Bild: Pixabay / Willfried Wende

Drittstaat nach hartem Brexit

Die neue EU-Grenze könnte Datenströme kappen

Der Brexit muss bis Ende Oktober über die Bühne gehen, doch er droht ungeregelt zu erfolgen. Ohne Austrittsabkommen aber wäre Großbritannien gegenüber der EU ein Drittland ohne konforme Datenschutzstandards. Sehr viele IT-Prozesse würden dann von einem Tag auf den anderen illegal.

Von Arne Grävemeyer

Inzwischen ist es amtlich: Großbritannien schafft keinen kurzfristigen Brexit, sondern nimmt noch an der Europawahl teil. Für ihren Austritt hat die EU den Briten eine Frist bis Ende Oktober gewährt. Groß ist nach wie vor die Gefahr, der Inselstaat könne ungeregelt, also ohne ein Austrittsabkommen, die EU verlassen. Sollte dies tatsächlich passieren, hätte das vereinigte Königreich aus Sicht der EU von einem Tag auf den anderen den Status eines Drittstaates wie Uruguay oder Nigeria – vor allem in Bezug auf den Datenschutz.

Ein Problem für die meisten Geschäftsbeziehungen zwischen EU-Angehörigen und britischen Unternehmen könnte dann die DSGVO darstellen. Oft ist diese Hürde gar nicht so offensichtlich. Immerhin von jedem siebten Unternehmen in Deutschland, das personenbezogene Daten über externe Dienstleister verarbeiten lässt, strömen diese Daten nach Großbritannien, wie der Branchenverband Bitkom in einer repräsentativen Studie ermittelte. Das passiert bei Bestellungen, zu denen einzelne Bestandteile oder Zubehör aus Großbritannien geliefert werden soll. Oder Anwenderdaten hängen an Software-Lizenzen, für die Updates auf der Insel bereitstehen. Viele Konzerne wie Amazon, Bosch und Siemens haben Websites mit europäischen und britischen Domains parallel.

Mit dem verhandelten Austrittsabkommen würde das britische Datenschutzniveau dem der EU gleichgestellt. Ohne gültiges Abkommen hingegen muss die EU-Kommission zunächst prüfen, ob ein vergleichbares Datenschutzniveau gegeben ist. Diese Prüfung würde allerdings erst mit dem Austritt der Briten in Angriff genommen und ab diesem Zeitpunkt sicher einige Monate oder gar Jahre beanspruchen. Jede Übertragung personenbezogener Daten von der EU nach Großbritannien wäre also mit einem harten Brexit von einem Tag auf den anderen widerrechtlich. Das kann konzerninterner Datenaustausch sein, das kann im Rahmen von Kundenbestellungen oder bei der Abwicklung von Software-Updates passieren oder sogar bei der Lohnabrechnung externer Mitarbeiter europäischer Unternehmen.

Datenschutz à la USA?

Wie problematisch ein ungeregelter Status sein kann, zeigt ein Blick auf das Verhältnis der EU zu den USA. Die Vereinigten Staaten sind datenschutzrechtlich für die EU ein Drittland. Ein angemessenes Datenschutzniveau konnte der USA nicht attestiert werden, das verhinderte die starke Rolle der US-Geheimdienste. Das ersatzweise geschaffene Safe-Harbor-Abkommen, das es EU-Unternehmen ermöglicht, personenbezogene Daten in Übereinstimmung mit der europäischen Datenschutzrichtlinie in die USA zu übermitteln, wurde später vom Europäischen Gerichtshof kassiert.

Heute gilt stattdessen der EU-US Privacy Shield, eine Reihe von Zusicherungen der US-Regierung. Die Vorgaben dieses Privacy Shield gelten per Kommissionsbeschluss als dem Datenschutzniveau der EU gleichwertig. Aber nur mit US-Unternehmen, die sich in die entsprechende Liste eintragen und sich somit zu einem EU-Datenschutzniveau verpflichten, kann Datenaustausch vollzogen werden.

Offenbar ist es vielen Online-Anbietern zu schwer gefallen, ihre Datensammelpraxis an die neue DSGVO anzupassen. Zahlreiche US-Medien beispielsweise entschieden sich stattdessen, ihre Portale für europäische IP-Adressen zu blocken – bis heute.

„Einige IT-Unternehmen vor allem aus den USA haben es sich in der Vergan-

genheit leicht gemacht und versucht, die gesamte EU lediglich von Großbritannien aus zu bedienen“, meint Marc Tenbieg, geschäftsführender Vorstand des Deutschen Mittelstands-Bundes (DMB). Im Falle eines ungeregelten Brexit könnte das zum Problem werden, denn der Umgang mit und die Speicherung von personenbezogenen Daten der EU-Kunden ist in der DSGVO streng geregelt, das kann dann kein Unternehmen mehr nach Großbritannien auslagern.

Tenbieg gibt noch etwas zu bedenken: „In den vergangenen zwölf Monaten hat die DSGVO stark für Aufmerksamkeit gesorgt. Die Kunden sind sensibilisiert, da muss ein IT-Dienstleister im Zweifelsfall sofort mit kritischen Nachfragen rechnen.“ Konkrete Probleme sind erst kürzlich bei einem sogenannten DMB-Turmgespräch zur Sprache gekommen: Gerade viele kleinere Unternehmen, zumeist ohne eigene Rechtsabteilung, haben Software gehostet, beispielsweise Shop-Software oder eine CRM-Lösung. Nun müssen rechtzeitig die wesentlichen Fragen geklärt werden: Wie ist die Grundstruktur der Software und Datenflüsse? Wer hat Zugang zu personenbezogenen Daten? Wo findet ganz konkret das Hosting statt?

Der Softwarekonzern Sage mit Sitz im englischen Newcastle teilte uns auf Anfrage mit: „Das Geschäft in Deutschland basiert im Wesentlichen auf Produkten, die im Land selbst entwickelt und verkauft werden. Fragen, bei denen die Speicherung von Kundendaten in Großbritannien und damit auch der Brexit eine wichtige Rolle spielen, sind für uns insofern kaum relevant.“ Das ist für den Einzelfall natürlich noch nicht hieb- und stichfest. Ähnlich vage antwortet Sophos mit Sitz in Abingdon und verweist auf seine internationale Konzernstruktur. Man habe Niederlassungen in jedem wichtigen Land, zum Teil mit eigener Forschung und Entwicklung. Wo im Einzelnen die Datenströme fließen, sagt ein solches Statement nicht aus.

Option „nur Server in Europa“

Dabei zeigt der Blick in die Nachrichten, dass selbst verbreitete Standardlösungen mit Blick auf die DSGVO umstritten sind. WhatsApp ist auf Firmenhandys in die Kritik geraten, weil die Anwendung auf die Kontakte des Nutzers zugreifen und diese auf Server außerhalb der EU senden könnte. Und bei der Auswahl von Office365-Diensten halten es Juristen nicht für ausreichend, auf „nur Server in Europa“ zu klicken. Für die DSGVO dürfte das zu schwammig sein, denn da fehlt ja jeder Hinweis auf die EU und erst recht auf die EU nach dem Brexit.

Auch die IHK Region Stuttgart sensibilisiert ihre Mitglieder für Datenschutz beim Kundendatenaustausch nach einem harten Brexit. „Darunter ist nicht nur der aktive Datentransfer zu verstehen, sondern allein schon die Möglichkeit des Zugriffs auf eine Datenbank“, erläutert Jurist Rainer Simshäuser. Bei einem unberechtigten Datentransfer drohen Bußgelder.

Unternehmen benötigen daher nicht nur eine Rechtsgrundlage für die Übermittlung von Kundendaten, also beispielsweise bei einer Bestellung. Zusätzlich brauchen sie Garantien zum Datenschutz beim Vertragspartner in Großbritannien für jede Datenübermittlung, sofern keine Ausnahmeregelung nach DSGVO greift, etwa bei der Erfüllung eines Vertrags oder Vorliegen einer expliziten Einwilligung des Kunden. In der Datenschutzerklärung und bei konkreten Auskunftsersuchen muss der Online-Kunde etwaige Datenübermittlungen nachlesen können, insbesondere in Drittländer wie Großbritannien nach einem ungeregelten Brexit. *(agr@ct.de)* c't