

Conrad S. Conrad

# Gilt das Vereinigte Königreich künftig als ein Drittland?

## Gesetzesänderungen im Blick

Am 29. März 2017 stellte die Premierministerin des Vereinigten Königreichs von Großbritannien und Nordirland, Theresa May, den folgeschweren Antrag gemäß Art. 50 des Vertrags über die Europäische Union. Damit startete der zweijährige Austrittsprozess, der mit der Beendigung der Mitgliedschaft in der Europäischen Union münden wird. Dies warf die Frage auf, wie das Vereinigte Königreich zukünftig mit Blick auf das Datenschutzniveau einzustufen sei. Eine Pressemitteilung vom 9. Januar 2017 gibt nunmehr Klarheit, woraus sich aber unter der Anwendung der Datenschutz-Grundverordnung durchaus datenschutzrechtliche Haftungsfragen ergeben können.

### 1 Hintergrund

Der Antrag nach Art. 50 des Vertrags über die Europäische Union wurde durch die Premierministerin des Vereinigten Königreichs von Großbritannien und Nordirland, Theresa May, am 29. März 2017 gestellt. Damit begann der Austrittsprozess, der 2019 mit der Beendigung der Mitgliedschaft in der Europäischen Union münden wird. Dies warf die Frage auf, wie das Vereinigte Königreich zukünftig mit Blick auf das Datenschutzniveau einzustufen sei. Nun gibt es endlich Klarheit: Die Europäische Kommission teilte in einer Pressemitteilung mit, dass „UK“ ab dem 30. Mai 2019 als „Drittland“ gelten werde („*The United Kingdom will then become a 'third country'.*“).<sup>1</sup>

(DS-GVO) heraus und wäre datenschutzrechtlich dann wie China, Indien, Russland oder die USA einzuordnen. Eine Übermittlung von personenbezogenen Daten in das Königreich, wie auch allgemein die Datenverarbeitung durch dortig ansässige Verantwortliche im Wege der Auftragsdatenverarbeitung ist dann nicht mehr ohne Weiteres wie bisher möglich. So lässt sich die Datenverarbeitung zwischen zwei Unternehmen dann nicht mehr allein auf Grundlage eines zuvor geschlossenen Vertrages über die Auftragsverarbeitung (Art. 28 DS-GVO) stützen und auch die allgemeinen Rechtsgrundlagen der Datenschutz-Grundverordnung greifen nicht mehr. Die Übermittlung besonderer Kategorien personenbezogener Daten wie beispielsweise Gesundheitsdaten (Art. 9 DS-GVO) unterliegt zudem höheren Anforderungen.

### 2 Datenschutzrechtliche Folgen

Nach dem „Brexit“ fällt das Vereinigte Königreich demnach aus dem Anwendungsbereich der Datenschutz-Grundverordnung

<sup>1</sup> Pressemitteilung der Europäischen Kommission vom 09.01.2018; [http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc\\_id=49245](http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245) (letzter Abruf: 11.01.2018).



**Conrad Sebastian Conrad**

Justiziar – datenschutz nord GmbH

E-Mail: [cconrad@datenschutz-nord.de](mailto:cconrad@datenschutz-nord.de)

### 2 Mögliche Lösungswege

Die britische Regierung kündigte<sup>2</sup> bereits im August vergangenen Jahres an, trotz des „Brexits“ die eigenen Gesetze zum Datenschutz (wie der „Data Protection Act“ von 1998) zu verschärfen und an den Standards der Datenschutz-Grundverordnung auszurichten<sup>3</sup> bzw. in dem Königreich zu etablieren („*The Bill will bring the European Union's General Data Protection Regulation (GDPR) into UK law, helping Britain prepare for a successful Brexit*“).<sup>4</sup>

Trotz dieses Vorhabens würde das Vereinigte Königreich zunächst als unsicherer Drittstaat gelten, denn nur der Angemes-

<sup>2</sup> Siehe: <https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law> (letzter Abruf: 11.01.2018).

<sup>3</sup> Vgl. <https://www.heise.de/newsticker/meldung/Trotz-Brexits-Britische-Regierung-will-EU-Datenschutzverordnung-uebernehmen-3794836.html> (letzter Abruf: 11.01.2018).

<sup>4</sup> Pressemitteilung der Regierung: <https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law> (letzter Abruf: 11.01.2018).



senheitsbeschluss der Europäischen Kommission nach Art. 45 DS-GVO kann ein Land auf die Stufe des sicheren Drittlandes heben, um einen „freien“ Datenfluss wie innerhalb der EU zu bewirken.<sup>5</sup> Die Kommission wird dem Vereinigten Königreich jedoch nur dann ein adäquates Datenschutzniveau attestieren, wenn die in UK geltenden Datenschutzregelungen den europäischen Datenschutzstandards entsprechen. Als Kriterien werden unter Anderem die Rechtsstaatlichkeit, die Einhaltung der internationalen Menschenrechtsnormen und -standards sowie auch die Vorschriften zur öffentlichen Sicherheit und Ordnung herangezogen.<sup>6</sup> An der Übereinstimmung mit den Grundwerten der Union könnten Bedenken bestehen, da beispielsweise den Strafverfolgungsbehörden in UK auf Grundlage des derzeitigen „Investigatory Powers Bill“<sup>7</sup> weitgehende Befugnisse zur Vorratsdatenspeicherung, Überwachung und Einsichtnahme von personenbezogenen Daten der EU-Bürger eingeräumt werden, die das Schutzniveau der Rechte des Einzelnen einschränken.<sup>8</sup>

Ohne die Feststellung des angemessenen Datenschutzniveaus durch die Europäische Kommission müssen für einen legitimen Datentransfer zusätzliche Voraussetzungen erfüllt werden. In Betracht kommt der Abschluss eines Vertrages nach den Standarddatenschutzklauseln (Art. 46 Abs. 2 lit c) DS-GVO). Der bloße Verweis auf diese Regelungen ist nicht ausreichend. Ebenso können verbindliche interne Datenschutzvorschriften, sog. „Binding Corporate Rules“<sup>9</sup>, nach (Art. 47 DS-GVO) innerhalb eines Konzerns die Grundlage für einen einheitlichen Rechtsrahmen für die Datenübermittlung und Verarbeitung von Unternehmen aus der Gruppe mit Sitz in einem unsicheren Drittland bilden. Allerdings muss zunächst die zuständige Aufsichtsbehörde (ggfs. nach dem Kohärenzverfahren gem. Art. 93 DS-GVO<sup>10</sup>) diesen umfassenden Regelungskatalog prüfen und genehmigen, was mit einem nicht unerheblichen Zeitaufwand verbunden sein kann.

Auf eine ausdrückliche Einwilligung des Einzelnen in die Datenübermittlung in ein Drittland (Art. 49 Abs. 1 lit. a) DS-GVO) sollten sich Unternehmen weder im Massengeschäft noch bei der Personaldatenverarbeitung stützen. Insbesondere bei Personaldaten könnte die Einwilligung des Angestellten infrage gestellt werden.<sup>11</sup>

### 3 Konsequenzen für betroffene Unternehmen

Für viele Firmen mit Sitz in London und in anderen Großstädten in UK bedeutet dieses in der Konsequenz: Sie wären zunächst einmal abgetrennt vom europäischen Datenfluss. Sie könnten daher gezwungen sein, ihr Geschäftsmodell oder sogar ihren Standort auf der Insel aufzugeben. Viele Unternehmen wählen anscheinend letztere Variante und verlegen ihren Sitz in eine der auch zukünftig noch zur Europäischen Union gehörenden Großstädte wie Paris, Madrid, Berlin oder Frankfurt am Main.<sup>12</sup>

Das skizzierte Szenario sollte daher von Unternehmen spätestens jetzt sowohl bei der Auftragsvergabe als auch beim internen Datenfluss (z. B. an die Personalstelle oder Buchführung) berücksichtigt werden. In jedem Fall muss der Verarbeiter die Betroffenen nach Art. 13 Abs. 1 lit. f) DS-GVO umfassend über die Übermittlung der bei ihnen direkt erhobenen personenbezogenen Daten an einen Verarbeiter im Drittland wie auch über das damit einhergehende Risiko und etwaige Garantien (BCRs) für den Datenschutz informieren.<sup>13</sup>

Den datenschutzrechtlichen Anforderungen gemäß der Datenschutz-Grundverordnung sollte bei europäischen Unternehmen angemessen Rechnung getragen werden. Schließlich haben die Aufsichtsbehörden in der Vergangenheit bei einer vergleichbaren Situation nach Wegfall des Safe-Harbor Abkommens verhältnismäßig streng die Rechtmäßigkeit des Datentransfers zu Unternehmen in den USA geprüft.<sup>14</sup> Es ist nicht auszuschließen, dass sie mit ähnlicher Entschlossenheit auch die Übermittlung von Daten in das Vereinigte Königreich beanstanden werden. Eine positive Angemessenheitsentscheidung (nach Art. 45 DS-GVO) würde die Rechtssicherheit deutlich erhöhen. Ein gewisses Restrisiko verbleibt weiterhin im Falle des Brexits.

5 Gola, DS-GVO, Kommentar, Art. 45, Rn. 1.

6 Erwägungsgrund 104 der DS-GVO.

7 Vgl. <http://www.telegraph.co.uk/technology/2016/11/29/investigatory-powers-bill-does-mean-privacy/> (letzter Abruf: 11.01.2018).

8 Vgl. <https://www.datenschutz-notizen.de/brexit-jetzt-wird-es-ernst-0217740/> (letzter Abruf: 11.01.2018).

9 Siehe dazu wie auch die Liste der Unternehmen, deren BCRs anerkannt worden sind: [http://ec.europa.eu/justice/data-protection/article-29/bcr/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm) (letzter Abruf: 11.01.2018).

10 Pauly, in: Paal/Pauly, DS-GVO, Kommentar, Art. 47, Rn. 9 ff.

11 Vgl. Zur Freiwilligkeit der Einwilligung nach der DS-GVO: Ernst, ZD 2017, S. 110 (111).

12 Vgl. <http://www.fr.de/wirtschaft/umzug-aus-london-frankfurt-ist-einer-der-grossen-brexit-profiteure-a-1312687> (letzter Abruf: 11.01.2018); Jedes siebte Unternehmen beabsichtigt den Umzug oder eine Ausgliederung von Teilen, siehe: <https://www.n-tv.de/wirtschaft/Brexit-vertreibt-Unternehmen-aus-Grossbritannien-article19679230.html> (letzter Abruf: 11.01.2018).

13 Bäcker, in: Kühling/Bucher, DS-GVO, Kommentar, Art. 13 DS-GVO, Rn. 33 ff.

14 So die Hamburger Datenschutz-Aufsichtsbehörde; <https://www.datenschutz-hamburg.de/news/detail/article/unzulaessige-datenuebermittlungen-in-die-usa.html> (Pressemitteilung vom 6.6.2016 (letzter Abruf: 11.01.2018); Vgl. das Positionspapier vom ULD: <https://www.datenschutzzentrum.de/artikel/967-Positionspapier-des-ULD-zum-Safe-Harbor-Urteil-des-Gerichtshofs-der-Europaeischen-Union-vom-6.-Oktober-2015,-C-36214.html> (letzter Abruf: 11.01.2018).