TRANSATLANTISCHER DATENSCHUTZ: EINE ENTDECKUNGSREISE

von Dr. Axel Spies

Dr. Axel Spies, Of Counsel

Kaum ein transatlantisches Thema erregt in Deutschland mehr Emotionen als der Datentransfer in die USA oder ein Zugriff von US-Behörden auf in Europa belegene personenbezogene Daten. Auslöser hierfür sind die *Snowden*-Enthüllungen und die Diskussionen über das Transatlantische Freihandelsabkommen TTIP. Für die einen sind personenbezogene Daten Handelsware („das Öl des 21. Jahrhunderts"), für die anderen sind sie ein unabdingbarer, der Vermarktung entzogener Teil der eigenen Person. Es gibt verschiedene Möglichkeiten, das Risiko des Datentransfers in die USA rechtlich zu minimieren, obwohl die EU und die USA beim Datenschutz unterschiedliche Ansätze verfolgen.

Ausgangspunkt aller Überlegungen ist die Tatsache, dass die Welt voll von grenzüberschreitenden Datentransfers ist. Globales Business erfordert globale Netze und im Falle von Ausfällen technischer Anlagen und als Backup kann dies sogar zwingend erforderlich sein. *Big Data* und *Geolocation* können Diebstähle verhindern und Verbrechen aufdecken. Neue Technologien und *Cloud Computing* senken die Kosten, z. B. bei der Verarbeitung von Personaldaten. All diese rasanten technischen Entwicklungen machen nicht an Grenzen halt. Neben dem Bedarf der Wirtschaft an immer feineren Datenstrukturen treten die Forderungen der Behörden, die weltweit Datenzugang bei Unternehmen zu verschiedenen Zwecken verlangen: nicht nur zur Terroristenverfolgung, sondern auch in Kartellverfahren, Strafverfahren mit Zugang zu Informationen in der Cloud, Ermittlungen nach den *Sarbanes Oxley Act*, *Federal Corrupt Practices Act* usw. Zivilgerichtsverfahren, insb. in den USA, erfordern regelmäßig die Aufbereitung und Vorlage von Millionen von Datensätzen durch die streitbefangenen Parteien weltweit im Wege der *E-Discovery*. Damit wächst auch der

Umfang der zu schützenden Daten in atemberaubender Schnelle. Das große US-Unternehmen *Wal-Mart* verarbeitet z. B. in der Stunde 167-mal mehr Daten als diejenigen, die sich in der gesamten *US Library of Congress* befinden. Durch das Anschwellen des Datenflusses wächst die Gefahr, dass Hacker oder einfach der Verlust von Daten durch Mitarbeiter durch simples menschliches Versagen gewaltige Schäden anrichtet.

Der kaum noch quantifizierbare internationale Datenfluss wirft zahlreiche schwierige Rechtsfragen auf: Was ist ein Datentransfer? Genauer: Was sind überhaupt „personenbezogene Daten"? Weiter: Ist es angemessen, dass der nationale Gesetzgeber die Übermittlung personenbezogener Daten getrennt vom Datentransfer über die Grenze hinweg regelt? Welche Rolle spielen Standards, welche die Industrie selbst erarbeitet? Was gehört in eine Datenschutzerklärung des Unternehmens hinein? Im Kern geht es bei den Regeln zum internationalen Datentransfer um die Gefahr eines Verlustes der Herrschaft über die Daten und damit um nationale Souveränität. Dies macht es schwierig, für alle Beteiligten annehmbare Lösungen zu finden, auch wenn die physische Sicherheit der Daten gewährleistet ist. Dies ist besonders in Deutschland ein Problem, wo der Datenschutz Verfassungsrang hat. Es ist unklar, wann und wie diese Herrschaft und die Pflicht des Staates – und abgeleitet der Unternehmen – zum Datenschutz endet. Das BVerfG hat im Jahr 2008 neben dem etablierten Recht auf informationelle Selbstbestimmung noch ein weiteres Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" im GG als „IT-Grundrecht" verankert. Der Inhalt und Umfang dieser Schutzrechte ist US-Unternehmen, die Daten auf der Grundlage des Prinzips *„Reasonable Expectation of Privacy"* verarbeiten, nur schwer zu vermitteln. Möglicherweise ist das in der EU landläufige Lokalitätsprinzip bei der Datenverarbeitung, das (mit einigen Ausnahmen) den Datenschutz an den Ort der Datenverarbeitung anknüpft, nicht mehr zeitgemäß.

Fest steht: Das Risiko des internationalen Datentransfers tragen in erster Linie die beteiligten Unternehmen, die z. B. bei einem Bruch der Datensicherheit unversehens an den Pranger der Öffentlichkeit gelangen. Von diesen Unternehmen wissen viele nicht einmal genau, wo auf der Welt die von ihnen als verarbeitende Stelle kontrollierten Daten verarbeitet werden. Sie müssen die Diskrepanz der verschiedenen Datenschutzregeln (z. B. in der EU verglichen mit den USA) in den Griff bekommen. Ihre Kenntnis, wo sich die personenbezogenen Daten befinden und wie sie verarbeitet werden, wird durch immer weiteres weltweites (möglicherweise mehrstufiges) Outsourcing verwässert.

Die Auslegung der relevanten, in großen Teilen überarbeitungsbedürftigen EU-Richtlinie mit all ihren Rechtsunsicherheiten, die Debatte in der EU über die Zukunft des Regimes der „*EU/US Safe Harbor Principles*" oder die Neuerungen der EU-Datenschutzreform kommen hinzu. Manche Länder, wie zuletzt Russland, verlangen eine Speicherung bestimmter Daten auf dem eigenen Territorium, um sie besser zu kontrollieren zu können. All dem sollten die Unternehmen Rechnung tragen – eine fast unlösbare Aufgabe, die ohne eine klare Strategie zum Scheitern verurteilt ist.

Datenschutz Strategie – einige Ansatzpunkte für Unternehmen:

- **Schritt 1:** Wie sieht der Datenfluss aus? In welchen Ländern werden die personenbezogenen Daten verarbeitet und wer hat auf sie Zugriff? Werden die Daten (nur) für eigene Zwecke verarbeitet?
- **Schritt 2:** Welche rechtlichen Instrumente sind anzusetzen, um die Rechtmäßigkeit der Datenübermittlung zu gewährleisten? Zum Zuge kommen die genannten *EU/US Safe Harbor Principles*, aber auch Standardverträge zur Datenübermittlung, so genannte konzernweite *Binding Corporate Rules* und individuelle Einwilligungen der Betroffenen.
- **Schritt 3:** Wie kann der Datenfluss hinreichend überwacht werden? Zu denken ist an Audits, Zertifizierungen usw. Wichtig: Besteht ausreichender Versicherungsschutz?
- **Schritt 4:** Wie wird der Datenschutz nach außen kommuniziert? Müssen die Aufsichtsbehörden informiert werden? Sind z. B. *Privacy Policies* erforderlich, die z. B. in den USA durch die FTC und andere Behörden unter Androhung empfindlicher Strafen durchgesetzt werden?
- **Schritt 5:** Was passiert, wenn es zu einer Verletzung der Datensicherheit kommt? Wer benachrichtigt wen? Gibt es einen Notfallplan? Wer trifft die notwendigen Entscheidungen?

Viele deutsche Unternehmen machen häufig die für sie frustrierende Erfahrung, dass das deutsche Konzept des Datenschutzes gegenüber US-Unternehmen schwer zu vermitteln ist, da schon die Begriffe verschieden sind (hier Datenschutz als Verfassungsgrundsatz, dort Datenschutz als Schutz der physischen Sicherheit der Daten). Umgekehrt haben viele US-Unternehmen erhebliche Schwierigkeiten mit den nur zum Teil EU-weit harmonisierten Regeln zum Datenschutz und zur Datenspeicherung. Hinzu kommt häufig ein offenes

oder latentes Desinteresse bei den Betroffenen (den Nutzern), die freiwillig für geringe Vorteile (Bonuspunkte, Gutscheine, Aufsehen und Ansehen) ihre personenbezogenen Daten der Welt offenbaren, aber sich wenig dafür interessieren, ob die Daten sicher sind oder an Dritte weitergegeben werden. Unternehmensintern bestehen häufig Bedenken, dem Datentransfer im Wirtschaftsbereich Beschränkungen aufzuerlegen, wenn anderenfalls Wettbewerbs- oder Kostenvorteile erzielt werden können. In diesen Fällen können externe Berater helfen, die Risiken besser einschätzen zu können. Ein guter Datenschutz gekoppelt mit Transparenz kann für Unternehmen ein Aushängeschild sein und einen Marktvorsprung durch Kundenvertrauen schaffen. Die Aufsichtsbehörden sind schlichtweg überfordert bei vielen komplizierten und aufwändigen Datenübermittlungen trotz des vorhandenen guten Willens.

Für die international tätigen Unternehmen bleibt zu hoffen, dass sich langfristig die dazu berufenen Gremien auf zwischenstaatlicher Ebene auf weltweite Standards einigen, z. B. zwischen der USA und der EU im Rahmen der *Transatlantic Trade and Investment Partnership (TTIP)* oder im Rahmen der Welthandelsorganisation (WHO). Der Transatlantische Datentransfer sollte sozusagen als „Voreinstellung" erlaubt werden; Einschränkungen sollten nur in klaren und für die Unternehmen vorhersehbaren Fällen vorgesehen werden. Ein anderer – möglicherweise kumulativer – Lösungsweg ist eine bessere Akzeptanz von Industriestands und Verhaltenskodizes zum Datenschutz in den betroffenen Ländern. Die Aussichten hierfür stehen zurzeit allerdings schlecht. Derzeit sieht es mehr danach aus, dass sich die USA und die EU beim Datenschutz im Wirtschaftsbereich durch neue Konzepte wie das „Recht auf Vergessen-Werden", das im letzten Jahr der EuGH für Suchmaschinen mit noch kaum abschätzbaren Konsequenzen propagiert hat, die Unterscheidung zwischen sensiblen und nicht sensiblen Daten und die Ausweitung der Prärogativen der Aufsichtsbehörden bei internationalem Datentransfer auseinanderentwickeln.