Schriftenreihe

# Recht & Steuer

Band 2

# Übermittlung personenenbezogener Daten

## Inland, EU-Länder, Drittländer

BITKOM

## Impressum


| | |
|---|---|
| Herausgeber: | BITKOM<br>Bundesverband Informationswirtschaft,<br>Telekommunikation und neue Medien e. V.<br>Albrechtstraße 10 A<br>10117 Berlin-Mitte<br>Tel.: 030.27576-0<br>Fax: 030.27576-400<br>bitkom@bitkom.org<br>www.bitkom.org |
| Ansprechpartner: | Dr. Kai Kuhlmann<br>Tel.: 030.27576-131<br>k.kuhlmann@bitkom.org |
| Redaktion: | Dr. Kai Kuhlmann |
| Redaktionsassistenz: | Karen Schlaberg, Michaela Henrichfreise |
| Gestaltung / Layout: | Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM) |
| Copyright: | BITKOM 2008 |

Band 2

# Übermittlung personenenbezogener Daten

## Inland, EU-Länder, Drittländer

BITKOM

# Inhaltsverzeichnis

# Vorwort

„Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer“ ist die vierte Publikation des BITKOM-Arbeitskreises Datenschutz. Der Arbeitskreis besteht aus Experten der BITKOM-Mitgliedsfirmen und befasst sich mit aktuellen Themen und datenschutzspezifischen Aspekten der Informations- und Kommunikationstechnik.

Besonderer Dank gilt folgenden Mitgliedern des Arbeitskreises Datenschutz, die mit ihrer Expertise und wertvollen praktischen Erfahrung ganz maßgeblich zur Entstehung des Leitfadens beigetragen haben:

- Anne Bernzen, Detecon International GmbH
- Dr. Sibylle Gierschmann, LL.M., Kanzlei Taylor Wessing
- Ulrike Schroth, T-Systems International GmbH
- Regina Wacker-Dengler, Alcatel SEL AG
- Wolfgang Braun, Giesecke & Devrient GmbH
- Helmut Glaser, IBM Deutschland GmbH
- Alexander Heimel, CSC Ploenzke AG
- Stefan Lerbs, Gemplus GmbH
- Ralf Maruhn, Nokia GmbH
- Mirko Schmidt, Motorola GmbH
- Florian Thoma, Siemens AG

Die Grafiken wurden erstellt von Herrn Braun (S. 26, 33 ff), Herrn Maruhn (S. 34) und Herrn Thoma (S. 31). Die Grafik auf Seite 28 und die Übersicht auf den Seiten 29 f wurde freundlicherweise vom Autorenteam des Arbeitskreises Datenschutz und Datensicherheit der GSE Europe zur Verfügung gestellt.

Die Version 1.0 der Publikation befindet sich auf dem inhaltlichen Stand von Dezember 2005. Bitte beachten Sie, dass die dargestellte Materie der fortlaufenden Entwicklung des Rechts und der Technik unterworfen ist.

Berlin, den 18. April 2006

## Als weitere Publikationen des BITKOM Arbeitskreises Datenschutz sind erhältlich:

- Leitfaden zur Nutzung von Email und Internet im Unternehmen (Version 1.3)
- Mustervertragsanlage zur Auftragsdatenverarbeitung
- Verfahrensverzeichnis und Verarbeitungsübersicht nach dem Bundesdatenschutzgesetz (Version 1.0)

# I Einführung: Die Übermittlung personenbezogener Daten

Die Übermittlung personenbezogener Daten begleitet täglich die Anbahnung und Abwicklung der Geschäfte zahlreicher Unternehmen. Ebenso wie die Geschäfte macht auch die Datenübermittlung dabei schon lange nicht mehr an den Landesgrenzen Deutschlands halt, sondern erfolgt häufig grenzübergreifend zwischen europäischen Staaten oder international. Durch die ständig zunehmende Mobilität und die Globalisierung des Welthandels gewinnt dieser grenzübergreifende Datenaustausch stetig an Bedeutung. Gefördert wird dieser Trend durch die rasante informationstechnische Entwicklung: Die weltweiten Kommunikationsmöglichkeiten über miteinander verknüpfte Netze, über die mit geringem Kostenaufwand zeitnah nahezu unbegrenzt große Datenmengen ausgetauscht werden können, hat die Datenverarbeitung endgültig von ihrer räumlichen Begrenztheit befreit. Dies betrifft nicht nur den Austausch von Daten zwischen Vertragspartnern, sondern auch den Austausch und die Weitergabe im Unternehmensverbund. In internationalen Konzernen werden z. B. häufig Personaldaten zwischen den Konzerntöchtern und der Konzernholding bzw. zwischen den Tochtergesellschaften ausgetauscht. So geben u. U. deutsche Tochterunternehmen Kunden- oder Mitarbeiterdaten an die Muttergesellschaft in den USA weiter. Durch die Vernetzung der Produktions- und Handelsbeziehungen bleiben personenbezogene Daten nicht nur im Unternehmen bzw. Konzern, sondern werden auch an ausländische Geschäftspartner oder internationale Datenbanken übermittelt. So ist es bspw. erforderlich, im Rahmen von Reisebuchungen Mitarbeiterdaten an eine Vielzahl Dritter weiterzugeben. Nicht zuletzt auch im Rahmen von Outsourcing-Projekten werden Daten häufig an weltweit tätige EDV-Dienstleistungsanbieter übermittelt.

Eine grafische Übersicht über den weltweiten Stand des Datenschutzes finden Sie unter IV 7).

Nicht immer aber sind alle Beteiligten mit den rechtlichen Anforderungen einer Datenübermittlung hinreichend vertraut. Die Anforderungen sollten jedoch von jedem Unternehmen ernst genommen werden. Eine Datenübermittlung, die nicht den gesetzlichen Voraussetzungen genügt, kann als Ordnungswidrigkeit oder sogar Straftatbestand mit Bußgeldern (bis zu 250.000 Euro) bzw. Freiheitsstrafe geahndet werden (§§ 43, 44 BDSG).

Vor diesem Hintergrund will die BITKOM-Publikation „Übermittlung personenbezogener Daten“ eine praktische Hilfestellung für den täglichen Gebrauch beim Transfer von Daten bieten. Neben einer kurzen Darstellung des Rechtsrahmens für die Datenübermittlung (II) wird vor allem die Datenübermittlung im Inland, in EU-Länder und in Drittländer erläutert (III). Die verschiedenen Konstellationen werden jeweils mit einem kurzen Fallbeispiel illustriert. Angesprochen wird auch die Datenübermittlung im Konzern (III 5). Abgerundet wird der Leitfaden schließlich durch ergänzende Materialien (IV), Links und Literaturhinweise (V).

**Bitte beachten Sie:**

Der Leitfaden kann angesichts der komplexen Materie keinen Anspruch auf Vollständigkeit erheben. Zudem ist die dargestellte Materie der fortlaufenden Entwicklung des Rechts und der Technik unterworfen. Letztlich versteht sich dieser Leitfaden daher als Einführung in die Problematik und Aufbereitung möglicher Handlungsmöglichkeiten, der jedoch die Einbindung professioneller unternehmensinterner oder externer Berater nicht überflüssig macht.

# II Rechtsrahmen

## II 1 Rechtliche Grundlagen

### II 1 a) Anwendungsbereich des Bundesdatenschutzgesetzes

Die zentrale Rechtsgrundlage für die Übermittlung von Daten ist das Bundesdatenschutzgesetz (BDSG). Anlässlich der Umsetzung der EU-Datenschutzrichtlinie vom 24.10.1995 „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ (95/46/EG) http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_de.htm wurde eine umfassende Novellierung des BDSG durchgeführt. Teil der Neuerungen sind die §§ 4 b und 4 c, die eigenständige Regelungen für Datenübermittlungen ins Ausland beinhalten. Die Neufassung des BDSG ist am 23.05.2001 in Kraft getreten. Der Text des BDSG ist (auch in englischer und französischer Sprache) beispielsweise abrufbar unter: http://www.bfdi.bund.de/cln_027/nn_531520/DE/GesetzeUndRechtsprechung/BDSG/BDSG__node.html__nnn=truel

Das Bundesdatenschutzgesetz gilt gemäß § 1 Abs. 2 BDSG für alle öffentlichen Stellen des Bundes (Bundesverwaltung) und für die Privatwirtschaft (nicht-öffentliche Stellen), soweit sie personenbezogene Daten erheben, verarbeiten oder nutzen.

Nicht-öffentliche Stellen können sein (§ 2 Abs. 4 BDSG):

- juristische Person des Privatrechts (z. B. GmbH, AG, Parteien, Vereinigungen)
- Personalgesellschaften und andere Personenvereinigungen (Gesellschaften des bürgerlichen Rechts)
  - Personengesellschaften des Handelsrechts (z.B. OHG, KG)
  - nicht-rechtsfähige Vereine
  - natürliche Personen (gewerblich oder freiberuflich Tätige)

Die Anwendbarkeit setzt weiterhin voraus, dass die nicht-öffentliche Stelle personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, nutzt oder erhebt oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, nutzt oder dafür erhebt, ausgenommen für rein private oder familiäre Tätigkeiten (§ 1 Abs. 1 Nr. 3 BDSG).

Für die Datenverarbeitung in der Privatwirtschaft sind insbesondere die Abschnitte 1 und 3 des BDSG maßgeblich (vgl. §§ 1 Abs. 2; 27 Abs. 1 BDSG).

### II 1 b) Spezielle Datenschutzgesetze

Das BDSG ist gemäß § 1 Abs. 3 BDSG ein Auffanggesetz. Die bereits in verschiedenen anderen Gesetzen vorhandenen spezielleren Rechtsvorschriften behalten daher ihre Gültigkeit und gehen dem BDSG vor. Dies gilt jedoch nur insoweit, als die entsprechenden Spezialgesetze eine Regelung enthalten. Fehlen solche speziellen Rechtsvorschriften dann findet für die nicht geregelten Bereiche wieder das BDSG Anwendung (Subsidiaritätsprinzip). So ist beispielsweise bei Tele-/Mediendiensten hinsichtlich der spezifischen, sich auf den jeweiligen elektronischen Kommunikationsvorgang beziehenden Daten des Nutzers das Teledienstedatenschutzgesetz (TDDSG) bzw. der Mediendienstestaatsvertrag (MDStV) anzuwenden. Da das TDDSG jedoch keine besonderen Regelungen enthält zur Erhebung, Verarbeitung und Nutzung von Inhaltsdaten, die keine Nutzungsdaten sind, bleibt für diese Bereiche das BDSG anwendbar. Relevanz können auch die Vorschriften des TKG haben, z. B. § 92, der die Datenübermittlung an ausländische nicht-öffentliche Stellen regelt. An ausländische nicht-öffentliche Stellen dürfen Diensteanbieter personenbezogene Daten nach Maßgabe des Bundesdatenschutzgesetzes nur übermitteln, soweit es für die Erbringung von Telekommunikationsdiensten, für die Erstellung oder Versendung von Rechnungen oder für die Missbrauchsbekämpfung erforderlich ist.

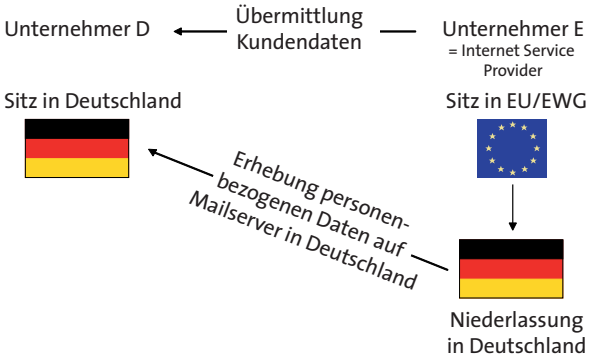
## II 1 c) Anwendbarkeit des BDSG bei grenzüberschreitenden Sachverhalten

Das BDSG geht vom „Sitzlandprinzip“ aus, wonach sich das anzuwendende nationale Recht nicht nach dem Ort der Verarbeitung, sondern nach dem Sitz der verantwortlichen Stelle richtet.

Das BDSG findet aber auch auf Unternehmen, die ihren Sitz außerhalb Deutschlands haben, Anwendung, wenn:

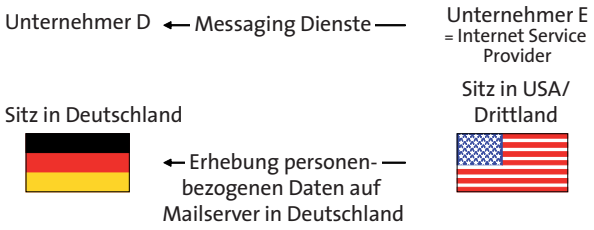
- ein Unternehmen mit Sitz in der EU oder im EWR in Deutschland eine Niederlassung hat, die die personenbezogenen Daten in Deutschland erhebt, verarbeitet oder nutzt (§ 1 Abs. 5 S. 1 BDSG),

Beispiel: Unternehmer E mit Sitz in der EU/EWG (z. B. Spanien) bietet Messaging- Dienste auf einem Mailserver, der sich in Deutschland befindet, an. Unternehmer D mit Sitz in Deutschland nimmt diese Dienste in Anspruch, indem die deutsche Niederlassung des Unternehmens E personenbezogene Daten (z. B. Kundendaten des Unternehmens D) mittels des Mailservers in Deutschland erhebt.




- ein Unternehmen seinen Sitz in einem Drittland hat, aber in Deutschland Daten erhebt, verarbeitet oder nutzt, es sei denn, die Daten werden nur durchgeleitet (§ 1 Abs. 5 S. 2 BDSG),

Beispiel: Unternehmer A mit Sitz in den USA/Drittland bietet Messaging-Dienste auf einem Mailserver, der sich in Deutschland befindet, an. Unternehmer D mit Sitz in Deutschland nimmt diese Dienste in Anspruch, indem das Unternehmen A personenbezogene Daten (z. B. Kundendaten des Unternehmens D) mittels des Mailservers in Deutschland erhebt.




- ein Unternehmen mit Sitz in der EU oder im EWR für eine in Deutschland niedergelassene Stelle als Auftragnehmer Datenverarbeitung durchführt (§ 3 Abs. 8 S. 3 BDSG, Auftragsdatenverarbeitung, § 11 BDSG). § 3 Abs. 8 BDSG ist insoweit eine Ausnahmevorschrift, als Auftragnehmer in der EU und EWR denen in Deutschland gleichgestellt werden. Sie sind somit nicht als Dritte anzusehen und eine Übermittlung liegt nicht vor.

Beispiel: Unternehmer A mit Sitz in Deutschland lässt die Abrechnung von Personaldaten durch ein in Norwegen ansässiges Unternehmen durchführen.

Keine Anwendung findet das BDSG, wenn eine verantwortliche Stelle mit Sitz außerhalb Deutschlands, aber innerhalb der EU/EWR, personenbezogene Daten erhebt, verarbeitet oder nutzt (§ 1 Abs. 5 S. 1 BDSG). In diesem Fall findet das am Sitz der verantwortlichen Stelle geltende Datenschutzrecht Anwendung. Ein vergleichbares Schutzniveau ist durch die jeweilige Umsetzung der EU-Richtlinie 95/46/EG sichergestellt.

## II 2) Gegenstand und Systematik des Datenschutzrechts

Als Konsequenz des Grundrechts auf „informationelle Selbstbestimmung“ gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten als allgemeiner Grundsatz ein sogenanntes Verbot mit Erlaubnisvorbehalt. Folglich liegt ein gesetzliches Regel-Ausnahme-Verhältnis in der Weise vor, dass die Verarbeitung fremder personenbezogener Daten regelmäßig unzulässig ist, soweit sie nicht ausnahmsweise erlaubt ist.

§ 4 Abs. 1 BDSG greift das Verbot mit Erlaubnisvorbehalt auf und erklärt eine Datenerhebung, -verarbeitung und -nutzung nur für zulässig, wenn sie durch das BDSG oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet ist oder der Betroffene dazu seine Einwilligung erklärt.

### II 2 a) Erlaubnistatbestände

Rechtsvorschriften, die den Umgang mit personenbezogenen Daten erlauben, finden sich im BDSG in den §§ 15 Abs. 1, 16 Abs. 1, 28-30, wobei – wie im weiteren Verlauf dargestellt – § 28 BDSG von zentraler praktischer Bedeutung für den nicht-öffentlichen Bereich ist.

Weitere Rechtsvorschriften, die eine Datenerhebung, -verarbeitung und -nutzung für zulässig erklären bzw. anordnen, können sich beispielsweise in bundesgesetzlichen Regelungen (Passrecht, Steuerrecht, Handelsgesetzbuch, ...), im Landesrecht und kommunalem Recht oder sonstigen bereichsspezifischen Regelungen finden, aber auch in den normativen Teilen von Tarifverträgen, Betriebsvereinbarungen, Dienstvereinbarungen etc. Auch EU-Verordnungen (z. B. Anti-TerrorVO, Verordnung EG Nr. 881/2002) können als Rechtsvorschrift, die den Umgang mit personenbezogenen Daten erlaubt, in Betracht kommen, da sie für Deutschland (und jeden anderen EU-Mitgliedstaat) unmittelbare Geltung haben. Ausländische Rechtsvorschriften bleiben regelmäßig jedoch außer Betracht.

### II 2 b) Einwilligung gem. § 4 a BDSG

Soll eine Einwilligung Grundlage für eine Erhebung, Verarbeitung oder Nutzung sein, ist zu beachten, dass

- die Einwilligung gemäß § 4 a Abs. 1 S. 3 BDSG der Schriftform bedarf, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist,
- der Betroffene zuvor über den konkreten Verwendungszweck zu informieren und auf vorgesehene Datenübermittlungen hinzuweisen ist (gem. § 4 a Abs. 1 S. 2 BDSG),
- die Einwilligung auf der freien Entscheidung des Betroffenen beruhen muss, d.h. sie muss frei von Zwang sein (§ 4a Abs. 1 S. 1 BDSG).

Wenn eine Rechtsvorschrift den Umgang mit personenbezogenen Daten ausdrücklich erlaubt oder sogar anordnet, kommt es auf die Einwilligung des Betroffenen nicht an.

(Zur Einwilligung vgl. auch noch unten III 3 c und III 5 c aa)

# III Datenübermittlung

Der Begriff der Datenübermittlung ist in § 3 Abs. 4 Nr. 3 BDSG definiert. Es handelt sich um die Phase der Datenverarbeitung, in der die geschützten personenbezogenen Daten von der verantwortlichen Stelle an andere Personen oder Stellen (Dritte) bekannt gegeben werden. Die Bekanntgabe kann durch aktive Weitergabe, gleich in welcher Form, oder durch Einsicht des Dritten oder Abruf der Daten durch einen Dritten erfolgen. Auch der Abgleich von geschützten Daten stellt eine Bekanntgabe dar. Die Weitergabe innerhalb der verantwortlichen Stelle wird hingegen nicht von dem Begriff der Übermittlung erfasst.

Eine Übermittlung liegt nicht vor, wenn die personenbezogenen Daten im Auftrag der verantwortlichen Stelle durch einen Auftragnehmer erhoben, verarbeitet oder genutzt werden (sog. Auftragsdatenverarbeitung) und dies in der EU oder dem EWR erfolgt, weil das Gesetz in diesem Falle den Auftragnehmer nicht als Dritten, sondern als Teil der verantwortlichen Stelle behandelt, § 3 Abs. 8 BDSG. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten richtet sich bei Vorliegen einer Auftragsdatenverarbeitung nach den Vorschriften des § 11 BDSG. Danach bleibt der Auftraggeber für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Weiterhin ist insbesondere sicherzustellen, dass die Beauftragung des Dienstleisters schriftlich erfolgt, wobei u. a. die Erhebung, Verarbeitung und Nutzung sowie technische und organisatorische Maßnahmen zum Schutz der Daten festzulegen sind.

Zu beachten ist jedoch, dass es sich bei der Ausgestaltung nicht um die Übertragung einer ganzen Funktion zur eigenverantwortlichen Wahrnehmung durch den Auftragnehmer handeln darf. In diesem Fall wäre wiederum eine Übermittlung gegeben[1].

### Abgrenzungskriterien zwischen Auftragsdatenverarbeitung und Funktionsübertragung:

Auftragsdatenverarbeitung liegt in der Regel bei folgenden Kriterien vor:

- Fehlende Entscheidungsbefugnis des Auftragnehmers über die Daten,
- Ausrichtung des Auftrags auf die Durchführung der Verarbeitung,
- Fehlen einer eigenständigen rechtlichen Beziehung des Auftragnehmers zum Betroffenen.

Funktionsübertragung ist entsprechend bei folgenden Kriterien anzunehmen:

- Recht der empfangenen Stelle auf Nutzung der personenbezogenen Daten zu eigenen Zwecken,
- Fehlender Einfluss des Auftraggebers auf Teile der Datenerhebung, -verarbeitung und -nutzung,
- Übernahme der Verantwortung für die Zulässigkeit der Datenverarbeitung durch den Auftragnehmer.

Schließlich wird auch die unbefugte Weitergabe durch einen Mitarbeiter oder die Weitergabe ohne Weisung des Auftraggebers bei Bestehen eines Auftragsdatenverarbeitungsverhältnisses nicht von dem Begriff der Übermittlung erfasst.

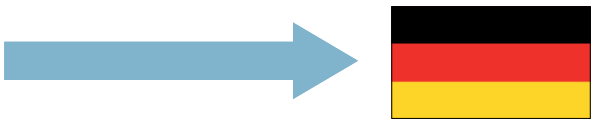
Liegt keine Übermittlung vor, müssen die im Folgenden dargestellten Rechtmäßigkeitsvoraussetzungen nicht beachtet werden. Es können jedoch die Vorschriften des § 11 zur Auftragsdatenverarbeitung relevant sein.

BITKOM hat zur Auftragsdatenverarbeitung eine Mustervertragsanlage formuliert, die unter dem folgenden Link abgerufen werden kann:
www.bitkom.org/de/publikationen/1357_25976.aspx

Eine Entscheidungshilfe zur Datenübermittlung im Inland, in der EU oder in Drittländer finden Sie unter IV 4)!

1 vgl. zur Abgrenzung auch Simitis u.a.: Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. Baden-Baden 2003, § 2 RdNr. 151f.; Gola/Wronka: Handbuch zum Arbeitnehmerdatenschutz, 3. Aufl. Frechen 2004 RdNr. 501ff., 607; Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer" des „Düsseldorfer Kreises", veröffentlicht durch das Regierungspräsidium Darmstadt unter http://www.rpda.de/dezernate/datenschutz/download/Arbeitsbericht-Endfassung.pdf, 2005, Kap. 2.

## III 1) Datenübermittlung innerhalb Deutschlands



### III 1 a) Gesetzliche Erlaubnis

Wie oben bereits ausgeführt, ist § 28 BDSG die zentrale Erlaubnisnorm für die Datenübermittlung in der täglichen Unternehmenspraxis innerhalb Deutschlands. Gemäß der Vorgaben der Alternativen des § 28 BDSG ist eine Datenverarbeitung und -nutzung im nicht-öffentlichen Bereich zulässig

- bei einem Vertragsverhältnis (oder vertragsähnlichen Vertrauensverhältnis) mit dem Betroffenen, wenn es dem Zweck des Verhältnisses dient (§ 28 Abs. 1 Nr. 1 BDSG),

- wenn die Datenerhebung zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung das Interesse der verantwortlichen Stelle an der Datenerhebung überwiegen (§ 28 Abs. 1 Nr. 2 BDSG),

- wenn Daten allgemein zugänglich sind oder veröffentlicht werden dürften, es sei denn, schutzwürdige Interessen des Betroffenen würden gegenüber den berechtigten Interessen der verantwortlichen Stelle offensichtlich überwiegen (§ 28 Abs. 1 Nr. 3 BDSG),

  sowie u. a. auch

- bei der Übermittlung von Stammdaten zu Marketingzwecken (Werbung, Markt- und Meinungsforschung bei listenmäßig oder sonst zusammengefassten Daten über Angehörige einer Personengruppe, § 28 Abs. 3 Nr. 3 BDSG).

Besteht ein Vertragsverhältnis zwischen der verantwortlichen Stelle und dem Betroffenen, so ist, um die Schutzwirkung nicht zu unterlaufen, vorrangig § 28 Abs.1 Nr. 1 BDSG anzuwenden. Für die Berufung auf „berechtigte Interessen“ der verarbeitenden Stelle nach § 28 Abs. 1 Nr. 2 BDSG bleibt deshalb bei Bestand einer vertraglichen Beziehung, wie z. B. einem Arbeitsverhältnis, einem Bankvertrag oder einem auf einem besonderen Vertrauensverhältnis basierenden Vertragsverhältnis, nur ein eingeschränkter Anwendungsbereich (zu § 28 BDSG vgl. auch unten III 5 c bb).

Eine ausführliche grafische Darstellung der Erlaubnistatbestände des § 28 BDSG finden Sie unter IV 7)!

### III 1 b) Einwilligung des Betroffenen

Eine Datenübermittlung ist auch möglich, wenn der Betroffene eingewilligt hat. Zusätzlich zum Vorliegen der gesetzlichen Voraussetzungen einer Einwilligung (vgl. oben II 2 b) sind dabei jedoch mehrere Punkte zu beachten, die sich in der Praxis als problematisch erweisen können:

- Der Kreis der Betroffenen sollte überschaubar sein (Unternehmensgröße).

- Die verantwortliche Stelle muss die Betroffenen über jeden beabsichtigten Verarbeitungszweck konkret informieren, u. U. ist daher (bei geändertem oder erweitertem Verarbeitungszweck) auch eine Aktualisierung erforderlich.

- Es muss die Möglichkeit in Betracht gezogen werden, dass einzelne Betroffene die Einwilligung nicht erteilen oder später widerrufen, was die gesamte Maßnahme in Frage stellen kann.

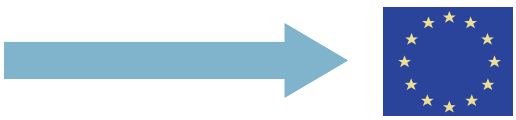
- Bei Arbeitnehmerdaten: Nach wie vor umstritten ist die Frage, ob im Arbeitsverhältnis überhaupt wirksam eingewilligt werden kann, da der theoretischen Entscheidungsfreiheit des Arbeitnehmers

ein faktisches Abhängigkeitsverhältnis gegenüber stehen kann. Hier ist gem. § 94 BetrVG u. U. auch die Zustimmung des Betriebsrates für Einwilligungserklärungen in Personalfragebögen oder Formulararbeitsverträgen einzuholen. Tatsächlich dürfte die Datenerhebung bei Arbeits- und Dienstverhältnissen im Regelfall mit Bezug zur konkreten Tätigkeit häufig im Rahmen des § 28 Abs. 1 Nr. 1 BDSG erfolgen.

In der Praxis ist die Einwilligung daher häufig nur eine bedingt geeignete Lösung.

## III 2) Datenübermittlung in ein Land der EU/EWR

Durch die Umsetzung der EU-Datenschutzrichtlinie 95/46/EG in allen Mitgliedstaaten der EU wurde ein weitgehend einheitliches und adäquates Schutzniveau

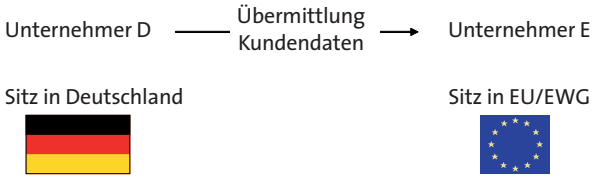


für personenbezogene Daten eingeführt („Angemessenes Datenschutzniveau"). Auch für die EWR-Staaten Norwegen, Island, Liechtenstein ist die Angemessenheit des Datenschutzniveaus anerkannt. Diese Länder sind bezüglich der Datenübermittlung daher mit Ländern innerhalb der EU gleichzusetzen.

Das hat zur Folge, dass der Datenverkehr innerhalb der Mitgliedstaaten der Europäischen Union und mit den EWR-Staaten im Anwendungsbereich des Gemeinschaftsrechts genauso zu behandeln ist wie die inländische Datenübermittlung (vgl. § 4 b Abs. 1 BDSG) und in diesem Rahmen zulässig ist.

Für den Fall, dass ein deutsches Unternehmen Daten in ein anderes EU/EWR-Land übermitteln will, kann daher in vollem Umfang auf die Ausführungen oben III 1) verwiesen werden.

Beispiel: Unternehmer D mit Sitz in Deutschland übermittelt Kundendaten an das Unternehmen E mit Sitz in der EU/EWG (z. B. Spanien).




## III 3) Datenübermittlung in ein Drittland

**Eine tabellarische Darstellung der Möglichkeiten der Übermittlung in Drittländer finden Sie unter IV 5)!**

Das BDSG geht davon aus, dass die Übermittlung von Daten an ausländische Stellen außerhalb der EU/EWR unterbleiben muss, wenn der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Ein solches entgegenstehendes schutzwürdiges Interesse ist insbesondere dann anzunehmen, wenn bei der empfangenden Stelle die Angemessenheit des Datenschutzniveaus nicht gegeben ist, § 4 b Abs. 2 S. 2 BDSG.

- Hieraus ergibt sich zunächst, dass eine Datenübermittlung in ein Drittland rechtmäßig möglich ist, wenn die Angemessenheit des Niveaus der Datenschutzgesetzgebung dieses Landes anerkannt ist (dazu sogleich unten III 3 a) und keine anderen schutzwürdigen Interessen des Betroffenen entgegenstehen.

- Ist das Datenschutzniveau eines Landes nicht durch einheitliche Gesetze gesichert, kann eine Angemessenheit im Sinne des § 4 b Abs. 2 BDSG gleichwohl dann angenommen werden, wenn eine Vereinbarung des Landes mit der EU getroffen wurde, die ein angemessenes Datenschutzniveau sicherstellt und der Übermittlungsempfänger dieser Vereinbarung beigetreten ist (Beispiel: „Safe Harbor Principles" der USA, dazu unten III d bb).

Auch wo keine derartige Angemessenheit gegeben ist, kann eine Datenübermittlung jedoch möglich sein, denn der Grundsatz des § 4 b Abs. 2 S. 2 BDSG wird durch mehrere Ausnahmen durchbrochen, die die rechtmäßige Datenübermittlung in ein Drittland ermöglichen:

- § 4 c Abs. 1 Nr. 1 und Nr. 2 BDSG ermöglichen als Ausnahmevorschriften Übermittlungen an Stellen ohne angemessenes Datenschutzniveau, wenn der Betroffene eingewilligt hat oder die Übermittlung zur Erfüllung eines Vertrags mit dem Betroffenen notwendig ist (siehe dazu unten III 3 b und 3 c)

- Eine Datenübermittlung nach § 4 c Abs. 2 BDSG schließlich setzt voraus, dass das fehlende angemessene Datenschutzniveau durch ausreichende Garantien ausgeglichen wird. Die Garantien können sich insb. aus Vertragsklauseln (dazu unten III d aa) und verbindlichen Unternehmensregelungen ergeben (dazu und zum Streit um die Einordnung von Unternehmensregelungen unten III d cc).

Diese Übermittlungsmöglichen und ihre Voraussetzungen werden in den folgenden Abschnitten erläutert.

Eine grafische Darstellung der §§ 4b und 4c BDSG finden Sie unter IV 6)!

**Bitte beachten Sie**

Die Voraussetzungen für eine rechtmäßige Übermittlung im Inland (z. B. nach § 28 BDSG) sind auch bei einer Datenübermittlung in ein Drittland relevant, denn bei jeder Datenübermittlung ins Ausland muss neben der Frage nach den speziellen Voraussetzungen für die Übermittlung in ein bestimmtes Land (§§ 4 b und 4 c BDSG) zusätzlich geprüft werden, ob darüber hinaus auch die allgemeinen Voraussetzungen für eine Übermittlung vorliegen (§ 4 Abs. 1, 28 BDSG, zu § 28 BDSG vgl. oben III 1 a). Erforderlich ist also eine ZWEISTUFIGE PRÜFUNG.

## III 3 a) Datenübermittlung in ein Drittland mit angemessenem Datenschutzniveau, § 4 b Abs. 2 BDSG

Hat ein Drittland ein angemessenes Datenschutzniveau, ist eine Datenübermittlung rechtmäßig möglich, wenn nicht sonstige schutzwürdige Interessen des Betroffenen dem entgegenstehen. Die Feststellung der Angemessenheit erfolgt in einem förmlichen Verfahren durch die EU-Kommission (Art. 25 Abs. 6 EU-Datenschutzrichtlinie).

Ein angemessenes Datenschutzniveau wurde von der EU-Kommission in einer förmlichen Entscheidung für folgende Länder festgestellt:

- Argentinien
- Guernsey
- Isle of Man
- Kanada
- Schweiz

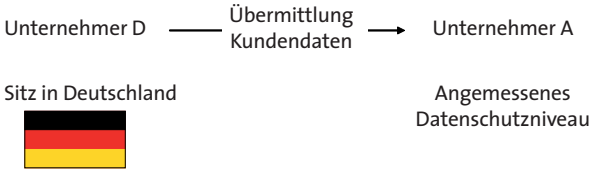
Die Angemessenheit des Datenschutzniveaus bedeutet dabei nicht zwingend, dass die Verhältnisse gleichartig oder gleichwertig sind.

Zurzeit wird von der Kommission dem Vernehmen nachgeprüft, ob die Länder Japan, Neuseeland und Australien ein angemessenes Datenschutzniveau aufweisen, die Entscheidungen stehen jedoch noch aus.

Weitere Informationen zu den Entscheidungen der Kommission können auf der EU-Datenschutz-Homepage unter dem folgenden Link abgerufen werden:

http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_de.htm

Beispiel: Unternehmer D mit Sitz in Deutschland übermittelt z. B. Kundendaten an das Unternehmen A mit einem angemessenen Datenschutzniveau (z. B. Schweiz, Guernsey, Argentinien, Kanada...)




## III 3 b) Ausnahme 1: Zur Vertragserfüllung notwendige Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau

Eine Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau ist ausnahmsweise zulässig, wenn zwischen dem Betroffenen und der verantwortlichen Stelle ein Vertrag abgeschlossen worden ist, für dessen Erfüllung die Datenübermittlung erforderlich ist, § 4 c Abs. 1 Nr. 2 BDSG. In gleicher Weise ist eine Datenübermittlung zulässig, die zur Durchführung von vorvertraglichen Maßnahmen erforderlich ist.

Der praktische Anwendungsbereich dieser Zulässigkeitsalternative liegt neben dem internationalen Zahlungsverkehr und Kaufverträgen im Fernabsatz vor allem im Tourismusgewerbe. Die Durchführung von vertraglichen Vereinbarungen über internationale Beförderungsleistungen, Reservierungen von Mietwagen, Unterkünften oder Hotelzimmern in Drittländern wird so ermöglicht.

Beispiel: Kunde K möchte, dass sein Reisebüro für ihn in Sydney ein Hotelzimmer reserviert. Das Reisebüro kann sich für die Übermittlung der Daten des K an das Hotel in Sydney auf § 4 c Abs. 1 Nr. 1 BDSG berufen, da zur Durchführung bzw. Erfüllung des Vertrages zwischen Kunde K und dem Reisebüro die Weitergabe seiner Daten zwingend notwendig ist.

Ein Vertrag i.S.d. Nr. 2 kann auch ein Arbeitsvertrag sein, so dass die Übermittlung von Arbeitnehmerdaten in ein Drittland auf Grund eines Arbeitsvertrages zulässig sein kann. Entscheidend für die Beurteilung der Zulässigkeit ist, ob die Übermittlung für die Durchführung bzw. Erfüllung der jeweiligen einzelnen Regelung des Arbeitsvertrags erforderlich ist. Dies ist für jeden Arbeitnehmer gesondert zu prüfen. Denkbar ist die Zulässigkeit der Datenübermittlung z. B., wo der Mitarbeiter zu Auslandseinsätzen verpflichtet ist oder bei der Gewährung von Aktienbezugsrechten, die in einem Drittland verwaltet werden.

Etwas anders liegt die Konstellation, für die § 4 c Abs. 1 Nr. 3 BDSG die Zulässigkeit einer Datenübermittlung begründen kann. Nach der Nr. 3 kann eine Übermittlungen zulässig sein, die zur Erfüllung eines Vertrags notwendig ist, der zwar nicht vom Betroffen selbst mit der verantwortlichen Stelle geschlossen wurde, aber im Interesse des Betroffenen zwischen der verantwortlichen Stelle und einem Dritten.

Beispiel: Der Arbeitgeber überträgt Daten eines Arbeitnehmers, für den er eine Mitarbeiterversicherung abgeschlossen hat, an eine ausländische Versicherungsgesellschaft. Häufig wird es sich bei der Anwendung der Nr. 3 um Verträge zugunsten Dritter i.S.d. § 328 BGB handeln.

Zu beachten ist bei allen Zulässigkeitsalternativen des § 4 c Abs. 1, dass der Datenempfänger darauf hinzuweisen ist, dass die Daten nur zweckgebunden verarbeitet oder genutzt werden dürfen (vgl. § 4 c Abs. 1 S. 2 BDSG), wobei sich der Zweck z. B. aus dem Vertrag ergibt.

## III 3 c) Ausnahme 2: Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau auf der Grundlage einer Einwilligung

Wie bei der Datenübermittlung innerhalb Deutschlands oder innerhalb der EU/EWR kann auch eine Datenübermittlung in ein Drittland auf der Grundlage einer Einwilligung des Betroffenen zulässig sein, § 4 c Abs. 1 Nr. 1 BDSG.

Für die Einwilligung in die Drittlandübermittlung von Daten gelten die schon oben II 2 b) dargestellten, strengen Anforderungen ebenso wie die oben III 1 b) erläuterten praktischen Schwierigkeiten (dazu auch unten III 5 c 1).

Beim Datentransfer in ein Drittland kann jedoch noch eine weitere Schwierigkeit hinzutreten, denn nach überwiegender Ansicht ist der Betroffene (zusätzlich zu den oben aufgeführten Umständen der Datenübermittlung) umfassend über die Risiken der Übermittlung seiner Daten in ein Land ohne ausreichendes Datenschutzniveau zu informieren (vgl. § 4 a BDSG). Erforderlich ist also die Transparenz bezüglich der Schutzmaßnahmen bzw. Datenschutzgarantien bei der empfangenden Stelle oder im Empfängerland.

Die in III 3 b) erwähnte Zweckbindung mit Hinweispflicht gilt auch hier.

## III 3 d) Ausnahme 3: Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau auf Grundlage ausreichender Garantien

Ist für das Zielland kein angemessenes Datenschutzniveau festgestellt und greifen auch die bislang aufgeführten Ausnahmetatbestände nicht, besteht die Möglichkeit, dass das für den Datentransfer verantwortliche Unternehmen eigene Maßnahmen trifft, um „ausreichende Garantien“ für den Datenschutz zu schaffen und so ein fehlendes allgemeines Datenschutzniveau ausgleicht. Das BDSG gibt dafür ausdrücklich zwei Möglichkeiten vor, nämlich vertragliche Vereinbarungen zwischen den Vertragsparteien des Datenaustausches oder verbindliche Unternehmensregelungen. Neben diesen beiden Möglichkeiten ist als Fall des § 4 c Abs. 2 BDSG auch das sog. „Safe Harbor“ Abkommen für Datentransfer in die USA in der Praxis relevant.

### III 3 d aa) Vertragliche Vereinbarungen, insb. aufgrund der EU-Standardvertragsklauseln

Eine Übermittlung von personenbezogenen Daten in „unsichere Drittländer“ ist grundsätzlich auch aufgrund von vertraglichen Vereinbarungen zwischen den beteiligten Unternehmen möglich. Die Kommission hat hierzu sog. Standardvertragsklauseln verabschiedet, die von Unternehmen verwendet werden können, um vertraglich ein „angemessenes Datenschutzniveau“ herzustellen.

Im Einzelnen:

- Erste Möglichkeit: Individueller Datenschutzvertrag

  Zwischen dem Datenübermittler und dem Datenempfänger kann ein individueller, d. h. selbst formulierter Vertrag zum Datenschutz geschlossen werden.

  Voraussetzung für die Zulässigkeit der Datenübermittlung aufgrund der eigenen vertraglichen Datenschutzvereinbarungen ist die Genehmigung dieser durch die Aufsichtbehörde, § 4 c Abs. 2 BDSG (vgl. auch Art. 26 Abs. 2 EU-DatSchRL). Prüfungsmaßstab ist, ob sich die Parteien mit ihren Vertragsklauseln auf die Einhaltung der Grundregeln des EU-Datenschutzrechts und des BDSG verpflichten und dadurch ausreichende Garantien vorliegen. Das Genehmigungsverfahren kann in der Praxis langwierig sein.

  Genehmigung der Aufsichtsbehörde ist für die Datenübermittlung erforderlich!

- Zweite Möglichkeit: Die Standardvertragsklauseln der Europäischen Kommission

  Die EU-Kommission ist gemäß Art. 26 Abs. 4 i. V. m. Art. 31 Abs. 2 EU-DatSchRL ermächtigt, Klauseln zum Datenschutz bei der Übermittlung personenbezogener Daten zu erarbeiten und/oder zu genehmigen. In Anwendung dieser Befugnis hat die EU-Kommission mittlerweile drei Versionen für sog. Standardvertragsklauseln verabschiedet. Die Übermittlung

personenbezogener Daten in „unsichere Drittländer“ kann auf Grundlage dieser Standardvertragsklauseln der EU-Kommission vorgenommen werden. Die Kommissionsentscheidung verpflichtet die EU-Mitgliedstaaten anzuerkennen, dass Unternehmen, die diese Vertragsklauseln unverändert verwenden, einen angemessenen Schutz und ausreichende Garantien bieten.

Auch hier ist zwischen dem Datenübermittler und dem Datenempfänger ein Vertrag zum Datenschutz erforderlich, der die Standardklauseln einbezieht; die Genehmigung durch die Aufsichtsbehörde ist jedoch entbehrlich, wenn die Klauseln unverändert verwendet werden. Zum Teil wird in der Praxis jedoch eine Information der Behörde erwartet. Dies ist abhängig von der jeweilig zuständigen Aufsichtsbehörde, die man nach den Gepflogenheiten befragen sollte.

Keine Genehmigung der Aufsichtsbehörde erforderlich! Die Behörde sollte jedoch informiert werden.

Die Standardvertragsklauseln für die Übermittlung personenbezogener Daten ins Ausland sind:

- Standardvertragsklauseln (Entscheidung 2001/497/EG vom 15. Juni 2001 bezüglich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG)
- Spezielle Klauseln für die Übermittlung an Auftragsdatenverarbeiter in „unsichere Drittländer“ (Entscheidung 2002/16/EG vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG)
- ICC-Standardvertragsklauseln (Entscheidung C [2004] 5271 vom 27.12.2004, abgedruckt im ABl. EG Nr. L 385 vom 29.12.2004 S. 74ff.)

Die ICC-Standardvertragsklauseln können als Alternative zu den Standardvertragsklauseln von Juni 2001 verwendet werden. Sie sind von der Internationalen Handelskammer unter Beteiligung weiterer Wirtschaftsvertreter formuliert worden, um Schwächen der Standardvertragsklauseln von Juni 2001, die sich in der praktischen Anwendung gezeigt haben, auszugleichen. Die ICC-Standardvertragsklauseln werden daher von vielen Unternehmen insgesamt als vorzugswürdig eingestuft.

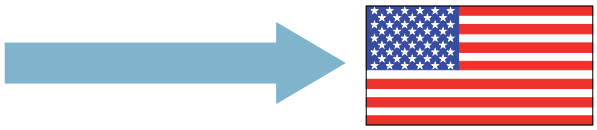
Der neue ICC-Standardvertrag enthält gegenüber dem bisherigen Standardvertrag von 2001 insbesondere eine Erleichterung der Haftungsregelungen, andererseits aber eine Ausweitung der Eingriffsmöglichkeiten der Datenschutzbehörden. Unternehmensfreundlicher sind beispielsweise auch die Klauseln über die Beilegung von Streitigkeiten, die Zuweisung von Verantwortlichkeiten und die Prüfungspflichten[2].

Die Standardvertragsklauseln sowie weitere Informationen sind unter dem folgenden Link eingestellt:

http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_de.htm

Eine ausführliche Gegenüberstellung der Inhalte der drei Standardverträge finden Sie unter IV 8)!

### III 3 d bb) Datenübermittlung in die USA auf Grundlage der „Safe Harbor Principles“



Da in den USA kein einheitlich normiertes Datenschutzrecht existiert, das dem Betroffenen „ausreichende Garantien“ im Sinne des europäischen Datenschutzes zur Verfügung stellt, bedarf eine Übermittlung von personenbezogenen Daten in die USA der Absicherung

2 Eine nützliche Zusammenfassung der Unterschiede zu den Standardvertragsklauseln 2001 gibt der Anhang zum Aufsatz von Kuhner/Hjadlk in RDV 2005 S. 200

durch die beteiligten Unternehmen. Zu diesem Zweck haben sich die EU-Kommission und die amerikanische Regierung auf das sog. Safe Harbor Paket geeinigt. Das Safe-Harbor-Paket besteht aus sieben Datenschutzprinzipien und 15 sog. „Frequently Asked Questions, FAQ". Unterwirft sich ein amerikanisches Unternehmen den Prinzipien, kann das deutsche, übermittelnde Unternehmen von einem „angemessenen Datenschutzniveau" ausgehen.

Die Safe-Harbor-Principles sind:

- Informationspflicht
- Sicherheit
- Datenintegrität
- Wahlmöglichkeit
- Auskunftsrecht
- Durchsetzung
- Weitergabe.

Die Prinzipien werden durch die FAQ, die als Leitlinien dienen, ergänzt und konkretisiert.

Die Inhalte der Prinzipien und der FAQ finden Sie unten IV 2 a) und 2 b).

Weitere Informationen dazu können (z. T. in deutscher Sprache) unter dem folgenden Link abgerufen werden:

http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_de.htm

Die Eintragung in der Liste, die vom US-Handelsministerium im Internet veröffentlicht wird, muss von den Unternehmen jedes Jahr aktualisiert werden. Die Liste kann eingesehen werden unter dem folgenden Link:

http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

Bei der Übermittlung von Daten an ein Safe-Harbor-Unternehmen ist zu beachten, dass jedes Unternehmen eigenständig darüber entscheidet, welche Datenarten und Bereiche von der Safe-Harbor-Registrierung erfasst sind. Auch diese Informationen sind in der Liste ersichtlich und sollten vor der Übermittlung genau geprüft werden. Mitarbeiterdaten sind beispielsweise von der Registrierung nicht automatisch erfasst.

**Bitte beachten Sie**

Die Voraussetzungen für eine rechtmäßige Übermittlung im Inland (z.B. nach § 28 BDSG) sind auch bei einer Datenübermittlung in die USA relevant. Neben der Frage, ob die empfangende Stelle in den USA sich auf die Einhaltung der Safe-Harbor-Principles verpflichtet hat, (§ 4 b BDSG) muss zusätzlich geprüft werden, ob darüber hinaus auch die allgemeinen Voraussetzungen für eine Übermittlung vorliegen (§ 4 Abs. 1, 28 BDSG, zu § 28 BDSG vgl. oben III 1 a). Erforderlich ist also eine ZWEISTUFIGE PRÜFUNG.

Bei einer Auftragsdatenverarbeitung bleibt die Verpflichtung zu einem schriftlichen Vertrag gem. § 11 BDSG mit dem Auftragsdatenverarbeiter bestehen (vgl. oben III).

Weitere Informationen zum Safe Harbor-Paket:

http://web.ita.doc.gov/safeharbor/shreg.nsf/safeharbor?openform

http://www.export.gov/safeHarbor/

### III 3 d cc) Verbindliche Unternehmensregelungen („Binding Corporate Rules")

Als angemessene Schutzgarantien für die von einer Datenübermittlung Betroffenen können auch verbindliche Unternehmensrichtlinien dienen, die die internationale Weitergabe von personenbezogenen Daten innerhalb internationaler Konzerne regeln. Durch solche „Binding Corporate Rules" (auch „Codes of Conduct" genannt) werden Datenschutzgrundsätze für den Umgang mit personenbezogenen Daten, insbesondere Daten von Kunden, Aktionären und Mitarbeitern sowie Vertrags- oder Geschäftspartnern verbindlich und allgemein festgelegt. Dazu gehört unter anderem, dass die Betroffenen über den Umgang mit ihren personenbezogenen Daten in geeigneter Art und Weise leicht zugänglich informiert werden müssen, dass die Daten nur für den ursprünglichen Zweck erhoben werden dürfen und

dass die Weitergabe an Dritte einer rechtlichen Grundlage bedarf.

Das Schutzniveau durch Binding Corporate Rules ist dann angemessen, wenn der Schutz im Wesentlichen den Kernprinzipien der europäischen Datenschutzrichtlinie entspricht. Leitlinien für die inhaltlichen Anforderungen sind von der Art. 29-Datenschutzgruppe in den folgenden beiden Dokumenten (Working Paper 74, Working Paper 12 und Working Paper 108) zusammengestellt worden:

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2003_de.htm

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/1998_de.htm

Die Art. 29-Datenschutzgruppe hat mit dem Arbeitspapier 108 eine Checkliste für die Zulassung von bindenden Unternehmensrichtlinien international tätiger Unternehmen entwickelt. Anhand derer können die entworfenen Unternehmensregelungen daraufhin überprüft werden, ob sie den Vorgaben der europäischen Datenschutzrichtlinie entsprechen und Regelungen über Entschädigungen für Betroffene für den Fall der Verletzung von datenschutzrechtlichen Vorschriften enthalten.[3]

Genehmigung der Binding Corporate Rules?

Auf die Frage, ob die Binding Corporate Rules Gegenstand einer Genehmigung durch die Aufsichtsbehörde sein können oder müssen, gibt weder die EU-Datenschutzrichtlinie noch das BDSG eine eindeutige Antwort.

Vor diesem Hintergrund haben sich in den Bundesländern unterschiedliche Auffassungen und Handhabungen bzw. Verfahren der Aufsichtsbehörden entwickelt.

Die Aufsichtsbehörden der Länder kommen bei der Einordnung von Binding Corporate Rules in die Vorschriften von BDSG und EU-DatSchRL zu zwei unterschiedlichen Ergebnissen. Zum einen wird die Einordnung unter § 4 b Abs. 2 Satz 2 BDSG (vgl. auch Art. 25 Abs. 1 EU-DatSchRL) vertreten. Da die Verantwortung für die Zulässigkeit der Übermittlung die übermittelnde Stelle trage (§ 4 b Abs. 5 BDSG), sei es Aufgabe dieser Stelle, selbst die Angemessenheit des Schutzniveaus beim Empfänger zu beurteilen; für eine Genehmigung durch die Aufsichtsbehörde fehle insoweit die Rechtsgrundlage. Dies hätte eine genehmigungsfreie Datenübermittlung zur Folge. Dem entgegengesetzt wird die Einordnung unter § 4 c Abs. 2 BDSG vertreten (vgl. auch Art. 26 Abs. 2 EU-DatSchRL). Als Argument hierfür wird der Wortlaut des § 4 c Abs. 2 BDSG sowie die Behandlung dieser Frage durch die EU-Kommission angeführt. Diese Ansicht hat zur Konsequenz, dass die Binding Corporate Rules die Grundlage für eine hiernach zu beantragende Genehmigung zur Datenübermittlung bilden. Eine Genehmigung der zuständigen Aufsichtsbehörde sei also erforderlich. Diese Auffassung wird zurzeit von den Aufsichtsbehörden in Brandenburg, Bremen, Hamburg, Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein vertreten. Als weitere Variante wird von einigen Aufsichtsbehörden die Auffassung vertreten, dass neben oder an Stelle der Bindung Corporate Rules die einzelnen Übermittlungen oder gleichartigen Fälle von Übermittlungen genehmigungspflichtig seien.

Binding Corporate Rules kommen gegenwärtig (wegen des damit verbunden Aufwands) nur für größeren Unternehmen in Betracht, bei denen wegen der Unternehmensgröße Datenübermittlungen regelmäßig vorkommen und oft auch eine Reihe von Aufsichtsbehörden (auch in anderen EU-Staaten) betroffen sind.

Sofern eine Genehmigungspflicht bejaht wird, sieht die Praxis etwa wie folgt aus:

Legt ein Unternehmen Binding Corporate Rules zur Genehmigung vor, werden diese von der zuständigen Aufsichtsbehörde in die AG „Internationaler Datenverkehr“ des Düsseldorfer Kreises (gemeinsames Gremium der Landesaufsichtsbehörden) eingebracht. Dort wird

3 vgl. dazu auch Datenschutz-Berater, DSB 7+8/2005, Drittländertransfer mit bindenden Unternehmensrichtlinien, Seite 5

eine inhaltliche Überprüfung vorgenommen und die Binding Corporate Rules werden ggf. einvernehmlich akzeptiert. Federführend bei den Beratungen ist die (z. B. nach der Hauptniederlassung des Unternehmens) zuständige Aufsichtsbehörde. Das Unternehmen kann anschließend, sofern die jeweils zuständige Aufsichtsbehörde dies für erforderlich hält, auf der Grundlage der Binding Corporate Rules die Genehmigung der konkreten Datenübermittlung bzw. gleichartigen Übermittlungsfälle stellen.

Wegen des Streits über die Genehmigungspflicht ergeht in der Regel kein formeller Beschluss des Düsseldorfer Kreises, sondern es bleibt der für die einzelnen Unternehmen zuständigen Aufsichtsbehörde im Einzelfall überlassen, ob sie die Binding Corporate Rules nach § 4 c BDSG formell genehmigt oder sie ohne formelle Genehmigung als Grundlage für ein angemessenes Datenschutzniveau nach § 4 b BDSG anerkennt.

### Abstimmung der Binding Corporate Rules in der EU

**Angesichts der unterschiedlichen Handhabung und unklaren Rechtslage sollte rechtzeitig vor einer geplanten Übermittlung Rücksprache mit der zuständigen Aufsichtsbehörde gehalten werden!**

Betreffen die Binding Corporate Rules Konzernunternehmen in mehreren Mitgliedstaaten, so kooperieren die Aufsichtsbehörden der Mitgliedstaaten nach Möglichkeit in der Art. 29-Arbeitsgruppe, um eine gemeinsame Stellungnahme zu erreichen. Das Genehmigungsverfahren ist im Arbeitspapier 107 der Art. 29-Gruppe näher skizziert[4]. Zwar streben die beteiligten Behörden an, sich in diesem Rahmen darauf zu einigen, welche Aufsichtsbehörde die Federführung haben soll, und sehen Fristen für die Stellungnahmen der jeweiligen Behörden vor; es bleibt allerdings dabei, dass jede betroffene Aufsichtsbehörde im Ergebnis selbst über eine evtl. erforderliche Genehmigung entscheidet. Gemeinsame Stellungnahmen der Aufsichtsbehörden im Kooperationsverfahren über die dazu bereits vorliegenden Anträge von Unternehmen sind bislang (Stand 11/2005) noch nicht bekannt geworden. Es bleibt daher abzuwarten, ob das Kooperationsverfahren (insb. bei einer größeren Zahl von Anträgen) praktikabel ist und vor allem in angemessener Zeit abgewickelt werden kann. Eine europaweite Anerkennung der Entscheidungen einer Aufsichtsbehörde durch die anderen Aufsichtsbehörden gibt es bislang nicht.

Die beiden Working Paper (107 und 108) finden Sie über den folgenden Link:

http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_de.htm

## III 3 e) Datenübermittlung in ein Drittland auf Anweisung einer Behörde

Auch bei der Datenübermittlung in ein Drittland auf Anweisung einer Behörde gilt, dass eine Datenübermittlung in ein Drittland nur zulässig ist, wenn beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist (§ 4 b Abs. 2 BDSG) und wenn die Datenübermittlung auf Grundlage eines Gesetzes oder einer Rechtsvorschrift erfolgt (§ 4 Abs. 1 BDSG).

Als Beispiel für eine Datenübermittlung in ein Drittland kann hier das das Abkommen zur Flugdatenweitergabe mit den USA auf Basis der EU-Regelungen verwendet werden. Dieses Abkommen verpflichtet die Fluggesellschaften einen Teil der Flugdaten aller Passagiere, die in die USA reisen, den amerikanischen Behörden zum Abruf zur Verfügung zu stellen.

http://www.datenschutz.de/feature/detail/?featid=3

Ein Verfahren, bei dem die Daten zur Verfügung gestellt werden und vom Empfänger abgerufen werden können, ist nach § 3 Abs. 4 Nr. 3 BDSG als Datenübermittlung einzustufen.

4 vgl. dazu auch das Working Paper 107 der Art. 29 Datenschutzgruppe: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_de.htm

Die EU-Kommission hat mit ihrer Entscheidung vom 14. Mai 2004 die Angemessenheit des Schutzniveaus für die Verarbeitung von Flugpassagierdaten in den Vereinigten Staaten anerkannt. Mit Bestätigung des Schutzniveaus wurde am 17. Mai 2004 das Abkommen zur Übermittlung der Flugpassagierdaten beschlossen. Damit ist für die Fluggesellschaften zunächst die erforderliche Rechtsgrundlage
(§ 4 Abs. 1 BDSG) gegeben, ein angemessenes Datenschutzniveau liegt vor (§ 4 b Abs. 2 BDSG) und die Datenübermittlung ist daher rechtmäßig. Es steht jedoch noch eine Entscheidung des Europäischen Gerichtshofes über die Rechtmäßigkeit der Kommissionsentscheidung aus.

## III 4) Funktion einer Betriebsvereinbarung

Das Betriebsverfassungsgesetz verpflichtet sowohl den Arbeitgeber als auch den Betriebsrat, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern (§ 75 Abs. 2 BetrVG).

Entsprechende Regelungen werden i.d.R. in Form von Betriebsvereinbarungen zwischen Betriebsrat und Arbeitgeber festgelegt. Sie richten sich nach den Vorgaben des § 77 BetrVG. Die getroffenen Regelungen sind grundsätzlich verbindlich für alle Arbeitnehmer des Betriebs mit Ausnahme der leitenden Angestellten. Die Durchführung obliegt dem Arbeitgeber.

Eine Betriebsvereinbarung kann zum einen die datenschutzrechtlich erforderliche Zulässigkeitsnorm für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten darstellen. Sie gilt insofern als „andere Rechtsvorschrift“ im Sinne des § 4 BDSG.

Zum anderen kann eine Betriebsvereinbarung die mitbestimmungsrechtliche Voraussetzung für die Einführung und Anwendung von technischen Einrichtungen bilden, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG).

Insgesamt stellt die Einhaltung der Beteiligungsrechte der Mitarbeitervertretung eine zwingende Wirksamkeits- und Rechtmäßigkeitsvoraussetzung dar. Ihre Nichtbeachtung führt zur Unrechtmäßigkeit der Datenverarbeitung und löst Korrekturansprüche sowohl auf Seiten der betroffenen Beschäftigten als auch seitens der betrieblichen Interessenvertretungen aus.[5]

Fraglich ist jedoch das Maß, in dem einzelne Regelungen in Betriebsvereinbarungen von den Schutzbestimmungen des BDSG abweichen dürfen:

Als unstrittig gilt zunächst, dass die Betriebsvereinbarungen die Normen zwingenden Rechts einhalten müssen sowie sich an den grundgesetzlichen Werten auszurichten haben.

Datenschutzrechtlich ist weiterhin ein Interessenausgleich zwischen Arbeitgeber- und Arbeitnehmerinteressen nach billigem Ermessen durchzuführen. Pauschalermächtigungen scheiden somit als Bestimmungen ebenfalls aus.

Nach verbreiteter Auffassung der Aufsichtsbehörden[6] können Betriebsvereinbarungen nur soweit vom BDSG abweichen, wie sie die dort getroffenen Regelungen durch Schutzvorkehrungen ersetzen, die den besonderen Beschäftigungsbedingungen besser angepasst, allerdings mindestens so weitreichend, sind.

In der Praxis muss daher zunächst eine Beziehung zum Arbeitsverhältnis gegeben sein. Der Arbeitgeber muss weiterhin ein objektiv gerechtfertigtes Interesse haben, wobei die Interessen des Arbeitnehmers nicht in unangemessenem Maße unberücksichtigt bleiben dürfen.

Ein Abweichen von den Regelungen des BDSG kann insbesondere dann als vertretbar gelten, wenn ein objektives Interesse der Arbeitnehmer an der Datenverarbeitung besteht.

5 BAG, Urteil vom 22.10.1986 - 5 AZR 660/85; Gola/Wronka: Handbuch zum Arbeitnehmerdatenschutz, 3. Auflage, Frechen, 2004, RdNr. 54.
6 vgl. z. B. Hamburgischer Datenschutzbeauftragter, Tätigkeitsbericht 2000/01, S. 193

Bezüglich der Übermittlung von Arbeitnehmerdaten in das Ausland stehen die Aufsichtsbehörden im Übrigen auf dem Standpunkt, dass in ihrer Wirkung auf Deutschland beschränkte Betriebsvereinbarungen zwar im Rahmen der §§ 28-30 BDSG Bedeutung haben können, aber i.d.R. nicht geeignet seien, zur Sicherstellung eines angemessenen Schutzniveaus im Ausland beizutragen.

## III 5) Konzerninterne Datenübermittlung

### III 5 a) Allgemeines

Durch die Tendenz zur konzerninternen Zentralisierung von Verwaltungsdienstleistungen gerade auch im Personalbereich gewinnt die Übermittlung von Personaldaten im Konzern zunehmend an Bedeutung.

Zur Abgrenzung der Auftragsdatenverarbeitung von der Funktionsübertragung vgl. oben III.

Datenschutzrechtlich hat der Gesetzgeber anders als in anderen Gebieten wie dem Steuerrecht bewusst auf ein Konzernprivileg verzichtet. Dies hat zur Folge, dass sich die Übermittlung von personenbezogenen Daten über die Grenzen rechtlich selbständiger Unternehmen hinweg an den Vorschriften des Bundesdatenschutzgesetzes, insbesondere den §§ 4, 11 und 28 BDSG auszurichten hat. Dies gilt auch dann, wenn sowohl das übermittelnde Unternehmen als auch das empfangende Unternehmen Teil des gleichen Konzern sind.

### III 5 b) Keine Übermittlung bei Auftragsdatenverarbeitung

Eine Übermittlung liegt nicht vor,

- wenn die personenbezogenen Daten durch ein anderes selbständiges Konzernunternehmen im Auftrag der verantwortlichen Stelle erhoben, verarbeitet oder genutzt werden

  und

- der Auftragnehmer seinen Sitz innerhalb der EU oder im EWR hat (§ 3 Abs. 8 Satz 3 i.V.m. § 3 Abs. 4 Nr. 3 BDSG).

Durch die Annahme einer Auftragsdatenverarbeitung wird die Schaffung der rechtlichen Voraussetzungen für eine Weitergabe personenbezogener Daten innerhalb des Konzerns wesentlich vereinfacht.

In der Praxis ist für die rechtliche Einordnung als Auftragsdatenverarbeitung zunächst maßgeblich, dass eine entsprechende rechtliche Vereinbarung zwischen den Konzernunternehmen getroffen wurde, durch die der Auftraggeber die volle datenschutzrechtliche Verantwortung für die gesamte Datenverarbeitung übernimmt. Weiterhin ist entscheidend, dass der Arbeitgeber die eigentliche Entscheidung trifft. Wird diese lediglich ausgeführt, liegt keine Auftragsdatenverarbeitung mehr vor. Hierdurch entsteht ein gewisser Gestaltungsspielraum für die Konzernunternehmen[7].

BITKOM hat zur Auftragsdatenverarbeitung eine Mustervertragsanlage formuliert, die unter dem folgenden Link abgerufen werden kann: http://www.bitkom.org/de/publikationen/1357_25976.aspx

### III 5 c) Zulässigkeitsnormen für die Übermittlung

Die Übermittlung personenbezogener Daten ist nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG).

7 vgl. ebd.

### III 5 c aa) Einwilligung

Die Einwilligung scheidet i.d.R. als Rechtsgrundlage aus. Ihre Wirksamkeit unterliegt zum einen der notwendigen Unabhängigkeit des Betroffenen als Voraussetzung einer freien Entscheidung, was im Abhängigkeitsverhältnis zwischen Arbeitnehmer und Arbeitgeber regelmäßig angezweifelt werden kann.[8] Zum anderen ist die Einwilligung widerrufbar, was wesentliche organisatorische Einschränkungen in der Gestaltung der Übermittlungsprozesse mit sich bringen würde. Einwilligungen sind allenfalls dann denkbar, wenn auch dem Arbeitnehmer ein eindeutiger Vorteil aus der Einwilligung entsteht (z. B. bei der Teilnahme an Aktienoptionsprogrammen).

### III 5 c bb) § 28 BDSG als Erlaubnistatbestand

Als Erlaubnistatbestände des BDSG kommen § 28 Abs. 1 Satz 1 Nr. 1 sowie § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 3 Nr. 1 in Betracht.

Die Anwendung von § 28 Abs. 1 Satz 1 Nr. 1 BDSG setzt zunächst das Vorhandensein eines (Arbeits-)Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses (z. B. in Bewerbungssituationen) zwischen dem Betroffenen und der verantwortlichen Stelle voraus. Im Verhältnis zu Konzernunternehmen, die nicht gleichzeitig Arbeitgeber des Betroffenen sind ist dies z.B. dann gegeben, wenn ein konzerndimensionales Arbeitsverhältnis vorliegt (z. B. bei Führungskräften, die sich verpflichtet haben, bei Bedarf in anderen Gesellschaften zu arbeiten).

Darüber hinaus lässt sich die Notwendigkeit der Datenübermittlung durch den Arbeitgeber an ein anderes Konzernunternehmen im Rahmen des Arbeitsvertragszwecks dadurch rechtfertigen, dass einzelne Funktionen für den Mitarbeiter transparent und klar abgegrenzt an andere Konzernunternehmen übertragen werden.

In Anwendung der § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 3 Satz 1 Nr. 1 BDSG ist zunächst die Vorgabe des Gesetzgebers zu berücksichtigen, der explizit auf die Einführung eines Konzernprivilegs verzichtet hat.

Hingegen ist nach Auffassung der Aufsichtsbehörden für den nicht-öffentlichen Bereich eine Übermittlung als zulässig zu betrachten, „wenn die beteiligten Konzernunternehmen besondere Maßnahmen zugunsten der Arbeitnehmer treffen, so dass das Ergebnis der Abwägung doch noch zugunsten der berechtigten Interessen der Konzernunternehmen ausfällt.“[9] Hierzu gehören z. B. die Schaffung eines konzernweiten Datenschutzkonzepts sowie Maßnahmen zu Sicherstellung von Transparenz und Betroffenenrechten. Diese Regelungen sind sowohl zwischen den beteiligten Konzernunternehmen als auch im Verhältnis zu den Arbeitnehmern verbindlich zu vereinbaren.

### III 5 c cc) Die Betriebsvereinbarung als Erlaubnistatbestand

Auch eine Betriebsvereinbarung als andere Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG kommt als Erlaubnistatbestand für eine Übermittlung in Betracht. Hierbei ist der Regelungsspielraum jedoch begrenzt (vgl.oben III 4).

8 Däubler: Gläserne Belegschaften? Datenschutz in Betrieb und Dienststelle, 4. Auflage, Frankfurt, M., 2002, RdNr. 135ff; Gola/Wronka: Handbuch zum Arbeitnehmerdatenschutz, 3. Auflage, Frechen, 2004, RdNr. 145ff.

9 Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“ des „Düsseldorfer Kreises“, veröffentlicht durch das Regierungspräsidium Darmstadt, 2005.

# IV Begriffsbestimmungen, Materialien, Grafiken und Übersichten

## IV 1) Begriffsbestimmungen

Im Folgenden werden einige zentrale Begriffe des Datenschutzes kurz erläutert:

**Automatisierte Verarbeitung**
Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

**Besondere Arten personenbezogener Daten**
Nach § 3 Abs. 9 BDSG sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeiten, Gesundheit oder Sexualleben „besondere Arten personenbezogener Daten" (häufig auch als „sensitive Daten" bezeichnet).

**Betroffener**
Betroffener ist die natürliche Person, deren Daten erhoben bzw. verarbeitet werden.

**Datei mit personenbezogenen Daten bzw. nicht automatisierte Datei**
Eine Datei ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird.

**Datenexporteur**
Datenexporteur ist der für die Verarbeitung Verantwortliche, der personenbezogene Daten übermittelt.

**Datenimporteur**
Datenimporteur ist der für die Verarbeitung Verantwortliche, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten für die Verarbeitung entgegenzunehmen.

**Dritter**
Dritter ist jede Stelle außer

- der betroffenen Person,
- dem für die Verarbeitung Verantwortlichen und
- den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen befugt sind, die Daten zu verarbeiten.

Nicht unter den Begriff „Dritter" fallen rechtlich unselbstständige Zweigstellen eines Unternehmens (wie z. B. Filialen). Rechtlich selbstständige Einrichtungen – wie Betriebskrankenkassen – sind jedoch auch dann Dritte, wenn sie organisatorisch, räumlich oder personell mit der speichernden Stelle verbunden sind.

**Drittland**
Als Drittländer werden alle anderen Staaten außerhalb der EU bzw. des EWR gesehen.

**Einwilligung**
Einwilligung ist jede Willensbekundung, die ohne Zwang für den konkreten Fall und in Kenntnis der Sachlage erfolgt. Mit der Einwilligung akzeptiert die betroffene Person, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.

**EWR (häufig auch EWG genannt)**
Europäischer Wirtschaftsraum. Er umfasst die Länder der EU, sowie die drei EFTA-Staaten Norwegen, Liechtenstein und Island.

**Empfänger**
Empfänger ist jede Stelle, die Daten erhält.

**Messaging-Dienste**
Instant Messaging ist ein Dienst, der es erlaubt, sich in Echtzeit über das Internet zu unterhalten oder kurze Nachrichten an andere Teilnehmer zu schicken oder diesen kleinere Dateien zukommen zu lassen.

**Nutzen von Daten**
Jede Verwendung außer Verarbeitung (z. B. Duplizieren oder Kopieren von Daten, Erstellung personenbezogener Auswertungen).

**Personenbezogene Daten**
Personenbezogene Daten sind Einzelangaben über persönliche Verhältnisse (z. B. Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit, Konfession, Berufs- und Branchenbezeichnung, Zeugnisnoten, Beurteilungen, Krankheiten, Vorstrafen) oder sachliche Verhältnisse (z. B. Einkommen, Besitzverhältnisse, Steuern, Versicherungen, Vertragskonditionen) einer bestimmten oder bestimmbaren natürlichen Person. Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Geschützt sind also alle Informationen über die einzelne natürliche Person, aber nicht über juristische Personen (AG, GmbH, e.V. etc.).

**Übermitteln**
Übermitteln ist die Bekanntgabe von Daten aus einer Datei an Dritte durch aktive Weitergabe in jeglicher Form (mündlich, schriftlich, versenden usw.) oder durch Bereithalten der Daten zur Einsichtnahme oder zum Abruf. Bei automatisierten Abrufverfahren liegt ein Übermitteln nach dem BDSG erst dann vor, wenn der Dritte die Daten einsieht (Lesen oder Betrachten) oder abruft (z. B. Sichtbarmachung der Daten auf seinem Monitor).

**Verantwortliche Stelle**
Verantwortliche Stelle ist die Stelle, die eine Verarbeitung selbst durchführt oder durch andere im Auftrag durchführen lässt.

**Verarbeitung personenbezogener Daten**
Verarbeitung ist jeder Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Wiederauffinden, das Abfragen, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten von personenbezogenen Daten.

- Speichern (Erfassen, Aufnehmen, Aufbewahren)
- Verändern (inhaltliches Umgestalten)
- Übermitteln (Bekanntgabe, Weitergabe, Einsichtnahme, Abrufen)
- Sperren (Kennzeichnung zur Verarbeitungs- und Nutzungseinschränkung)
- Löschen (Unkenntlichmachung)

## IV 2) Materialien zu Safe Harbor

### IV 2 a) Die Safe-Harbor Principles

**Informationspflicht**
Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

**Wahlmöglichkeit**
Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen („opt out"), ob ihre personenbezogenen Daten a) an Dritte (2) weitergegeben werden sollen oder b) für einen Zweck verwendet werden sollen, der mit dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck

unvereinbar ist. Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare und verständliche, leicht zugängliche und kostengünstige Verfahren ermöglicht werden.

Bei sensiblen Daten (wie z. B. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder philosophische Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung („opt in“) der betroffenen Personen, wenn die Daten an Dritte weitergegeben oder für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat. In jedem Fall sollen die Organisationen alle ihnen von Dritten übermittelten Informationen als sensibel behandeln, die der Übermittler als sensibel einstuft und behandelt.

**Weitergabe**
Eine Organisation darf Daten nur dann an Dritte weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Möchte eine Organisation Daten an einen Dritten weitergeben, der in ihrem Auftrag und auf ihre Anweisung tätig ist (vergleiche Fußnote), kann sie dies tun, sofern der Dritte entweder dem „sicheren Hafen“ angehört oder der Richtlinie unterliegt, oder von einer anderen Feststellung angemessenen Schutzniveaus erfasst wird oder sich schriftlich in einer Vereinbarung mit der Organisation dazu verpflichtet, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den entsprechenden Grundsätzen des „sicheren Hafens“ gefordert wird. Eine Organisation, die diese Forderungen erfüllt, kann nicht haftbar gemacht werden (sofern sie nichts anderes vereinbart hat), wenn ein Dritter, an den sie Daten übermittelt hat, Beschränkungen der Verarbeitung dieser Daten missachtet oder sie in einer Weise verarbeitet, die seinen Erklärungen widerspricht, es sei denn, die Organisation wusste oder konnte wissen, dass der Dritte die Daten in unzulässiger Weise verarbeiten würde, und hat keine angemessenen Schritte unternommen, um das zu unterbinden.

**Sicherheit**
Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene Sicherheitsvorkehrungen treffen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen.

**Datenintegrität**
In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten für den beabsichtigten Verwendungszweck erheblich sein. Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. In dem für diese Zwecke notwendigen Umfang muss die Organisation durch angemessene Maßnahmen gewährleisten, dass die Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind.

**Auskunftsrecht**
Privatpersonen müssen Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt, und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind, es sei denn, die Belastung oder die Kosten für die Gewährung des Zugangs würden in dem jeweiligen Fall in einem Missverhältnis zu den Nachteilen für den Betroffenen stehen, oder Rechte anderer Personen als des Betroffenen würden verletzt.

Durchsetzung
Für einen effektiven Schutz der Privatsphäre müssen Mechanismen geschaffen werden, die die Einhaltung der Grundsätze des sicheren Hafens gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens Folgendes umfassen:
a) leicht zugängliche, erschwingliche und von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, behandelt werden

und nach denen Schadenersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen;
b) Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Unternehmen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden;
c) Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Organisationen die Einhaltung der Grundsätze zwar erklärt, sich aber trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.

## IV 2 b) 15 Frequently Asked Questions zu Safe Harbor

In den 15 Frequently Asked Questions zu Safe Harbor werden die folgenden Bereiche erläutert und konkretisiert:

FAQ 1 - Sensible Daten

FAQ 2 - Ausnahmen für den journalistischen Bereich

FAQ 3 - Hilfsweise Haftung

FAQ 4 - Investmentbanken und Wirtschaftsprüfer

FAQ 5 - Die Rolle der Datenschutzbehörden

FAQ 6 - Selbstzertifizierung

FAQ 7 - Anlassunabhängige Kontrolle

FAQ 8 - Auskunftsrecht

FAQ 9 - Personaldaten

FAQ 10 - Datenverarbeitung im Auftrag (Artikel 17 der Datenschutzrichtlinie)

FAQ 11 - Schiedsverfahren und Durchsetzungsprinzip

FAQ 12 - Wahlmöglichkeit – Zeitpunkt des Widerspruchs

FAQ 13 - Reisedaten

FAQ 14 - Arzneimittel und Medizinprodukte

FAQ 15 - Daten aus öffentlichen Registern und öffentlich zugängliche Daten

Die Fragen und Antworten sind in der Entscheidung der Kommission 2000/520/EG vom 26.7.2000 - ABl. L 215/7 vom 25.8.2000 enthalten.

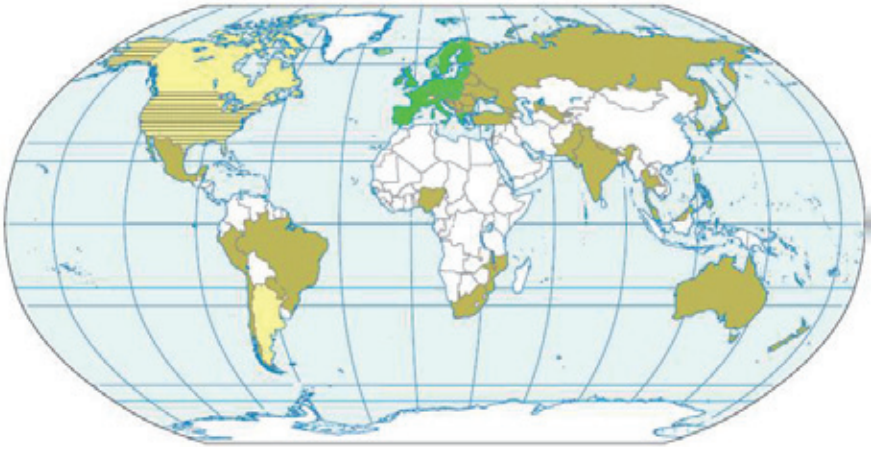
Die Entscheidung kann unter dem folgenden Link abgerufen werden:

http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm

(Vierter Unterpunkt in der Rubrik „USA - Vereinigte Staaten - Safe Harbor“)

## IV 3 Übersicht über den weltweiten Stand des Datenschutzes

### IV 3 a) Grafische Übersicht über den weltweiten Stand des Datenschutzes



- Datenschutz-Gesetze gemäß EU-Richtlinie 95/46/EG
- EFTA-Staaten (Island, Lichtenstein, Norwegen)
- Angemessenes Datenschutzniveau durch EU-Komission anerkannt
- Safe Harbour Abkommen
- Nationale Datenschutz-Gesetze
- Keine Information über Datenschutz-Gesetze vorhanden

*Quellenangabe: www.datenschutz-berlin.de, www.lda.brandenburg.de, www. datenschutz.de*

*Stand: Januar 2006 / Kein Anspruch auf Vollständigkeit*

### IV 3 b) Erläuterung zur graf. Übersicht über den weltweiten Stand des Datenschutzes

**Datenschutz-Gesetze gemäß EU-Richtlinie 95/46/EG**

- Belgien
- Dänemark
- Estland
- Finnland
- Frankreich
- Griechenland
- Großbritannien
- Irland
- Italien
- Lettland
- Litauen
- Luxemburg
- Malta
- Niederlande
- Österreich
- Polen
- Portugal
- Schweden
- Slowakei
- Slowenien
- Spanien
- Tschechien
- Ungarn
- Zypern

**EFTA - Staaten**

- Island
- Lichtenstein
- Norwegen

**Angemessenes Datenschutzniveau durch EU-Kommission anerkannt**

- Argentinien
- Kanada
- Schweiz
- Guernsey
- Isle of Man

**Safe Harbor Abkommen**

- USA

**Datenschutzbehörden in Europa (außerhalb EWR)**

- Bulgarien
- Georgien
- Kroatien
- Moldawien
- Rumänien
- Russland
- Türkei

**Datenschutzbehörden International**

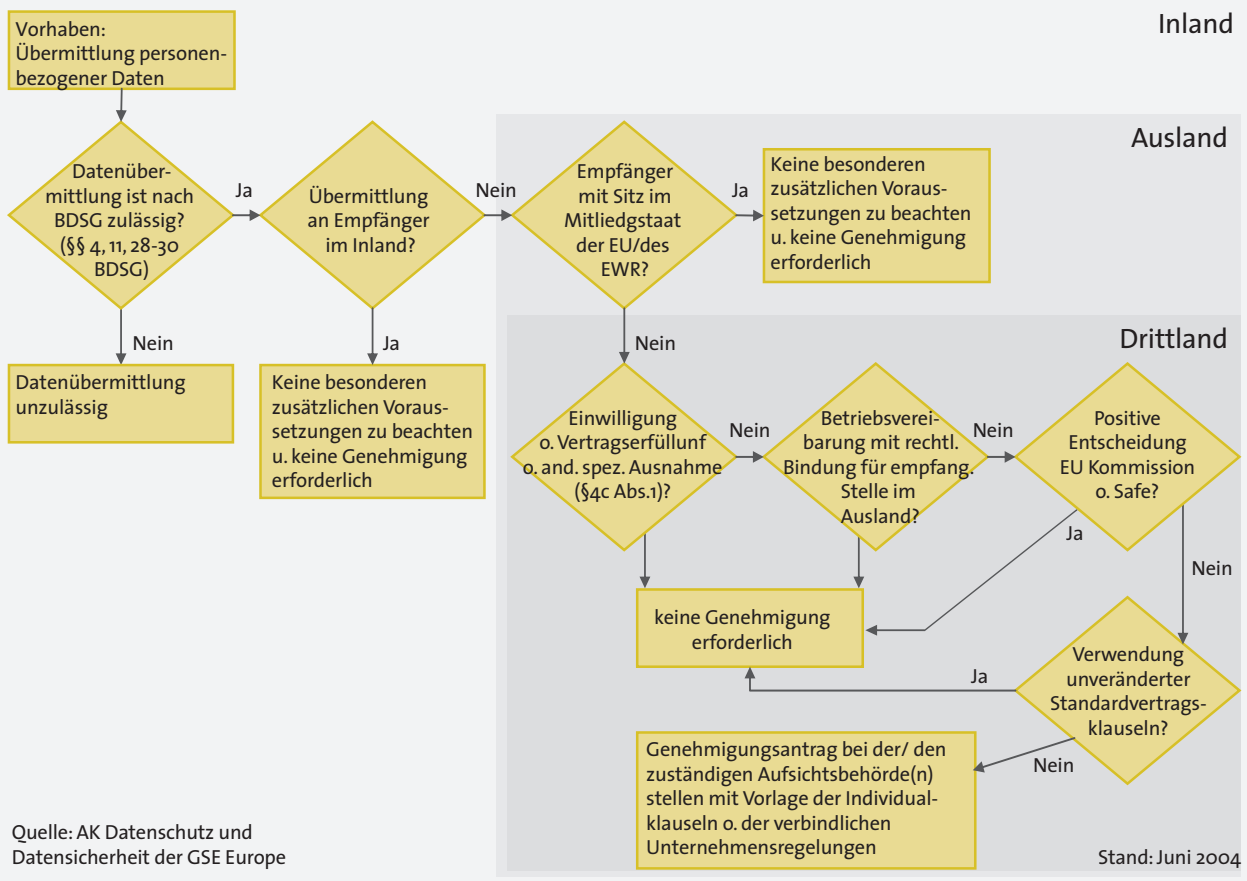
- Australien
- Brasilien
- Hong Kong
- Israel
- Japan
- Malaysia
- Neuseeland
- Paraguay
- Singapur
- Südkorea
- Taiwan
- Thailand

**Nationale Datenschutz-Gesetze**

- Armenien
- Weißrussland
- Belize
- Bosnien Herzegowina
- Chile
- Ecuador
- Indien
- Malawi
- Mazedonien
- Mexiko
- Mosambik
- Nepal
- Nigeria
- Pakistan
- Peru
- Philippinen
- Rumänien
- Serbien u. Montenegro
- Südafrika
- Trinidad und Tobago
- Ukraine
- Usbekistan

## IV 4) Entscheidungshilfe Auslandsdatenverarbeitung

Überblick über die „Zonen“ eines Drittlandtransfers




Die Entscheidungshilfe wurde von einer Arbeitsgruppe (M. Schmidt, V. Backes, H. Eul, M. Guthmann. R. Martwich) des Arbeitskreises Datenschutz und Datensicherheit der GSE Europe erstellt und erstmals veröffentlicht in der RDV 2004 S. 156 ff.

## IV 5) Übersicht über die rechtlichen Möglichkeiten der Übermittlung personenbezogener Daten in Drittländer*

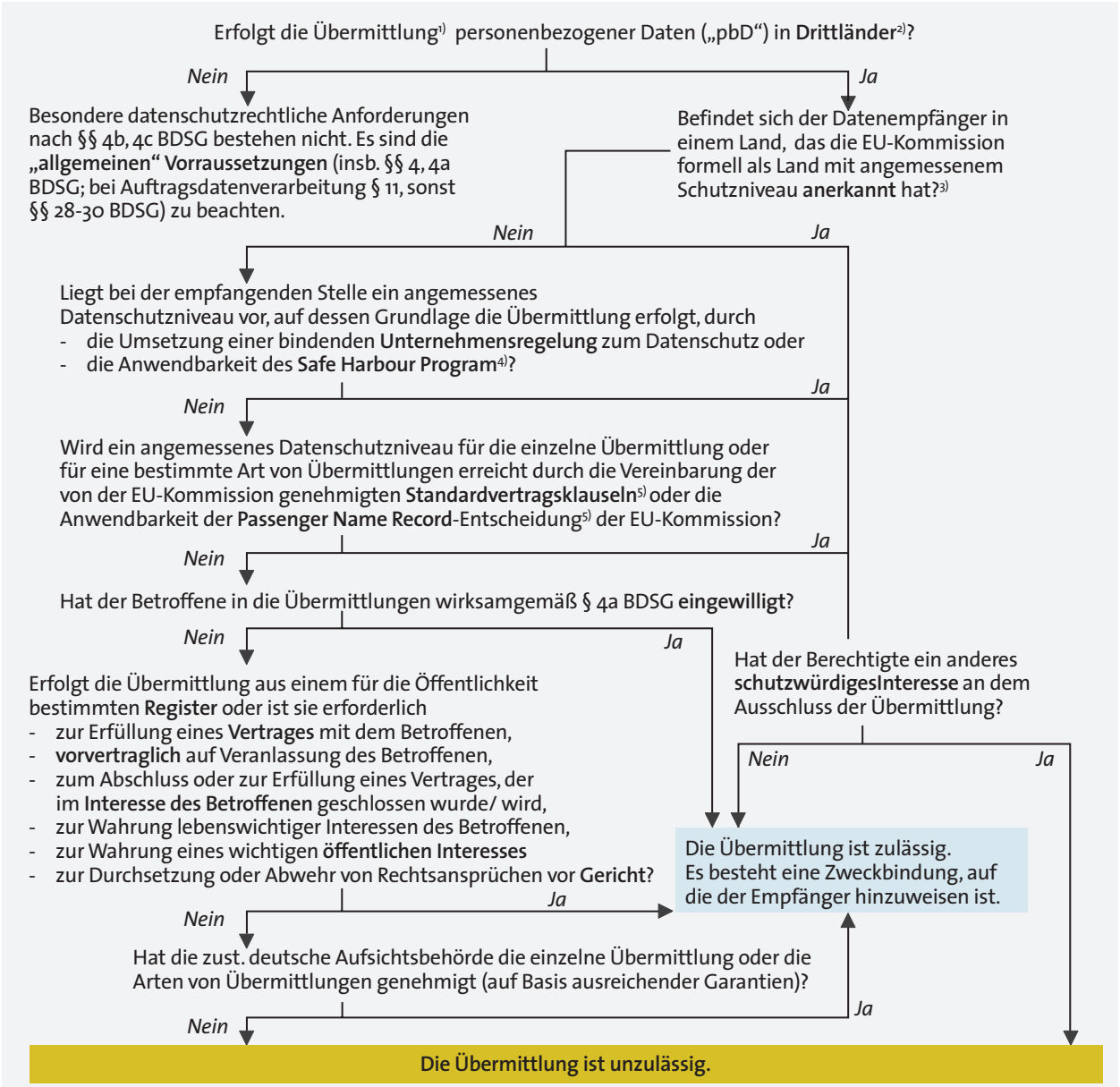
| | „Art“ | Geltungs-bereich | Abschluss | Pb Daten | Aufsichts-behörde | Bemer-kungen |
|---|---|---|---|---|---|---|
| Datenüber-mittlung ist zur Erfüllung des Vertrages o. zur Durchführung vorvertragli-cher Maßnah-men erforder-lich (§ 4 c Abs. 1 Nr. 2 BDSG) | Vertrag o. vertragsähnli-che Beziehung zwischen verantwortli-cher Stelle und Betroffenem | Individuell; zwischen Betroffenen und verant-wortlicher Stelle | Durch Abgabe der entspre-chenden Willenserklä-rungen von der verant-wortlichen Stelle und dem Betroffenen | Grundsätzlich die pb Daten des Betroffe-nen, die für die Durchführung des Vertrages erforderlich sind | Keine Mitwirkung erforderlich | Vertragsbei-spiele: Hotel-reservierung im Ausland; Arbeitsvertrag mit ausländ-dischem Arbeitgeber; Warenbestel-lung (auch online) im Ausland |
| Einwilligung (§ 4 c Abs. 1 Nr. 1 BDSG) | Einseitige, empfangs-bedürftige Einwilligungs-erklärung | Individuell; zwi-schen Betrof-fenem und verantwortli-cher Stelle | Durch Abgabe der entspre-chenden Wil-lenserklärung seitens des Einwilligenden | Grundsätzlich die autorisier-ten pb Daten des Betroffe-nen; Umfang im Rahmen der gesetzlichen Möglichkei-ten, der guten Sitten u. des vorgesehenen Zwecks | Keine Mitwirkung erforderlich | Einwilligung muss Aussagen zum gewähr-leisteten o. nicht gewähr-leisteten Datenschutzni-veau enthalten |
| Gesetzliche Ausnahmen (§ 4 c Abs. 1 Nr. 3-6 BDSG) | Gesetzlicher Ausnahmetat-bestand | Begrenzt auf den Sach-verhalt der Ausnahmere-gelung | Prüfung erforderlich, ob die Voraus-set-zungen des Ausnahme-tatbestands vorliegen | Mitarbeiter-, Kunden-, Nichtkunden, -Interessenten und Liefe-rantendaten, soweit für die Übermittlung im Rahmen der Ausnahme-regelung erforderlich | Keine Mit-wirkung erforderlich | z.B. Wahrung eines wichtigen öffentlichen Interesses; Gel-tendmachung, Ausübung oder Verteidigung von Rechts-ansprüchen vor Gericht; Wahrung lebenswichti-ger Interessen |
| Drittländer mit durch die EU Kommission festgestelltem angemessenen Datenschutzni-veau (§ 4 b Abs. 3 BDSG) | Entscheidung gemäß Art. 25 Abs. 6 EU-DSRL (EU-Kommis-sionsentschei-dung) | Gilt für alle Empfänger im entscheidungs-gegenständli-chen Drittland | n.a. | Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferan-tendaten | Keine Mit-wirkung erforderlich | Eine Emp-fehlung der Arbeitsgruppe nach Art 29 bzw. eine Kom-missionsent-scheidung lie-gen derzeit vor für: Schweiz, Canada (teil-weise), Argenti-nien, Guernsey, Isle of Man |

| | „Art“ | Geltungs-bereich | Abschluss | Pb Daten | Aufsichts-behörde | Bemer-kungen |
|---|---|---|---|---|---|---|
| Individueller Datenschutz-vertrag (§4 c Abs. 2 BDSG) | Vertragliche, verbindliche Regelung zwischen den Parteien (auch mehrere, auch Unterauftrags-nehmer) über den Umgang mit Personen bezogenen Daten | Zwischen den Vertragspar-teien (auch mehr als 2) | Durch Abgabe der entspre-chenden Wil-lenserklärun-gen zwischen den vertrags-schließenden Parteien | Mitarbeiter-, Kunden-, Nicht-kunden-, Inte-ressenten und Lieferanten-daten soweit sie Gegen-stand des individuellen Datenschutz-vertrages sein sollen | Genehmigung einzelner Datenüber-mittlungen oder bestimm-ter Arten von Übermittlun-gen pb Daten gem. § 4 c Abs. 2 BDSG | Flexibel; je nach Umfang auch zeitaufwendig |
| Vertrag auf Basis der EU-Standardver-tragsklauseln für die Über-mittlung Perso-nen bezogener Daten (auch an Auftrags-verarbeiter) in Drittländer (§4 c Abs. 2 BDSG) | Vertrag zwi-schen Daten-expoteur und Datenimpoteur auf Basis der EU-Kommissi-onsentscheid-dung zu den Standardklau-seln | Zwischen Daten-impoteur(en) in einem Drittland und Expoteur (en) mit Sitz im EWR. | Durch Abgabe der entspre-chenden Wil-lenserklärun-gen zwischen den vertrag-schließenden Parteien | Mitarbeiter-, Kunden-, Nicht-kunden-, Inte-ressenten und Lieferantenda-ten soweit sie Gegenstand des EU-Stan-dard-Vertrages sein sollen | Bei unver-ändertem Abschluss des Vertrages keine Genehmigung erforderlich. Information der Aufsichts-behörden über den Abschluss sinnvoll. Einige Aufsichtsbe-hörden erwar-ten Vorlage der entsprechend. Verträge | Schnell umsetzbar. Ein-fach. Für große internationale Unterneh-mensverbünde wohl unprak-tikabel, da umfangreiches Vertragsma-nagement erforderlich |
| Binding Cor-porate Rules („verbindliche unterneh-mensinterne Vorschriften für den internatio-nalen Daten-transfer“; § 4 c Abs. 2 BDSG) | Verbindliche Unterneh-mensregelun-gen („Binding Corporate Rules“) für Teile oder die Gesamtheit eines multi-nationalen Unterneh-mensverbun-des (Konzern) oder anderen Wirtschafts-gebildes, die die entspre-chenden Datenschutz-anforderungen definieren | Die Teile des Konzerns, für die die Unter-nehmens-regelungen („Binding Cor-porate Rules“) verbindlich sind | Verbindliche, interne Anwei-sung durch die führende Gesellschaft | Mitarbeiter-, Kunden-, Nicht-kunden-, Inter-essenten- und Lieferantenda-ten soweit sie Gegenstand des Binding Corporate Rules sein sollen | Genehmigung einzelner Datenüber-mittlungen oder bestimm-ter Arten von Übermittlun-gen pb Daten gem. § 4 c Abs. 2 BDSG | Anforderun-gen siehe WP 74 der Art. – 29-Gruppe – Zur Zeit Diskus-sion innerhalb der Aufsichts-behörden, ob überhaupt Genehmigung notwendig |

| | „Art“ | Geltungs-bereich | Abschluss | Pb Daten | Aufsichts-behörde | Bemer-kungen |
|---|---|---|---|---|---|---|
| Safe Harbor (§ 4 c Abs. 2 BDSG) | Vereinbarung zwischen den USA und der EU über verbindliche Verhaltensregeln zum Datenschutz für US-amerikanische Unternehmen | Datenverkehr pb Daten zwischen Datenexporteuren mit Sitz in der EU und an Safe Harbor teilnehmenden Unternehmen (Datenimporteur) in den USA | Beitritt des US-Unternehmens zu dem Safe-Harbor-Programm durch Beitrittserklärung, Registrierung auf einer Internet- Webseite und Veröffentlichung bestimmter Informationen; Datenexporteur muss in der EU seinen Sitz haben | Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten im Rahmen der Registrierung | Keine Mitwirkung erforderlich; ggf. Hinweis des Übermittlers auf Teilnahme des Datenempfängers an dem Safe-Harbor-Programm | 20.7.2004: 537 Teilnehmer |
| Betriebsvereinbarung | Vereinbarung zwischen der Geschäftsleitung eines Unternehmens/ Betriebs und dem Betriebsrat | Je nach Mandat des Betriebsrats variabel: zwischen einfachem Betrieb bis hin zu großen Konzerngebilden | Durch freiwillige Vereinbarung; hat den Rang einer Rechtsvorschrift i.S.d. § 4 Abs. 1 BDSG | I.d.R. nur Mitarbeiterdaten | Keine Mitwirkung erforderlich; ggf. Überprüfung bei einer Kontrolle durch die Aufsichtsbehörde | Setzt Betriebsrat voraus; die Reglungsreichweite einer Betriebsvereinbarung auf den Datentransfer in Drittländer ohne angemessenes Datenschutzniveau wird zum Teil von Aufsichtsbehörden bezweifelt |
| Nichts tun | Keine Regelung implementieren | n.a. | n.a. | n.a. | n.a. | Hohes Risiko für die Verantwortlichen (Bußgeld/Haftstrafe) und das Unternehmen (Schadensersatz/Risiko der Untersagung der Geschäftstätigkeit/des EDV-Betriebs/ neg. Auswirkungen auf Image, Umsatz, Ertrag, Shareholder-Value) |

Quelle: AK Datenschutz und Datensicherheit der GSE Europe
Die Entscheidungshilfe wurde von einer Arbeitsgruppe (M. Schmidt, V. Backes, H. Eul, M. Guthmann. R. Martwich) des Arbeitskreises Datenschutz und Datensicherheit der GSE Europe erstellt und erstmals veröffentlicht in der RDV 2004 S. 156 ff.
* Drittländer sind: Staaten, in die personenbezogene Daten aus einem Mitgliedstaat der EU oder eines Vertragsstaates des EWR weitergegeben bzw. übermittelt werden, die selbst aber nicht Mitgliedstaat der EU oder ein Vertragsstaat des EWR sind. Seit 1.5.2004 umfasst die EU 25 Mitgliedstaaten.

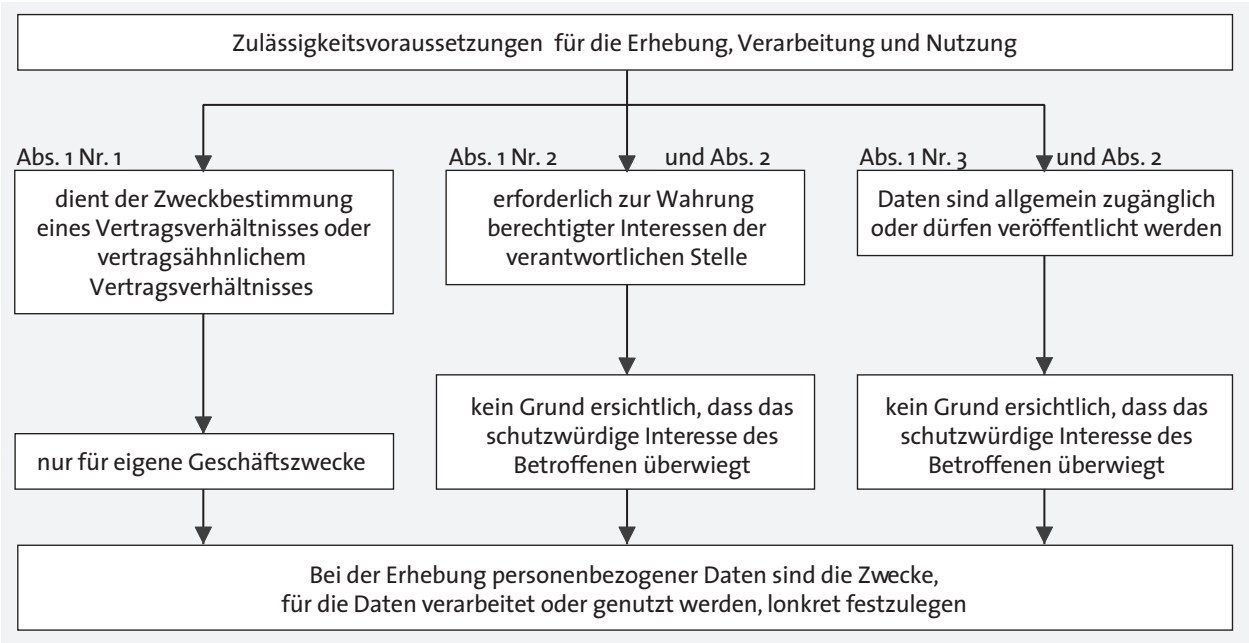
## IV 6) Möglichkeiten zur Erreichung eines angemessenen Datenschutzniveaus bzw. Ausnahmen vom Schutzerfordernis gem. §§ 4 b, 4 c Bundesdatenschutzgesetz (BDSG)?

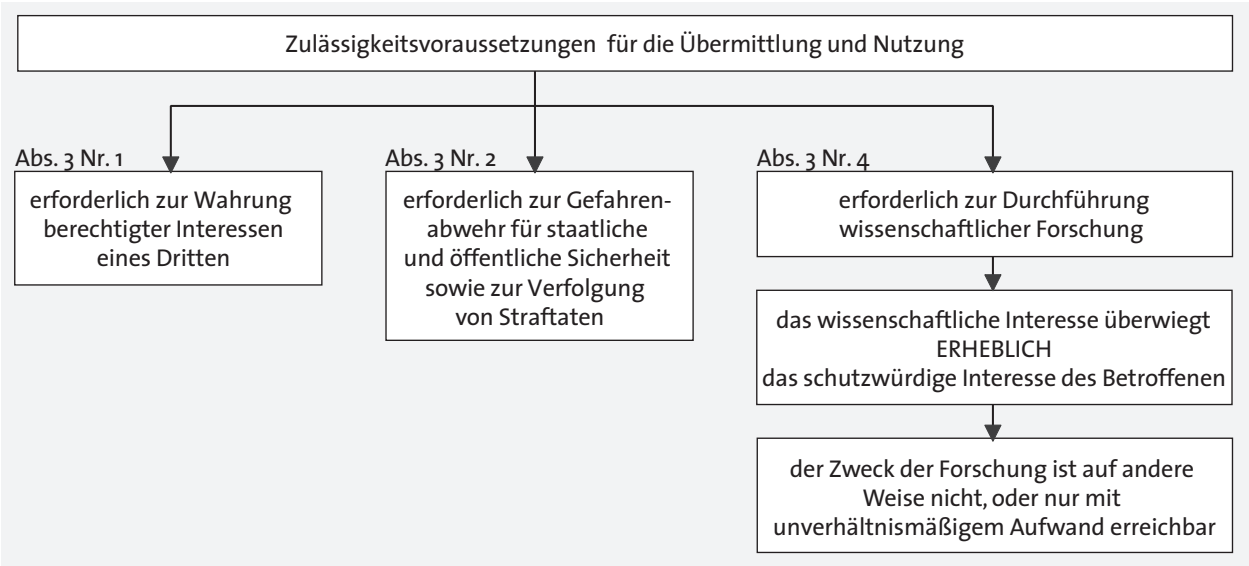


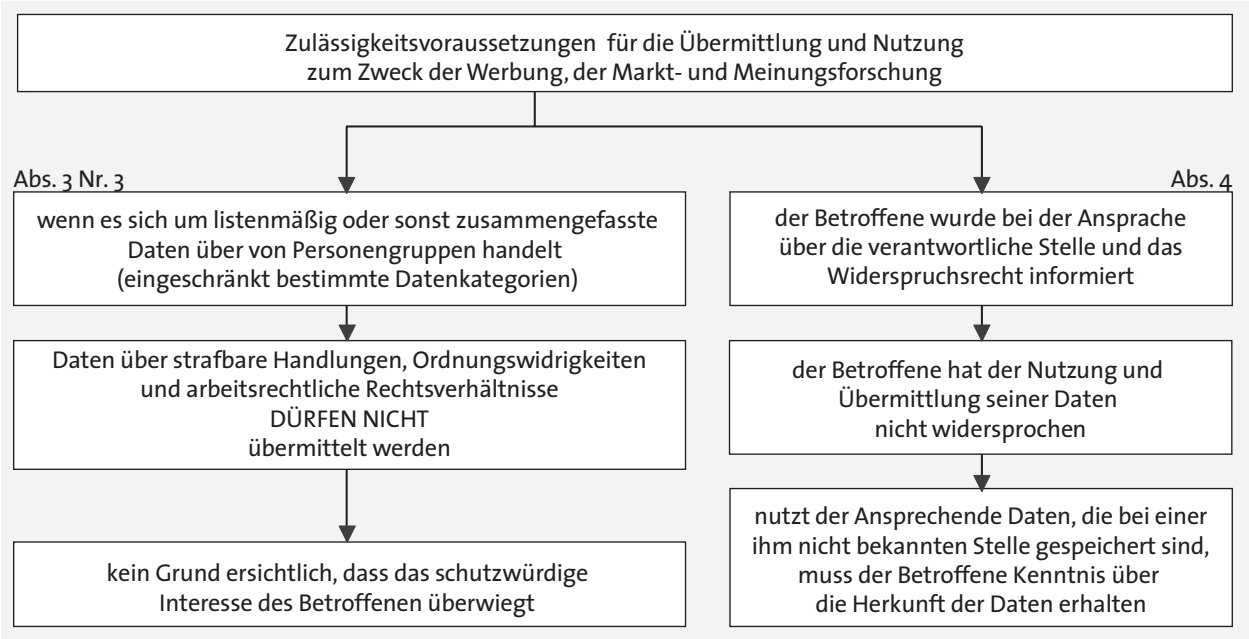

1) Übermittlung liegt auch vor, wenn der Datenempfänger Daten online abruft; bei Drittländern liegt außerdem auch bei der Datenverarbeitung im Auftrag eine Übermittlung vor.
2) Drittländer sind alle Staaten mit Ausnahme der EU-Staaten und der Staaten des Europäischen Wirtschaftsraumes (z. Zt. Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Großbritannien, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Zypern sowie die EWR-Staaten Island, Liechtenstein und Norwegen).
3) Zur Zeit sind als Länder mit angemessenem Datenschutzniveau Argentinien, Guernsey, Isle of Man, Kanada und die Schweiz von der EU-Kommission anerkannt.
4) Programm für US-Unternehmen, die sich eindeutig und öffentlich verpflichtet haben, die sogenannten Safe Harbour Principles einzuhalten (s. Safe Harbour List unter: www.export.gov/safeharbour).
5) Siehe die Entscheidungen unter http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_de.htm

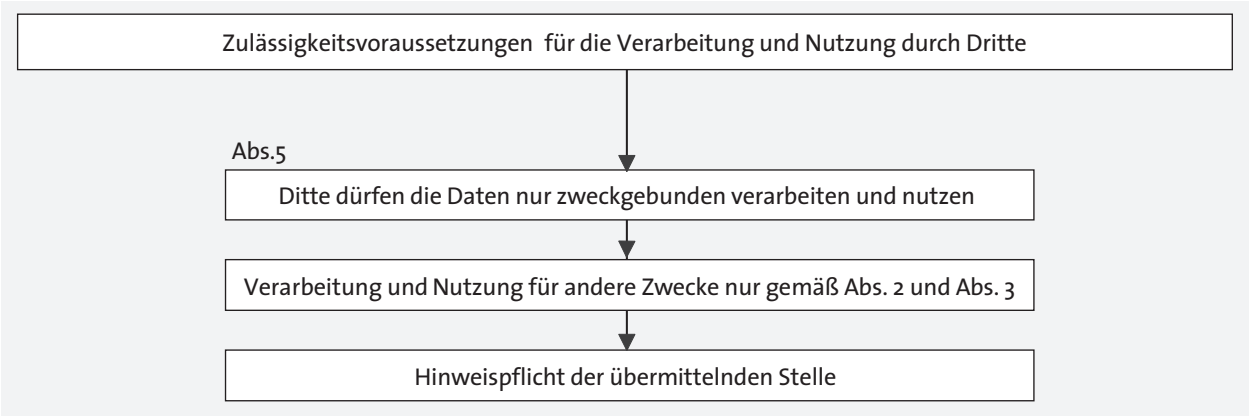
Grafik: Florian Thoma, Siemens AG

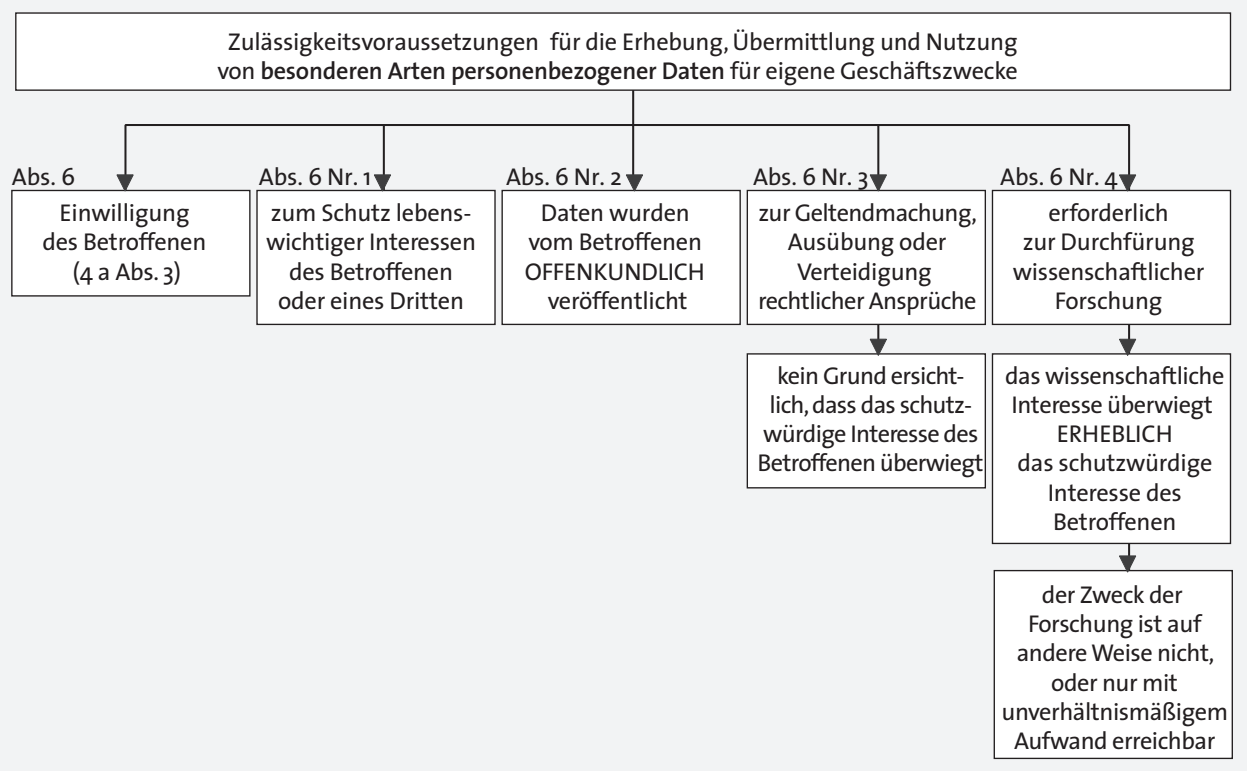
## IV 7) § 28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke

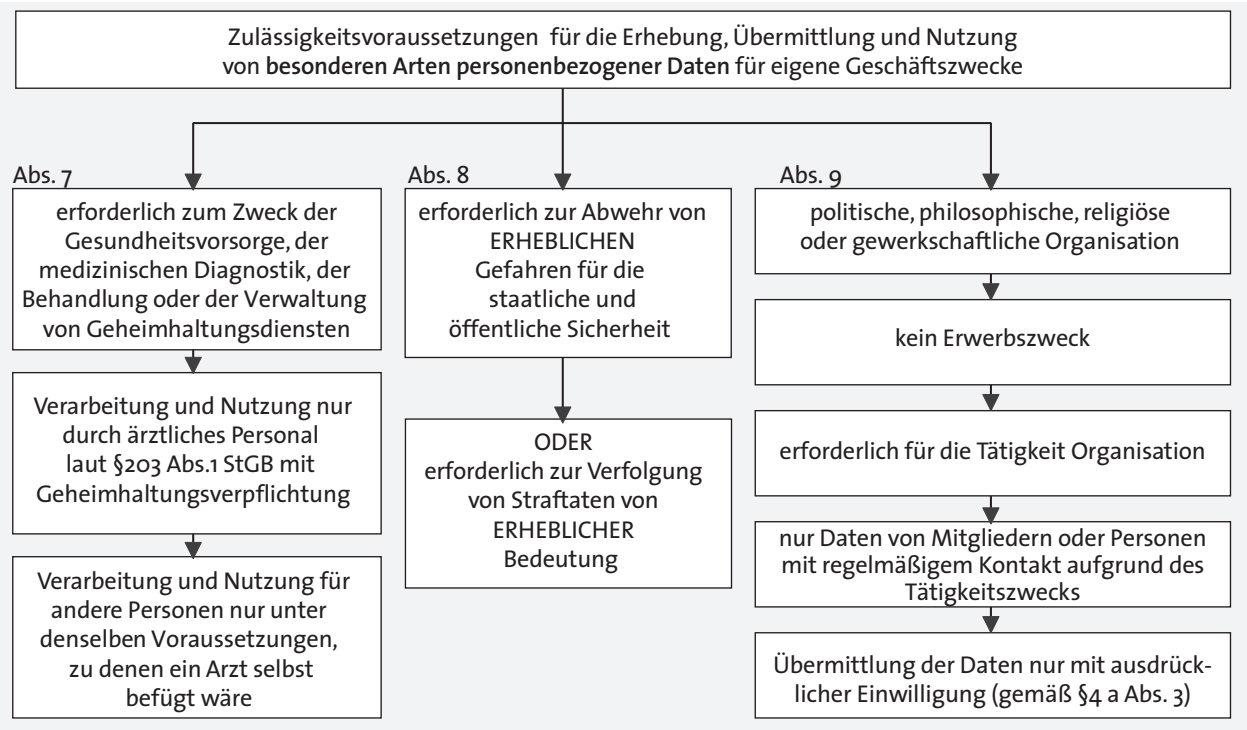



Zulässigkeitsvoraussetzungen für die Übermittlung und Nutzung zum Zweck der Werbung, der Markt- und Meinungsforschung
Abs. 3 Nr. 3
wenn es sich um listenmäßig oder sonst zusammengefasste Daten über von Personengruppen handelt (eingeschränkt bestimmte Datenkategorien)
Daten über strafbare Handlungen, Ordnungswidrigkeiten und arbeitsrechtliche Rechtsverhältnisse DÜRFEN NICHT übermittelt werden
kein Grund ersichtlich, dass das schutzwürdige Interesse des Betroffenen überwiegt
Abs. 4
der Betroffene wurde bei der Ansprache über die verantwortliche Stelle und das Widerspruchsrecht informiert
der Betroffene hat der Nutzung und Übermittlung seiner Daten nicht widersprochen
nutzt der Ansprechende Daten, die bei einer ihm nicht bekannten Stelle gespeichert sind, muss der Betroffene Kenntnis über die Herkunft der Daten erhalten


Zulässigkeitsvoraussetzungen für die Verarbeitung und Nutzung durch Dritte
Abs.5
Ditte dürfen die Daten nur zweckgebunden verarbeiten und nutzen
Verarbeitung und Nutzung für andere Zwecke nur gemäß Abs. 2 und Abs. 3
Hinweispflicht der übermittelnden Stelle




Grafik: Wolfgang Braun (Giesecke & Devrient), Ralf Maruhn (Nokia GmbH)

## IV 8) Gegenüberstellung der Standardvertragsklauseln

Gegenüberstellung der

- Standardvertragsklauseln vom 15. Juni 2001 (Verhältnis Controller – Controller)
- Standardvertragsklauseln vom 27. Dezember 2004 (ICC – Standardvertragsklauseln, Verhältnis Controller – Controller)
- Standardvertragsklauseln vom 27. Dezember 2001 (Verhältnis Controller – Processor, Auftragsdatenverarbeitung)

### 1. Grundlage der EU Standardvertragsklauseln

Basierend auf Art. 26 Abs. 2 der EU Datenschutzrichtlinie hat die Kommission der Europäischen Gemeinschaften Standardvertragsklauseln veröffentlicht.

- 15. Juni 2001: Standardvertragsklauseln für das Verhältnis Datenexporteur – Datenimporteur. Der Datenimporteur verwendet dabei die personenbezogenen Daten für eigene Zwecke (Controller – Controller).
- 27. Dezember 2001: Standardvertragsklauseln für das Verhältnis Datenexporteur – Datenimporteur. Der Datenimporteur wird dabei als Auftragsdatenverarbeiter tätig (Controller – Processor).
- 27. Dezember 2004: Alternativ-Vorschlag für die Klauseln vom 15. Juni 2001 (Controller – Controller)

### 2. Standardvertragsklauseln vom 15. Juni 2001

Diese Klauseln wurden von der Kommission unter dem Grundsatz entworfen, dass die Klauseln helfen sollen, das Datenschutzniveau im Drittland unter Berücksichtigung aller Umstände zu beurteilen und auf Basis der Forderungen der Klauseln dem Niveau in der EU anzupassen.

Die Aussagen in der offiziellen Begründung zur Veröffentlichung der Klauseln lassen erkennen, dass sich die Kommission bereits 2001 bewusst war, dass bei der modernen Datenverarbeitung der Transfer von personenbezogenen Daten auch in Drittstaaten immer mehr an Bedeutung gewinnt.

Allerdings hat die Kommission gleichzeitig auch festgelegt, dass diese Klauseln keine Anwendung finden können, wen der Datenimporteur nur als Auftragsverarbeiter tätig wird. Hierzu wird begründet, dass für derartige Übermittlungen nicht die gleichen Garantien erforderlich sind, da der Auftragsverarbeiter ausschließlich im Auftrag des Datenexporteurs tätig wird und an dessen Weisungen gebunden ist.

#### 2.1 Problematische Formulierungen in den Standardvertragsklauseln vom 15. Juni 2201:

##### 2.1.1 Klausel 3

Bereits beim Entwurf der Standardvertragsklauseln wurde untersucht, welche Schutz- und Sorgfaltspflichten angewandt werden könnten, um den Schutz der betroffenen Personen gegenüber dem Datenimporteur und Datenexporteur beim Datentransfer in Drittländern zu verbessern. Vor diesem Hintergrund wurde Klausel 3 formuliert, die eine „Drittbegünstigtenregelung“ beinhaltet. Nach dieser Regelung können von der Datenverarbeitung betroffene Personen als Drittbegünstigte einen Großteil der (in den Standardvertragsklauseln festgelegten) Pflichten des Datenexporteurs und –importeurs als eigene Rechte geltend machen und sich auf deren wechselseitige Haftung berufen.

##### 2.1.2 Klausel 6

Klausel 6 enthält Haftungsregelungen, die im Zusammenhang mit der „Drittbegünstigtenregelung“ aus Klausel 3 sehr problematisch sein können. In Klausel 6 heißt es in Ziffer 1:

*Die Parteien vereinbaren, dass betroffene Personen, die durch eine Verletzung der Bestimmungen in Klausel 3 Schaden erlitten haben, berechtigt sind, von den Parteien Schadensersatz für den erlittenen Schaden zu verlangen.*

*Die Parteien vereinbaren, dass sie nur von der Haftung befreit werden können, wenn sie nachweisen, dass keine von ihnen für die Verletzung dieser Bestimmungen verantwortlich ist.*

Dies bedeutet, dass betroffene Personen, die durch eine Verletzung der Bestimmungen in Klausel 3 einen Schaden erlitten haben, berechtigt sind, von beiden Parteien (Datenexporteur und Datenimporteur) Schadenersatz zu verlangen. Die Parteien sind allerdings dann von der Haftung befreit, wenn sie nachweisen, dass keine von ihnen für die Verletzung der Bestimmungen verantwortlich ist. Die Regelungen dieser Ziffer erlauben der betreffenden Person, als Dritter eigene Rechte direkt aus dem Vertrag abzuleiten.

Ziffer 2 der Klausel 6 bestimmt:
*„Der Datenexporteur und der Datenimporteur vereinbaren, dass sie gesamtschuldnerisch für Schäden der betroffenen Personen haften, die durch eine Verletzung im Sinne von Absatz 1 entstehen. Im Falle einer Verletzung dieser Bestimmungen kann die betroffene Person gegen den Datenexporteur oder den Datenimporteur oder beide gerichtlich vorgehen."*

Diese Regelung ist sehr problematisch. Nach ihr haften der Datenimporteur und der Datenexporteur gesamtschuldnerisch für Schäden, die der Datenimporteur verursacht hat. Hat der Datenimporteur eine Schaden zu vertreten, kann sich der Betroffene also aussuchen, gegen wen er seine Ansprüche geltend macht; Datenimporteur und –exporteur sind unabhängig von der Schadensverursachung gleichermaßen gegenüber dem Betroffenen verpflichtet. Erst im Innenverhältnis kann der Datenexporteur beim Datenimporteur Rückgriff nehmen, wenn er gegenüber dem Betroffenen gehaftet hat.

Die Drittbegünstigtenklausel ist im Zusammenhang mit den Haftungsregelungen aus Klausel 6 der Hauptgrund, warum viele Unternehmen in der Vergangenheit nur sehr zurückhaltend die Standardverträge angeschlossen haben. Dies hat auch die EU-Kommission erkannt und in ihrer Entscheidung vom 27.12. 2004 die sogenannten ICC – Standardvertragsklauseln verabschiedet. Diese werden unter 3. behandelt.

### 2.1.3 Klausel 8

Klausel 8 verpflichtet die Parteien, eine Kopie des Vertrages bei der Kontrollstelle (Aufsichtsbehörde) zu hinterlegen, falls diese es verlangt. Dies wird in Deutschland – je nach Bundesland – unterschiedlich gehandhabt. So hat z.B. die Aufsichtsbehörde Baden-Württemberg in ihrem Hinweis Nr. 40 (HIM 40: http://www.im.bwl.de/de/infomaterial/83471.html) folgende Auffassung veröffentlicht:

„Erfolgt die Datenübermittlung in Drittländer auf der Grundlage der im Einzelnen vollständig ergänzten und im Übrigen unveränderten, vertraglich vereinbarten Standardvertragsklauseln der Europäischen Kommission, bedarf die Datenübermittlung keiner zusätzlichen Genehmigung. Es besteht auch grundsätzlich keine Verpflichtung zur Vorlage der Standardvertragsklauseln bei der Aufsichtsbehörde, damit diese überprüfen kann, ob diese auch tatsächlich vollständig und unverändert vereinbart wurden. Dies schließt jedoch nicht aus, dass die Aufsichtsbehörde im Rahmen ihrer Aufsichtstätigkeit nach § 38 BDSG die Vorlage der vereinbarten Standardvertragsklauseln zu Überprüfungszwecken verlangen kann. Dieser Aufforderung muss nachgekommen werden."

Das „Unabhängige Landeszentrum für den Datenschutz Schleswig-Holstein" hingegen fordert die Zusendung einer Kopie des abgeschlossenen Vertrages.

## 2.2 Fazit

Die Standardvertragsklauseln vom Juni 2001 werden bzw. wurden von vielen Unternehmen als problematisch angesehen. Insbesondere die Haftungsregelung ist ein erheblicher Hinderungsgrund, der immer wieder angeführt wurde, wenn in den Unternehmen über den Abschluss der Standardverträge beraten wurde.

## 3. Standardvertragsklauseln vom 27. Dezember 2004 (ICC – Standardvertragsklauseln)

Diese Klauseln können als Alternative zu den vorher genannten Klauseln (Entscheidung vom 15. Juni 2001) verwendet werden. Die Klauseln enthalten Erleichterungen der Haftungsregelungen, gewähren aber gleichzeitig den Datenschutz-Aufsichtsbehörden eine größere Einwirkungsmöglichkeit. Die Regelungen wurden in Zusammenarbeit mit der Internationalen Handelskammer (ICC) und Vertretern der Wirtschaft entwickelt.

Bereits die offizielle Begründung für diese Klauseln zeigt deutlich, dass die Klauseln vom 15. Juni 2001 von den Unternehmen nicht in der beabsichtigten Weise akzeptiert wurden. Auch die Ursache dafür wurde erkannt und in der Ziffer 5 der Begründung aufgeführt:

„(5) Als Alternative zur gesamtschuldnerischen Haftung gemäß der Entscheidung 2001/497/EG beinhaltet der nun vorgelegte Standardvertrag außerdem ein auf die Sorgfaltspflicht abstellendes Haftungssystem, das Datenexporteur und Datenimporteur gegenüber der betroffenen Person für die Verletzung ihrer jeweiligen Vertragspflichten haftbar macht; ebenso ist der Datenexporteur haftbar, wenn er sich nicht im Rahmen des Zumutbaren davon überzeugt, dass der Datenimporteur seine Rechtspflichten aus den Klauseln zu erfüllen in der Lage ist (Auswahlverschulden – culpa in eligendo), in welchem Fall die betroffene Person gerichtlich gegen den Datenexporteur vorgehen kann. Die Durchsetzung von Klausel I Buchstabe b) des neuen Standardvertrags ist in dieser Hinsicht besonders wichtig, vor allem in Hinblick auf das Recht des Datenexporteurs, Prüfungen in den Räumlichkeiten des Datenimporteurs durchzuführen oder Nachweise zu verlangen, dass dieser über genügend Finanzmittel verfügt, um seinen Verpflichtungen nachzukommen."

Hieraus lässt sich ersehen, dass die Kommission zwar den Vertragsparteien mehr Flexibilität einräumt, gleichzeitig aber die Kontrollmöglichkeiten – insbesondere der Aufsichtsbehörden – verstärkt.

### 3.1 Wesentliche Unterschiede der Vertragsklauseln von 2001 und 2004

#### 3.1.1 Erleichterung bei den Haftungsregelungen

Die neuen Klauseln sehen keine gesamtschuldnerische Haftung der Parteien vor. Die Parteien sind nun verpflichtet, vor Abschluss des Vertrages zu prüfen, ob die jeweils andere Partei in der Lage ist, ihre datenschutzrechtlichen Verpflichtungen zu erfüllen. Haben die Parteien gegenseitig ihre Fähigkeit überprüft, die Pflichten aus den Standardvertragsklauseln einzuhalten, haftet jede Partei nur noch für die von ihr selbst zu vertretenden Schäden.

#### 3.1.2 Ausweitung der Eingriffsmöglichkeiten der Datenschutzbehörden

Die Klauseln erweitern die Möglichkeiten der Aufsichtsbehörden sehr weitgehend. Wie allerdings in der Praxis eine Überprüfung durch die Behörden im internationalen Bereich durchgeführt werden soll, ist noch offen. Es ist schwer vorstellbar, dass die zuständige Behörde des Datenexporteurs in das Land des Datenimporteurs reist und dort Kontrollen vornimmt. Von daher sind Befürchtungen, z.B. dass deutsche Aufsichtsbehörden im internationalen Umfeld ständig Kontrollen durchführen, zunächst unbegründet.

#### 3.1.3 Wahlmöglichkeiten des Datenimporteurs bzgl. der Rechtsgrundlage des Verarbeitung

Der Datenimporteur muss gemäß Abschnitt II. h) der Klauseln festlegen, nach welchen Bestimmungen er die Daten verarbeiten wird. Dafür hat er drei Möglichkeiten:

Er verarbeitet die Daten gemäß den Bestimmungen des Landes, in dem der Datenexporteur ansässig ist, also z.B. nach den Anforderungen des BDSG.

Er verarbeitet die Daten gemäß den einschlägigen Bestimmungen etwaiger Kommissionsentscheidungen nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG.

Er verarbeitet die Daten gemäß den Grundsätzen für die Datenverarbeitung in Anhang A der Klauseln. In der Anlage A hat die Kommission Regelungen zu folgenden Punkten erlassen: Zweckbindung, Recht auf Auskunft, Berichtigung, Löschung und Widerspruch, Sensible Daten, Direktmarketing, Automatisierte Entscheidungen

Die Entscheidung, für welche der drei Möglichkeiten sich der Datenimporteur entscheidet, ist im Vertrag zu dokumentieren.

#### 3.1.4 Prüfpflichten

Dem Datenexporteur wird in Ziffer I. b) auferlegt, sich „im Rahmen des Zumutbaren" davon zu überzeugen, dass der Datenimporteur in der Lage ist, seine Pflichten aus den Vertragsklauseln zu erfüllen. Dies kann durchaus bedeuten, dass der Datenexporteur sich vor Ort von der Einhaltung der Anforderungen überzeugt bzw. zumindest vom Datenimporteur eine ausreichende Dokumentation über die getroffenen Sicherheitsmaßnahmen fordert.

### 3.2 Fazit

Da die ursprünglichen Klauseln vom 15. Juni 2001 immer wieder auf Kritik bei den Unternehmen gestoßen sind, ist die Entscheidung der EU Kommission vom 27.12.2004 sehr zu begrüßen.

## 4. Standardvertragsklauseln vom 27. Dezember 2ßß1 für Auftragsdatenverarbeitung

Für das Verhältnis Controller – Processor (Auftragsdatenverarbeitung) hat die EU Kommission am 27. Dezember 2001 eigene Klauseln veröffentlicht. Diese entsprechen im Wesentlichern den Klauseln vom Juni 2001, die das Verhältnis Controller – Controller regeln, sie wurden jedoch in einigen Punkten den speziellen Erfordernissen bei der Auftragsdatenverarbeitung angepasst.

Die wichtigsten Änderungen / Ergänzungen finden sich in:

#### 4.1.1 Klausel 1

Neben den Begriffen „personenbezogene Daten" und „Datenexporteur" und „Datenimporteur" definiert die Klausel 1 auch die Begriffe „anwendbares Datenschutzrecht" und „technische und organisatorische Sicherheitsmaßnahmen". Bezüglich des „anwendbaren Datenschutzrechts" wird festgelegt, dass das Recht des Landes gilt, in dem der Datenexporteur ansässig ist. Unter den „technischen und organisatorischern Sicherheitsmaßnahmen" zählt die Klausel 1 Punkte auf, die vergleichbar mit den Anforderungen der Anlage zu § 9 BDSG sind.

#### 4.1.2 Klausel 3

Die Drittbegünstigtenklausel wurde dahingehend geändert, dass der Betroffene seine Ansprüche gegen den Datenimporteur geltend machen kann, wenn der Datenexporteur „sich tatsächlich aufgelöst hat oder rechtlich nicht mehr besteht". Die Geltendmachung etwaiger Ansprüche gegen den Datenimporteur ist auf diesen Fall beschränkt.

#### 4.1.3 Klausel 4

Die Pflichten des Datenexporteurs sind deutlich umfangreicher als bei den Klauseln „Controller – Controller". So ist z.B. Klausel 4 b das „Gegenstück" zur Weisungsbefugnis des Auftraggebers in § 11 BDSG (Auftragsdatenverarbeitung). Mit dieser Klausel legt sich der Datenexporteur darauf fest, dass er „den Datenexporteur angewiesen hat und während der Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und diesen Klauseln zu verarbeiten (...).". Gemäß Unterpunkt c) hat sich der Datenexporteur davon überzeugt, dass der Datenimporteur bei der Datenverarbeitung ausreichende Garantien in Bezug auf die technischen und

organisatorischen Maßnahmen bietet. Hierzu sind in der Anlage 2 zu den Klauseln die getroffenen Maßnahmen detailliert aufzuführen und von beiden Parteien zu unterzeichnen.

Unterpunkt d) der Klausel 4 bezieht sich auf Unterpunkt c) und gibt den Rahmen für die Sicherheitsbedingungen vor. Diese entsprechen ungefähr der Anlage zum § 9 BDSG.

#### 4.1.4 Klausel 5

Klausel 5 beinhaltet die Pflichten des Datenimporteurs. Im Unterpunkt a) verpflichtet sich der Datenimporteur, die Daten nur gemäß den Weisungen des Datenexporteurs zu verarbeiten. Als weitere Pflicht des Datenimporteurs wird in Klausel 5 c) angeführt, dass der Datenimporteur verpflichtet ist, die in der Anlage 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen bereits vor der Verarbeitung zu ergreifen.

#### 4.1.5 Klausel 6

Klausel 6 ist eine Haftungsklausel, die sich deutlich von der Haftungsklausel in den Standardverträgen „Controller Controller“ unterscheidet. Absatz 1 bestimmt, dass der Betroffene einen möglichen Schadensersatz beim Datenexporteur geltend machen kann – ein wesentlicher Unterschied zur gesamtschuldnerischen Haftung der Standardverträge vom Juni 2001.

Schadensersatzansprüche gegen den Datenimporteur sind auch möglich. Das setzt allerdings voraus, dass sich „der Datenexporteur tatsächlich aufgelöst hat oder rechtlich aufgehört hat zu bestehen oder zahlungsunfähig geworden ist“. Schadensersatzforderungen gegen den Datenimporteur sind also nur dann möglich, wenn der Datenexporteur als Unternehmen nicht mehr existiert. Obwohl dieser Fall sicherlich nicht sehr häufig ist, ist diese Regelung jedoch einer der Gründe dafür, dass die Unternehmen die Klauseln ablehnen und nur dann abschließen, wenn sich keine der anderen Möglichkeiten anwenden lässt. Dies betrifft insbesondere amerikanische Unternehmen, die die dort üblichen, teilweise ruinösen Schadensersatzprozesse fürchten.

Wenn eine Partei für einen Verstoß gegen die Datenschutzbestimmungen bzw. die Klauseln haftbar gemacht wird, obwohl der Pflichtverstoß tatsächlich durch die andere Partei begangen wurde, hat gemäß Klausel 6 die verursachende Partei der anderen Partei alle hierbei entstandenen Kosten, Schäden, Ausgaben und Verluste zu ersetzen. Die Höhe der Entschädigung ist jedoch davon abhängig, dass im Falle einer Entschädigungsforderung (Schadensersatz) der Datenexporteur sofort den Datenimporteur entsprechend unterrichtet. Außerdem sind beide Parteien zur Zusammenarbeit verpflichtet, um im Streifall gemeinsam eine Einigung mit dem Betroffenen zu erreichen.

#### 4.1.6 Klausel 8

Mit Absatz 2 von Klausel 8 vereinbaren die Parteien, dass die für den Datenexporteur zuständige Kontrollstelle berechtigt ist, beim Datenimporteur die gleichen Kontrollen durchzuführen, wie beim Datenexporteur. Dies gilt damit auch für anlassunabhängige Kontrollen.

Vor allem US-Unternehmen sind häufig nicht bereit, diese Regelungen zu akzeptieren. Sie scheinen unangekündigte Kontrollen und daraus resultierende überzogene Forderungen der Aufsichtsbehörde zu fürchten.

Aber schon angesichts der Kostenfrage muss der Datenimporteur im Drittstaat – ähnlich wie bei den ICC Klauseln – nicht befürchten, mit (ständigen) Kontrollen der Aufsichtsbehörde konfrontiert zu werden. Es sollte deshalb sorgfältig abgewogen werden, ob die Klausel 8 wirklich einen Hinderungsgrund für den Abschluss der Standardverträge darstellt.

Zu einer Prüfung beim Datenimporteur könnte es wohl höchstens dann kommen, wenn die Behörde feststellt, dass es der Datenexporteur ablehnt oder nicht in der Lage ist, dem Datenimporteur angemessene Anweisungen zu erteilen. Insbesondere im Falle eines Verstoßes wird die Behörde aber immer zuerst den Datenexporteur

auffordern, die Ursache festzustellen und zu beseitigen, bevor sie sich direkt an den Datenimporteur wenden wird.

### 4.2 Fazit:

Wie die Standardvertragsklauseln vom Juni 2001 werden die Standardvertragsklauseln vom Dezember 2001 für das Vertragsverhältnis Controller – Processor von vielen Unternehmen als problematisch angesehen. Hauptsächlich sind es die Haftungsregelungen in den Standardverträgen, die zu diesen Akzeptanzproblemen führen. Die Unternehmen wollen sich vielfach nicht der Gefahr von Schadensersatzprozessen mit extrem hohen Summen – z.B. nach US-Recht – aussetzen (Sammelklagen, exorbitante Schadensersatzsummen).

## 5. Zusammenfassung

Neben der persönlichen Einwilligung stellen die Standardverträge sicherlich die „einfachste“ Möglichkeit dar, personenbezogene Daten in ein nicht sicheres Drittland transferieren zu dürfen. Es muss jedoch darauf geachtet werden, dass der jeweils einschlägige Vertrag gewählt wird.

# V Weiterführende Links und Literatur

Code of Conduct von DaimlerChrysler

www.daimlerchrysler.com/Projects/c2c/channel/documents/184264_coc_itr_g.pdf

Bindende Unternehmensrichtlinie der Siemens AG

http://w1.siemens.com/about/pool/de/datenschutz-guidelines.pdf

Code of Conduct der MTU

www.mtu.de/channel/files/30753deutsch_CodeofConduct_neu.pdf

Virtuelles Datenschutzbüro

www.datenschutz.de

V.Backes/H.Eul/M. Guthmann/R. Martwich/M. Schmidt in RDV 2004 S. 156: „Entscheidungshilfe für die Übermittlung personenbezogener Daten in Drittländer“

Hinweis zum Datenschutz Nr. 39 des Innenministeriums Baden-Württemberg, Staatsanzeiger Baden-Württemberg Nr. 2 vom 24.01.2000 S. 12

Christoph Kuner / Jörg Hladjk in RDV 2005 S. 193 ff „Die alternativen Standardvertragklauseln der EU für internationale Datenübermittlungen“

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.100 Unternehmen, davon 850 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org