GASTBEITRAG

Keine Daten in die Staaten!?

Börsen-Zeitung, 29.10.2020

Datenschutz wird in Europa und den USA kulturell grundsätzlich unterschiedlich diskutiert. Die entsprechenden Konfliktlinien aus starker Innovationsorientierung und freier Datennutzung einerseits sowie tendenzieller Technologieskepsis und engagiertem Schutz personenbezogener Daten andererseits hatte die Politik bislang über Abkommen mit so imposanten Namen wie Safe Harbour oder Privacy Shield kitten können. Doch die Brücken zwischen den hoch unterschiedlichen Datenschutz-Welten tragen nicht mehr. Hatte der Europäische Gerichtshof (EuGH) im Jahr 2015 schon den vermeintlich sicheren Hafen für den Kontinente übergreifenden Datentransfer für ungültig erklärt, hat er am 16. Juli 2020 auch das Nachfolgeabkommen Privacy Shield gekippt, weil personenbezogene Daten europäischer Bürger nicht genügend vor dem Zugriff von US-Sicherheitsbehörden geschützt seien und kein ausreichender Rechtsschutz zur Verfügung stehe.

Sprengstoff-Charakter

Trotz des Sprengstoff-Charakters sind die Konsequenzen dieses Urteils zum Datenschutz auch gut vier Monate später in ihrer Dimension überraschend wenig öffentlich diskutiert. Denn was eigentlich als Schlag gegen datenhungrige Social Networks wie Facebook & Co. gedacht war, entpuppt sich bei näherer Betrachtung als eines der größten Handelshemmnisse, seit Schiffe zwischen Europa und Amerika verkehren. Aus einer Konfliktlinie wurde ein tiefer Graben, der nahezu alle Unternehmen im EU-Raum zum Handeln zwingt, denn seit Mitte Juli gilt: keine Daten in die Staaten! Und Stand heute agiert der Großteil der Unternehmen nicht im Einklang mit geltender europäischer Gesetzgebung.

Michael H. Kramarsch

Managing Partner hkp group

Laut EuGH-Urteil muss bei Übertragung personenbezogener Daten in ein Drittland ein Schutzniveau gewahrt sein, das dem der EU-Datenschutzgrundverordnung (DSGVO) entspricht. Da angesichts der Rechtslage in den USA hiervon nicht ausgegangen werden könne, sei auch das Privacy Shield hinfällig. Findet eine Datenübermittlung weiterhin statt, können Betroffene Schadenersatz für erlittenen immateriellen Schaden verlangen und Aufsichtsbehörden gegen Verantwortliche nach EU-Recht ein Bußgeld in „abschreckender“ Höhe verhängen. Damit drohen erhebliche Rechts- und Reputationsrisiken. Durch die Urteilsbegründung zu den staatlichen Eingriffsmöglichkeiten werden auch andere Wege zur Datenübermittlung wie Standarddatenschutzklauseln und unternehmensinterne Datenschutzvorschriften deutlich erschwert, wenn nicht gar in vielen Fällen unmöglich gemacht.

Einzige rechtssichere Lösung ist derzeit die Speicherung und Verarbeitung personenbezogener Daten in der EU und nach DSGVO-Vorgaben. Und mit personenbezogenen Daten sind alle Informationen gemeint, die Rückschlüsse auf eine natürliche Person zulassen: Klassische Beispiele sind die Telefonnummer, die IP-Adresse oder das Kfz-Kennzeichen sowie Kreditkarten- oder Personalnummern, Kontodaten, Kundennummern oder die Aufzeichnungen über Arbeits- und Pausenzeiten.

Damit wird klar: Es sind nicht allein Website-Betreiber, die für ihre Analyse-Software eine europäische Alternative finden müssen, um online gesetzeskonform zu sein. Es betrifft auch Unternehmen, die beispielsweise Personaldaten externen Spezialisten außerhalb der EU überlassen – sei es zur Gehaltsabrechnung oder für anderer Dienstleistungen. Viele Unternehmen haben in den vergangenen Jahren massiv in entsprechende Prozesse investiert, diese global vereinheitlicht und Cloud-basierte Systeme eingeführt. Dabei wurden nicht selten die Speicherung und Verarbeitung personenbezogener Daten sowie auch die Systembetreuung ins außereuropäische Ausland ausgelagert.

Compliance-Risiko

Doch der Datenschutz-Graben verläuft nicht nur zwischen Unternehmen und Dienstleistern, sondern teilweise auch mitten durch Unternehmen, beispielsweise im Fall von in der EU agierenden Tochterunternehmen von US-Konzernen. In der Vergangenheit haben sich diese darauf zurückziehen können, dass Daten auf deutschen beziehungsweise europäischen Servern verarbeitet werden. Dieses Schutzniveau allein ist nun nicht mehr ausreichend, da die Töchter weisungsgebunden sind und sich die US-Mütter – und damit auch US-Sicherheitsbehörden – in der Regel Zugriff auf die entsprechenden Daten verschaffen können.

Außerdem wird jeder Warenverkehr heutzutage von Daten begleitet, von denen eine Vielzahl personenbezogen ist. Compliance-Vorgaben für Führungskräfte enthalten daher immer öfter auch datenschutzrechtliche Aspekte. Zudem werden Manager inzwischen häufig per Dienstvertrag zur Einhaltung der DSGVO verpflichtet. Damit wird aus dem Datenschutz auch ein Compliance- und ein arbeitsrechtliches Risiko. Selbst die Vergütung von Vorständen ist betroffen: Denn insbesondere in börsennotierten Unternehmen werden zunehmend sogenannte Clawback-Klauseln vereinbart, die eine Rückforderung ausgezahlter Vergütung bei Compliance-Verstößen erlauben.

Die Beispiele zeigen: Sich den neuen Gegebenheiten anzupassen, ist ein Kraftakt, der mit immensen Kosten und Einschränkungen verbunden ist. Unternehmen dürfen dabei nicht allein gelassen werden, zumal es keine einfache und erst recht keine schnelle Lösung gibt.

Politische Lösung

Das unterschiedliche Datenschutzverständnis in den USA und Europa kann nur politisch gelöst werden. Hinter den Kulissen sind derzeit intensive Anstrengungen von Unternehmen und Verbänden beiderseits des Atlantiks zu beobachten. Sie zielen darauf ab, Politikern zu verdeutlichen, wie sehr das EuGH-Urteil vor allem die Realwirtschaft und eben nicht nur die Facebooks dieser Welt trifft. Handel und Wirtschaften ohne Daten gibt es heute nicht mehr. Und Datenströme sind global.

Ungeachtet dieser Bemühungen ist der Handlungsdruck auf Seiten der Unternehmen groß. Landesschutzbeauftragte haben sich bereits geäußert und planen, wie beispielsweise in Baden-Württemberg, bei der Beurteilung spezifischer Sachverhalte zu prüfen, ob es vergleichbare, rein europäische Angebote gibt, um ihre Sanktionen davon abhängig zu machen.

Auch die Mitbestimmungsseite ist alarmiert. Es ist nur noch eine Frage der Zeit, bis Betriebsräte, verärgerte Mitarbeitende oder Datenschutzaktivisten aktiv werden.

Handlungsdruck

In der Vergangenheit getroffene strategische Entscheidungen zur Speicherung und Verarbeitung personenbezogener Daten zwischen Unternehmensteilen, gegenüber Dienstleistern, Lieferanten und Kunden sind zügig neu zu bewerten und nach einer Risikobeurteilung unverzüglich zu revidieren. Dabei sind Lieferungen von Daten an Unternehmen, die diese in den USA speichern und verarbeiten – und auf die US-Sicherheitsbehörden potenziell Zugriff haben – nicht nur schnellstmöglich zu stoppen, sie sind auch vollständig zurückzuholen. In Anlehnung an eine Fußball-Hymne ließe sich auch sagen: „Data’s coming home!“. Ohne schnelles Handeln der Politik drohen Chaos und ein weiterer extremer Dämpfer für die so sehr herbeigesehnte wirtschaftliche Erholung.