BREXIT – Datenschutzrechtliche Auswirkungen seit dem 1. Januar 2021

11.01.2021

Datenschutz | Digital Business | Arbeitsrecht | Brexit | Brüssel

Ablauf des Übergangszeitraums

Schon seit geraumer Zeit stellen sich für in der EU ansässige Unternehmen Fragen zu den datenschutzrechtlichen Auswirkungen des Brexit nach Ablauf des Übergangszeitraums. Mit Abschluss des Handels- und Kooperationsabkommens haben die EU und das Vereinigte Königreich Ende Dezember letzten Jahres nun zwar einen „No Deal" Brexit noch in letzter Minute verhindert – doch was bedeutet das für Transfers personenbezogener Daten aus der Europäischen Union nach UK? Ist das Vereinigte Königreich nun im datenschutzrechtlichen Sinn ein unsicheres „Drittland"? Was müssen europäische Unternehmen beachten, um weiterhin Compliance mit den EU-Datenschutzvorschriften sicherzustellen?

Hintergrund

Am 1. Januar 2021 hat das Vereinigte Königreich den EU-Binnenmarkt und die Zollunion verlassen. Bis zuletzt verhandelten die Europäische Kommission und das Vereinigte Königreich über die Bedingungen ihrer zukünftigen Zusammenarbeit. Schließlich kam eine Einigung zustande, so dass am 31. Dezember 2020 das Handels- und Kooperationsabkommen zwischen der EU und dem Vereinigten Königreich in Kraft treten konnte. Dieses Abkommen regelt in seinen Schlussbestimmungen unter anderem auch Datentransfers aus der EU nach Großbritannien und deren datenschutzrechtliche Bewertung.

Anforderungen an Datentransfers in „Drittländer" außerhalb der Europäischen Union

In der EU legt die Datenschutz-Grundverordnung (DS-GVO) den Rechtsrahmen und die Voraussetzungen fest, unter denen personenbezogene Daten international übertragen werden dürfen. Sie differenziert dabei zwischen sicheren und unsicheren Drittländern. Sichere Drittländer sind solche, deren Datenschutzniveau die Europäische Kommission durch einen Angemessenheitsbeschluss als dem Datenschutzniveau in der EU vergleichbar eingestuft hat. Zu diesen sicheren Drittländern gehören unter anderem Kanada, Neuseeland, die Schweiz und Japan.

Die USA gehören derzeit beispielsweise nicht dazu. Mit dem Urteil „Schrems II" vom 16. Juli 2020 hat der EuGH den Angemessenheitsbeschluss über das EU-US-Datenschutzschild (Privacy Shield) für ungültig erklärt. Um Daten in die USA zu übertragen, müssen die Verantwortlichen daher individuell sicherstellen, dass die personenbezogenen Daten beim Empfänger ausreichend geschützt sind. Hierzu sieht die DS-GVO in Art. 44 ff. eine Reihe von Instrumenten vor, beispielsweise den in der Praxis sehr relevanten Abschluss von Standarddatenschutzklauseln. Allerdings hat der EuGH in Schrems II auch betont, dass Standarddatenschutzklauseln einen Drittstaatentransfer nicht rechtfertigen können, wenn Rechtslage und Praxis im Drittland dazu führen, dass der Datenimporteur die Verpflichtungen aus den Standarddatenschutzklauseln nicht einhalten kann. Es liegt in der Verantwortung der Unternehmen, die konkreten Datentransfers im Einzelnen zu analysieren und festzustellen, welche Gesetze des Drittlandes jeweils Anwendung finden und ob diese Gesetze die von ihnen mit Unterzeichnung der Standarddatenschutzklauseln gegebenen Garantien beeinträchtigen. Gegebenenfalls müssen der Datenexporteur und -importeur zusätzlich zu den Standarddatenschutzklauseln ergänzende Maßnahmen treffen, um ein angemessenes Datenschutzniveau zu gewährleisten.

Die Einordnung als unsicheres Drittland birgt also eine Reihe von Risiken und Unsicherheiten und führt zu erheblichem Mehraufwand bei Unternehmen, die Daten an Empfänger in Drittländern übermitteln möchten.

Vorläufige Regelung: Keine Behandlung des Vereinigten Königreichs als Drittland

Die EU und das Vereinigte Königreich haben sich nun darauf geeinigt, dass das Vereinigte Königreich mit seinem jetzigen Datenschutzstandard zumindest zunächst nicht als Drittland zu betrachten ist (Teil 7, Artikel FINPROV.10A). Datentransfers aus der EU bedürfen daher derzeit neben den allgemeinen Voraussetzungen (die auch bei Übermittlungen innerhalb der EU gelten) keiner zusätzlichen Rechtfertigung. Dies gilt jedoch nur übergangsweise zunächst bis zum 1. April 2021. Sofern weder die EU noch das Vereinigte Königreich widersprechen, verlängert sich dieser Zeitraum nochmals automatisch bis zum 1. Juni 2021.

Sollte die Kommission bis dahin einen Angemessenheitsbeschluss treffen, gilt das Vereinigte Königreich auch danach als sicheres Drittland und Datentransfers aus der EU ins Vereinigte Königreich sind unverändert ohne Probleme möglich. Zumindest derzeit unterscheidet sich das Datenschutzniveau des Vereinigten Königreichs nicht signifikant von dem der Europäischen Union. Dies liegt daran, dass die Datenschutz-Grundverordnung mit nur wenigen Anpassungen Bestandteil des britischen Datenschutzrechts unter dem Data Protection Act 2018 geworden ist.

Gewisse Änderungen kann das Vereinigte Königreich in dieser Übergangszeit an seinem Datenschutzrecht vornehmen, ohne dass es automatisch in die Rolle eines Drittlandes fällt. Mit Blick auf die Übergangsregelung unproblematisch sind etwa Änderungen, die lediglich der Anpassung des britischen Rechts an das europäische Datenschutzrecht dienen. Auch andere Änderungen sind möglich, sofern der im Handels- und Kooperationsabkommen festgelegte Partnerschaftsrat zuvor seine Zustimmung erteilt oder auf eine entsprechende Beratung in stiller Zustimmung verzichtet.

Wie sich Unternehmen vorbereiten können

Die Übergangsregelung für das Datenschutzrecht verschafft etwas Zeit, damit sich Unternehmen bei ihrem Datenverkehr ins Vereinigte Königreich absichern können. Zwar kann die Europäische Kommission die Problematik durch einen Angemessenheitsbeschluss lösen. Allerdings ist es ratsam, dass Unternehmen sich auch auf eine Situation vorbereiten, in der ein solcher Beschluss ausbleibt und das Vereinigte Königreich zumindest vorübergehend zu einem Drittland wird (vgl. *Brexit und DS-GVO*).

Die erforderlichen Maßnahmen (beispielsweise Standarddatenschutzklauseln oder Binding Corporate Rules) lassen sich nicht „über Nacht“ umsetzen, sondern bedürfen in Abstimmung mit den beteiligten Datenempfängern in UK einer sorgfältigen Vorbereitung, um etablierte Geschäftsprozesse und Datenflüsse möglichst wenig zu beeinträchtigen.

Weiterführende Links:

- Handels- und Kooperationsabkommen zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinigten Königreich Großbritannien und Nordirland andererseits, AblEU 2020 L 444 v. 31.12.2020, S. 14-1462
- EuGH - Urteil vom 16.07.2020 - Rechtssache C-311/18 - Data Protection Commissioner gegen Facebook Ireland Ltd („Schrems II“)
- Europäische Kommission - Entwurf eines Durchführungsbeschlusses zu „Standarddatenschutzklauseln“ für Übermittlungen personenbezogener Daten in Drittländer

Haben Sie Fragen? Kontaktieren Sie gerne: Dr. Daniel Rücker oder Pascal Schumacher
Praxisgruppen: Datenschutz , Digital Business

Contact Person

Dr. Daniel Rücker, LL.M.
Leiter Datenschutz
Mitglied der Practice Group Digital Business
Rechtsanwalt

T +49 89 28628457

Pascal Schumacher
Mitglied der Practice Group Telekommunikation
Mitglied der Practice Group Datenschutz
Rechtsanwalt

T +49 30 20942030