"DSGVO-Gefahren und Verfahren beim Brexit"

Die Diskussionen um den Brexit nehmen seit Monaten kein Ende. Und egal, welche Meinung man dazu vertritt und welche Lösung man favorisiert, klar ist, dass eine Großzahl deutscher Unternehmen von dem Austritt Groß-Britanniens aus der EU betroffen sein wird - und das wahrscheinlich deutlich heftiger, als vielen bisher klar ist.

Nun wollen wir uns nicht einreihen in die politischen Diskussionen oder in die Diskussionen über Ursachen und Auslöser des Brexit. Fakt ist aber, der 29.03.2019, das voraussichtliche Austrittsdatum Groß-Britanniens aus der EU, rückt immer näher, schneller als gewollt, und viele Unternehmen sind sich der Folgen gerade eines ungeregelten Brexits nicht bewusst.

Zwar sieht der zwischen der EU-Kommission und der britischen Regierung ausgehandelte Vertragstext in Art. 70 f vor, dass die DSGVO (mit Ausnahme der Bestimmungen über die Zusammenarbeit der Aufsichtsbehörden, Kapitel VII, Art.60 ff DSGVO) für die vorgesehene Übergangszeit von 2 Jahren weiter Geltung behalten soll. Mittlerweile ist aber wohl sicher, dass der verhandelte Vertragstext keine Anwendung wird finden können.

Datenschutzrechtliche Konsequenzen des Brexit für die Verantwortlichen i.S.d. DSGVO

Nun macht sich kaum ein Unternehmen Gedanken darüber, welche datenschutzrechtlichen Konsequenzen ein ungeregelter Brexit mit sich bringt. Viele Unternehmen übermitteln Kunden- oder Beschäftigtendaten nach Groß-Britannien, nutzen IT-Leistungen von Anbietern in Groß-Britannien, Rechenzentren, setzen damit Auftragsverarbeiter in Groß-Britannien ein oder arbeiten mit Auftragsverarbeitern zusammen, die Subunternehmer in Groß-Britannien einsetzen etc. Häufig betroffen sind Unternehmensgruppen/Konzerne, Joint-Ventures, Lieferketten, IT-gestützte Prozesse etc.

Fakt ist und bleibt aber, dass mit dem 29.03.2019 Groß-Britannien, wenn es aus der EU austritt, zu einem „Drittland“ im Sinne der Art. 44 ff DSGVO wird. Und das bedeutet, dass Verantwortliche in Deutschland (und auch im Rest der EU) ab diesem Zeitpunkt bei der weiteren Zusammenarbeit mit Konzernunternehmen, Kunden, Partnern, Dienstleistern etc. in Groß-Britannien, die Regelungen der Art. ff 44 DSGVO hinsichtlich der Übermittlung personenbezogener Daten in ein Drittland konsequent einhalten müssen, andernfalls die Datenübermittlungsvorgänge illegal werden.

Erforderliche Anpassungen

Folgende Konstellationen sollte jedes verantwortliche Unternehmen daher umgehend für sich prüfen, damit nicht kurzfristig und hektisch kurz vor dem 29.03.2019 wichtige Dokumente erstellt oder angepasst werden müssen, um zu verhindern, dass die Zusammenarbeit mit den Partnern in Groß-Britannien mangels Rechtsgrundlage für eine Datenübermittlung, rechtswidrig wird:

1. Es muss geprüft werden, ob Auftragsverarbeiter nach Art. 28 DSGVO eingesetzt werden, die ihren Sitz/ihre Niederlassung in Groß-Britannien haben oder zumindest dort personenbezogene Daten verarbeiten.
2. Es muss festgestellt werden, ob das verantwortliche Unternehmen selber Niederlassungen (selbständig oder unselbständig) in Groß-Britannien hat.
3. Es muss geprüft werden, ob die eingesetzten Auftragsverarbeiter selber Sub-Unternehmer (Unter-Auftragsverarbeiter) nach Art. 28 Abs. 2 DSGVO in Groß-Britannien einsetzten.

Wenn auch nur eine dieser Konstellationen zutrifft, ist das verantwortliche Unternehmen gezwungen, die besonderen Voraussetzungen der Art. 44 ff DSGVO als zusätzliche Maßnahmen zur Sicherstellung des Datenschutzniveaus zu ergreifen.

Das bedeutet zumindest folgendes:

- Einerseits sind bei der Übermittlung personenbezogener Daten nach Groß-Britannien (als Drittland) natürlich die allgemeinen Voraussetzungen der DSGVO zu berücksichtigen, d.h., insbesondere die Grundsätze nach Art. 5 DSGVO, sowie das Vorliegen einer Erlaubnisnorm nach Art. 6 Abs. 1 Satz 1 DSGVO (sowie ggf. zusätzlicher nationaler Regelungen)
- Außerdem sind die Voraussetzungen der Art. 44 ff DSGVO an die Datenübermittlung einzuhalten: d.h. es ist die sog. zweistufige Prüfung durchzuführen.
- Schließlich sind die erweiterten Informationspflichten zu berücksichtigen, da ja ein Datentransfer in ein Drittland erfolgt, worüber jeder ausdrücklich Betroffene informiert werden muss. D.h., es müssen sämtliche bereit gestellten Informationen angepasst werden (z.B. Datenschutzerklärung auf der Website, Information gegenüber Beschäftigten oder Geschäftspartnern, etc.). Denn nach Art. 13 Abs. 1 lit. f sowie Art. 14 Abs. 1 lit. f DSGVO muss der Verantwortliche den Betroffenen gesondert darüber informieren, dass ein Datentransfer in ein Drittland erfolgt.
- Ebenso muss die Information des anfragenden Betroffenen im Falle der Geltendmachung eines Auskunftsrechts nach Art. 15 Abs. 1 lit. c DSGVO um den Hinweis auf die Übermittlung in ein Drittland ergänzt werden.
- Nicht zu vergessen, dass Verfahren, bei denen eine Datenübermittlung in ein Drittland erfolgt ,als solche nach Art. 30 Abs. 1 lit. d und e bzw. Abs. 2 lit. c DSGVO in das Verzeichnis von Verarbeitungstätigkeiten aufgenommen werden müssen.

Schaffung geeigneter Garantien für den Datentransfer in ein Drittland?

Sicher wäre der schönste und für die verantwortlichen Unternehmen einfachste Weg ein sog. Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO. Damit würde nämlich einheitlich festgestellt, dass Groß-Britannien ein Datenschutzniveau bietet, welches dem der EU entspricht, so dass Unternehmen dann ohne weitere Hürden personenbezogenen Daten nach Groß-Britannien übermitteln dürften. Es ist jedoch vollkommen unrealistisch, anzunehmen, dass eine entsprechende Entscheidung, bzw. ein derartiger Beschluss der EU-Kommission so kurzfristig getroffen werden könnte. Denn es müsste nicht nur das im Jahr 2018 verabschiedete neue britische Datenschutzgesetz bewertet werden, sondern die gesamte britische Rechtsordnung - darunter auch der äußerst umstrittene „Investigatory Power Act“ (IPA) (der laut UK High Court gegen EU-Recht verstößt, was dann ja eigentlich nicht mehr relevant wäre) und dessen Nachbesserungsgesetzt „Data Retention and Acquisition Regulations 2018“, welche den britischen Sicherheitsbehörden umfassende Befugnisse hinsichtlich personenbezogener Daten einräumen. Außerdem dürfte in der EU politisch wohl kaum ein Bedürfnis oder der Wunsch nach einer derartigen Lösung (über einen Angemessenheitsbeschluss) bestehen. Das bedeutet letztlich, dass die Verantwortlichen selber gefordert sind geeignete Lösungen und Garantien zu schaffen.

Grundsätzlich sind dies die Folgenden:

- Der Abschluss der EU-Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO für den Datentransfer zwischen Verantwortlichem und Auftragsverarbeitern bzw. weiteren Verantwortlichen, wodurch ein angemessenes Datenschutzniveau erreicht würde.
- Der Abschluss von sog. Binding Corporate Rules (BCR) nach Art. 47 DSGVO, welche von den Aufsichtsbehörden unter gewissen Voraussetzungen genehmigt werden und die für einen freien Datenfluss innerhalb von internationalen Konzernen/Unternehmensgruppen geeignet sind. Allerdings ist **nicht** davon auszugehen, dass in der kurzen Zeit bis zum 29.03.2019 das Genehmigungsverfahren für solche BCR noch erfolgreich durgeführt werden könnte.
- Gleiches gilt für genehmigte Verhaltensregeln oder Zertifizierungen nach Art. 40 f DSGVO, welche ebenfalls von den Aufsichtsbehörden zu genehmigen wären, was bis zum 29.03.2019 aber ebenfalls **nicht** erfolgreich sein dürfte.

Fazit

Jeder Verantwortliche im Sinne der DSGVO sollte dringend und schnellst möglich geeignete Maßnahmen treffen, um sicher zu stellen, dass ein momentan noch zulässiger Datentransfer nach Groß-Britannien auch nach dem 29.03.2019 zulässig bleibt, um nicht ab dem Zeitpunkt des voraussichtlich ungeregelten Austritts Groß-Britanniens aus der EU rechtswidrig zu handeln. Es ist nicht davon auszugehen, dass bis zum 29.03.2019 eine politische Lösung gefunden wird. Wer daher jetzt keine Maßnahmen für den Datentransfer nach Groß-Britannien ergreift, handelt grob fahrlässig und ab dem 29.03.2019 rechtswidrig.

Wir möchten Ihnen daher dringend ans Herz legen, die oben unter den Punkten 1 bis 3 aufgezählten Konstellationen für Ihr Unternehmen zu prüfen und, wenn Sie betroffen sind, dementsprechend schnell zu handeln. Gerne beraten und unterstützen wir Sie bei den datenschutzrechtlichen Herausforderungen durch - den aller Voraussicht nach anstehenden - ungeregelten Brexit.

REVIDATA GmbH

Düsseldorf, den 30.01.2019
Autorin: Rechtsanwältin, Ulrike-Alexandra Seitzinger MBA

REVIDATA GmbH
Tel.: +49 211 49690-0
Fax: +49 211 49690-29
E-Mail: info@revidata.de
Home: www.revidata.de

Wir beraten Sie gerne und freuen uns auf Ihre geschätzte Kontaktaufnahme!