Cloud-Dienst zur Speicherung von Daten) alle Datenkategorien, die der Verantwortliche verarbeitet, betroffen sein können.

Denken Sie zB an **Mitarbeiter- oder Bewerberdaten**, wenn Sie im Rahmen von Bewerbungsprozessen Tools einsetzen, die in GB gehostet werden, oder an Daten von **Kunden** oder **Lieferanten** bei der Speicherung von Daten im Rahmen von Cloud-Diensten. Wenn Sie Online-Dienste in ihrem Webshop oder auf der

Website nutzen, bei denen der Dienstleister seinen Sitz in GB hat, betrifft es auch Daten von Website-Besuchern, Interessenten oder Kunden.

Übermittlung von personenbezogenen Daten in ein unsicheres Drittland.

Damit die Übermittlung (Weitergabe) von personenbezogenen Daten von Betroffenen in ein Drittland zulässig ist, sind die Voraussetzungen der Art 44 ff DSGVO zu erfüllen. Es ist sicherzustellen, dass beim Empfänger der Daten ein angemessenes Schutzniveau für die Daten gegeben ist.

Auch in einem Konzernverbund ist dafür zu sorgen, dass die notwendige Rechtsgrundlage für die Übermittlung der Daten an einem Empfänger außerhalb der EU gegeben ist. Ein Konzernprivileg, das den „freien Fluss der personenbezogenen Daten“ im Konzern ermöglicht, gibt es in der DSGVO nicht.

Angemessenheitsbeschluss.

Dies kann durch einen sog. **Angemessenheitsbeschluss** der EU-Kommission erfolgen. Die EU prüft das Datenschutzniveau in einem Land und erklärt dann, ob in diesem Land ein angemessenes Schutzniveau für die personenbezogenen Daten herrscht, sodass eine Übermittlung der Daten an einen Empfänger in diesem Land ohne weitere Maßnahmen (so wie innerhalb der EU) zulässig ist. Es ist jedoch nicht zu erwarten, dass ein derartiger Beschluss kurzfristig erfolgt. In einem [Blogartikel vom 19.05.2018](#) habe ich die Länder, für die ein Angemessenheitsbeschluss besteht aufgezählt. Mittlerweile ist **Japan** dazugekommen.

Wenn keine „generelle Freigabe“ durch einen Angemessenheitsbeschluss besteht, dann ist auf individueller Ebene zwischen dem Verantwortlichen und dem Empfänger der Daten sicherzustellen, dass die Daten ordnungsgemäß behandelt werden.

Es ist nicht zu erwarten, dass für GB in Kürze ein Angemessenheitsbeschluss vorliegt.

Standarddatenschutzklauseln

Mit dem Abschluss einer Vereinbarung auf Basis von sog.

Standarddatenschutzklauseln („standard data protection clauses“) wird die Rechtmäßigkeit der Übermittlung der Daten eines Verantwortlichen an einen Empfänger in GB sichergestellt. Da derzeit noch keine „neuen“ Standarddatenschutzklauseln von einer Aufsichtsbehörde oder der EU-Kommission veröffentlicht sind, muss man auf die bisherigen [Standardvertragsklauseln](#) zurückgreifen, die gem. Art 46 Abs 5 DSGVO nach wie vor Gültigkeit haben.

Neben dem Abschluss des relevanten Vertrages mit dem Empfänger wird es auch nötig sein, die Einhaltung der Vorgaben, die sich aus dem Vertrag ergeben zu prüfen. Jedenfalls sollte sich jeder Verantwortliche das Datenschutzkonzept des Empfängers vorlegen lassen, und auf Angemessenheit prüfen.

Die Übermittlung ist vertraglich erforderlich.

Eine Übermittlung von Daten an einen Empfänger in Großbritannien, ist ohne weitere Maßnahmen zulässig, wenn diese für „**die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich**“ (Art 49 Abs 1 lit b DSGVO; Ausnahme)

Wenn ihr Unternehmen zB ein Reisebüro ist, das Buchungen für Hotels von Kunden in Großbritannien vorgenommen hat, dann ist die Übermittlung der Daten auf dieser Grundlage zulässig, da ihr Unternehmen als Verantwortlicher einen Vertrag mit den betroffenen Personen (Kunden) abgeschlossen hat, und die Übermittlung der personenbezogenen Daten (Name, Vorname, Adresse etc..). Auch wenn ein Sub-Unternehmer, der zur Leistungserbringung gegenüber den betroffenen Personen eingesetzt wird, und es notwendig ist, dass diesem auch personenbezogene Daten zur Verfügung gestellt werden, damit der Vertrag erfüllt werden kann, ist diese Datenweitergabe zulässig.

Einzelgenehmigung durch die DSB.

Art 46 Abs 3 lit a DSGVO sieht dies vor, dass die **DSB konkrete Vertragsklauseln**, die zwischen dem **Verantwortlichen** oder dem

Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, **genehmigen** kann. Ein Verantwortlicher kann sich daher auch – wie schon zu Zeiten des DSGVO 2000 – an die DSB wenden, und den „internationalen Datenverkehr“ genehmigen lassen.

Notwendigkeit zur Vertragserfüllung im Interesse von betroffenen Personen.

Wenn die Übermittlung zum **Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person** von dem **Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich** ist, dann ist die Übermittlung ebenfalls zulässig. Es ist nicht nötig, dass die betroffene Person selbst Vertragspartner des Vertrages ist, dessen Abschluss oder Erfüllung die Datenübermittlung erforderlich macht. Wenn ein Sub-Unternehmer, der zur Leistungserbringung gegenüber den betroffenen Personen eingesetzt wird, und es notwendig ist, dass diesem auch personenbezogene Daten zur Verfügung gestellt werden, damit der Vertrag mit der betroffenen Person („in deren Interesse“) erfüllt werden kann, ist diese Datenweitergabe zulässig.

Diese Ausnahmebestimmung ist nur dann anwendbar, wenn die Datenübermittlung gelegentlich erfolgt (siehe ErwG 111). Wenn die Übermittlung im Massenkundengeschäft erfolgt, zB Zahlungsverkehr oder Flugbuchungen, dann sollte auf andere Rechtsgrundlagen (zB Standarddatenschutzklauseln) zurückgegriffen werden.

nicht wiederholte Drittlandsübermittlung / begrenzte Anzahl von Personen

Übermittlungen, die als nicht wiederholt erfolgend gelten können und nur eine begrenzte Zahl von betroffenen Personen betreffen, könnten auch zur Wahrung der zwingenden berechtigten Interessen des Verantwortlichen möglich sein, sofern die Interessen oder Rechte und Freiheiten der betroffenen Person nicht überwiegen und der Verantwortliche sämtliche Umstände der Datenübermittlung geprüft hat, und der Verantwortliche alle Umstände der

Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung angemessene Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat.

Es ist zu beachten, dass auch diese konkreten berechtigten Interessen den betroffenen Personen mitzuteilen sind.

Rechtsansprüche

Es ist zulässig, personenbezogene Daten in ein Drittland zu übermitteln, wenn dies zur Geltendmachung, Ausübung oder zur Verteidigung von Rechtsansprüchen erforderlich ist.

genehmigte Verhaltensregeln

Auch auf Basis von genehmigten Verhaltensregeln gem. Art 40 DSGVO, die zB für eine Branche Geltung haben können, und in denen auch die Garantien für die betroffenen Personen festzulegen sind. Auch bei diesem „Instrument“ der Festlegung von datenschutzrechtlichen Verhaltensweisen innerhalb einer Branche ist eine Genehmigung durch eine Aufsichtsbehörde erforderlich.

Derzeit bestehen in Österreich [Verhaltensregeln des Direct Marketing Verbandes Österreich](#) sowie [Verhaltensregeln für Glückspielbetreiber](#), die jeweils noch nach DSGVO genehmigt wurden, und [Verhaltensregeln der Internet Service Provider \(ISPs\)](#) nach DSGVO.

Was ist konkret zu tun?

- 1. Analyse der Zulässigkeit der Datenübermittlung**, wobei insbes. auch zu prüfen ist, ob es erforderlich ist, dass die Daten in personenbezogener Form an den Empfänger übermittelt werden, oder ob es zB möglich wäre, die Daten in einer Form zu übermitteln, die es dem Empfänger nicht erlaubt, auf die natürliche Person Rückschlüsse zu ziehen. Dies entspricht mE auch dem Grundprinzip der Datenminimierung.

2. Prüfung der Frage, ob die Daten **regelmäßig** oder nur **gelegentlich** übermittelt werden, und daran anschließend die **Festlegung** auf welcher **konkreten Rechtsgrundlage** die Daten übermittelt werden können bzw. ob diese Rechtsgrundlage (zB Standardvertragsklauseln) noch geschaffen werden müssen.



dataprotect
— it-recht

3. Informationspflicht iSd Art 13 und 14 DSGVO

Sie müssen die Betroffenen über die Tatsache, dass deren Daten in ein „unsicheres Drittland“ übermittelt werden informieren. Etwaige Datenschutzinformationen (zB auf der Website, im Kundenportal oder sonstige Dokumentationen) sind daher zu ergänzen bzw. zu überarbeiten.

4. Verzeichnis gem. Art 30 DSGVO

Im Verzeichnis ist immer anzugeben, ob Daten in ein Drittland übermittelt werden. Da mit dem Austritt Großbritannien zu einem unsicheren Drittland wird, ist auch das Verzeichnis zu überarbeiten.

5. Datenschutz-Folgenabschätzungen

Es ist zu analysieren, ob Datenschutz-Folgenabschätzungen zu überarbeiten sind, zB weil Übermittlungen nun in ein unsicheres Drittland erfolgen. Da die österreichische [DSFA-V](#) nicht auf Empfängerländer als Kriterien für das Risiko abstellt, wird jedoch vermutlich die Analyse keine Änderungen bei einer DSFA bringen.



Disclaimer:

Dieses Dokument kann eine individuelle Beratung nicht ersetzen.

Es enthält allgemeine Hinweise.

Es wird keine Haftung dafür übernommen.

Version 1.0

24.02.2019