Bild: Leon Neal/PA Wire/dpa

In letzter Minute

Wie sich der Brexit auf den Datenschutz auswirkt

Den drohenden GAU im Datenverkehr zwischen der EU und Großbritannien konnte der Brexit-Vertrag gerade noch mal abwenden. Doch juristisch abgesichert sind künftige Übertragungen persönlicher Daten ins Vereinigte Königreich noch lange nicht. Firmen müssen deshalb jetzt vorbeugen.

Von Joerg Heidrich

Es war so eine Art Weihnachtswunder, die Vereinbarung zwischen der Europäischen Union und dem Vereinten Königreich, die am 24. Dezember 2020 und damit wenige Tage vor dem Fristende am 31. Dezember geschlossen wurde. Durch das Handelsabkommen konnte der harte Brexit in letzter Minute erst einmal vermieden werden. Der Vertrag betrifft auf 1246 Seiten nicht nur den Warenverkehr, sondern auch Bereiche wie Luft- und Straßenverkehr sowie soziale Sicherung – und regelt auch den Datenschutz.

Hätte es keine Regelung zum Export von Daten über den Ärmelkanal gegeben, so wäre Großbritannien über Nacht zu einem sogenannten Drittland geworden. Übermittlungen personenbezogener Daten wären dann nur noch unter sehr engen Voraussetzungen möglich gewesen. Die Beschränkungen hätten katastrophale Auswirkungen auf den Datenverkehr gehabt.

Einer Studie der Branchenverbände Digitaleurope und techUK zufolge transferieren sechs von zehn europäischen Unternehmen Daten in das Vereinigte Königreich. Für sie bleibt nun ein kurzer Zeitkorridor, in dem sie sich über den künftigen Umgang mit persönlichen Daten einigen müssen. Schaffen sie das nicht, steht viel auf dem Spiel, nicht nur für die Unternehmen, sondern auch für EU-Bürger.

Sechs Monate Frist

Ziel des Brexit-Vertrags ist nach Aussagen der EU-Kommission, „den digitalen Handel zu erleichtern, indem ungerechtfertigte Hindernisse beseitigt" werden. Gleichzeitig sollen „hohe Standards für den Schutz personenbezogener Daten gewährleistet werden".

Die Übereinkunft legt fest, dass Großbritannien für eine Übergangsfrist nicht als unsicherer Drittstaat eingestuft wird. Voraussetzung ist, dass die Briten für diesen Zeitraum an ihren auf der DSGVO basierenden nationalen datenschutzrechtlichen Regelungen festhalten. Eine Abweichung wäre nur mit Zustimmung der EU zulässig.

Bis Ende April kann der Datenverkehr also unverändert weiter fließen. Diese Übergangsfrist kann dann noch einmal um zwei Monate verlängert werden. Bis spätestens Ende Juni muss die EU-Kommission einen sogenannten Angemessenheitsbeschluss mit dem Vereinigten Königreich vereinbaren. Die Verhandlungen dazu sollen unverzüglich beginnen.

Umstrittene Sonderregelung

Allerdings vertreten namhafte britische Juraprofessoren die Ansicht, dass das EU-Recht derartige Sonderregelungen wie im Brexit-Vertrag gar nicht erlaubt. Zudem stünde die Vereinbarung im Widerspruch zur DSGVO, welche den Datenexport außerhalb der EU regelt. Denn formal hat das Vereinigte Königreich zum 1. Januar 2021 die EU verlassen und ist kein Mitgliedsstaat mehr. Dagegen wird etwa argumentiert, dass es sich bei dem Übereinkommen um einen völkerrechtlichen Vertrag handelt, der dem EU-Recht vorgeht.

Kein Problem mit dem vereinbarten Sonderweg hat offenbar die Konferenz der hiesigen Datenschutzaufsichtsbehörden. Diese begrüßen in einer Presseerklärung Ende Dezember ausdrücklich die beschlossene „vorläufige Rechtssicherheit für Datenübermittlungen in das Vereinigte Königreich". Das Abkommen würde den „bisher befürchteten gravierenden Rechtsunsicherheiten" vorbeugen. Die britische Datenschutzbehörde ICO lobte den Vertrag als „bestmögliche Regelung für UK-Organisationen, die personenbezogene Daten aus der EU verarbeiten".

Sichere Drittstaaten

Endet die durch den Vertrag geschaffene Frist, stehen Ende Juni zwei Szenarien im Raum: Die beiden bislang arg zerstrittenen Parteien einigen sich auf den Angemessenheitsbeschluss. Einigt man sich nicht, folgt der harte Datenschutz-Brexit mit Verspätung.

Grundsätzlich unterteilt man hierzulande die Welt in drei Bereiche. Rechtlich unproblematisch ist die Weitergabe von persönlichen Informationen innerhalb der EU, in der einheitlich die DSGVO gilt. In der zweiten Kategorie stehen sichere Drittländer, in die ein Transfer uneingeschränkt möglich und erlaubt ist. „Sicher" sind solche Staaten, denen die Europäische Kommission ein den europäischen Vorgaben entsprechendes Datenschutzniveau bestätigt hat. Hierzu gehören derzeit beispielsweise Argentinien, Kanada (nur kommerzielle Organisationen), Israel, Neuseeland, die Schweiz und seit einiger Zeit auch Japan.

In diese zweite Kategorie könnte vom Sommer 2021 an auch das Vereinigte Königreich eingeordnet werden. Entsprechende Verhandlungen sollen nach Aussage der zuständigen EU-Kommission bereits seit einigen Monaten laufen. Experten bezweifeln allerdings, dass eine dafür nötige Vereinbarung in einem derart kurzen Zeitraum erreicht werden kann. Die Verhandlungen mit Japan dauerten etwa weitaus länger.

Und auch inhaltlich gibt es Zweifel, dass in UK tatsächlich von einem mit der EU vergleichbaren Datenschutzniveau auszugehen ist. Kritisch gesehen wird dabei vor allem die starke Rolle der Geheimdienste. Diese sind eng mit den amerikanischen Diensten vernetzt und auch Teil der „Five Eyes"-Gemeinde. Zu diesem elitären Kreis von überwachungsfreundlichen Staaten gehören neben den USA und Großbritannien auch Australien, Kanada und Neuseeland. Zumindest bei den beiden letztgenannten Ländern stand dies allerdings einer Anerkennung als sicherer Drittstaat nicht im Wege.

Unsichere Drittstaaten

Alle anderen Länder werden als unsichere Drittstaaten qualifiziert, deren nationales Recht keinen hinreichenden Schutz der Daten europäischer Bürger gewährleistet. Kommt es bis Ende Juni zu keiner Einigung, würde auch Großbritannien in diese Einordnung fallen, in der sich bereits China, Indien, Russland sowie die USA finden. Eine Weitergabe von Informationen in diese Länder ist zwar nicht grundsätzlich verboten. Allerdings gibt es einige rechtliche Hürden, die vor der ersten Übertragung geklärt werden müssen.

Für solche Staaten gelten die strengen Vorschriften der Art. 44 ff. DSGVO. Praktisch relevant ist hierbei vor allem der Abschluss von sogenannten Standarddatenschutzklauseln (SDK). Das sind von der EU-Kommission fertig formulierte Vertragsklauseln, die zwischen dem die Daten exportierenden Unternehmen und dem Empfänger im Drittstaat abgeschlossen werden.

Die Idee dahinter ist, dass sich die Beteiligten schriftlich verpflichten, die hohen Datenschutzstandards der EU zu wahren. Geregelt werden durch diese Vorgaben zum Beispiel die Pflichten der Beteiligten, die Haftung oder Teilnahme an Schlichtungsverfahren. Wichtig ist in der Praxis, dass die Formulierungsvorlagen unverändert übernommen werden müssen. Allerdings arbeitet die EU-Kommission derzeit an Neuformulierungen der Klauseln, die vermutlich Anfang 2021 fertig werden.

Zudem sind nach der Rechtsprechung des EuGH meist noch zusätzliche technische und organisatorische Schutzmaßnahmen zu ergreifen, insbesondere um die EU-Bürger vor dem allzu leichtfertigen Zugriff fremder Geheimdienste zu schützen. Zu diesen Schutzmaßnahmen gehören zum Beispiel die Anonymisierung und Verschlüsselung von Daten.

Eine Datenübertragung in ein Drittland kann zudem auch durch eine Einwilligung der jeweiligen Betroffenen legitimiert werden. Dabei sind die Anforderungen an deren Freiwilligkeit zu beachten. Eine weitere Schwierigkeit in der Praxis stellt die Vorgabe dar, dass der Betroffene vor seiner Einwilligung explizit über die geplante Verarbeitung seiner Daten informiert werden muss und seine Zustimmung jederzeit widerrufen kann. In diesem Fall müssen die Informationen über ihn unverzüglich gelöscht werden.

Auf den Ernstfall vorbereiten

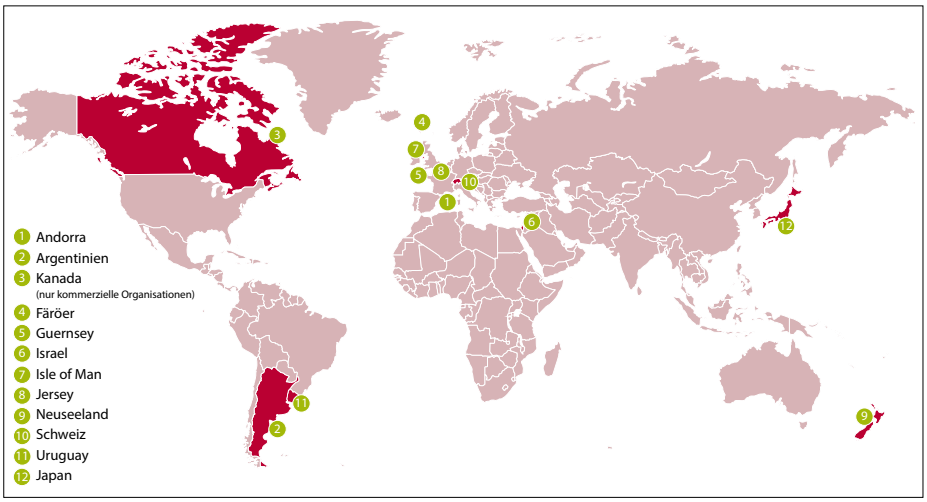
IT-Unternehmen sind gut beraten, die drohenden Gefahren ernst zu nehmen und den Aufschub zu gründlichen Vorbereitungen auf den möglichen „Datenschutz-Brexit" zu nutzen. Hierzu gehört es zunächst, die eigene Abhängigkeit von UK-Unternehmen zu analysieren und Ausschau nach möglichen Alternativen zu halten.

Für wichtige und unverzichtbare Partner, zum Beispiel im Bereich IT, Personalwesen oder Finanzen, empfiehlt es sich, rechtzeitig ein Szenario ohne Angemessenheitsbeschluss zu planen. Hierzu werden vor allem Standarddatenschutzklauseln das Mittel der Wahl sein. Wer diese bis Ende Juni vorbereitet, kann Mitte des Jahres im Notfall schnell umsteigen. Hierzu gehört es auch, zusätzliche technische und organisatorische Maßnahmen zum Schutz der Daten der EU-Bürger zu definieren und vorzubereiten.

Anders als bei der vergleichbaren Rechtslage in den USA nach dem Schrems-II-Urteil im vergangenen Jahr ist kaum damit zu rechnen, dass die hiesigen Datenschutzbehörden bei Verstößen gegen die strengen DSGVO-Vorgaben zum Datentransfer nach UK Milde walten lassen werden. *(hag@ct.de)* **c't**

Literatur

[1] Holger Bleich, FAQ: Das Ende des Privacy Shields, c't 21/2020, S. 178



Ein Dutzend Länder gelten für die EU-Kommission in Sachen Datenschutz derzeit als sichere Drittstaaten. Hierzu soll 2021 auch das Vereinigte Königreich gehören.