

# Standardklauseln bei Übermittlung personenbezogener Daten in Drittländer

*Renate Riedl*

*Studentin an der Universität Wien  
A-1190 Wien, Hameaustraße 9a/4  
a9303391@unet.univie.ac.at*

**Schlagworte:** Datenschutz, grenzüberschreitender Datenverkehr, Standardvertragsklauseln, personenbezogene Daten

**Abstract:** Durch zwei Entscheidungen der Europäischen Kommission im Jahr 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer steht ein weiteres Instrument zur Verfügung, das dem verlangten angemessenen Schutzniveau in der EU-Datenschutzrichtlinie genügt. Trotz Unterschriftenreife für die Vertragspartner, den Datenexporteur und den Datenimporteur bleiben einige Punkte in den Klauseln zu überlegen, die auch im Vorfeld der Entscheidung von verschiedenen Seiten nicht unbestritten waren.

## 1. Übermittlung personenbezogener Daten in Drittländer

Immer mehr personenbezogene Daten, vor allem von Beschäftigten und Kunden im Marketing eines privaten Unternehmens, werden wegen niedrigerer Kosten und zwecks Konzentrierung in Länder außerhalb der Europäischen Union ausgelagert. Personenbezogene Daten sind Daten über eine bestimmte oder bestimmbare Person, die direkt oder indirekt identifiziert werden kann. Wo die Übermittlung und Verarbeitung personenbezogener Daten aufgrund der Datenschutzrichtlinie<sup>1</sup> innerhalb der Europäischen Union keine größeren Schwierigkeiten bereitet, kann es bei der Übermittlung in Drittländer aufgrund des Art 25 besagter Richtlinie zu Problemen bis hin zur Untersagung der Übermittlung kommen. Das Land in das die Daten übermittelt werden, hat ein angemessenes Schutzniveau zu gewährleisten, welches unter Berücksichtigung aller Umstände

---

<sup>1</sup> Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABi Nr L 281 v 23. 11. 1995, S 31.

zu beurteilen ist. Zum derzeitigen Zeitpunkt sind nur Kanada<sup>2</sup>, die Schweiz, Ungarn und US-Unternehmen<sup>3</sup> im Rahmen des Safe-Harbor-Konzeptes<sup>4</sup> von der Kommission als Länder mit angemessenem Schutzniveau anerkannt.

Eine Übermittlung in andere Länder ohne Schutzniveau kann nach Art 26 Abs 1 der Richtlinie auch dann stattfinden, wenn unter anderem zum Beispiel eine zweifelsfreie Einwilligung der betroffenen Person vorliegt, ein lebenswichtiges Interesse der betroffenen Person besteht oder die Übermittlung personenbezogener Daten zum Abschluss oder der Erfüllung eines Vertrages im Interesse der betroffenen Person nötig ist. Nach Art 26 Abs 2 der Richtlinie können sich die Garantien, welche die entsprechenden Kernrechte des Betroffenen, wie Zweckbindung, Recht auf Zugriff, Löschung, Widerspruch, und Nichtunterworfenheit bei automatisierter Einzelentscheidung enthalten, auch aus entsprechenden Vertragsklauseln ergeben, die nach Abs 4 des Artikels von der Kommission angenommen und von den Mitgliedstaaten durch entsprechende Maßnahmen erfüllt werden.

## 2. Entscheidungen der Europäischen Kommission

Mit zwei Entscheidungen<sup>5</sup> der Kommission, beide ergangen im letzten Jahr, gibt es nun Muster für Standardvertragsklauseln, welche ausreichende Garantien gemäß Art 26 bieten. Diese Vertragsklauseln sollen den Datenfluss personenbezogener Daten zwischen der Europäischen Union und Drittländern vereinfachen, basieren auf Freiwilligkeit und beziehen sich ausschließlich auf den Datenschutz, wobei es den Vertragspartnern frei-

<sup>2</sup> E der Kommission v 20. Dezember 2001 gemäss der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet.

<sup>3</sup> E der Kommission v 26. Juli 2000 gemäss der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in Ungarn, der Schweiz und des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglich „Häufig Gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABI L 215 v 25. August 2000.

<sup>4</sup> Siehe <http://www.exports.gov/safeharbor/>.

<sup>5</sup> E der Kommission v 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG, ABI L 181 v 4. Juli 2001 S 19 und E der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer nach der Richtlinie 95/46/EG, ABI L 6 vom 10. Jänner 2002 S 52.

steht andere Geschäftsklauseln mit in den Vertrag aufzunehmen. Nationale Regelungen zur Durchführung der Datenschutzrichtlinie, die sich auf die Verarbeitung personenbezogener Daten beziehen, bleiben davon unberührt. Die Entscheidungen beziehen sich sowohl auf die für die Verarbeitung Verantwortlichen als auch auf solche, bei die nur als Auftragsverarbeiter im Drittland tätig werden.

Die Begriffsbestimmungen sind im wesentlichen mit denen in der Richtlinie ident. Der Datenexporteur ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt. Der Datenimporteur ist der in einem Drittland ansässige Verarbeiter, der sich bereit erklärt, vom Datenexporteur dessen Anweisungen und den Vorschriften dieser Entscheidungen entsprechend Daten entgegenzunehmen und/oder die nach der Übermittlung in dessen Auftrag verarbeitet werden sollen, und der nicht dem System eines Drittlandes unterliegt, das ein angemessenes Datenschutzniveau bietet. Beiden Vertragsparteien sind Pflichten zur Sicherung des Datenschutzes wie Einhaltung der Bestimmungen oder hinreichende technische und organisatorische Maßnahmen zum Schutz vor zufälliger oder unrechtmäßiger Zerstörung, zufälligem Verlust, Änderung, unberechtigter Weitergabe und Zugang auferlegt. Anwendbares Recht sind jene Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, welche in dem Land, in dem der Datenexporteur ansässig ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind.

### **3. Wichtige Punkte und Kritik**

Das bedeutet faktisch eine Erweiterung des Europäischen Rechtes auf das Ausland, was bei einigen Ländern bekannterweise nicht gerne gesehen wird. Insbesondere die Vereinigten Staaten haben sich in der Vergangenheit mehr als kritisch dazu geäußert. Es besteht zwar für private Unternehmen in den Vereinigten Staaten die Möglichkeit dem Datenschutzkonzept Safe Harbor beizutreten, in diesem Konzept sind aber nicht alle Daten erfasst. Gerade wichtige Datengruppen wie Telekommunikation oder Finanzdienstleistungen unterliegen nicht der Zuständigkeit der Federal Trade Kommission und müssen deshalb rechtlich auf andere Weise abgesichert werden, eben etwa durch die Verwendung von Standardvertragsklauseln. Die Hauptrolle in der Durchsetzung der Vertragsklauseln liegt nicht nur bei den Vertragsparteien, sondern im Besonderen auch bei der betroffenen Person, besonders wenn dieser ein Schaden entstanden ist. Für die Vertragsparteien ist eine gesamtschuldnerische Haftung vorgese-

hen, was bei verschiedenen Wirtschaftsverbänden (zB: International Chamber of Commerce, Confederation of British Industry) die im Vorfeld der Entscheidungen Stellung<sup>6</sup> genommen haben, auf Kritik stieß, da diese Haftung als zu weit angesehen wird. Ein weiterer nicht unbestrittener Punkt ist die für einige Punkte in den Klauseln vorgesehene Drittbegünstigtenklausel, die der begünstigten Person direkt aus dem Vertrag Rechte einräumt. Zu bemerken ist hier vor allem, dass die Form des Vertrages zu Gunsten Dritter, die in der österreichischen Rechtsordnung hier in Frage kommt, nicht in allen Rechtsordnungen anerkannt ist. Wie dieses Problem in einigen Mitgliedsstaaten zu lösen ist, bleibt unklar. Wenn sich die betroffene Person bei Streitigkeiten auf die Drittbegünstigtenklauseln beruft hat sie die Wahl zwischen einem Schlichtungsverfahren durch eine unabhängige Person, durch die Kontrollstelle oder einem Gerichtsverfahren in dem Mitgliedsstaat in dem der Datenexporteur ansässig ist. Auf Verlangen der Kontrollstelle der Mitgliedsstaaten oder wenn es im Datenschutzrecht vorgesehen ist muss der Datenexporteur eine Kopie des Vertrages bei der Kontrollstelle hinterlegen. Für Unternehmen ist dieser Punkt sicher nicht als risikofrei einzuschätzen, da Daten ohne besonderen Schutz der Betriebsgeheimnisse weitergegeben werden, auch wenn die Kontrollstellen ihre Sensibilität bezüglich dieser Problematik bekräftigt haben. Die Kontrollstellen können unter bestimmten Voraussetzungen in Ausnahmefällen die Übermittlung der Daten auf Vertragsbasis in Drittländer verbieten oder aussetzen, falls sich ein Nachteil für Garantien und Pflichten durch die Übermittlung auf den angemessenen Schutz der betroffenen Personen bieten sollte. Übereinstimmende Einwände von den oben erwähnten Wirtschaftsinteressengruppen bemängeln die mangelnde Transparenz beim Zustandekommen der Standardvertragsklauseln, vor allem da die Europäische Kommission in bewährter Manier die Entscheidung rasch und ohne viel Federlesen erlassen hat. Im weiteren wird von den Verbänden Realitätsferne attestiert, die sich in der Zukunft in der mangelnden Akzeptanz der Standardvertragsklauseln durch ausländische Unternehmen äußern könnte. Meines Erachtens ist dieser Punkt durchaus berechtigt, da gerade der Datenschutz eher vernachlässigt wird und sich niemand freiwillig zu mehr verpflichtet als unbedingt notwendig ist.

Eine weitere Alternative im Rahmen der Richtlinie 95/46/EG für die rechtmäßige Übermittlung personenbezogener Daten in Drittländer bietet Kapitel V der Richtlinie, in dem die Berufsverbände und andere Vereinigungen die Möglichkeit haben Verhaltensregeln auszuarbeiten und in

---

<sup>6</sup> Siehe [http://europa.eu.int/comm/internal\\_market/de/dataprot/news/index.htm](http://europa.eu.int/comm/internal_market/de/dataprot/news/index.htm).

Übereinstimmung mit den einzelstaatlichen Stellen oder im gemeinschaftlichen Rahmen mit der Art 29 Gruppe zu veröffentlichen. Diese Art der kontrollierten Selbstregulierung ist schon allein aus psychologischer Sicht zu bevorzugen, da Unternehmen eher gewillt sein werden eine Regelung zu befolgen, wenn sie die Chance hatten daran mitzuarbeiten, vorausgesetzt die Kontrolle der Mitgliedsstaaten wird ernsthaft ausgeführt und die vorgeschlagenen Verhaltensregeln erschöpfen sich nicht in reiner Absichtsbezeugung. Ich räume dieser Variante gute Erfolgsaussichten ein, wenn die Verbände entsprechendes Engagement zeigen und sich die Einhaltung von Datenschutzvorschriften als Wettbewerbsvorteil gegenüber Konkurrenten erweisen kann.