EuGH: Kein angemessener Datenschutz in den USA

Die europäische Richtlinie über die Verarbeitung von personenbezogenen Daten (Richtlinie 95/46/EG) bestimmt, dass eine Übermittlung solcher Daten in ein Drittland außerhalb der EU grundsätzlich nur dann erfolgen darf, wenn das betreffende Drittland ein angemessenes Schutzniveau dieser Daten gewährleistet.

Die Europäische Kommission kann nach der Richtlinie feststellen, dass ein bestimmtes Drittland dieses Schutzniveau erreicht. Das geschah hinsichtlich der USA. Im Rahmen der so genannten „Safe-Harbour-Regelung" stellte die Kommission im Jahre 2000 fest, dass die USA dieses Schutzniveau erfüllen würden.

Der Europäische Gerichtshof hat mit Urteil vom 06.10.2015 festgestellt, dass die nationalen Datenschutzbehörden bei einer Beschwerde eines Bürgers befugt sind, diese Feststellung der Kommission gerichtlich überprüfen zu lassen. Ist eine nationale Datenschutzbehörde oder die Person, die sie angerufen hat, also der Auffassung, dass eine Entscheidung der Kommission ungültig ist, muss diese Behörde oder diese Person die nationalen Gerichte anrufen können, damit diese, falls sie ebenfalls Zweifel an der Gültigkeit der Entscheidung der Kommission haben, die Sache dem Gerichtshof vorlegen können.

Der Gerichtshof prüft dann in dem Urteil die Gültigkeit der Entscheidung der Kommission hinsichtlich der USA selbst und stellt fest, dass die Kommission sich bei ihrer Feststellung darauf beschränkt hatte, die Safe-Harbor-Regelung zu prüfen. Diese gilt aber nur für die amerikanischen Unternehmen, die sich ihr unterwerfen, nicht aber für die Behörden der Vereinigten Staaten. Außerdem haben die Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses und der Durchführung von Gesetzen der Vereinigten Staaten Vorrang vor der Safe-Harbor-Regelung, so dass die amerikanischen Unternehmen ohne jede Einschränkung verpflichtet sind, die in dieser Regelung vorgesehenen Schutzregeln unangewandt zu lassen, wenn sie in Widerstreit zu solchen Erfordernissen stehen. Die amerikanische Safe-Harbor-Regelung ermöglicht daher Eingriffe der amerikanischen Behörden in die Grundrechte der Personen.

Dann stellt der Gerichtshof fest, dass nach dem Unionsrecht eine Regelung nicht auf das absolut Notwendige beschränkt ist, wenn sie generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne objektive Kriterien vorzusehen, die es ermöglichen, den Zugang der Behörden zu den Daten und deren spätere Nutzung zu beschränken.

Der Gerichtshof fügt hinzu, dass eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens verletzt. Ferner führt der Gerichtshof aus, dass eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des Grundrechts auf wirksamen gerichtlichen Rechtsschutz verletzt. Damit erklärt der Gerichtshof die Entscheidung der EU-Kommission für ungültig.

(EuGH, Urteil vom 06.10.2015, Aktenzeichen: C-362/14 - Maximillian Schrems / Data Protection Commissioner)

Fazit

Der Europäische Gerichtshof (EuGH) hat mit der Entscheidung jedenfalls für einen regelrechten Paukenschlag im Datenschutzrecht gesorgt. Das Urteil stellt sowohl alle Unternehmen, als auch die Politik vor große, ggf. sogar in der Praxis unlösbare Probleme und zwingt zu sofortigem Handeln.

Datentransfer im Sinne des Datenschutzrechts bezieht sich immer auf personenbezogene Daten. Alle Daten, die mittelbar oder unmittelbar auf eine natürliche Person zurückgeführt werden können, sind dem Datenschutzrecht unterworfen, das in Europa wesentlich strenger geregelt ist, als dies in den Vereinigten Staaten der Fall ist. Personenbezogen ist dabei nach zumindest aktuell herrschender Meinung auch die IP-Adresse, da sie über ein Auskunftsverlangen des zuständigen Internetserviceproviders auch wiederum auf eine bestimmte natürliche Person zurückgeführt werden kann. Das bedeutet, dass gerade im Internet und bei internetbezogenen Datentransfers nahezu immer auch personenbezogene Daten betroffen sind.

Zwar können diese Datentransfers weiterhin unter bestimmten Umständen zulässig sein aber ein Bezug auf diese Vereinbarung ist ab sofort nicht mehr möglich. Das bedeutet, dass jedes Unternehmen in Europa genau prüfen muss, welche Daten aus welchen Gründen und aufgrund welcher Vereinbarung den Raum der Europäischen Union verlassen und insbesondere in die USA transferiert werden. Das betrifft beispielsweise alle Arten von Cloud-Lösungen, die von US-amerikanischen Anbietern stammen, als auch sämtlicher Datenverkehr über Google, Facebook, Apple, LinkedIn usw.

Nach unserem Dafürhalten gibt es daher kein Unternehmen, das nicht von dieser Entscheidung betroffen ist und nicht unverzüglich auf das Urteil reagieren sollte. Es ist daher unbedingt zu empfehlen, alle Datenübermittlungen in die USA innerbetrieblich unverzüglich zu prüfen.

Wie genau die Reaktion auszusehen ist, ist allerdings aktuell sehr schwer konkret darzustellen, da sich die zuständigen Behörden gar nicht bzw. widersprüchlich zu der Gerichtsentscheidung geäußert haben. Es wurde jedenfalls von den deutschen Datenschützern eine Galgenfrist bis zum 31.01.2016 postuliert. Bis dahin wolle man Verstöße aufgrund der EuGH-Entscheidung nicht sanktionieren: Danach aber wurden bereits Prüfungen angekündigt, so dass jetzt unverzüglich in den Unternehmen mit der Evaluierung der Datentransfers begonnen werden sollte.

Möglich und ratsam ist es daneben, den jeweils für das Unternehmen zuständigen Landesdatenschutzbeauftragten nach seiner Rechtsauffassung und der weiteren Vorgehensweise zu befragen. Daneben wird auf jeden Fall eine Rechtsberatung nötig sein, um den weiteren Prozess nach der Urteilsverkündung rechtssicher begleiten und die sich in Zukunft herausstellenden Änderungen unverzüglich vornehmen zu können.

Doch auch bereits bei der erforderlichen Evaluation der Datentransfers und der möglichen Alternativen ist eine Rechtsberatung nach unserer Meinung unverzichtbar. Der Grundsatz, dass eine Rechtsberatung im Vorfeld nicht nur die sicherere, sondern auch die günstigere Variante ist im Vergleich zu einem Abwarten bzw. einem bloßen „Weiter so“, dürfte hier insbesondere anwendbar sein.

Inhaltlich kann dem Urteil übrigens nur beigepflichtet werden. Es gibt keinen „sicheren Hafen“ in den USA, da durch verschiedene Gesetze, wie den Patriot-Act, amerikanische Behörden das jederzeitige Recht haben solche personenbezogenen Daten einzusehen und zu verwenden. Das hat mit einem angemessenen Datenschutzniveau aus europäischer Sicht nichts zu tun.

BGH: Hinwirken auf Löschung rechtswidriger Tatsachenbehauptungen

Werde ich im Internet mit unwahren Tatsachenbehauptungen in meiner Persönlichkeit verletzt, habe ich gegen den Täter, aber auch gegen den Störer, bspw. den Betreiber eines Meinungsforums, einen Anspruch auf Beseitigung, also Löschung des Beitrags, ggf. auch auf Berichtigung der Behauptung.

Doch was, wenn sich die rechtswidrige Behauptung vorher bereits selbständig gemacht hat, also weitere Kreise zieht und nicht nur auf der Ursprungsquelle zu finden ist? Wie weit geht die

Verantwortung des Täters oder Störers bzw. anders herum, wie weit geht mein Anspruch als Betroffener?

Der Bundesgerichtshof (BGH) hat zu einem solchen Fall im Sommer 2015 entschieden, dass bei einer fortdauernden Rufschädigung im Internet der Betroffene den – in dem Falle – Störer grundsätzlich nicht nur auf Berichtigung, sondern auch auf Löschung bzw. Hinwirken auf Löschung rechtswidriger, im Internet abrufbarer Tatsachenbehauptungen in Anspruch nehmen kann.

Die Löschung bzw. das Hinwirken auf die Löschung solcher im Internet abrufbarer Tatsachenbehauptungen kann im Rahmen eines Beseitigungsanspruchs aber nur verlangt werden, so der BGH, wenn und soweit die beanstandeten Behauptungen nachweislich falsch sind und die begehrte Abhilfemaßnahme unter Abwägung der beiderseitigen Rechtspositionen, insbesondere der Schwere der Beeinträchtigung, zur Beseitigung des Störungszustands geeignet, erforderlich und dem Störer zumutbar ist.

(Bundesgerichtshof, Urteil vom 28. Juli 2015, Aktenzeichen VI ZR 340/14)

Fazit

Die Pflichten des Täters aber auch des Störers gehen also noch weiter, als die Löschung der unwahren Behauptungen. Damit trägt der BGH dem Umstand Rechnung, dass solche Informationen im Netz in der Regel weiter verbreitet werden. Derjenige, der die Ursache gesetzt hat (Täter) bzw. zumindest für diese verantwortlich ist (Störer) muss dann alles Zumutbare unternehmen, um auch auf andere Hinzuwirken, diese Inhalte wieder zu entfernen.

Denken Sie also daran, dass Sie vor Abgabe einer Unterlassungserklärung über die bloße Löschung des betroffenen Contents hinaus auch zumindest nach weiteren Fundstellen suchen und Dritte, insbesondere auch Suchmaschinenbetreiber, zur Beseitigung auffordern müssen. Wichtig: Dokumentieren Sie die Aufforderung zur Löschung, denn Sie müssen beweisen können, dass Sie alles Zumutbare getan haben.

Timo Schutt
Rechtsanwalt
Fachanwalt für IT-Recht

www.schutt-waetke.de
ra-schutt@schutt-waetke.de