Hinweise zur Übermittlung von Daten nach der Datenschutz-Grundverordnung (DSGVO) im Fall eines ungeregelten Brexit

Angenommen am 12. Februar 2019

Einleitung

Kommt es zu keiner Vereinbarung zwischen dem EWR und dem Vereinigten Königreich (ungeregelter Brexit), wird das Vereinigte Königreich am 30. März 2019 um 00:00 Uhr MEZ zum Drittland werden. Das bedeutet, dass die Übermittlung personenbezogener Daten an das Vereinigte Königreich ab dem 30. März 2019 auf der Grundlage folgender Instrumente[1] zu erfolgen hat:

- Standard- oder Ad-hoc-Datenschutzklauseln
- Verbindliche interne Datenschutzvorschriften
- Verhaltensregeln und Zertifizierungsmechanismen
- Ausnahmen[2]

Die vorliegenden Hinweise enthalten Informationen für nicht-öffentliche und öffentliche Organisationen über die nach der DSGVO vorgesehenen Instrumente zur Übermittlung personenbezogener Daten an das Vereinigte Königreich im Fall eines ungeregelten Brexit.

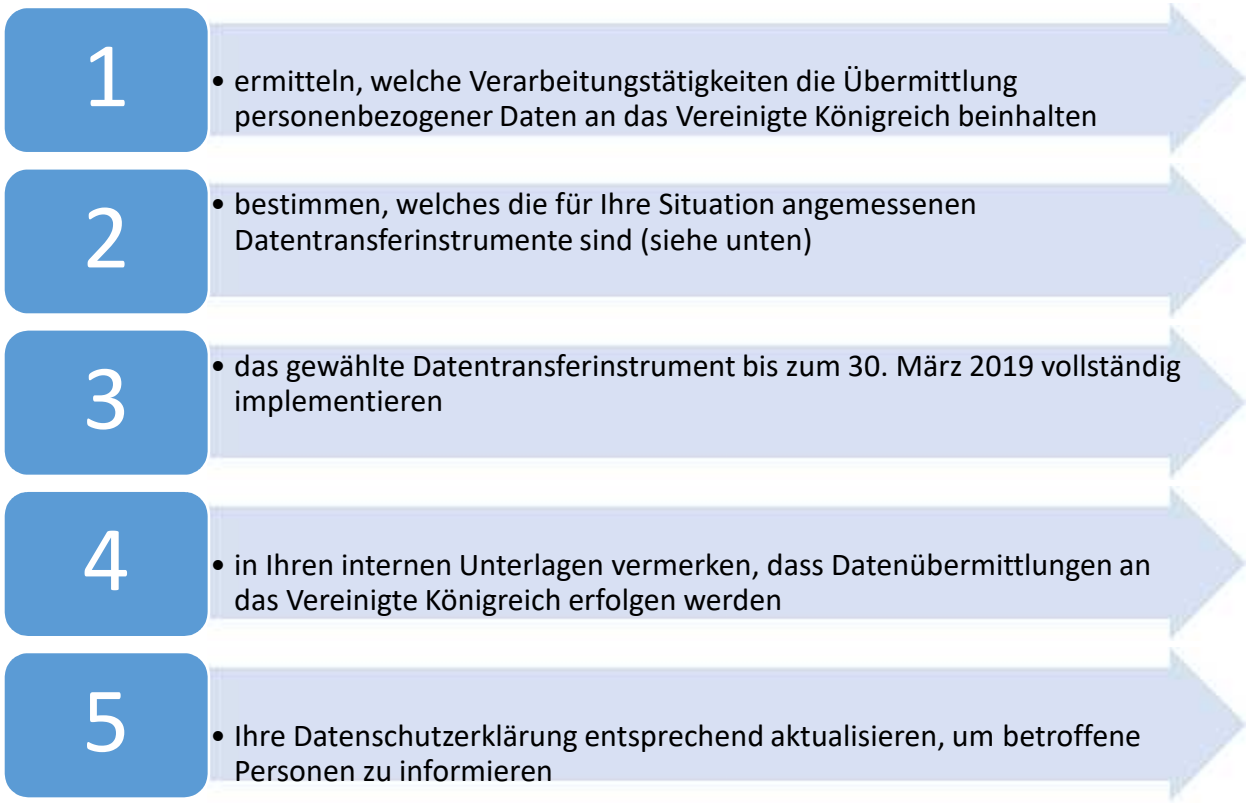
Der Europäische Datenschutzausschuss (EDSA) zieht die Orientierungshilfen heran, die in dieser Angelegenheit von den Aufsichtsbehörden und der Europäischen Kommission bereitgestellt wurden. Organisationen im EWR können sich erforderlichenfalls an die für die Aufsicht der entsprechenden Verarbeitungstätigkeiten zuständigen nationalen Aufsichtsbehörden wenden.

[1] Vgl. Kapitel V DSGVO.

[2] Diese können nur angewendet werden, wenn Standarddatenschutzklauseln oder andere geeignete Garantien fehlen.

I. 5 Maßnahmen, die Organisationen zur Vorbereitung auf einen ungeregelten Brexit ergreifen sollten

Bei der Übermittlung von Daten an das Vereinigte Königreich sollten Sie



II. Datenübermittlungen aus dem EWR an das Vereinigte Königreich

1. *Verfügbare Datentransferinstrumente*

Liegt zum Zeitpunkt des Brexit kein Angemessenheitsbeschluss[3] vor, stehen folgende Instrumente zur Datenübermittlung zur Verfügung.

a. Standard- und Ad-hoc-Datenschutzklauseln

Sie und Ihr Ansprechpartner im Vereinigten Königreich können die Verwendung von Standarddatenschutzklauseln vereinbaren, die von der Europäischen Kommission genehmigt wurden. Solche Verträge bieten die zusätzlichen angemessenen Garantien im Hinblick auf den Datenschutz, die im Falle der Übermittlung personenbezogener Daten an Drittländer erforderlich sind.

[3] Ein Angemessenheitsbeschluss ist ein von der Europäischen Kommission auf der Grundlage von Art. 45 DSGVO angenommener Beschluss (wie beispielsweise der von der Kommission am 23. Januar 2019 angenommene Angemessenheitsbeschluss über Japan. Auch für Drittländer wie u. a. Argentinien, Neuseeland und Israel hat die Kommission in der Vergangenheit Angemessenheitsbeschlüsse angenommen). Derzeit ist für das Vereinigte Königreich kein Angemessenheitsbeschluss in Kraft.

Derzeit stehen drei Zusammenstellungen von Standarddatenschutzklauseln zur Verfügung:

- Datenübermittlung von einem für die Verarbeitung Verantwortlichen in einem EWR-Land an einen für die Verarbeitung Verantwortlichen in einem Drittland (z. B. das Vereinigte Königreich): Hierzu sind zwei Zusammenstellungen verfügbar:
  - 2001/497/EG
  - 2004/915/EG
- Datenübermittlung von einem für die Verarbeitung Verantwortlichen in einem EWR-Land an einen Auftragsverarbeiter in einem Drittland (z. B. das Vereinigte Königreich):
  - 2010/87/EU

Hervorzuheben ist, dass die Standarddatenschutzklauseln nicht geändert werden dürfen und so zu unterzeichnen sind, wie sie von der Europäischen Kommission zur Verfügung gestellt wurden. Diese Vereinbarungen können jedoch in einen umfassenderen Vertrag eingebettet werden, in den zusätzliche Klauseln aufgenommen werden können, sofern diese mit den von der Europäischen Kommission angenommenen Standarddatenschutzklauseln nicht direkt oder indirekt in Widerspruch stehen. Mit Blick auf den Zeitrahmen bis zum 30. März bestätigt der EDSA, dass die Standarddatenschutzklauseln ein Instrument sind, das zur Verwendung fertig bereitsteht.

Werden zusätzliche Änderungen an den Standarddatenschutzklauseln vorgenommen, so führt dies dazu, dass sie als Ad-hoc-Vertragsklauseln gelten. So können geeignete Garantien geschaffen werden, die Ihre besondere Situation berücksichtigen.

Diese maßgeschneiderten Vertragsklauseln müssen vor jeglicher Übermittlung von Daten von der zuständigen Aufsichtsbehörde genehmigt werden, nachdem der EDSA Stellung genommen hat.

b. Verbindliche interne Datenschutzvorschriften

Verbindliche interne Datenschutzvorschriften sind Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich eine Unternehmensgruppe (d. h. multinationale Unternehmen) verpflichtet, um geeignete Garantien für die Übermittlung personenbezogener Daten auch außerhalb des EWR zu gewährleisten.

Möglicherweise verwenden Sie bereits verbindliche interne Datenschutzvorschriften oder arbeiten mit Auftragsverarbeitern zusammen, die verbindliche interne Datenschutzvorschriften für Auftragsverarbeiter verwenden. Organisationen dürfen solche nach der früheren Richtlinie 95/46/EG genehmigten verbindlichen internen Datenschutzvorschriften auch weiterhin verwenden, die unter der DSGVO wirksam bleiben[4].

[4] Gemäß Art. 46 Abs. 5 DSGVO. Beachten Sie bitte, dass verbindliche interne Datenschutzvorschriften, die nach der früheren Richtlinie 95/46/EG genehmigt wurden, unter der DSGVO gültig bleiben, jedoch aktualisiert werden müssen, um mit den Bestimmungen der DSGVO vollständig im Einklang zu stehen.

Diese verbindlichen internen Datenschutzvorschriften müssen jedoch aktualisiert werden, um mit den Bestimmungen der DSGVO vollständig im Einklang zu stehen.

Falls Sie noch keine verbindlichen internen Datenschutzvorschriften implementiert haben, müssen diese von der zuständigen nationalen Aufsichtsbehörde genehmigt werden, nachdem der EDSA Stellung genommen hat.

Weitere Informationen zu den Antragsbedingungen für verbindliche interne Datenschutzvorschriften finden Sie auf der Website des EDSA.

c. Verhaltensregeln und Zertifizierungsmechanismen

Verhaltensregeln und Zertifizierungsmechanismen können geeignete Garantien für die Übermittlung personenbezogener Daten bieten, wenn sie rechtlich verbindliche und durchsetzbare Pflichten für die Organisation im Drittland zugunsten natürlicher Personen enthalten.

Diese Instrumente wurden in der DSGVO neu geschaffen und der EDSA arbeitet an Leitlinien, die die harmonisierten Bedingungen und Verfahren zur Nutzung dieser Instrumente näher erläutern.

2. *Ausnahmen*

Hervorzuheben ist, dass die Ausnahmen Datenübermittlungen unter bestimmten Bedingungen erlauben und es sich dabei um Ausnahmen von der Regel handelt, dass geeignete Garantien zu implementieren sind (siehe die vorstehend genannten Instrumente wie verbindliche interne Datenschutzvorschriften, Standarddatenschutzklauseln etc.) oder die Daten auf der Grundlage eines Angemessenheitsbeschlusses übermittelt werden. Sie sind daher eng auszulegen und beziehen sich überwiegend auf Verarbeitungstätigkeiten, die nur gelegentlich erfolgen und sich nicht wiederholen[5].

Diese Ausnahmen gelten nach Art. 49 DSGVO unter anderem für Fälle, in denen

- eine natürliche Person ausdrücklich in die vorgeschlagene Datenübermittlung eingewilligt hat, nachdem sie sämtliche erforderlichen Informationen über die für sie bestehenden möglichen Risiken der Datenübermittlung erhalten hat,
- die Übermittlung zur Erfüllung oder zum Abschluss eines Vertrags zwischen der natürlichen Person und dem für die Verarbeitung Verantwortlichen erforderlich ist oder der Vertrag im Interesse der natürlichen Person geschlossen wurde,
- die Übermittlung aus wichtigen Gründen des öffentlichen Interesses notwendig ist,
- die Übermittlung aufgrund zwingender berechtigter Interessen der Organisation notwendig ist.

Weitere Erklärungen zu den verfügbaren Ausnahmen und deren Anwendung finden Sie in den Leitlinien des EDSA zu den Ausnahmen nach Art. 49 DSGVO.

3. *Instrumente, die ausschließlich Behörden oder öffentlichen Stellen zur Verfügung stehen*

[5] Vgl. Erwägungsgrund 113 und Art. 49 Abs. 1 DSGVO.

Behörden können Mechanismen verwenden, die der DSGVO zufolge ihrer Situation besser entsprechen.

Eine Möglichkeit ist die Verwendung eines rechtlich bindenden und durchsetzbaren Dokuments wie beispielsweise Verwaltungsvereinbarungen und bi- oder multilaterale internationale Abkommen. Eine solche Vereinbarung muss für die Unterzeichner rechtsverbindlich und durchsetzbar sein.

Eine zweite Möglichkeit ist, administrative Regelungen wie etwa ein Memorandum of Understanding zu verwenden, die zwar nicht rechtsverbindlich sind, jedoch durchsetzbare und wirksame Rechte für betroffene Personen vorsehen müssen. Die administrativen Regelungen müssen von der zuständigen nationalen Aufsichtsbehörde genehmigt werden, nachdem der EDSA Stellung genommen hat.

Darüber hinaus stehen die vorstehend genannten Ausnahmen auch für durch Behörden vorgenommene Datenübermittlungen zur Verfügung, sofern die entsprechenden Voraussetzungen erfüllt sind.

Für Strafverfolgungsbehörden[6] sind zusätzliche Instrumente zur Datenübermittlung verfügbar[7].

III. Datenübermittlungen aus dem Vereinigten Königreich an *Mitglieder* des EWR.

Der Regierung des Vereinigten Königreichs zufolge wird die derzeitige Praxis, wonach der freie Fluss personenbezogener Daten aus dem Vereinigten Königreich an den EWR erlaubt ist, im Falle eines ungeregelten Brexit weitergeführt[8].

Hierzu sollten Sie die Websites der britischen Regierung und des britischen Datenschutzbeauftragten (Information Commissioner Office - ICO) regelmäßig konsultieren.

Für den Europäischen Datenschutzausschuss
Die Vorsitzende

(Andrea Jelinek)

[6]Diese fallen in den Anwendungsbereich der JI-Richtlinie (Richtlinie (EU) 2016/680).
[7] Vgl. Art. 37 und 38 der JI-Richtlinie. Beispielsweise dürfen Datenübermittlungen stattfinden, wenn die EU-Behörde nach eigener Beurteilung aller Umstände im Zusammenhang mit der Datenübermittlung zu dem Schluss kommt, dass in dem Drittland geeignete Garantien bestehen. Ferner können zusätzliche Ausnahmen für bestimmte Fälle Anwendung finden (vgl. Art. 38 der JI-Richtlinie).
[8]https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal