11639/02/DE
WP 74

Arbeitsdokument: Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer

Angenommen am 3. Juni 2003

DIE GRUPPE FÜR DEN SCHUTZ DER RECHTE VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Europäischen Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe a) und Absatz 3 jener Richtlinie,

gemäß den Verfahrensregeln jener Richtlinie und insbesondere der Artikel 12 und 14

HAT FOLGENDES ARBEITSDOKUMENT ANGENOMMEN:

1 Amtsblatt L 281 vom 23.11.1995, S. 31, abrufbar unter:
http://europa.eu.int/comm/internal_market/de/dataprot/index.htm

Arbeitsdokument über verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer

1. EINFÜHRUNG

Datenschutzbehörden erhalten Anträge auf Genehmigungen für die Übermittlung personenbezogener Daten in Drittländer im Sinne von Artikel 26 Absatz 2 der Richtlinie. Traditionell werden meistens vertragliche Lösungen beantragt, die nationale Behörden angesichts der Grundsätze in Betracht ziehen, die in der Arbeitsunterlage WP 12[2] dargestellt sind, wie auch in anderen Unterlagen dieser Gruppe und insbesondere auch in den Kommissionsentscheidungen über Standardvertragsklauseln.

Vertragliche Lösungen werden von multinationalen Unternehmen bereits genutzt, und derzeit wird in einigen Mitgliedstaaten die Möglichkeit erörtert, ihre Nutzung zu erweitern. Diesen Erfahrungen muss bei der Evaluierung der möglichen Entwicklungen der einschlägigen rechtlichen Vorschriften ernsthaft Rechnung getragen werden.

Gleichzeitig würden einige multinationale Unternehmen wegen ihrer komplexen weltweiten Strukturen gerne die Möglichkeit nutzen, „Verhaltenskodizes für internationale Transfers“[3] über die internationale Übertragung personenbezogener Daten innerhalb eines Unternehmens auf multinationaler Ebene, für die nach Artikel 26 Absatz 2 der Richtlinie die Genehmigung der zuständigen Datenschutzbehörden erforderlich ist, anzunehmen. Diese multinationalen Unternehmen sind außerdem der Auffassung, dass die Möglichkeit einseitiger Verpflichtungen, die zuverlässigen Garantien unterliegen, ebenfalls genutzt werden sollte.

Sofern eine einseitige Verpflichtung tatsächliche und garantierte rechtliche Auswirkungen haben kann, insbesondere im Hinblick auf den wirksamen Schutz der betroffenen Personen nach der Übermittlung und was das mögliche Eingreifen der nationalen Kontrollstellen oder anderer Behörden angeht (weitere Ausführungen dazu in Kapitel 3 und 5) sollte es keinen Grund geben, eine solche Möglichkeit auszuschließen:

---

[2] Arbeitsdokument: Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 25 und 26 der EU-Datenschutzrichtlinie, angenommen am 24. Juli 1998.

[3] Es kommt recht häufig vor, dass Unternehmen Verhaltenskodizes annehmen. Typische Gegenstände von Verhaltenskodizes, die von multinationale Unternehmen angenommen werden, sind beispielsweise: (a) korrekte Führung und Aufbewahrung von Büchern und sonstigen Aufzeichnungen; (b) Ehrlichkeit und Genauigkeit im Umgang mit der Öffentlichkeit und der Regierung; (c) Verfahren, z.B. Chinesische Mauern, um sicherzustellen, dass die Beratung von Kunden und Geschäftsentscheidungen nicht von Interessenskonflikten beeinflusst werden; (d) Schutz vertraulicher Informationen; (e) Verbot des Missbrauchs von Vermögenswerten der Unternehmens; (f) Verzicht auf unangebrachte Diskriminierung und Belästigung; (g) Verbot von Bestechung und Schmiergeldzahlungen; (h) Einführung ethischer Geschäftspraktiken und Einhaltung von Gesetzen, die den Wettbewerb auf dem Markt fördern; und (i) Verbot von Wertpapierhandel auf der Grundlage von Insiderinformationen.

Artikel 26 Absatz 2 der Richtlinie 95/46/EG lässt den Mitgliedstaaten hier einen weiten Handlungsspielraum.

Es muss jedoch unbedingt anerkannt werden, dass einseitige Verpflichtungen nach den nationalen Rechtsvorschriften einiger Mitgliedstaaten keine rechtsverbindlichen Pflichten und Rechte schaffen. Unter diesem Gesichtspunkt möchte die Gruppe darauf hinweisen, dass das vorliegende Dokument zu diesem Thema allgemein gehalten ist, um die Gefahr eines Konflikts mit den geltenden nationalen Rechtsvorschriften zu vermeiden; sie behält sich das Recht vor, andere Lösungen zur Harmonisierung der weiteren Nutzung verbindlicher unternehmensinterner Vorschriften in allen Mitgliedstaaten vorzuschlagen.

Verbindliche unternehmensinterne Vorschriften sollten nicht als das einzige oder beste Mittel zur Durchführung internationaler Übermittlungen angesehen werden, sondern nur als zusätzliches Mittel, wo der Einsatz vorhandener Instrumente (d.h. Kommissionsentscheidungen über Standardvertragsklauseln oder ggf. die Grundsätze des sicheren Hafens) besonders problematisch erscheint. Das vorliegende Arbeitspapier soll nicht dazu dienen, die Mitgliedstaaten zu zwingen oder auch nur anzustiften, bei der Bearbeitung der Anträge internationaler Unternehmen ein bestimmtes Instrument einzusetzen. Den nationalen Kontrollstellen oder anderen zuständigen Stellen ist es völlig freigestellt, die ihnen vorgelegten Vorschläge auf die Art und Weise zu prüfen und zu bearbeiten, die ihren nationalen Rechtsvorschriften und den Merkmalen des Antrags am besten entspricht.

Die Gruppe ist dennoch der Auffassung, dass es sinnvoll wäre, diese Überlegungen auf die Gemeinschaftsebene auszudehnen und sich auf eine Reihe von Grundsätzen und Verfahren zu einigen, die sowohl die Arbeit der Unternehmen und Behörden der Mitgliedstaaten erleichtern als auch die Konsistenz innerhalb der EU gewährleisten werden. Auf alle Fälle zielt das vorliegende Papier darauf ab, zu einer harmonisierteren Anwendung und Auslegung von Artikel 26 Absatz 2 der Richtlinie in den Mitgliedstaaten beizutragen und die Datenströme in Fällen zu erleichtern, in denen ein angemessener Schutz gewährleistet wird.[4]

Schließlich möchte die Artikel 29-Datenschutzgruppe erneut hervorheben, dass das Bieten ausreichender Garantien im Sinne von Artikel 26 Absatz 2 ein weiter Begriff ist, der natürlich vertragliche Lösungen und verbindliche unternehmensinterne Vorschriften umfasst, der aber auch andere hier nicht angesprochene Instrumente umfassen kann, die Datenschutzbehörden ebenfalls als geeignet für die Erteilung von Genehmigungen ansehen können. Im vorliegenden Arbeitsdokument wird jedoch nur die Anwendung von Artikel 26 Absatz 2 der Richtlinie auf den speziellen Fall verbindlicher unternehmensinterner Vorschriften untersucht.

Darüber hinaus teilt die Artikel 29-Datenschutzgruppe die Bedenken einige nationaler Datenschutzbehörden in dem Sinne, dass sie möglicherweise nicht über ausreichende Mittel verfügen, um eine große Zahl von Genehmigungsanträgen zeitaufwändig und auf dem Verhandlungsweg zu bearbeiten. Sie ist zuversichtlich, dass die Unternehmen diese Beschränkungen berücksichtigen und sich bemühen werden, Anträge einzureichen, die

4

möglichst eng an die im vorliegenden Dokument enthaltenen Empfehlungen angelehnt sind.

2. DIE MÖGLICHKEITEN VERTRAGLICHER LÖSUNGEN

Die Artikel 29-Datenschutzgruppe möchte darauf hinweisen, dass die Tatsache, dass in diesem Arbeitsdokument verbindliche unternehmensinterne Vorschriften (oder Verhaltenskodizes nach der traditionelleren Terminologie) behandelt werden, nicht dahingehend ausgelegt werden darf, vertragliche Lösungen seien außer Kraft gesetzt worden. Im Gegenteil, nach den Kommissionsentscheidungen über Standardvertragsklauseln und der Erstellung der Leitlinien durch diese Gruppe und durch nationale Datenschutzbehörden machen Unternehmen in einer sehr positiven und ermutigenden Art regen Gebrauch von diesen Instrumenten (d.h. Standardvertragsklauseln mit vielen Vertragsparteien).

Die Artikel 29-Datenschutzgruppe ist der Auffassung, dass die Betroffenen erst angefangen haben, das Potenzial der Standardvertragsklauseln zu nutzen. Hier muss auf zwei Aspekte hingewiesen werden.

Zum einen hindern die Kommissionsentscheidungen über Standardvertragsklauseln die Mitgliedstaaten daran, festzustellen, ob ein Datenexporteur, der einen Vertrag gemäß den Standardvertragsklauseln abschließen möchte, nicht die angemessenen Garantien für die Übermittlung bietet, außer unter den besonderen Gegebenheiten, die in den Kommissionsentscheidungen spezifiziert werden. Mit anderen Worten handelt es sich bei den Standardvertragsklauseln um eine nützliches praktisches Instrument – das den Betroffenen bereits zur Verfügung steht -, das sowohl auf EU- wie auch auf nationaler Ebene anerkannt und angenommen ist, und das ein einheitliches angemessenes Niveau harmonisierter Garantien für Verarbeiter und betroffene Personen bietet. Gleichzeitig haben die Mitgliedstaaten das Recht, andere vertragliche Lösungen in Erwägung zu ziehen, solange kein Zweifel besteht, dass sie ein angemessenes Schutzniveau für die betroffenen personenbezogenen Daten bieten.

Zweitens ist es offensichtlich auch möglich, auf der Grundlage von Standardvertragsklauseln die Nutzung verbindlicher unternehmensinterner Vorschriften vorzusehen, um unter bestimmten Bedingungen[5] Weiterübermittlungen an andere Empfänger als den Datenimporteur zu ermöglichen, ohne dass weitere Verträge mit diesen Empfängern erforderlich sind. Es gibt hier offensichtlich interessante Kombinationen zwischen den vertraglichen Lösungen und der Nutzung der verbindlichen unternehmensinternen Vorschriften, die die Hindernisse aufgrund der fehlenden rechtlichen Auswirkungen einseitiger Verpflichtungen in einigen Mitgliedstaaten überwinden könnten. Daher könnte die Verbreitung personenbezogener Daten innerhalb eines Unternehmens nach dieser Lösung erlaubt sein, sofern die erforderlichen Garantien geleistet werden.

---

[5] Beispielsweise bei der Identifizierung weiterer Empfänger im Vertrag und der Aufnahme der verbindlichen unternehmensinternen Vorschriften im Vertragsanhang als integraler Bestandteil des Vertrags mit allen rechtlichen Folgen.

3. DEFINITION UND RECHTSFRAGEN

3.1. Anwendungsbereich dieses Instruments und Definitionen

Bei der Bearbeitung von Anträgen nach Artikel 26 Absatz 2 der Richtlinie muss vor Erteilung einer Genehmigung geprüft werden, welche Garantien der für die Verarbeitung Verantwortliche für einen ausreichenden Schutz personenbezogener Daten hinsichtlich ihrer Übermittlung in ein Drittland bietet.

Diese Maßnahme unterscheidet sich also von der in Artikel 27 der Richtlinie vorgesehenen Annahme von Verhaltenskodizes, d. h. berufsständischen Regeln für die praktische Anwendung nationaler Datenschutzvorschriften in einem bestimmten Sektor. Auf keinen Fall können unternehmensinterne Vorschriften den Datenschutz ersetzen, zu dessen Einhaltung die Unternehmensteile gesetzlich verpflichtet sind. Und natürlich ist die Einhaltung nationaler gesetzlicher Bestimmungen eine *conditio sine qua non* für jede zu erteilende Genehmigung.

Eine Übermittlung in ein Drittland ist die Mitteilung von Daten an einen anderen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter in einem Drittland; die Rechtmäßigkeit ist unter Berücksichtigung der allgemeinen Umstände des Falls anhand der in der Richtlinie festgelegten Grundsätze (Artikel, 6, 7, 8, 17 usw.) zu bewerten.

Wenn die Verarbeitung im Rahmen der Tätigkeiten eines Unternehmensteils im Gebiet der Gemeinschaft durchgeführt wird, oder wenn die Verarbeitung durch einen Unternehmensteil außerhalb des Gebiets der Gemeinschaft, aber mit einer im Gebiet der Gemeinschaft gelegenen Einrichtung durchgeführt wird, gelten die Bestimmungen der Richtlinie und die nationalen Rechtsvorschriften.

Die Grundsätze des Datenschutzes in den verbindlichen unternehmensinternen Vorschriften müssen weitgehend mit den Grundsätzen des Datenschutzes der Richtlinie 95/46/EG übereinstimmen. Aus dieser Sicht stellt grundsätzlich die Einführung verbindlicher unternehmensinterner Vorschriften innerhalb der Gemeinschaft kein Problem dar, sofern die Vorschriften den nationalen Datenschutzvorschriften genügen. Werden diese Bedingungen eingehalten, können Unternehmen echte globale Grundsätze zur Privatsphäre aufstellen.

Verbindliche unternehmensinterne Vorschriften sind in diesem Sinne und per Definition global, und daher sollten bei ihrer Anwendung keine Unterschiede gemacht werden. Die Vorschriften müssen allgemein im gesamten Unternehmen gelten, unabhängig vom Standort des Unternehmensteils oder der Staatsangehörigkeit der betroffenen Person, deren personenbezogene Daten verarbeitet werden, oder von sonstigen Kriterien oder Erwägungen. Aber auch wenn die Vorschriften immer gleich sind und das Unternehmen sich bemüht, sie angemessen zu beachten, könnte ihre rechtliche Durchsetzbarkeit gegenüber dem Unternehmen unterschiedlich sein, je nachdem ob die Daten ihren Ursprung in der EU haben – anders ausgedrückt, personenbezogene Daten, die einmal unter EU-Recht fielen und später in das Ausland übermittelt werden – oder ob es sich um andere Datenkategorien handelt.

Im Fall anderer Datenkategorien ist das Unternehmen nicht verpflichtet, den betroffenen Personen das Recht zu erteilen, Ansprüche im Gebiet der Gemeinschaft geltend zu machen oder durchzusetzen. Auch wenn eine solche Einbeziehung nicht als *conditio sine qua non* für die Erteilung einer Genehmigung angesehen werden kann, wäre sie stets sehr

willkommen und würde als ernsthaftes Engagement des Unternehmens hinsichtlich der Datenschutzanforderungen angesehen werden.

Da sich der Zweck dieser Instrumente von den Verhaltenskodizes nach Artikel 27 der Richtlinie unterscheidet, erscheint es angemessener, diese Instrumente nicht als "Verhaltenskodizes" zu bezeichnen (was missverstanden werden könnte), sondern eine Bezeichnung zu finden, die der tatsächlichen Natur dieser Instrumente entspricht, d. h. die Bereitstellung ausreichender Garantien für den Schutz personenbezogener Daten, die nach außerhalb der Gemeinschaft übermittelt werden.

Eine mögliche Bezeichnung für diese Instrumente könnte **"verbindliche unternehmensinterne Vorschriften für internationalen Datentransfer"** oder **"rechtlich durchsetzbare unternehmensinterne Vorschriften für internationalen Datentransfer"** sein.

a) - **verbindlich oder rechtlich durchsetzbar**, weil dies die Voraussetzung ist, dass Klauseln als "ausreichende Garantien" im Sinne von Artikel 26 Absatz 2 gelten können

b) - **unternehmensintern** in dem Sinn, dass es sich um von multinationalen Unternehmen eingeführte Vorschriften handelt, für die in der Regel die Zentrale zuständig ist. Im Sinne dieses Dokuments ist ein Unternehmen eine Gruppe von Unternehmensteilen, die nach den Bestimmungen im Kapitel 3.3. an die Vorschriften gebunden sind.

c) - **für internationalen Datentransfer** als Hauptgrund ihres Bestehens.

Der Ausdruck "Unternehmen" kann von Land zu Land sehr unterschiedliche Geschäftsgebilde umfassen: von eng verbundenen, streng hierarchisch strukturierten multinationalen Unternehmen bis zu losen Zusammenschlüssen, von Unternehmen mit sehr ähnlichen wirtschaftlichen Tätigkeiten – und somit auch sehr ähnlichen Verarbeitungen – bis zu Partnerschaften mit sehr unterschiedlichen wirtschaftlichen Tätigkeiten und unterschiedlichen Verarbeitungen. Diese Unterschiede in Struktur und Tätigkeit wirken sich natürlich auf die Anwendbarkeit, die Auslegung und den Anwendungsbereich der verbindlichen unternehmensinternen Vorschriften aus, und die Unternehmen müssen das bei der Einreichung ihrer Vorschläge berücksichtigen.

Für lose Zusammenschlüsse sind verbindliche unternehmensinterne Vorschriften höchstwahrscheinlich kein geeignetes Instrument. Wegen der Verschiedenheit der Mitglieder und der großen Bandbreite der Verarbeitungstätigkeiten wäre es sehr schwierig (wenn nicht unmöglich), die in diesem Arbeitsdokument aufgeführten Anforderungen zu erfüllen. Für diese Zusammenschlüsse wäre eine Differenzierung zwischen den Unternehmensteilen des Unternehmens, die Aufstellung strikter Einschränkungen und Bedingungen für den Informationsaustausch und die Spezifizierung der Vorschriften erforderlich. Anders ausgedrückt: Ein nach Artikel 26 Absatz 2 der Richtlinie annehmbares Endprodukt würde sicher ganz anders aussehen als die in diesem Arbeitsdokument diskutierten verbindlichen unternehmensinternen Vorschriften.

In der Praxis wird damit gerechnet, dass multinationale Unternehmen diese Instrumente am häufigsten nutzen werden, weil sie weltweite unternehmensinterne Übermittlungen auf diese Art werden regeln wollen.

Die Artikel 29-Datenschutzgruppe möchte erneut hervorheben, dass eine auf der Grundlage dieses Instruments erteilte Genehmigung nur die Übermittlungen oder Übermittlungskategorien innerhalb des Unternehmens betreffen würde, oder anders ausgedrückt, den Austausch personenbezogener Daten zwischen Unternehmensteilen, die an diese unternehmensinternen Vorschriften gebunden sind. Übermittlungen personenbezogener Daten an fremde Unternehmen sind nach wie vor möglich, aber nicht auf der Grundlage rechtlich durchsetzbarer verbindlicher unternehmensinterner Vorschriften, sondern auf der Grundlage sonstiger rechtmäßiger Gründe nach Artikel 26 (z. B. nach Standardvertragsklauseln – Musterverträgen oder Ad-hoc-Verträgen – mit den Empfängern der Informationen).

3.2. Weiterübermittlungen

Weiterübermittlungen, das heißt Übermittlungen von Unternehmensteilen außerhalb der Gemeinschaft an fremde Unternehmen sind nur möglich, wenn die von der Europäischen Kommission in ihren Entscheidungen 2001/497/EG (Übermittlungen an für die Verarbeitung Verantwortliche) und 2002/16/EG (Übermittlungen an Auftragsverarbeiter) angenommenen Standardvertragsklauseln oder die darin enthaltenen Bedingungen gebilligt werden.

Dieser Entscheidung zufolge dürfen Weiterübermittlungen personenbezogener Daten an einen anderen für die Verarbeitung Verantwortlichen in einem Drittland, der keinen angemessenen Schutz bietet noch unter eine Entscheidung der Kommission nach Artikel 25 Absatz 6 der Richtlinie fällt, im Fall besonderer Datenkategorien stattfinden, wenn die betroffenen Personen ihre ausdrückliche Zustimmung zur Weiterübermittlung erteilt haben, oder in allen anderen Fällen, wenn ihnen die Möglichkeit geboten wurde, sich dagegen auszusprechen.

Zu den Angaben, die den betroffenen Personen in einer für sie verständlichen Sprache zu machen sind, gehören mindestens:

- der Zweck der Weiterübermittlung;
- die Identität des in der Gemeinschaft ansässigen Datenexporteurs, von dem die personenbezogenen Daten stammen;
- die Kategorien der Empfänger der personenbezogenen Daten und die Bestimmungsländer;
- eine Erklärung darüber, dass die Daten nach der Weiterübermittlung von einem für die Verarbeitung Verantwortlichen verarbeitet werden können, der nicht an die verbindlichen unternehmensinternen Vorschriften gebunden ist, und die Verarbeitung in einem Land stattfindet, in dem es kein angemessenes Schutzniveau für die Privatsphäre von Einzelpersonen gibt.

Die nach Kapitel 4.4. vorgesehenen Audits der verbindlichen unternehmensinternen Vorschriften werden ein spezielles Kapitel über Weiterübermittlungen enthalten, in dem die Benutzung von Musterverträgen durch das Unternehmen überprüft wird. Das Unternehmen stellt diese Verträge auf Antrag den Datenschutzbehörden sowie den betroffenen Personen unter den in den oben erwähnten Kommissionsentscheidungen aufgeführten Bedingungen zur Verfügung.

3.3. Überlegungen zur Verbindlichkeit unternehmensinterner Vorschriften

Organisationen tragen ihren Datenverarbeitungsbedürfnissen auf der Grundlage unterschiedlicher rechtlicher und kultureller Hintergründe und unterschiedlicher Geschäftsphilosophien und -praktiken Rechnung. Die begrenzte Erfahrung mit diesen Instrumenten macht deutlich, dass fast alle multinationalen Unternehmen dieses Problem unterschiedlich angehen. Es gibt jedoch ein Merkmal, das alle Systeme aufweisen müssen, wenn sie als Garantie für den Datentransfer in Drittländer angeführt werden sollen: die **Verbindlichkeit** der unternehmensinternen Vorschriften, sowohl intern als auch in bezug auf die Außenwelt (rechtliche Durchsetzbarkeit der Vorschriften).

3.3.1. Verbindlichkeit unternehmensinterner Vorschriften innerhalb des Unternehmens[6]

Es kann unterschieden werden zwischen dem Problem der Einhaltung der Vorschriften und dem Problem ihrer rechtlichen Durchsetzbarkeit.

Die Bewertung der "Verbindlichkeit" unternehmensinterner Vorschriften verlangt eine Bewertung sowohl ihrer *rechtlichen (rechtliche Durchsetzbarkeit)* als auch ihrer *praktischen (Einhaltung)* Verbindlichkeit. Aber auch wenn die rechtliche Durchsetzbarkeit solcher einseitigen Verpflichtungen oder Verträge mit gleicher Wirkung konzeptuell besteht, so zeigt die Wirklichkeit, dass die grenzüberschreitende Durchsetzung von Rechten stets sehr komplex ist und für die betroffenen Personen unverhältnismäßig hohe Anstrengungen bedeuten kann. Daher ist es erstrebenswert, dass interne Vorschriften nicht nur rechtlich durchsetzbar sondern auch in der Praxis verbindlich sind[7].

Die *praktische* Verbindlichkeit von Vorschriften bedeutet, dass die Unternehmensteile und alle Mitarbeiter des Unternehmens sich gezwungen fühlen, die unternehmensinternen Vorschriften einzuhalten. Diesbezügliche Elemente könnten unter anderem Disziplinarmaßnahmen bei Verstößen gegen die Vorschriften sein, individuelle und wirksame Informationen von Mitarbeitern, Aufstellung spezieller Schulungsprogramme für Mitarbeiter und Unterauftragnehmer usw. Alle diese Elemente, auf die auch in Abschnitt 5 eingegangen wird, könnten dafür sorgen, dass sich die Personen eines Unternehmens verpflichtet fühlen, diese Vorschriften einzuhalten.

Es ist nicht Sache der Datenschutzgruppe, die Methoden festzulegen, mit denen Unternehmen garantieren, dass alle Unternehmensteile an die Vorschriften gebunden werden oder sich ihnen verpflichtet fühlen, auch wenn Beispiele dafür allseits bekannt sind, z. B. interne Grundsätze, für deren Anwendung die Unternehmenszentrale verantwortlich ist, oder interne Verhaltenskodizes, die durch unternehmensinterne

---

7 Die Annahme eines Verhaltenskodex ist ein Schritt, den Unternehmen nicht unbedacht vornehmen, weil sie erhebliche Risiken birgt und für Unternehmen, die gegen ihren eigenen Kodex verstoßen, sogar rechtliche Folgen haben kann.

8 Das Arbeitsdokument WP 12 befürwortet einen funktionellen Ansatz und vertritt die Meinung, dass der bestimmende Faktor für die Angemessenheit der gebotene Schutz in der Praxis ist.

Abkommen gestützt werden[8]. Unternehmen müssen sich jedoch bewusst sein, dass die Antragsteller dem Aussteller einer Genehmigung nachweisen müssen, dass dies im gesamten Unternehmen wirksam geschieht.

Die unternehmensinterne Verbindlichkeit der Vorschriften muss klar sein und die Einhaltung der Vorschriften außerhalb der Gemeinschaft garantieren können, üblicherweise unter der Verantwortung der europäischen Zentrale oder des mit dem Datenschutz beauftragten, in der EU ansässigen Unternehmensteils, die die erforderlichen Maßnahmen treffen, um zu garantieren, dass ausländische Unternehmensteile ihre Verarbeitung an die verbindlichen unternehmensinternen Vorschriften anpassen[9].

Es gibt in der Praxis immer einen in der EU ansässigen Unternehmensteil, der ausreichende Garantien anführt und den Antrag bei der Datenschutzbehörde stellt. Befindet sich die Zentrale des Unternehmens anderswo, sollte sie diese Zuständigkeiten an einen in der EU ansässigen Unternehmensteil delegieren. Es ist sinnvoll, dass der tatsächliche Bieter der Garantien für die tatsächliche Einhaltung der Vorschriften und die Durchsetzung der Garantien verantwortlich bleibt. Siehe hierzu die Abschnitte 5.5. und 5.6. zu Haftung und Gerichtsbarkeit.

3.3.2. Rechtliche Durchsetzbarkeit der unternehmensinternen Vorschriften durch die betroffenen Personen (Drittbegünstigungsrechte) und durch Datenschutzbehörden

Betroffene Personen, die unter die verbindlichen unternehmensinternen Vorschriften fallen, müssen Drittbegünstigte sein, und zwar entweder aufgrund der rechtlichen Folgen einseitiger Verpflichtungen (möglichst nach einzelstaatlichem Recht) oder aufgrund vertraglicher Vereinbarungen zwischen den Unternehmensteilen. Als Drittbegünstigte sollten betroffene Personen berechtigt sein, die Einhaltung der Vorschriften durchzusetzen, sowohl durch Einreichen einer Beschwerde bei der zuständigen Datenschutzbehörde als auch bei dem zuständigen Gericht im Gebiet der Gemeinschaft, wie weiter unten in Abschnitt 5.6. näher erläutert wird.

Die Artikel 29-Datenschutzgruppe legt großen Wert auf beide Möglichkeiten. Auch wenn es grundsätzlich für die betroffene Person viel einfacher erscheint, eine Beschwerde bei der zuständigen Datenschutzbehörde einzureichen, und die Verpflichtung des Unternehmens zur Zusammenarbeit mit dieser Behörde in den meisten Fällen wahrscheinlich zur Lösung des Problems führen wird, gibt es zwei Gründe, das Recht vorzusehen, dass Rechtsmittel eingelegt werden können, auch unter der Annahme, dass das Beschwerdesystem gut funktioniert (siehe Abschnitt 5.6):

a) weil die Verpflichtung zur Zusammenarbeit niemals eine 100%ige Einhaltung der Vorschriften garantieren kann und die betroffenen Personen nicht notwendigerweise immer mit den Standpunkten der Datenschutzbehörde übereinstimmen, und

---

9 Ideal wäre es, wenn die verbindlichen unternehmensinternen Vorschriften vom Vorstand des Mutterunternehmens angenommen würden.

10 Nach dem internationalen Gesellschaftsrecht können angegliederte Unternehmen Verhaltenskodizes gegeneinander durchsetzen, wenn Verstöße gegen quasivertragliche Vereinbarungen sowie Falschdarstellungen oder Fahrlässigkeit geltend gemacht werden.

b) weil die Zuständigkeit der Datenschutzbehörden in der Gemeinschaft von Land zu Land leicht unterschiedlich sein (z. B. können manche Behörden keine Sanktionen verhängen oder Übermittlungen direkt blockieren) und keine Datenschutzbehörde Entschädigung für Schäden zuerkennen kann; das können nur Gerichte.

Die Artikel 29-Datenschutzgruppe möchte betonen, dass die Möglichkeit der betroffenen Personen, die Vorschriften bei Gericht durchzusetzen, aus den erwähnten Gründen notwendig ist, sie aber mehr Wert darauf legt, dass die Vorschriften in der Praxis vom Unternehmen eingehalten werden, was das Ziel jedes Systems der Selbstkontrolle ist.

Was einen weiteren Aspekt betrifft, so werfen Unterschiede im Zivil- und Verwaltungsrecht die Frage auf, ob einseitige Erklärungen als Ursprung von Drittbegünstigungsrechten für Personen angesehen werden können oder nicht.

In manchen Fällen ist die rechtliche Durchsetzbarkeit einseitiger Erklärungen eindeutig, in anderen Mitgliedstaaten dagegen ist die Lage nicht so klar, und einseitige Erklärungen könnten unzureichend sein. Sollten einseitige Erklärungen nicht als rechtlich durchsetzbare Drittbegünstigungsrechte angesehen werden können, muss das Unternehmen entsprechende vertragliche Vereinbarungen treffen. Solche Verpflichtungen können in allen Mitgliedstaaten privatrechtlich durchgesetzt werden[10].

Die Drittbegünstigtenrechte sollten mindestens diejenigen Rechte umfassen, die nach der Kommissionsentscheidung 2001/947/EG für Standardvertragsklauseln gegen den Datenexporteur und den Datenimporteur gewährt werden (siehe Klausel 3 "Drittbegünstigte"[11]): Dies ist ein deutlicher Beweis für den Wert und die Bedeutung der vorliegenden Standardvertragsklauseln.

---

12 Heute ist es in allen Mitgliedstaaten möglich, Drittbegünstigungsrechte in einem Vertrag zu gewähren. Siehe hierzu frühere Erfahrungen mit Standardvertragsklauseln und Drittbegünstigten.

13 Die betroffenen Personen sollten befugt sein, die folgenden Rechte durchzusetzen (zum einfacheren Auffinden sind in Klammern die entsprechenden Klauseln der Kommissionsentscheidung über Standardvertragsklauseln angegeben):

Betrifft die Übermittlung besondere Datenkategorien, muss die betroffene Person vor der Übermittlung darüber informiert worden sein oder informiert werden, dass diese Daten in ein Drittland übertragen werden könnten, das keinen angemessenen Schutz bietet (Klausel 4b).

Sie muss das Recht haben, auf Antrag ein Exemplar der verbindlichen unternehmensinternen Vorschriften zu erhalten (Klauseln 4c und 5e).

Sie muss das Recht haben, innerhalb einer angemessenen Zeit und in einem zumutbaren Umfang eine Antwort auf Beschwerden zur Verarbeitung dieser personenbezogenen Daten außerhalb der Gemeinschaft zu erhalten (Klauseln 4d und 5c).

Sie muss das Recht haben, anzuzeigen, dass ein an die Vorschriften gebundener Unternehmensteil nicht mit der zuständigen Datenschutzbehörde zusammenarbeitet und/oder sich nicht an die Stellungnahme der Datenschutzbehörde über die Verarbeitung der übertragenen Daten hält (Klausel 5c).

Sie muss das Recht haben, anzuzeigen, dass die für die Unternehmensteile außerhalb der Gemeinschaft geltenden einschlägigen Rechtsvorschriften sie daran hindern, ihre Verpflichtungen nach den verbindlichen unternehmensinternen Vorschriften zu erfüllen (Klausel 5a).

Solche vertraglichen Vereinbarungen müssen nicht komplex oder lang sein. Sie dienen nur als Instrumente, um den betroffenen Personen in denjenigen Ländern, in denen es nicht klar ist, ob einseitige Erklärungen ein ähnliches Ergebnis erzielen können, Drittbegünstigungsrechte zu bieten. Manchmal kann dieses Ziel durch Aufnahme einer einfachen Klausel in bestehende Verträge zwischen den Unternehmensteilen erreicht werden. Zur Einhaltung dieser Forderung wäre es zum Beispiel in den Fällen, in denen Verträge zwischen der Zentrale und den Niederlassungen zur Sicherstellung der unternehmensinternen Einhaltung der Vorschriften bestehen – siehe vorstehenden Abschnitt – ausreichend, eine Drittbegünstigungsklausel aufzunehmen.

Hinsichtlich der rechtlichen Durchsetzbarkeit verbindlicher unternehmensinterner Vorschriften durch die zuständige Datenschutzbehörde verpflichtet sich das Unternehmen natürlich mit dem Antrag auf Genehmigung des internationalen Datentransfers gegenüber der Datenschutzbehörde zur Einhaltung der angeführten Garantien (in diesem Fall der verbindlichen unternehmensinternen Vorschriften). Das ist unabhängig von der Frage, ob die Verantwortung für die Durchsetzung dieser Verpflichtung bei der Datenschutzbehörde selbst oder einer anderen Behörde (z. B. bei einem Gericht nach Stellungnahme der Datenschutzbehörde) liegt.

Darüber hinaus haben betroffene Personen immer das Recht, wie in Abschnitt 5.6 ausgeführt, eine Beschwerde bei der nationalen Datenschutzbehörde oder einem Gericht einzureichen. Das könnte für betroffene Personen einen zufriedenstellenderen Verlauf eines rechtlichen Verfahrens bedeuten, und auf jeden Fall eine Art "indirekter" Drittbegünstigungsrechte für die betroffenen Personen.

3.3.3. Für Unternehmensteile geltende zwingende Anforderungen nach nationalen Rechtsvorschriften

Die verbindlichen unternehmensinternen Vorschriften sollten eine Bestimmung enthalten, nach der ein Unternehmensteil, wenn er Anlass hat anzunehmen, dass die ihn betreffenden Rechtsvorschriften ihn daran hindern, seinen Verpflichtungen im Rahmen der verbindlichen unternehmensinternen Vorschriften nachzukommen, und dass sie eine wesentliche nachteilige Wirkung auf die durch die Vorschriften gebotenen Garantien haben, unverzüglich die Zentrale in der EU oder den mit dem Datenschutz beauftragten in der EU ansässigen Unternehmensteil informieren wird, sofern dies nicht durch eine

---

Sie muss das Recht haben, anzuzeigen, dass die Verarbeitung personenbezogener Daten eines Unternehmensteils, der an die Vorschriften gebunden ist, mit den verbindlichen unternehmensinternen Vorschriften nicht im Einklang ist (Klausel 5b).

Sie muss das Recht haben, eine Haftung und gegebenenfalls eine Entschädigung entsprechend den Bestimmungen in den verbindlichen unternehmensinternen Vorschriften zu fordern (Klausel 6).

Sie muss das Recht haben, entsprechend den Bestimmungen in den verbindlichen unternehmensinternen Vorschriften die europäische Gerichtsbarkeit anrufen zu können (Klausel 7).

Sie muss das Recht haben, anzuzeigen, dass die Klauseln entgegen den verbindlichen unternehmensinternen Vorschriften oder ohne Beachtung der vorgesehenen Verfahrensweise geändert worden sind, oder dass ein Unternehmensteil seinen Verpflichtungen nicht mehr nachkommt, sobald er nicht mehr an die Vorschriften gebunden ist (Klauseln 9 und 11).

Der Umfang der Drittbegünstigtenrechte muss klar aus den vertraglichen Vereinbarungen hervorgehen, die sie gewähren.

Vollstreckungsbehörde verboten ist, zum Beispiel als Verbot im Rahmen des Strafrechts, die Vertraulichkeit einer Vollstreckungsermittlung zu wahren.

Die Zentrale in der EU oder der mit dem Datenschutz beauftragte in der EU ansässige Unternehmensteil sollte eine verantwortliche Entscheidung treffen und die zuständigen Datenschutzbehörden konsultieren müssen. Alle die Vorschriften betreffenden Vorfälle nach diesem Kapitel werden in den nach Kapitel 5.2. vorgesehenen regelmäßigen Audits erfasst und überprüft.

Die nach nationalen Rechtsvorschriften für Unternehmensteile geltenden zwingenden Anforderungen, die nicht weitergehen, als es in einer demokratischen Gesellschaft unter Zugrundelegung der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgeführten Interessen erforderlich ist[12], stehen grundsätzlich nicht im Widerspruch zu den verbindlichen unternehmensinternen Vorschriften. Beispiele für solche zwingenden Anforderungen, die nicht weitergehen, als es in einer demokratischen Gesellschaft erforderlich ist, sind unter anderem international anerkannte Sanktionen, Anforderungen an Steuerberichte oder Anforderungen an Berichte zur Bekämpfung von Geldwäsche. In Zweifelsfällen sollten Unternehmen umgehend die zuständige Datenschutzbehörde konsultieren.

4. WESENTLICHER INHALT DER VERBINDLICHEN UNTERNEHMENSINTERNEN VORSCHRIFTEN

4.1. Wesentlicher Inhalt und Maß an Ausführlichkeit

Die Datenschutzgruppe bestätigt die in ihrem Arbeitsdokument Nr. 12[13] enthaltenen Grundsätze, insbesondere Kapitel 3 (*Anwendung des Ansatzes auf die Selbstkontrolle der Wirtschaft*) und in geringerem Maße Kapitel 6 (*Verfahrensfragen*). Es muss klar sein, dass diese Grundsätze an sich den Unternehmen und Arbeitnehmern, die personenbezogene Daten außerhalb der Gemeinschaft verarbeiten, sehr wenig bedeuten könnten, insbesondere in den Ländern, die keine Datenschutzvorschriften aufweisen und sehr wahrscheinlich überhaupt keine Datenschutzkultur besitzen.

Diese Grundsätze müssen in den verbindlichen unternehmensinternen Vorschriften weiterentwickelt und ausgeführt werden, so dass sie in der Praxis und Wirklichkeit mit den Verarbeitungsmaßnahmen übereinstimmen, die von dem Unternehmen in Drittländern vorgenommen werden, und von den Personen, die innerhalb des Unternehmens für den Datenschutz zuständig sind, verstanden und tatsächlich angewandt werden können.

---

[15] das heißt, wenn es sich um Maßnahmen handelt, die notwendig sind für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, ein wichtiges wirtschaftliches oder finanzielles Interesse des Staates oder den Schutz der betroffenen Person oder die Rechte und Freiheiten anderer Personen.

[16] **Arbeitsdokument: Übermittlungen personenbezogener Daten in Drittländer: Anwendung der Artikel 25 und 26 der EU-Datenschutzrichtlinie**

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12de.pdf

Unter diesem Gesichtspunkt haben die verbindlichen unternehmensinternen Vorschriften vielleicht etwas gemein mit den in Artikel 27 der Richtlinie vorgesehenen Verhaltenskodizes, und zwar in dem Sinne, dass sie die Abstraktheit der Gesetzgebung ausgleichen sollen (in diesem Fall die Grundsätze des Arbeitsdokuments 12). Die unternehmensinternen Vorschriften sollten sowohl maßgeschneiderte Bestimmungen als auch ein vernünftiges Maß an Ausführlichkeit in der Beschreibung der Datenströme, der Verarbeitungszwecke usw. enthalten.

Nach Artikel 26 Absatz 2 der Richtlinie kann eine Genehmigung eine Übermittlung oder eine Kategorie von Übermittlungen betreffen, aber in jedem Fall müssen die genehmigten Übermittlungen erläutert werden. Die Ausführlichkeit muss ausreichend sein, um den Datenschutzbehörden die Beurteilung zu ermöglichen, dass die in Drittländern durchgeführten Verarbeitungen angemessen sind (z. B. eine genaue Beschreibung der wirtschaftlichen Tätigkeiten, der die einzelnen Teile des Unternehmens nachgehen).

Ein praktischer Vorschlag könnte beispielsweise - und sofern die nationalen Vorschriften ein Meldesystem vorsehen - darin bestehen, dass in denjenigen Ländern, in denen das Meldesystem ein hohes Maß an Ausführlichkeit enthält, dieser Abschnitt der verbindlichen unternehmensinternen Vorschriften die Vorschriften über das Verfahren der Meldung der für die Verarbeitung Verantwortlichen an die Datenschutzbehörden widerspiegeln sollte: So wie die Meldung es der Datenschutzbehörde ermöglicht, die Verarbeitungen zu verstehen, die von dem für die Verarbeitung Verantwortlichen durchgeführt werden[14], sollten diese Informationen grundsätzlich auch ausreichen, um es der Datenschutzbehörde zu ermöglichen, die Verarbeitung nach den verbindlichen unternehmensinternen Vorschriften innerhalb des Unternehmens zu verstehen. Wenn das Maß an Ausführlichkeit im Meldesystem nicht ausreicht (Artikel 18 Absatz 2 der Richtlinie gibt den Mitgliedstaaten in dieser Hinsicht einen großen Spielraum), sind weitere Angaben erforderlich, um eine angemessene Beschreibung der in Drittländer zu übermittelnden personenbezogenen Daten zu bieten. In Mitgliedstaaten, die gemäß Artikel 18 Absatz 2 der Richtlinie die Meldung durch ein System interner Datenschutzbeauftragter ersetzt haben, kann das von diesen Datenschutzbeauftragten geführte Verzeichnis herangezogen werden. Verbindliche unternehmensinterne Vorschriften ersetzen keinesfalls Anforderungen an Meldungen nach EU-Recht.

4.2. Spezifizierung und Aktualisierung von Vorschriften

In verbindlichen unternehmensinternen Vorschriften können Vorschriften für verschiedene Länder oder Regionen außerhalb der Gemeinschaft weiter spezifiziert werden, wenn das entsprechende Unternehmen dies wünscht. Die Spezifizierung würde jedoch das System, das im Prinzip für die Aufstellung globaler Grundsätze gedacht ist, komplexer machen.

Bezüglich der Aktualisierung von Übermittlungen und damit verbunden der Aktualisierung der Vorschriften erkennt die Artikel 29-Datenschutzgruppe an, dass Unternehmen sich verändernde Organisationen sind, deren Unternehmensteile und Praktiken sich ändern können, daher könnte es sein, dass zu einem bestimmten Zeitpunkt keine 100%ige Übereinstimmung mit den Gegebenheiten zum Zeitpunkt der Erteilung

---

[17] Siehe Artikel 19 der Richtlinie

der Genehmigung besteht. Aktualisierungen (ohne dass ein neuer Genehmigungsantrag erforderlich ist) sind unter folgenden Bedingungen möglich:

a) Es darf keine Übermittlung personenbezogener Daten an einen neuen Unternehmensteil erfolgen, solange der Datenexporteur nicht sichergestellt hat, dass der neue Unternehmensteil an die Vorschriften gebunden ist und sie erfüllen kann.

b) Eine benannte Person oder Abteilung des Unternehmens muss eine stets aktualisierte Liste der Unternehmensteile führen, alle Aktualisierungen der Vorschriften aufzeichnen und auf Antrag den betroffenen Personen oder Datenschutzbehörden die erforderlichen Auskünfte erteilen.

c) Einmal jährlich sind die Aktualisierungen der Vorschriften oder die Änderungen in der Liste der Unternehmensteile den die Genehmigungen erteilenden Datenschutzbehörden mitzuteilen mit einer kurzen Begründung der Aktualisierung.

Die Aktualisierung der Vorschriften ist in dem Sinne zu verstehen, dass sich Arbeitsverfahren geändert haben können und die Vorschriften an die geänderte Umgebung anzupassen sind. Signifikante Änderungen – nicht nur der Grundsätze des Datenschutzes sondern auch der Verarbeitungsziele, der verarbeiteten Datenkategorien oder der Kategorien betroffener Personen – wirken sich grundsätzlich auf die Genehmigung aus.

5. EINHALTUNG LEISTEN UND DURCHSETZUNG GARANTIEREN

Neben den Vorschriften, die wesentliche Datenschutzgrundsätze betreffen, müssen verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer auch Folgendes enthalten:

5.1. Bestimmungen, mit denen ein hohes Maß an Erfüllung garantiert wird

Es wird erwartet, dass die Vorschriften ein System errichten, das Bewusstheit und Durchführung der Vorschriften innerhalb und außerhalb der Europäischen Union garantiert. Die Einführung unternehmensinterner Grundsätze zur Privatsphäre durch die Zentrale ist lediglich als erster Schritt im Rahmen der Einführung ausreichender Garantien im Sinne von Artikel 26 Absatz 2 der Richtlinie anzusehen. Das antragstellende Unternehmen muss auch nachweisen können, dass solche Grundsätze bekannt sind, verstanden werden und im ganzen Unternehmen von den Mitarbeitern angewandt werden, die eine geeignete Schulung erhalten haben und denen die relevanten Informationen jederzeit zur Verfügung stehen, zum Beispiel im Intranet. Für Aufsicht und Sicherstellung der Einhaltung ernennt das Unternehmen einen geeigneten Stab, der von der oberen Leitungsebene unterstützt wird.

5.2. Audits

Die Vorschriften müssen regelmäßige Eigenaudits und/oder eine externe Überwachung durch akkreditierte Auditoren vorsehen, die dem Aufsichtsrat des Mutterunternehmens

direkt Bericht erstatten[15]. Datenschutzbehörden erhalten eine Kopie dieser Audits, wenn eine Aktualisierung der Vorschriften gemeldet wird, und auf Antrag, falls erforderlich, im Rahmen der Zusammenarbeit mit der Datenschutzbehörde.

In den Vorschriften muss auch angegeben sein, dass die Verpflichtung zur Zusammenarbeit mit den Datenschutzbehörden (siehe Kapitel 5.4.) Audits erforderlich machen kann, die von Prüfern der Kontrollstelle selbst oder von unabhängigen Auditoren im Auftrag der Kontrollstelle durchgeführt werden. Das wird vor allem dann der Fall sein, wenn die im vorstehenden Absatz vorgesehenen Audits aus welchen Gründen auch immer nicht verfügbar sind, wenn sie die für eine normale Weiterverfolgung der erteilten Genehmigung erforderlichen Angaben nicht enthalten, oder wenn die Dringlichkeit der Lage eine direkte Beteiligung der zuständigen Datenschutzbehörde oder in ihrem Auftrag handelnder unabhängiger Auditoren angeraten erscheinen lässt.

Solche Audits werden nach den einschlägigen Gesetzen und Vorschriften durchgeführt, die ungeachtet der Überprüfungsbefugnisse der einzelnen Datenschutzbehörden für die Untersuchungsbefugnisse von Datenschutzbehörden gelten und über die das Unternehmen durch die zuständige Datenschutzbehörde ordnungsgemäß informiert wird. Auf jeden Fall werden solche Audits unter Beachtung der Vertraulichkeit und der Geschäftsgeheimnisse durchgeführt und sind strikt begrenzt auf die Feststellung der Einhaltung der unternehmensinternen Vorschriften.

5.3. Handhabung von Beschwerden

Die Vorschriften müssen ein System vorsehen, in dem Beschwerden Einzelner von einer klar bezeichneten Beschwerdeabteilung behandelt werden. Datenschutzbeauftragte oder andere mit diesen Beschwerden befasste Personen müssen bei der Ausübung ihrer Tätigkeiten über eine entsprechende Unabhängigkeit verfügen. Es sollten auch alternative Methoden zur Beilegung von Streitfällen entsprechend den geltenden nationalen Gesetzen und Vorschriften gefördert werden, gegebenenfalls unter Einbeziehung von Datenschutzbehörden.

5.4. Pflicht zur Zusammenarbeit mit Datenschutzbehörden

Wie im Arbeitsdokument WP 12 ausgeführt ist eines der wichtigsten Merkmale für die Bewertung der Angemessenheit eines Systems der Selbstkontrolle das Maß an Unterstützung und Hilfe, die es betroffenen Personen bietet:

"Von einem angemessenen und wirksamen Datenschutzsystem ist zu fordern, dass der Einzelne bei einem Problem im Zusammenhang mit den eigenen personenbezogenen Daten nicht allein gelassen wird, sondern institutionelle Hilfe erhält, um die Schwierigkeiten zu beheben."

Dies ist eines der wichtigsten Merkmale verbindlicher unternehmensinterner Vorschriften für internationalen Datentransfer: Die Vorschriften müssen eindeutig die

---

[18] Diese Audits müssen umfassend sein und in jedem Fall auf bestimmte in diesem Arbeitsdokument bereits aufgeführte Einzelheiten eingehen, zum Beispiel die Weiterübermittlung auf der Grundlage von Standardvertragsklauseln (siehe Abschnitt 3.2.) oder die Entscheidungen hinsichtlich der zwingenden Anforderungen nach nationalen Rechtsvorschriften, die zu Konflikten mit den verbindlichen unternehmensinternen Vorschriften führen könnten (siehe Abschnitt 3.3.3.)

Pflicht zur Zusammenarbeit mit Datenschutzbehörden enthalten, damit einzelnen Personen die institutionelle Unterstützung zuteil wird, die in WP 12 erwähnt wird.

Es muss eine eindeutige Verpflichtung vorliegen, dass das Unternehmen als Ganzes und jeder Unternehmensteil für sich die im Kapitel 5.2. aufgeführten Auditanforderungen akzeptiert. Es muss ebenfalls eine eindeutige Verpflichtung vorliegen, dass das Unternehmen als Ganzes und jeder Unternehmensteil für sich die Stellungnahme der zuständigen Datenschutzbehörde zu allen Problemen der Auslegung und Anwendung dieser verbindlichen unternehmensinternen Vorschriften einhalten wird. Die Stellungnahme der zuständigen Datenschutzbehörde besteht aus an das Unternehmen gerichteten Empfehlungen, entweder als Antwort auf eine Anfrage vom Unternehmen, als Folge einer Beschwerde einer betroffenen Person oder auf Eigeninitiative der Datenschutzbehörde.

Vor einer Stellungnahme kann die zuständige Datenschutzbehörde die Meinung des Unternehmens, der betroffenen Person sowie der Datenschutzbehörden einholen, die im Rahmen der in diesem Arbeitsdokument vorgesehenen Zusammenarbeit beteiligt sein könnten[16]. Die Stellungnahme der Behörde kann veröffentlicht werden.

Zusätzlich zu den einschlägigen nationalen Bestimmungen kann eine ernsthafte und/oder anhaltende Weigerung des Unternehmens zur Zusammenarbeit oder zur Befolgung der Stellungnahme der zuständigen Datenschutzbehörde die Aussetzung oder Aufhebung der erteilten Genehmigung entweder durch die Datenschutzbehörde selbst oder durch die nach den nationalen Rechtsvorschriften dazu befugte Behörde zur Folge haben. Diese Entscheidung erfolgt in Form eines Verwaltungsakts, den der Empfänger nach nationalem Recht vor dem zuständigen Gericht anfechten kann. Die Entscheidung wird der Europäischen Kommission und den anderen beteiligten Datenschutzbehörden mitgeteilt und kann ebenfalls veröffentlicht werden.

5.5. Haftung

5.5.1. Allgemeines Recht auf Rechtsbehelfe und gegebenenfalls Entschädigung

In den Vorschriften ist anzugeben, dass die betroffenen Personen die in den Artikeln 22 und 23 der Richtlinie (oder ähnlicher Bestimmungen, mit denen die Richtlinie in das Recht der Mitgliedstaaten umgesetzt wird) aufgeführten Rechtsbehelfe und Haftungen in der gleichen Weise und im gleichen Umfang in Anspruch nehmen können, die ihnen zustünden, wenn die im Unternehmen durchgeführte Verarbeitung unter die Datenschutzrichtlinie oder eine nationale Umsetzung fallen würde.

Der Zweck dieser Vorschriften ist demnach darauf gerichtet sicherzustellen, dass von Datenschutzbehörden erteilte Genehmigungen (die eine Übermittlung personenbezogener Daten ins Ausland ermöglichen oder rechtmäßig machen, die andernfalls unrechtmäßig wäre) nicht darauf hinauslaufen, dass betroffene Personen ihr Recht auf Rechtsbehelfe oder Entschädigungen verlieren, auf die sie Anspruch hätten, wenn die Daten das EU-Gebiet nie verlassen hätten[17].

---

19 Siehe Kapitel 6.

20 Einige multinationale Unternehmen lehnten in der Vergangenheit die Annahme weltweiter Grundsätze zur Privatsphäre ab mit der Begründung, sie könnten zwar der Einführung eines angemessenen

Als Ergänzung dieses allgemeinen Rechts müssen die Vorschriften auch Bestimmungen über Haftung und Gerichtsbarkeit enthalten, die ihre Wahrnehmung in der Praxis erleichtern.

5.5.2. Vorschriften zur Haftung

In erster Linie sollte die Zentrale (wenn sie in der EU ansässig ist) oder der mit dem Datenschutz beauftragte in der EU ansässige Unternehmensteil die Haftung dafür übernehmen und bereit sein, die erforderlichen Änderungen vorzunehmen, um Taten anderer Unternehmensteile außerhalb der Gemeinschaft zu beheben und gegebenenfalls (in dem im vorherigen Kapitel angegeben Umfang) Schadenersatz zu leisten für Schäden, die aus der Verletzung der verbindlichen unternehmensinternen Vorschriften durch einen an die Vorschriften gebundenen Unternehmensteil resultieren.

Das Unternehmen fügt seinem Antrag auf Genehmigung einen Nachweis bei, dass die in der EU ansässige Zentrale oder der mit dem Datenschutz beauftragte in der EU ansässige Unternehmensteil in der Gemeinschaft über ausreichende Mittel verfügt, um unter normalen Umständen Schadenersatz für Verletzungen der verbindlichen unternehmensinternen Vorschriften leisten zu können, oder dass angemessene Maßnahmen getroffen wurden, um sicherzustellen, dass solche Ansprüche erfüllt werden können (zum Beispiel Abschluss einer entsprechenden Haftpflichtversicherung).

Die Zentrale (sofern sie ihren Sitz in der EU hat) oder der mit dem Datenschutz beauftragte in der EU ansässige Unternehmensteil muss auch akzeptieren, dass sie/er in der EU verklagt werden kann und gegebenenfalls Schadenersatz leistet:

a) in den Fällen, in denen Schäden wegen Verletzung der verbindlichen unternehmensinternen Vorschriften geltend gemacht werden, oder

b) wenn Schäden nicht geltend gemacht wurden, aber die betroffene Person nicht zufrieden war mit den Abhilfen durch das unternehmensinterne Beschwerdeverfahren (siehe Kapitel 5.3) oder mit der Behandlung einer Beschwerde durch die zuständige Datenschutzbehörde.

Wenn die europäische Zentrale oder der mit dem Datenschutz beauftragte in der EU ansässige Unternehmensteil nachweisen kann, dass der Unternehmensteil im Drittland nicht für die Handlung verantwortlich ist, die zu dem von der betroffenen Person geltend gemachten Schaden geführt hat, ist er von jeder Haftung befreit.

Die Regeln sollten festhalten, dass es immer der europäischen Zentrale oder dem mit dem Datenschutz beauftragten in der EU ansässigen Unternehmensteil obliegt, nachzuweisen, dass der Unternehmensteil außerhalb der Gemeinschaft nicht für den von

---

Schutzes für die unter europäisches Recht fallenden Personen zustimmen, wollten aber nicht das gleiche Schutzniveau auf andere Länder oder Regionen ausweiten, in denen das Schutzniveau nicht so hoch oder gar kein Datenschutz vorhanden ist. Sie haben sich traditionell skeptisch gezeigt über die Aufnahme von Bestimmungen über Rechtsbehelfe oder Schadenersatz für betroffene Personen. Diese Formulierung geht auf diese Skepsis ein, weil die Durchsetzbarkeit der unternehmensinternen Vorschriften (und damit auch der Schadenersatz), wie in Kapitel 3.1. bereits erläutert, auf Daten begrenzt sein kann, die aus der EU stammen.

der betroffenen Person geltend gemachten Schaden haftbar ist, und nicht etwa der betroffenen Person, nachzuweisen, dass ein Unternehmen in einem Drittland Verarbeitungen entgegen den unternehmensinternen Vorschriften vorgenommen hat (dieser Nachweis wäre meist unmöglich zu erbringen und würde auf jeden Fall unverhältnismäßige Anstrengungen, zeitlichen und finanziellen Aufwand für die betroffene Person bedeuten).

5.6. Vorschrift zur Gerichtsbarkeit

Wie im Kapitel 5.5.2. ausgeführt muss das Unternehmen auch akzeptieren, dass betroffene Personen das Recht haben, Verfahren gegen das Unternehmen einzuleiten und den Gerichtsstand auszuwählen:

a) entweder im Gerichtsstand des Unternehmensteils, von dem die Übermittlung stammt, oder

b) im Gerichtsstand der europäischen Zentrale oder des mit dem Datenschutz beauftragten in der EU ansässigen Unternehmensteils.

Unter der Annahme, dass das System gut funktioniert – dazu gehören ein hohes Maß an Einhaltung innerhalb des Unternehmens, regelmäßige Audits, effiziente Behandlung von Beschwerden, Zusammenarbeit mit Datenschutzbehörden usw. – erscheint die Anrufung von Gerichten unwahrscheinlich, kann aber jedenfalls nicht ausgeschlossen werden. Aber nur die Erfahrung mit diesen Instrumenten wird zeigen, ob diese Vorhersage richtig ist.

Es gelten die in der Richtlinie und in den nationalen Rechtsvorschriften enthaltenen einschlägigen Grundsätze über den Gerichtsstand.

5.7. Transparenz

Zusätzlich zu der Bereitstellung von Informationen nach Artikel 10 und 11 der Richtlinie und den entsprechenden einzelstaatlichen Umsetzungen müssen Unternehmen, die eine ausreichende Garantie bieten, in der Lage sein nachzuweisen, dass es den betroffenen Personen bewusst ist, dass personenbezogene Daten anderen Unternehmensteilen außerhalb der Gemeinschaft mitgeteilt werden, und dass dies auf der Grundlage von Genehmigungen durch Datenschutzbehörden geschieht, die auf rechtlich durchsetzbaren unternehmensinternen Vorschriften beruhen, deren Existenz und Inhalt für den Einzelnen leicht zugänglich sein muss.

Diese umfassende Informationspflicht bedeutet, dass – unbeschadet des Zugangs zu den unternehmensinternen Vorschriften als Ganzes – Unternehmen in der Lage sein müssen nachzuweisen, dass der Einzelne einfachen Zugang zu den wesentlichen Datenschutzvorschriften des Unternehmens hat, sowie zu den aktualisierten Angaben über die Unternehmensteile, die an die Vorschriften gebunden sind, ebenso wie zu den Mitteln, die den betroffenen Personen zur Verfügung stehen, um sich von der Einhaltung der Vorschriften zu überzeugen.

6. VERFAHREN FÜR DIE ZUSAMMENARBEIT ZWISCHEN NATIONALEN BEHÖRDEN BEI NATIONALEN ANTRÄGEN NACH ARTIKEL 26 ABSATZ 2 DER RICHTLINIE

Die Datenschutzgruppe ist sich der Bedeutung der Meldungen über erteilte Genehmigungen an andere Mitgliedstaaten und an die Europäische Kommission nach Artikel 26 Absatz 3 der Richtlinie bewusst. Diese Meldungen können trotzdem durch zusätzliche Kooperationsmaßnahmen zwischen den nationalen Datenschutzbehörden vor Erteilung der entsprechenden Genehmigungen ergänzt werden. Diese Zusammenarbeit ist nämlich nach Artikel 28 der Richtlinie in Fällen vorgesehen, in denen sich eine nationale Entscheidung auf die Verarbeitung desselben Unternehmens in einem anderen Mitgliedstaat auswirken könnte.

Unternehmen, die an einer Genehmigung für ähnliche Arten des Datenexports aus verschiedenen Mitgliedstaaten interessiert sind, können sich eines koordinierten Genehmigungsverfahrens bedienen.[18]

Die dieser Vorgehensweise zugrunde liegende Hauptidee besteht darin, dass Unternehmen durch das koordinierte Verfahren zwischen den beteiligten Datenschutzbehörden nur einen Antrag auf Genehmigung bei einer Datenschutzbehörde eines Mitgliedstaats stellen können, der zur Erteilung von Genehmigungen durch alle Datenschutzbehörden der Mitgliedstaaten, in denen das Unternehmen tätig ist, führt. Die Einzelheiten des Verfahrens werden von Fall zu Fall umgehend von den betroffenen Datenschutzbehörden festgelegt.

Das vorliegende Arbeitsdokument beeinträchtigt nicht die Rechte und Pflichten, die die nationalen Kontrollstellen gegebenenfalls nach einzelstaatlichem Recht in bezug auf die Behandlung von Beschwerden von Einzelpersonen sowie generell auf die Überprüfung der Anwendung der Richtlinie in den Fällen haben, die in ihre Zuständigkeit fallen. Diese Maßnahmen sind aber eine Reaktion auf die Pflicht zur Zusammenarbeit nach Artikel 28 Absatz 6 der Richtlinie in Fällen, in denen es um die rechtlichen Voraussetzungen der Zusammenarbeit auf nationaler Ebene geht.

---

[18] Die Artikel 29-Datenschutzgruppe kann baldmöglichst auf den Erfahrungen mit diesem Verfahren basierende weitere Leitlinien zu dieser Frage vorlegen. Zwischen den Kontrollstellen in den Mitgliedstaaten besteht eine kooperative Arbeitsbeziehung, weshalb nicht für jede Eventualität vorgesorgt werden muss. Der Antragsteller sollte den Eintrittspunkt benennen und erläutern, weshalb er gewählt wurde; außerdem muss er weitere nationale Kontrollstellen angeben, die an dem Verfahren teilnehmen sollten. Die Erteilung der erforderlichen Genehmigungen nach Artikel 26 Absatz 2 der Richtlinie und der diesbezüglichen nationalen Rechtsvorschriften und die Mitteilung an die Europäische Kommission wären die letzten Schritte des koordinierten Verfahrens.

7. SCHLUSSFOLGERUNG

Die Datenschutzgruppe ist der Meinung, dass die hier vorgetragene Leitlinie die Anwendung von Artikel 26 Absatz 2 der Richtlinie vereinfachen kann. Die Ausführungen sollten auch zu einer gewissen Vereinfachung des routinemäßigen Austauschs personenbezogener Daten durch internationale Unternehmen auf weltweiter Basis führen.

Die in der vorliegenden Arbeitsunterlage enthaltenen Leitlinien sollten nicht als das letzte Wort der Artikel 29-Datenschutzgruppe zu diesem Thema angesehen werden, sondern als ein fundierter erster Schritt zur Förderung nationaler Genehmigungen nach Artikel 26 Absatz 2 auf der Grundlage eines Systems der Selbstkontrolle und der Zusammenarbeit zwischen den Behörden, unbeschadet der Möglichkeit, andere Instrumente für die Übermittlung personenbezogener Daten ins Ausland heranzuziehen, beispielsweise die Standardvertragsklauseln oder gegebenenfalls die Grundsätze des sicheren Hafens.

Weitere Beiträge interessierter Kreise und Fachleute auf der Grundlage der Erfahrung mit dem Einsatz dieser Arbeitsunterlage sind willkommen. Die Datenschutzgruppe könnte beschließen, dieses Thema angesichts künftiger Erfahrungen zu überprüfen.

Geschehen zu Brüssel, am 3.Juni 2003
Für die Arbeitsgruppe
Der Vorsitzende
Stefano RODOTA