Bild: dpa

Nach der Bombe

Was das Ende des Privacy Shield für den Datenverkehr mit den USA bedeutet

Für einen lauten Knall sorgte am 16. Juli der Europäische Gerichtshof (EuGH), als er das „Privacy Shield"-Abkommen zwischen der EU und den USA für unwirksam erklärte. Damit fällt auf einen Schlag die wichtigste Rechtsgrundlage für Datentransfers über den Atlantik weg. Experten fordern, bis auf Weiteres keine geschützten Informationen mehr in die USA zu übertragen.

Von Joerg Heidrich

Für viele war es ein Déjà-vu: Wieder einmal hat der EuGH die zentrale Regelung für Datenübermittlungen von Europa in die USA gekippt (Az. C-311/18). Wieder einmal war der Kläger der österreichische Datenschutzaktivist Max Schrems. Und wieder einmal gab Facebook den Anlass. Die Parallelen der jetzigen Entscheidung gegenüber dem Urteil zu „Safe Harbor" aus dem Jahr 2015 (Az.: C-362/14) sind so offensichtlich wie bemerkenswert. Doch anders als 2015 könnte die jetzige Entscheidung dauerhafte Konsequenzen für den transatlantischen Informationsaustausch haben. In jedem Fall sind die Folgen schwerwiegend.

Formal hat der EuGH „den Beschluss 2016/1250 der Europäischen Kommission über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes" für ungültig erklärt. Dem Gerichtsbeschluss liegt die Überlegung zugrunde, dass Daten zwar innerhalb der EU ohne weitere Vorgaben frei transferiert werden dürfen. Für Staaten außerhalb der EU gilt diese Freiheit aber nicht. Es gibt eine Reihe von privilegierten Ländern, bei denen angenommen wird, dass dort ähnliche Datenschutzstandards herrschen wie im Unionsraum. Dazu gehören etwa Israel, Kanada, die Schweiz, Neuseeland oder auch Japan. Zu diesem Kreis wird nach dem Brexit wohl auch das Vereinigte Königreich zählen.

Nicht zu diesem exklusiven Kreis gehören allerdings die USA. Dort gibt es zwar in einzelnen Staaten ausgeprägte Datenschutzvorgaben, etwa in Kalifornien. Dies gilt aber nicht für das ganze Land. Um dennoch Daten übermitteln zu können, bediente man sich eines bemerkenswerten Verfahrens: Ein amerikanisches Unternehmen konnte sich in ein Verzeichnis eintragen lassen und verpflichtete sich damit, die Datenschutzrechte der europäischen Bürger angemessen zu würdigen. Dieses Verzeichnis hieß bis 2015 Safe Harbor. Nach dem ersten Urteil des EuGH 2015 folgte darauf der Privacy Shield.

Lippenstift auf Schweinen

Allerdings war das auch schon fast die einzige Änderung. Max Schrems nannte den Vorgang damals „Putting lipstick on a pig" – das identische Schwein, nur etwas aufgehübscht. Denn was bisweilen euphemistisch „Privacy-Shield-Zertifizierung" genannt wurde, bestand in der Praxis im Wesentlichen daraus, dass sich ein amerikanisches Unternehmen in ein vom U. S. Department of Commerce geführtes Verzeichnis eintragen und einige Selbstverpflichtungen abnicken musste. Einen wirklichen Schutz der Daten von EU-Bürgern enthielt dagegen keines der beiden Abkommen. Diese sind und waren nahezu uneingeschränkt den Zugriffen der US-Geheimdienste und diverser Behörden ausgesetzt. Ebenso fehlt es an wirksamen Rechtsmitteln der Betroffenen gegenüber solchen Zugriffen in den USA – ein Zustand, den Datenschutzbehörden seit Jahren bemängeln.

Die Entscheidung des EUGH hat daher kaum jemanden überrascht. Das Gericht prüfte neben der DSGVO auch die Europäische Grundrechtecharta, die unter anderem die Achtung des Privat- und Familienlebens, den Schutz personenbezo-

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover

gener Daten und das Recht auf effektiven gerichtlichen Rechtsschutz verbürgt. Das Gericht stellte fest, dass den Erfordernissen der nationalen Sicherheit der USA, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang gegenüber den Rechten der Europäer eingeräumt wird. Hieraus ergebe sich, dass Eingriffe in die Grundrechte der Personen ermöglicht werden, deren Daten in die Vereinigten Staaten übermittelt wurden.

Insbesondere seien die auf die amerikanischen Rechtsvorschriften gestützten Überwachungsprogramme nicht auf ein zwingend erforderliches Maß beschränkt. Überhaupt sei nach Ansicht des Gerichts hinsichtlich bestimmter Überwachungsprogramme nicht einmal erkennbar, dass für die darin enthaltenen Ermächtigungen gegenüber EU-Bürgern irgendwelche Einschränkungen bestehen. Auch würden diesen betroffenen Personen keine Rechte verliehen, die sie gegenüber den amerikanischer Behörden gerichtlich durchsetzen könnten.

Wacklige Klauseln

Neben dem Privacy Shield prüfte der EuGH in seiner Entscheidung auch die so genannten Standarddatenschutzklauseln (SDK) auf ihre Wirksamkeit. Diese stellen eine alternative Rechtsgrundlage zum transatlantischen Datenverkehr dar. Wer diese Vorgaben nutzen will, muss einige Klauseln, welche von der EU vorgegeben sind, mit seinem amerikanischen Partner vertraglich vereinbaren. Im Rahmen dieser Vertragsbestandteile wird zwischen den Partnern ein datenschutzfreundlicher Umgang mit persönlichen Informationen vereinbart. In der Praxis sind solche SDK auch beim Transfer von Daten in andere außereuropäische Länder höchst relevant, etwa nach Indien.

Bei der Prüfung kam der EuGH zu dem Ergebnis, dass die SDK weiter zulässig bleiben. Voraussetzung sei jedoch, dass die Personen, deren Daten in andere Länder übermittelt werden, ein Schutzniveau genießen müssen, „das dem in der Union durch die DSGVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist“. Praktisch bedeutet dies, dass das Zielland geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe bieten muss.

Hier bringt der EuGH die lokalen Datenschutzbehörden im EU-Mitgliedsstaat ins Spiel. Diese hätten einen Datenexport zu verbieten, wenn sie der Auffassung sind, dass die SDK im betreffenden Land nicht eingehalten werden. Kritiker bezweifeln, dass Datenschutzbehörden SDK mit amerikanischen Partnern überhaupt zulassen dürfen. Denn die Klauseln hätten keinerlei Einfluss auf übertriebene Zugriffsmöglichkeiten von US-Behörden und den fehlender Rechtsschutz. Allenfalls könnten sie technische Maßnahmen festlegen, die den Zugriff Dritter etwa durch Verschlüsselung erschweren.

Ob sich künftige Datenexporte in die USA per SDK absichern lassen, ist deshalb fraglich. Damit blieben nicht mehr viele Rechtsgrundlagen. Sehr eingeschränkt lassen sich Daten innerhalb eines Konzerns weitergeben. Als letzte Möglichkeit könnten Firmen explizite Einwilligungen jedes einzelnen Betroffenen einholen. Dazu müssten sie die Nutzer jedoch detailliert informieren, was mit ihren Daten in Übersee geplant ist und wer dort alles Zugriff hat.

Autonomes Europa

Bemerkenswert ist, wie unterschiedlich Datenschutzbehörden auf die Entscheidung reagieren. Die britische Behörde, immerhin derzeit noch an die DSGVO gebunden, rät zu einem „keep calm and carry on“ und dazu, in Sachen Datenexport erst mal wie bisher weiterzumachen. Ulrich Kelber, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), sieht in dem Urteil eine Stärkung der Rechte der Bürger. Der EuGH mache deutlich, „dass internationaler Datenverkehr weiter möglich ist“. Dabei müssten aber die Grundrechte der europäischen Bürgerinnen und Bürger beachtet und „besondere Schutzmaßnahmen ergriffen“ werden.

Strenger legt die Datenschutzbeauftragte Berlins, Maja Smoltczyk, das Urteil aus. Sie beschwört die digitale Eigenständigkeit Europas und fordert sämtliche Verantwortliche auf, „umgehend zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln“. Die Zeiten seien vorbei, in denen personenbezogene Daten aus Bequemlichkeit oder Kostenersparnissen in die USA übermittelt werden könnten. Bereits übermittelte Daten müssten „zurückgeholt werden“.

Die Vertreter der deutschen Wirtschaft sind dagegen wenig angetan von der Entscheidung. Der Bitkom e. V. beklagt, dass durch dieses Urteil massive Unsicherheit entstehe, und befürchtet ein „Daten-Chaos“. Die EU sei aufgerufen, schnell für Rechtssicherheit zu sorgen und eine Datenverarbeitung in Drittländern wie den USA langfristig zu ermöglichen. Daten ausschließlich in Europa zu verarbeiten, sei einerseits technisch kaum umsetzbar und würde andererseits einen massiven Wettbewerbsnachteil für europäische Unternehmen bedeuten.

Dass es allerdings zu schnellen neuen Lösungen für den transatlantischen Datenverkehr kommt, ist derzeit unwahrscheinlich. Es ist kaum zu erwarten, dass eine Trump-Regierung den Bitten der Europäer nach mehr Datenschutz für die eigenen Bürger nachkommen wird. Ebenso wird ein Joe Biden, sollte er im November die Wahl gewinnen, die eigenen Geheimdienste und Behörden in ihren Zugriffsmöglichkeiten kaum beschneiden. Europäische Firmen und Anwender müssen sich auf einen längeren Zeitraum mit rechtlicher Ungewissheit bei der Zusammenarbeit mit US-Unternehmen einstellen. Umso wichtiger ist es, rechtssichere Alternativen voranzutreiben, die nicht auf ein Placet aus Washington angewiesen sind. *(hag@ct.de)* c't

Bild: Matthias Röder/dpa

Er hat sie gezündet: Max Schrems vom Wiener Datenschutzverein noyb bemängelte in seiner Klage unter anderem, dass europäische Nutzer gegen Datenschutzverstöße durch Geheimdienste in den USA keine Rechtsmittel einlegen können.

Urteile: ***ct.de/yszu***

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover