Erstes Kapitel: Die Einordnung des grenzüberschreitenden Datenschutzes im Aufbau der Richtlinie 95/46/EG

Den Ausgangspunkt für die Beurteilung der Reichweite und der Umsetzung des Datenschutzes für aus der Europäischen Union in Drittländer exportierte Daten liefert die „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“[1], die zum 25. Oktober 1998 von den Mitgliedstaaten in nationales Recht umzusetzen war.[2]

Mit der Richtlinie wurde die erste rechtsverbindliche Regelung auf dem Gebiet des internationalen Datenschutzes geschaffen,[3] die zur Harmonisierung der Rechtsordnungen ihrer Mitglieder verpflichtet. Zugleich stellt sie die erste Rechtssetzung der Europäischen Union im Bereich der Grund- und Freiheitsrechte dar.[4]

Die Richtlinie legt insgesamt fest, unter welchen Bedingungen eine Datenverarbeitung in der Europäischen Union zulässig ist. In diesem Rahmen gibt die so genannte Drittländerregelung in Kapitel IV der Richtlinie Auskunft darüber, nach welchen Maßgaben personenbezogene Daten in Drittländer übermittelt, also in solche Staaten exportiert werden dürfen, die weder Mitglied in der Europäischen Union[5] sind noch dem Europäischen Wirtschaftsraum[*] angehören, der neben den Mitgliedstaaten der Europäischen Union die Staaten Island, Liechtenstein und Norwegen[6] umfasst.

---

[1] ABl. EG Nr. L 281 vom 23.11.1995, S. 31.

[2] Umsetzung in der Bundesrepublik Deutschland durch das Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954), in der Fassung des Änderungsgesetzes vom 18. Mai 2001 (BGBl. I S. 904), die am 23. Mai 2001 in Kraft trat. In Irland trat ein neues Datenschutzgesetz am 1.7.2003 in Kraft, während sich Frankreich, das Schlusslicht bei der Umsetzung der Richtlinie 95/46/EG, sogar bis zum 7.8.2004 Zeit ließ.

[3] *Heil*, DuD 1999, S. 396, S. 397.

[4] *Brühann*, RDV 1996, S. 12, S. 13.

[5] Ausgenommen von den Untersuchungen sind aufgrund des Abschlusszeitpunktes der Arbeit im Jahr 2003 jene Mitgliedstaaten, die der Europäischen Union erst nach dem 30.4.2004 beigetreten sind.

[*] Im Folgenden wird dieser Geltungsbereich nicht mehr gesondert erwähnt. Die Ausführungen für die Europäische Union (auch als „Europa“ oder „die Mitgliedstaaten“ bezeichnet) gelten hier jedoch entsprechend.

[6] Die Einbeziehung dieser Staaten geht auf das Abkommen über den Europäischen Wirtschaftsraum vom 2.5.1992 sowie das Anpassungsprotokoll zu diesem Abkommen vom 17.3.1993 zurück; die EWR-Staaten haben die Richtlinie 95/46/EG mit Wirksamkeit zum 1. Juli 2000 übernommen.

Die nachfolgende Analyse der Reichweite und Umsetzung des Datenschutzes für in Drittländer exportierte Daten setzt zunächst einen Blick auf die Zielsetzung der Richtlinie 95/46/EG und der sich daraus ergebenden Notwendigkeit einer Beschränkung des Datentransfers in Drittländer voraus.

A. Der Hintergrund der Drittländerregelung

Primäres Ziel der Richtlinie 95/46/EG ist entsprechend ihrer Ermächtigungsnorm des Artikels 100a EGV (neu: Art. 95 EGV) die Angleichung der innergemeinschaftlichen Datenschutzgesetze, um den freien Verkehr personenbezogener Daten auf dem Binnenmarkt sicherzustellen sowie Wettbewerbsverzerrungen und daraus resultierende Risiken einer Standortverlagerung zu beseitigen,[7] die auf der Anwendung unterschiedlicher nationaler Vorschriften beruhen.

Zugleich strebt die Richtlinie gemäß ihrem Artikel 1 Absatz 1 einen gleichwertigen „Schutz der Grundrechte und Grundfreiheiten und insbesondere (...) der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“ in allen Mitgliedstaaten an,[8] der gleichsam die Bedingung für einen freien Datenverkehr auf dem Binnenmarkt darstellt und sonach den Auslegungsspielraum der einzelnen Schutzvorschriften nach unten begrenzt.[9]

In Anbetracht des auf diese Weise geschaffenen äquivalenten Datenschutzniveaus innerhalb des Gemeinschaftsgebiets verbietet Artikel 1 Absatz 2 der Richtlinie den Mitgliedstaaten, den freien Verkehr personenbezogener Daten auf dem Binnenmarkt aus Gründen des gemäß Artikel 1 Absatz 1 gewährleisteten Schutzes zu behindern. Nach oben ist die Auslegung der Richtlinie bei der Umsetzung ihrer Bestimmungen in nationales Recht demzufolge durch den Harmonisierungsgedanken beschränkt.

Innerhalb dieses Rahmens verbleibt den Mitgliedstaaten ein gewisser Handlungsspielraum, der einerseits Ergänzungen und Präzisierungen der teilweise generalklauselartigen Richtlinienbestimmungen zulässt und größtenteils sogar auch erfordert[10] sowie andererseits die Formen und Mittel zur Umsetzung der Richtlinie weitestgehend offen lässt.[11] Die Mitgliedstaaten können mithin zwar nach wie vor in Einzelheiten unterschiedliche Datenschutzvorschriften vorsehen, die jedoch bei einer

---

[7] *Begründung des Rates zum gemeinsamen Standpunkt*, ABl. EG Nr. C 93 vom 13.4.1995, S. 19.

[8] Vgl. auch Erwägungsgründe (2), (3), (10) und (11) der Richtlinie; *Begründung des Rates zum gemeinsamen Standpunkt*, ABl. EG Nr. C 93 vom 13.4.1995, S. 19.

[9] Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 15; *ders.*, NJW 1997, S. 281, S. 283, der auf das Erfordernis einer restriktiven Auslegung insbesondere der Generalklauseln durch die Mitgliedstaaten bei der Umsetzung der Richtlinie in nationales Recht hinweist.

[10] Vgl. etwa die Erwägungsgründe (9), (22) und (68) der Richtlinie.

[11] *Gola/Klug*, S. 16; *Klug*, RDV 2001, S. 266; *Scholz*, S. 120.

ordnungsgemäßen Umsetzung der Richtlinienbestimmungen aufgrund des von der Richtlinie gesteckten Rahmens einen gleichwertigen Schutz bieten und somit kein Hemmnis für den europäischen Binnenmarkt bedeuten.

Während die innereuropäischen Grenzen für den Transfer personenbezogener Daten durch die praktische Gleichstellung des Datenverkehrs auf dem Binnenmarkt mit jenem auf nationaler Ebene geöffnet wurden, intendiert die Richtlinie 95/46/EG mit den Vorschriften über den Drittländertransfer eine „gewisse Undurchlässigkeit“ des europäischen Datenschutzsystems nach außen.[12]

Die Notwendigkeit dieser Regelung ergibt sich aus dem mit der fortschreitenden Globalisierung des internationalen Handels[13] verbundenen weltweiten Datenaustausch, der insbesondere im Rahmen der steten Ausdehnung des Internets, das einschließlich des Electronic Commerce den ungehinderten Zugriff auf Daten aller Art jederzeit und ungeachtet nationaler Grenzen ermöglicht, ein kaum mehr fassbares Maß erreicht hat.

So sind ein multinational angelegter Kundenkreis, globale Netzwerke internationaler Konzerne sowie eine durch Kostenerwägungen motivierte zentralisierte Datenverarbeitung von Personal- und Kundendaten im außereuropäischen Ausland nicht mehr aus der Wirtschaftsrealität wegzudenken.[14] Beispielsweise kommen transnational arbeitende Kreditinformationssysteme sowie der internationale Flugreiseverkehr schon seit langem nicht mehr ohne eine grenzüberschreitende Kommunikation und den damit verbundenen Transfer von personenbezogenen Informationen aus.[15] Aber auch die Möglichkeit des Outsourcings der Informationssysteme insbesondere in Länder wie Indien und Weißrussland gewinnt zunehmend an Bedeutung.

Um den mit diesem umfangreichen, weltweiten Datenfluss einhergehenden Gefahren zu begegnen, spricht der Artikel 25 Absatz 1 der Richtlinie, abgesehen von den Ausnahmeregelungen des Artikels 26 der Richtlinie, ein Übermittlungsverbot personenbezogener Daten in solche Drittländer aus, die über kein „angemessenes Schutzniveau“ verfügen.

[12] *Begründung des Rates zum gemeinsamen Standpunkt*, ABl. EG Nr. C 93 vom 13.4.1995, S. 19, S. 20.
[13] Vgl. Erwägungsgrund (56) der Richtlinie.
[14] *Dressel*, S. 31 ff.; Dammann/Simitis, EG-Datenschutzrichtlinie (- *Simitis*), Einleitung, Rn. 27; *ders.*, NJW 1997, S. 281, S. 284.
[15] *Ellger*, RabelsZ 60, S. 738, S. 741; *Heil*, DuD 1999, S. 396.

Der innereuropäische Datenschutz wäre anderenfalls nicht hinreichend gewährleistet, da der Geltungsbereich des mitgliedstaatlichen Datenschutzrechts national beschränkt ist.[16] Zudem würde die unbegrenzte Zulässigkeit einer Übermittlung personenbezogener Daten in Drittländer die Rechtsposition des Betroffenen der Verarbeitung erheblich schwächen[17] und die Durchsetzung seiner Ansprüche unter Umständen sogar unmöglich machen.[18]

So könnten etwa Daten unter Umgehung der strengen Datenschutzbestimmungen der Mitgliedstaaten in das außereuropäische Ausland zur dortigen unkontrollierten Verarbeitung exportiert werden.[19] Zwar unterläge noch die Übermittlung der Daten in das Drittland den Rechtmäßigkeitsvoraussetzungen der Richtlinie. Im Drittland angekommen könnte mit den Daten jedoch gemäß den dort geltenden Vorschriften nach Belieben verfahren werden.

Besonderen Anreiz böte die Umgehung der „Datenschutzinsel Europa“ etwa für Betreiber von Datenbanken, die ungehindert ihre Hauptserver unter Anpassung der Struktur ihrer globalen Netzwerke in Ländern mit einem geringeren Datenschutzniveau ansiedeln könnten.[20] Auch stünde zu befürchten, dass Daten aus der Europäischen Union exportiert würden, um sie entweder absichtlich unkontrolliert oder schlicht aus Kostengründen in einem „unsicheren“ Drittland zu verarbeiten und anschließend zu reimportieren.[21]

Nicht zuletzt aber die bereits vor Erlass der Richtlinie in einigen Mitgliedstaaten existierenden Regelungen zum Datenexport erforderten eine einheitliche, gemeinschaftsrechtliche Drittländerregelung.

So setzte zum Beispiel das französische Datenschutzrecht eine aufsichtsbehördliche Registrierung sämtlicher Datenverarbeitungen voraus, bei der auch ein vorgesehener Drittländertransfer anzugeben war

---

[16] *Vassilaki*, REDP/ERPL, vol. 6, no 1, S. 109, S. 122; ausführlich zu der Frage des Datenschutzes im grenzüberschreitenden Datenverkehr und zu den Anfängen einer entsprechenden Diskussion in Europa: *Hondius*, S. 241 ff.

[17] *Ellger*, S. 88 ff.

[18] *Dressel*, S. 40; *Wittkämper*, DuD 1978, S. 59.

[19] *Ellger*, RabelsZ 60, S. 738, S. 742; *ders.*, S. 95 ff.; *Hahn*, S. 88; *Lavranos*, DuD 1996, S. 400, S. 403; *Moos* in: Kröger/Gimmy, S. 3, S. 13 f.; *TEIA*, Datenschutz im Internet, S. 599; *Wittkämper*, DuD 1978, S. 59, im Hinblick auf die generelle Umgehungsgefahr bei Drittländertransfers.

[20] *Heymann*, CRi 2000, S. 70; vgl. allgemein zur Attraktivität so genannter „Datenoasen“: *Bergmann*, S. 58 ff.

[21] *Brühann* in: Datenverkehr ohne Datenschutz?, S. 35, S. 39.

und verboten werden konnte. Schweden[22], Österreich und Finnland ließen die Übermittlung personenbezogener Daten nur nach vorheriger Genehmigung durch die Aufsichtsbehörde zu, während Portugal differenzierte, indem es Exporte in Drittländer mit gleichwertigem Schutzniveau von dieser Genehmigungspflicht ausnahm.[23] Das deutsche Bundesdatenschutzgesetz regelte demgegenüber ausdrücklich nur den Datenexport durch öffentliche Stellen,[24] ließ aber gleichwohl Übermittlungen durch private Stellen grundsätzlich nur bei einem gleichwertigen Schutzniveau in dem betreffenden Drittland zu, da der Transfer anderenfalls mit den schutzwürdigen Interessen des Betroffenen im Sinne der Tatbestände des § 28 Absatz 1 a. F. kollidiert wäre.

Im Rahmen des freien Verkehrs personenbezogener Daten auf dem Binnenmarkt könnten diese nationalen Bestimmungen bei Fehlen einer gemeinschaftsrechtlichen Drittländerregelung mittels eines Transits über einen anderen Mitgliedstaat ungehindert umgangen werden.[25]

[22] Nur für Übermittlungen in Dateien.
[23] Vgl. umfassend zu den vor der Umsetzung der Richtlinie 95/46/EG in den Mitgliedstaaten geltenden Datenschutzgesetzen: *Wuermeling*, Handelshemmnis Datenschutz, S. 33 ff.
[24] § 17 Absatz 2 BDSG a. F.
[25] *Brühann* in: Datenverkehr ohne Datenschutz?, S. 35, S. 39.

B. Die Struktur des Schutzmechanismus

Die Reichweite und Umsetzung des Datenschutzes für aus der Europäischen Union exportierte Daten bemisst sich nach den von der Richtlinie 95/46/EG aufgestellten Rechtmäßigkeitsvoraussetzungen für den Datentransfer in Drittländer.

Zunächst muss also der Anwendungsbereich der Richtlinie 95/46/EG eröffnet sein. Liegt sachlich eine Verarbeitung personenbezogener Daten im Sinne der Richtlinie vor, so ist der räumliche Anwendungsbereich der in Umsetzung der Richtlinie erlassenen mitgliedstaatlichen Datenschutzgesetze abzustecken, der bereits eine grenzüberschreitende Wirkung zu entfalten vermag und eine entscheidende Rolle dafür spielt, ob eine konkrete Übermittlung tatsächlich den Vorschriften über den Drittländertransfer unterworfen ist.

Da Artikel 25 Absatz 1 der Richtlinie ein unmittelbares Verbot der Übermittlung ausspricht, sofern ein „angemessenes Schutzniveau“ in dem Drittland nicht gewährleistet ist, wird die grenzüberschreitende Weitergabe schließlich durch die Auslegung dieses Zulässigkeitskriteriums limitiert. In diesem Zusammenhang soll das Schutzniveau in den USA einschließlich der Entscheidung der Europäischen Kommission über die Safe Harbor Privacy Principles erörtert werden.

Indessen vermögen die Ausnahmetatbestände des Artikels 26 Absatz 1 der Richtlinie eine Übermittlung in solche Drittländer zu legitimieren, die nicht über ein angemessenes Schutzniveau verfügen, und weichen somit das Übermittlungsverbot des Artikels 25 der Richtlinie auf.

Schließlich kann ein Drittländertransfer auch von den Mitgliedstaaten entsprechend dem Artikel 26 Absatz 2 der Richtlinie genehmigt werden, sofern der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten sowie hinsichtlich der Ausübung der damit verbundenen Rechte des Betroffenen bietet. Als Instrumente zur Gewährleistung derartiger Garantien kommen sowohl Verträge als auch verbindliche Unternehmensrichtlinien, so genannte Codes of Conduct in Betracht.