Gelbe Erläuterungsbücher

BDSG Bundesdatenschutzgesetz

Kommentar

von

Prof. Dr. Peter Gola, Christoph Klug, Dr. Rudolf Schomerus, Barbara Körffer

10., überarbeitete und ergänzte Auflage

BDSG Bundesdatenschutzgesetz – Gola / Klug / Schomerus / et al.

schnell und portofrei erhältlich bei beck-shop.de DIE FACHBUCHHANDLUNG

Thematische Gliederung:

Datenschutz- und Melderecht

Verlag C.H. Beck München 2010

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 59834 0

beck-shop.de

Büllesbach, Achim, Transnationalität und Datenschutz – Die Verbindlichkeit von Unternehmensregelungen, Diss., 2008; *Conrad,* Transfer von Mitarbeiterdaten zwischen verbundenen Unternehmen, ITRB 2005, 164; *Däubler,* Grenzüberschreitender Datenschutz – Handlungsmöglichkeiten des Betriebsrats, RDV 1998, 96; *ders.,* Übermittlung von Arbeitnehmerdaten ins Ausland, in: *Büllesbach* (Hrsg.), Datenverkehr ohne Datenschutz, S. 7; *Dammann,* Internationaler Datenschutz, RDV 2002, 70; *Dammann/Simitis,* EG-Datenschutzrichtlinie (1997), Art. 25, 26; *Dix/Gardain,* Datenexport in Drittstaaten, DuD 2006, 343; *Draf,* Die Regelung der Übermittlung personenbezogener Daten in Drittländer nach Art. 25, 26 der EG-Datenschutzrichtlinie, Diss., 1999; *Duhr/Naujok/Peter/Seiffert,* Neues Datenschutzrecht für die Wirtschaft, DuD 2002, 5 (14); *Ehmann/Helfrich,* EG-Datenschutzrichtlinie, 1999, Art. 25, 26; *Ehricke/Becker/Walzel,* Übermittlung von Fluggastdaten in die USA, RDV 2006, 149; *Ellger,* Der Datenschutz im grenzüberschreitenden Datenverkehr, 1990; *Eul/Godefroid,* Übermittlung personenbezogener Daten ins Ausland nach Ablauf der Umsetzungsfrist der EG-Datenschutzrichtlinie, RDV 1998, 185; *Gackenholz,* Datenübermittlungen ins Ausland unter besonderer Berücksichtigung internationaler Konzerne, DuD 2000, 727; *Giesen,* Datenverarbeitung im Auftrag in Drittstaaten – eine misslungene Gesetzgebung, CR 2007, 543; *ders.,* Die Kontrolle des Datenverkehrs mit Drittländern – Modelle und Grenzen, DuD 1996, 394; *Grapentin,* Datenschutz und Globalisierung – Binding Corporate Rules als Lösung?, CR 2009, 693; *Hanloser,* e-discovery – Datenschutzrechtliche Probleme und Lösungen, DuD 2008, 785; *Hartmann,* Konzernweiter Kundendatenschutz – mit oder ohne Codes of Conduct (CoC)?, DuD 2008, 455; *Heil,* Safe Harbor – Ein Zwischenstandsbericht, DuD 2000, 444; *ders.,* Europäische Herausforderung – Transatlantische Debatte, DuD 1999, 458; *Hillenbrand-Beck,* Aktuelle Fragestellungen des internationalen Datenverkehrs, RDV 2008, 231; *Kübler,* Die Säulen der Union: Einheitliche Grundrechte?, 2002; *Klug,* Persönlichkeitsschutz beim Datentransfer in die USA – Die Safe-Harbor-Lösung, RDV 2000, 212; *ders.,* Globaler Arbeitnehmerdatenschutz – Ausstrahlungswirkung der EG-Datenschutzrichtlinie auf Drittländer am Beispiel der USA, RDV 1999, 109; *Kuner,* European Data Privacy Law and Online Business, 2007; *Kuner/Hladjk,* Die alternativen Standardvertragsklauseln der EU für internationale Datenübermittlungen, RDV 2005, 193; *Lambrich/Cahlik,* Austausch von Arbeitnehmerdaten im multinationalen Konzern – Datenschutz- und betriebsverfassungsrechtliche Rahmenbedingungen, RDV 2002, 287; *Lejeune,* Datentransfer in das außereuropäische Ausland, ITRB 2005, 94; *Martin,* Kunden- und Mitarbeiterdaten im weltweiten Fluss, DuD 2007, 126; *Moritz/Tinnefeld,* Der Datenschutz im Zeichen einer wachsenden Selbstregulierung, JurPC Web-Dok. 181/2003; *Palm,* Die Übermittlung personenbezogener Daten in das Ausland, CR 1998, 65; *Rath/Klug,* e-Discovery in Germany?, K&R 2008, 596; *Räther,* Die EU-US-Flugdaten-Affäre, DuD 2004, 468; *Räther/Seitz,* Übermittlung personenbezogener Daten in Drittländer, MMR 2002, 425; *dies.,* Ausnahmen bei Datentransfer in Drittländer – Die beiden Ausnahmen nach § 4 c Abs. 2 BDSG, MMR 2002, 520; *Riemann,* Künftige Regelungen des grenzüberschreitenden Datenverkehrs, CR 1997, 762; *Rittweger/Weiße,* Unternehmensrichtlinien für den Datenschutz in Drittländern, CR 2003, 142; *ders./Saltzman,* Germany takes the lead on binding corporate rules, Privacy Laws Business International Newsletter, Issue 70 (Oct./Nov. 2003), 28; *ders./Schmidl,* Einwirkung von Standardvertragsklauseln auf § 28 BDSG, DuD 2004, 617; *Runte/Schreiber/Held/Bond/Dana/Flower,* Anonymous Hotlines for Whistleblowers, CRi 2005, 135; *Ruppmann,* Der konzerninterne Austausch personenbezogener Daten, Diss., 1998/99; *Scheja,* Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank, Diss., 2005; *Schmidl,* Datenschutzrechtliche Anforderungen an innereuropäische Personaldatenübermittlungen in Matrixorganisationen, DuD 2009, 364; *ders.,* Die Whistleblowing-Stellungnahme der Artikel-29-Gruppe, DuD 2008, 414; *ders.,* Datenschutz für Whistleblowing Hotlines, DuD 2006, 353; *Schröder,* Verbindliche Unternehmensregelungen, DuD 2004, 462; *ders.,* Der Zugriff der USA auf Daten europäischer Flugpassagiere – Neue Gefahren durch Passagier-Profilbildung? (CAPPS II), RDV 2003, 285; *Simitis,* Übermittlung der Daten von Flugpassagieren in die USA – Dispens von Datenschutz?, NJW 2006, 2011; *ders.,* Der Transfer von Daten in Drittländer – ein Streit ohne Ende?, CR 2000, 472; *Taraschka,* „Auslandsübermittlung" personenbezogener Daten im Internet, CR 2004, 280; *Tinnefeld/Rauhofer,* Whistleblower: Verantwortungsbewusste Mitarbeiter oder Denunzianten?, DuD 2008, 717; *Wedde,* Weltweite Datenübertragung – Arbeitnehmerdaten ins Ausland?, AiB 2007, 80; *Weniger,* Grenzüberschreitende Datenübermittlungen international tätiger Unternehmen, Diss., 2004; *Wisskirchen,* Grenzüberschreitender Verkehr von Arbeitnehmerdaten, CR 2004, 862; *Wuermeling,* Handelshemmnis Datenschutz – Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Diss., 2000; *von Zimmermann,* Whistleblowing und Datenschutz, RDV 2006, 242; *ders.,* Whistleblowing, Anforderungen des Sarbanes-Oxley-Acts, WM 2007, 1060.

beck-shop.de

Übersicht

	Rn.
1. Allgemeines	1
2. Ungehinderter Datenfluss innerhalb der EU/des EWR	2
3. Grundsätzliches Übermittlungsverbot bei entgegenstehenden Interessen des Betroffenen	6
4. Die Angemessenheit des Datenschutzniveaus	10
5. Feststellung der Angemessenheit durch die EU-Kommission	14
6. Unterrichtung der Betroffenen	17
7. Verantwortung für die Zulässigkeit der Übermittlung	18
8. Hinweispflicht gegenüber dem Empfänger	19
9. Landesrecht	21

1. Allgemeines

1 § 4 b regelt im Fall seiner Anwendbarkeit (vgl. hierzu § 1 Rn. 27 ff. und 22 ff.) die Übermittlung personenbezogener Daten durch **öffentliche** und **nicht öffentliche Stellen** ins Ausland und zwar sowohl in Länder innerhalb als auch außerhalb der EU/des EWR (vgl. Übersicht des Innenministeriums Baden-Württemberg, Hinweise zum BDSG für die Privatwirtschaft Nr. 39, A. – Staatsanzeiger für Baden-Württemberg Nr. 2 v. 24. 1. 2000, 12). Bei Übermittlungen innerhalb der EU/des EWR wird unterschieden zwischen Verarbeitungen, die von der EU-Datenschutzrichtlinie erfasst sind (Abs. 1), und solchen, für die weiterhin ausschließlich nationales Recht gilt. Diese bislang außerhalb des Anwendungsbereichs der EU-Richtlinie (sog. 2. bzw. 3. Säule des EU-Vertrages, s. Art. 3 Abs. 2 Spiegelstrich 1 EU-DatSchRL; zum bisherigen Drei-Säulen-Konzept vgl. Bergmann/Möhrle/Herb, Datenschutzrecht, § 4 b Rn. 3) stattfindenden EU-internen Verarbeitungen, betroffen sind im Wesentlichen die Sicherheits- und Strafverfolgungsbehörden, werden in Absatz 2 wie Übermittlungen in nicht der EU bzw. dem EWR angehörige Länder (sog. Drittstaaten) behandelt. In diesen Fällen ist im Rahmen der Zulässigkeitsprüfung nach den Erlaubnisnormen des BDSG ein besonderes Augenmerk auf das Datenschutzniveau beim Datenempfänger zu richten, es sei denn, dass eine Ausnahme nach § 4 c vorliegt. Der am 1. 12. 2009 in Kraft getretene Vertrag von Lissabon hat nicht nur ein europäisches Grundrecht auf Datenschutz (Art. 8 der EU-Grundrechte-Charta, ABl. EU vom 14. 12. 2007, Nr. C 303/1) mit sich gebracht, sondern auch zu einer weitgehenden Auflösung des Drei-Säulen-Konzepts geführt. Letzteres wird gegebenenfalls auch eine Anpassung der Anwendungsbereiche der EU-DatSchRL bzw. der §§ 4 b, 4 c nach sich ziehen (zur Lage nach Inkrafttreten des Lissabon-Vertrags vgl. Ronellenfisch, DuD 2009, 451 (460)). Bislang bestehende Abgrenzungsschwierigkeiten in diesem Bereich (vgl. EuGH, NJW 2006, 2029 – Flugpassagierdaten; EuGH, NJW 2009, 1801 – Vorratsdatenspeicherung; vgl. ferner Ehricke/Becker/Walzel, RDV 2006, 149; Simitis, NJW 2006, 2011; Räther, DuD 2004, 468; Schröder, RDV 2003, 285) könnten sich durch die Auflösung des Drei-Säulen-Konzepts langfristig relativieren. Zudem werden zukünftig die gestärkten Kompetenzen bzw. Mitentscheidungsbefugnisse des Europäischen Parlaments im Rahmen des Abschlusses internationaler Übermittlungsabkommen zunehmend ins Gewicht fallen, was sich bereits an der Notwendigkeit der Nachverhandlung des sog. SWIFT-Abkommens mit den USA hinsichtlich der Übermittlung von Geldüberweisungsdaten manifestiert hat.

2. Ungehinderter Datenfluss innerhalb der EU/des EWR

2 **2.1** Wie der vollständige Titel der EU-DatSchRL schon zum Ausdruck bringt, will sie einerseits **Persönlichkeitsrechtsschutz** und andererseits **freien Datenver-**

beck-shop.de

kehr gewährleisten. Aufgrund des durch die Richtlinie innerhalb der EU harmonisierten Datenschutzes verbietet es Art. 1 Abs. 2 EU-DatSchRL den Mitgliedstaaten, den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten aus Gründen des Datenschutzes zu beschränken oder zu untersagen. Nach dem Ersten Kommissionsbericht (KOM (2003) 265 endg.) haben alle zehn Länder, die der EU zum 1. 5. 2004 beigetreten sind, Datenschutzgesetze erlassen (Fundstellen in RDV 2004, 88). Sie nehmen an den Sitzungen der Art. 29-Gruppe und des Ausschusses nach Art. 31 der Richtlinie teil. Die EWR-Vertragsstaaten Norwegen, Island und Liechtenstein haben die Richtlinie übernommen und partizipieren ebenfalls am freien Datenverkehr.

2.2 Die **Zulässigkeit** der Datenübermittlung ist also im Anwendungsbereich der Richtlinie gemäß **Absatz 1** allein geknüpft an die – auch für Übermittlungen im Inland geltenden – das Verbotsprinzip durchbrechenden Erlaubnistatbestände. Sofern keine spezielleren Erlaubnisse oder Verbote bestehen (vgl. z. B. § 77 SGB X – hierzu Steinbach, NZS 2002, 21; § 92 TKG gilt nur für die Übermittlung an nicht öffentliche Stellen und verweist auf die Zulässigkeitsvoraussetzungen des BDSG) und der Betroffene nicht eingewilligt hat (zu den Voraussetzungen einer wirksamen Einwilligung beim Drittlandtransfer vgl. § 4 c Rn. 5), greifen die Übermittlungstatbestände des zweiten bzw. dritten Abschnitts des BDSG (§§ 15 Abs. 1, 16 Abs. 1 bzw. §§ 28–30 a; die unterbliebene Verweisung auf § 32 dürfte auf einem Versehen des Gesetzgebers beruhen). Dies gilt auch für Übermittlungen an Organe und Einrichtungen der Europäischen Gemeinschaft (zu diesen vgl. Gola/Klug, Grundzüge des Datenschutzrechts, S. 28). **3**

2.3 Im Falle automatisierter Übermittlung von Mitarbeiterdaten ist nach § 87 Abs. 1 Nr. 6 BetrVG regelmäßig die **Mitbestimmung** des Betriebsrats geboten. Als vorrangige Erlaubnisvorschrift i. S. v. § 4 Abs. 1 werden Betriebsvereinbarungen aber nur insoweit in Betracht kommen, als sie auch den Datenempfänger rechtlich zu binden vermögen. Empfohlen wird diesbezüglich, die Betriebsvereinbarung in Vertragsklauseln oder verbindlichen Unternehmensregelungen (s. hierzu § 4 c Rn. 10 ff.) für verbindlich zu erklären (BlnDSB, Jahresbericht 2002, Ziff. 4.7.3). **4**

2.4 Aufgrund der durch die EU-DatSchRL bewirkten Harmonisierung gilt auch hinsichtlich der Übergabe personenbezogener Daten an einen **Auftragsdatenverarbeiter** im **EU/EWR-Bereich** das Prinzip der Gleichbehandlung mit der inländischen Situation (§ 3 Abs. 8 Satz 3), so dass keine durch eine Erlaubnisnorm zu rechtfertigende Datenübermittlung an Dritte vorliegt (zur internationalen Auftragsdatenverarbeitung vgl. auch BlnDSB, Jahresbericht 2003, Ziff. 4.7.2). Für den Fall, dass der Auftragnehmer seinen Sitz in einem **Drittstaat** hat, wird die Auffassung vertreten, dass die Privilegierung des § 11 BDSG nicht greift und daher stets von einer Datenübermittlung auszugehen ist (vgl. z. B. Wedde in: DKWW, BDSG, § 11 Rn. 20; Dammann, RDV 2002, 70, 73; 15. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörde, LT-Drs. 15/4659, Ziff. 7.1; a. A. Müthlein/Heck, Outsourcing und Datenschutz, 2006, S. 73 ff.; vgl. auch Nielen/Thum, K & R 2006, 171; zur Anwendbarkeit des § 11 bei der Auftragsvergabe in Drittländer s. auch § 11 Rn. 16). Eigens für diese Konstellation hat die EU-Kommission Standardvertragsklauseln anerkannt (vgl. § 4 c Rn. 13). Auch sofern im Rahmen von sog. Cloud Computing personenbezogene Daten weltweit verteilt bearbeitet und abgelegt werden, sind die BDSG-Anforderungen an den Drittlandtransfer zu beachten (vgl. auch § 11 Rn. 8). Bei der Rückübertragung der Daten an einen Auftraggeber im Drittland gelten die §§ 4 b, 4 c nicht (vgl. § 11 Rn. 16 a). **5**

beck-shop.de

3. Grundsätzliches Übermittlungsverbot bei entgegenstehenden Interessen des Betroffenen

6 **3.1** Bei Datenflüssen innerhalb der EU/des EWR können sich entgegenstehende Interessen von Betroffenen aufgrund einer Interessenabwägung nach § 28 ergeben. Datenübermittlungen in Drittstatten dürfen gemäß **§ 4 b Abs. 2** nur stattfinden, wenn der Betroffene kein **schutzwürdiges Interesse** an dem Ausschluss der Übermittlung hat. Mit Blick auf den **Drittlandtransfer** bemerkenswert ist eine zutreffend kritisierte Entscheidung des EuGH (EuZW 2004, 245 = MMR 2004, 95 = DuD 2004, 244 = RDV 2004, 16, m. krit. Anm. Dammann; ferner CRi 1/2004 m. krit. Anm. Retzer/Ritter; ebenfalls krit. Brühann, DuD 2004, 201; ferner Taraschka, CR 2004, 280) im Rahmen derer das Gericht in der Speicherung personenbezogener Daten auf einer frei zugänglichen Website keine Datenübermittlung in Drittstaaten sah, solange der Hostprovider in einem EU-Mitgliedstaat ansässig ist (zur Anwendbarkeit des BDSG bei auslandsgesteuertem Rückgriff auf in Deutschland belegene Mittel wie z. B. Server, Modems, Leitungen etc. vgl. Duhr/Naujok/Peter/Seiffert, DuD 2002, 5, 7 sowie BlnDSB, Neuregelungen im Bundesdatenschutzgesetz, Materialien zum Datenschutz Nr. 30, Ziff. 3.1).

7 **3.2** Ein entgegenstehendes schutzwürdiges Interesse ist z. B. regelmäßig anzunehmen, wenn bei den empfangenden Stellen ein **angemessenes Datenschutzniveau** nicht gegeben ist. Zu beachten ist insofern jedoch, dass § 4 c als Ausnahmevorschrift unter bestimmten Voraussetzungen auch Übermittlungen an Stellen ohne angemessenes Schutzniveau gestattet. Anders als die EU-DatSchRL, die eine Angemessenheit im **Drittland** voraussetzt, verlangt Abs. 2 Satz 2 lediglich ein angemessenes Schutzniveau bei der empfangenden **Stelle** (vgl. hierzu Gola/Klug, Grundzüge des Datenschutzrechts, S. 63; Backes/Eul/Guthmann/Martwich/Schmidt, RDV 2004, 156). Diesbezüglich wird teilweise (vgl. Moritz/Tinnefeld, JurPC Web-Dok. 181/2003, Abs. 13; Rittweger/Weiße, CR 2003, 142, 147) eine mangelhafte Richtlinienumsetzung moniert.

8 **3.3** Neben dem Schutzniveau beim Datenimporteur können auch **andere** schutzwürdige **Interessen** des Betroffenen einer Datenübermittlung in Drittländer entgegenstehen. Insofern handelt es sich um voneinander unabhängige Tatbestandsmerkmale. Solche Interessen kommen insbesondere bei gefahrenträchtigen Datenübermittlungen in Betracht. Für die Übermittlung von sensiblen Daten gem. § 3 Abs. 9 gelten die restriktive Voraussetzungen nach den §§ 13 Abs. 2, 28 Abs. 6–9 (vgl. Simitis in: Simitis (Hrsg.), BDSG § 4 b Rn. 50). Soll die **Gehaltsabrechnung** durch einen Dienstleister im Drittland erfolgen, so müssten – soweit man die Privilegierung des § 11 hier nicht gelten lassen will (vgl. vorstehend Rn. 5) – auch sensitive Daten nach § 3 Abs. 9 (z. B. Krankheitszeiten, Religionszugehörigkeit) übermittelt werden. Der hiermit verbundene Datentransfer lässt sich ohne Einwilligung der Mitarbeiter allenfalls über eine weite Auslegung von § 28 Abs. 6 Nr. 3 rechtfertigen (vgl. etwa Rittweger/Schmidl, DuD 2004, 617, 620). Als rechtliche Anknüpfungspunkte kommen insofern die Gewerbefreiheit (vgl. BlnDSB Materialien zum Datenschutz Nr. 30, Ziff. 4.4) oder die Lohnzahlungspflicht des Arbeitgebers in Betracht. Im internationalen Unternehmensverbund spielt der grenzüberschreitende Transfer von **Mitarbeiterdaten** eine zunehmend wichtige Rolle. Ist der Konzernbezug bei Abschluss der Arbeitsvertrages erkennbar, so ist die Datenübermittlung an ein Verbundunternehmen im Ausland regelmäßig gem. § 32 Abs. 1 Satz 1 zulässig. Die Erstellung eines konzernweit verfügbaren elektronischen **Kommunikationsverzeichnisses** mit Namen der Mitarbeiter, dienstlicher Anschrift, Aufgabengebiet, dienstlicher Telefon- und Faxnummer sowie dienstlicher E-Mail-Adresse im Interesse einer reibungslosen konzerninternen Kommunikation wurde bislang weitgehend als zulässig angesehen, wobei im Einzelfall eine Zugriffs-

beck-shop.de

beschränkung auf Teile des Verzeichnisses geboten sein kann (vgl. 15. Bericht der Hessischen Landesregierung über die Tätigkeit der für den nicht öffentlichen Bereich zuständigen Aufsichtsbehörden – LT-Drs. 15/4659 vom 26. 11. 2002 –, Ziff. 7.4). International tätige Unternehmen realisieren zunehmend konzernübergreifende **Skill-Datenbanken,** um die Stellen im Konzern bestmöglich besetzen zu können. Die damit einhergehende Datenübermittlung kann nach § 32 Abs. 1 Satz 1 oder § 28 Abs. 1 Satz 1 Nr. 2 gerechtfertigt sein. Den schutzwürdigen Belangen der betroffenen Mitarbeiter kann durch die Einräumung eines Widerspruchsrechts Rechnung getragen werden (zur Einrichtung globaler Personalinformationssysteme vgl. den 13. Bericht der für den Datenschutz im nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden – LT-Drs. 15/1539 –, Ziff. 10.2 sowie HmbDSB, 18. Tätigkeitsbericht, 2000/2001, Ziff. 28.1). Bei sog. **Matrixstrukturen** arbeiten Mitarbeiter häufig abwechselnd an verschiedenen Stellen im Konzern, was sich u. a. auch in der Vorgesetztenstruktur widerspiegelt. Die damit einhergehenden Datenflüsse sind bei entsprechender Transparenz für den Mitarbeiter in der Regel über § 32 Abs. 1 Satz 1 oder ggf. auf Grundlage eines Datenschutzvertrags (hierzu Schmidl, DuD 2009, 364) gerechtfertigt. Ansonsten kann die Übermittlung auch auf Grundlage einer Interessenabwägung nach § 28 Abs. 1 Satz 1 Nr. 2 zulässig sein. Im Rahmen der Erfüllung allgemeiner Compliancevorgaben (z. B. Sarbanes Oxley Act, Corporate Governance Codex) entstehen unternehmensübergreifende Reportingstrukturen, über welche personenbezogene Informationen über die Verletzung gesetzlicher oder betrieblicher Vorgaben erfasst, unter Beteiligung der Konzernrevisions- und/oder Konzernsicherheitsabteilung zentral aufgeklärt und zentralen Entscheidungsstellen (Compliance Officer, Clearing Committee, Konzernvorstand) zugeleitet werden (zum sog. Whistleblowing vgl. Tinnefeld/Rauhofer, DuD 2008, 717; Breinlinger/Krader, RDV 2006, 60; von Zimmermann, RDV 2006, 242 sowie Schmidl, DuD 2006, 353). Als rechtliche Grundlagen kommen § 32 Abs. 1 Sätze 1 und 2, § 28 Abs. 1 Satz 1 Nr. 2 oder § 28 Abs. 2 in Betracht.

3.4 Für öffentliche Stellen des Bundes enthält Abs. 2 Satz 3 Ausnahmen von dem Übermittlungsverbot. Erlaubt sind danach Übermittlungen, die aus zwingenden Gründen der **Verteidigung** erfolgen. Ferner dürfen Übermittlungen stattfinden, wenn sie zur Erfüllung über- und zwischenstaatlicher Verpflichtungen im Bereich der **Krisenbewältigung** bzw. der **Konfliktverhinderung** oder für **humanitäre Hilfsmaßnahmen** erforderlich sind. **9**

4. Die Angemessenheit des Datenschutzniveaus

4.1 In **Absatz 3** wurden die in Art. 25 Abs. 2 EU-DatSchRL zur Beurteilung eines angemessenen Datenschutzniveaus beispielhaft vorgegebenen Kriterien fast wörtlich übernommen. Herangezogen werden können insbesondere: **10**

- die Art der Daten,
- die Zweckbestimmung,
- die Dauer der geplanten Verarbeitung,
- das Herkunfts- und das Endbestimmungsland,
- die für den Empfänger geltenden Rechtsnormen und Standesregeln sowie
- Maßnahmen der Datensicherheit.

4.2 Maßgebend für die Beurteilung des angemessenen Schutzniveaus sind aber **alle Umstände** der konkret in Aussicht genommenen Übermittlung. Wegen der Verwendung des wertausfüllungsbedürftigen Angemessenheitsbegriffs ermöglichen die Richtlinie und das BDSG eine Beurteilung von Fall zu Fall, wobei der Grad der Persönlichkeitsrechtsgefährdung als Maßstab dient. Die Risiken für den Betroffenen sind umso größer, je sensibler die Daten sind, je weiter die Zweckbestimmung **11**

beck-shop.de

gefasst wird, je länger der Verarbeitungszeitraum ist, je mehr Zwischenstationen zwischen dem Herkunfts- und dem Endbestimmungsland vorgesehen sind, je weniger Schutzgarantien die Datenschutzgesetze – soweit solche überhaupt vorhanden sind – und sonstigen Normen im Empfängerland bieten und je weniger Maßnahmen der Datensicherheit vom Datenimporteur getroffen werden. Grundlegende Bedeutung wird dem Arbeitspapier WP 12 der Datenschutzgruppe nach Art. 29 EU-DatSchRL beigemessen (GD XV D/5025/98, v. 24. 7. 1998). Darin wird u. a. festgestellt, dass jede sinnvolle Analyse des angemessenen Datenschutzniveaus zwei Grundelemente berücksichtigen muss, den Inhalt der im Drittland geltenden Vorschriften und die Mittel zur Sicherung ihrer wirksamen Anwendung (zur Beurteilungszuständigkeit s. Rn. 18).

12 **4.3** Entspricht das Schutzniveau beim Empfänger aufgrund der für den konkreten Fall geltenden **Datenschutznormen** in Deutschland geltendem Datenschutzrecht, so erleidet der Betroffene durch die Übermittlung in den Drittstaat keine Einbußen hinsichtlich seiner Datenschutzposition. Die Rechte des Betroffenen können ggf. auch durch verbindliche und beachtete **berufsständische Regeln** gewahrt sein. Angemessenheit bedeutet aber **nicht Gleichwertigkeit** (ebenso Däubler in: DKWW, BDSG, § 4 b Rn. 12). Das Schutzniveau im Drittland ist dann als angemessen anzusehen, wenn der betroffenen Person dort in Bezug auf die Verarbeitung ihrer Daten ein Schutz zuteil wird, der dem Kernbestand der Schutzprinzipien der EU-DatSchRL im Wesentlichen gerecht wird. Abstriche bei einzelnen Schutzinstrumenten sind ebenso möglich, wie eine gewisse Minderung des Schutzniveaus im Ganzen (vgl. Dammann in: Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 25 Erl. 8, a. A. Simitis in: Simitis (Hrsg.), BDSG, § 4 b Rn. 52).

13 **4.4** Ins Kalkül zu ziehen ist ferner die **Art der Daten,** die zur Übermittlung anstehen, wobei von besonderer Relevanz ist, ob auch besondere Arten von Daten nach § 3 Abs. 9 – hier müssen primär die restriktiven Zulässigkeitsvoraussetzungen der §§ 13 Abs. 2, 28 Abs. 6–9 vorliegen – betroffen sind, und wie hoch die Gefährdung von Persönlichkeitsrechten einzuschätzen ist. Ferner sind die **Zweckbestimmung** und die **Dauer** der geplanten Verarbeitung zu betrachten. Die Zweckbestimmung ist Grundlage der Abwägung des potenziellen Gefährdungsgrads der Betroffenenrechte. Schließlich ist der Kreis derjenigen, die die Daten zur Kenntnis erhalten im Sinne eines angemessenen Schutzes zu begrenzen. Zu den Verwendungsrestriktionen, die unter Angemessenheitsgesichtspunkten eine wichtige Rolle spielen, gehören daher auch die **Weiterübermittlung** sowie **Datensicherheitsmaßnahmen** zur Wahrung der Vertraulichkeit.

5. Feststellung der Angemessenheit durch die EU-Kommission

14 **5.1** Nach Art. 25 Abs. 6 EU-DatSchRL kann die Kommission im Rahmen des in Art. 31 Abs. 2 EU-DatSchRL geregelten Verfahrens für die Mitgliedstaaten verbindlich feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Datenschutzniveau aufweist. Bei Redaktionsschluss waren entsprechende Angemessenheitsentscheidungen für folgende Länder getroffen worden:

- Argentinien (ABl. EG v. 5. 7. 2003, Nr. L 168/19),
- Australien, Sonderfall PNR-Daten (ABl. EG v. 8. 8. 2008, Nr. L 213/47),
- Guernsey (ABl. EG v. 25. 11. 2003, Nr. L 308/27),
- Isle of Man (ABl. EG v. 30. 4. 2004, Nr. L 151/51 sowie Berichtigung in ABl. EG v. 10. 6. 2004, Nr. L 208/47),
- Jersey (ABl. EG v. 28. 5. 2008, Nr. L 138/21),
- Kanada (ABl. EG v. 4. 1. 2000. Nr. L 2/13), Sonderfall PNR-Daten (ABl. EG v. 29. 3. 2006, Nr. L 91/49),

beck-shop.de

– Schweiz (ABl. EG v. 25. 8. 2000, Nr. L 215/1),
– USA: *Sonderfall Safe Harbor* (ABl. EG v. 25. 8. 2000, Nr. L 215/7; s. hierzu nachstehend Anm. 5.2); Sonderfall PNR-Daten (ABl. EG v. 4. 8. 2007, Nr. L 204/16).

Vorbehaltlich des Vorliegens der Übermittlungsvoraussetzungen nach dem BDSG können Übermittlungen an in diesen Ländern ansässige Empfänger ohne eine gesonderte Überprüfung der Angemessenheit des Schutzniveaus erfolgen. Im Fall der Übermittlung in die USA bedarf es jedoch der zuvorigen Überprüfung, ob und inwieweit der Datenempfänger dem Safe Harbor angehört (Safe Harbor List unter http://www.export.gov/safeharbor; s. auch Rn. 15). Nachdem der EuGH das Abkommen zur Übermittlung sog. **Passenger Name Records** (PNR) in die USA für nichtig erklärt hatte (vgl. NJW 2006, 2029; ausführlich zu der Entscheidung Ehricke/Becker/Walzel, RDV 2006, 149 sowie Simitis, NJW 2006, 2011), bedurfte es eines neuen – auf anderer Rechtsgrundlage basierenden – PNR-Abkommens, das am 26. 7. 2007 abgeschlossen (ABl. EG v. 4. 8. 2007, Nr. L 204/18) und nachfolgend in Deutschland ratifiziert worden ist (BGBl. II 2007 S. 1978).

5.2 Eine spezielle Entscheidung nach Art. 25 Abs. 6 EU-DatSchRL hat die Kommission nach mehrjährigen Verhandlungen über Datenübermittlungen in die USA getroffen. Danach gewährleistet das mit dem US-Handelsministerium ausgehandelte **„Safe Harbor"-Paket** einen angemessenen Datenschutz. Voraussetzung ist, dass der Empfänger in den USA sich durch Erklärung gegenüber der zuständigen US-Behörde zur Einhaltung bestimmter Datenschutzprinzipien verpflichtet (vgl. Klug, RDV 2000, 212; Heil, DuD 2000, 444), wobei besondere Regelungen für den Datentransfer von Personaldaten greifen. Die sog. Safe Harbor-Prinzipien werden durch als Leitlinien fungierende „Frequently Asked Questions (FAQs)" sowie weitere Anlagen ergänzt (zum Safe-Harbor-Paket s. Dammann/Simitis, BDSG, S. 693 ff.; zur Kritik an der Safe-Harbor-Lösung vgl. Däubler in: DKWW, BDSG, § 4 b Rn. 16). **15**

5.3 Ein angemessenes Schutzniveau besteht auch dann, wenn zwischen den verantwortlichen Stellen die von der Kommission verabschiedeten **Standardvertragsklauseln** zur Gewährleistung der Schutzinteressen der Betroffenen vereinbart werden. Überdies können nach dem BDSG auch konzernweit **verbindliche Unternehmensregelungen** als Schutzgarantien dienen (zu den Schutzgarantien s. § 4 c Rn. 10 ff.). **16**

6. Unterrichtung der Betroffenen

Nach **Absatz 4** besteht für öffentliche Stellen, die Datenübermittlungen an nicht öffentliche Stellen im Rahmen der Erlaubnis des § 16 Abs. 1 Nr. 2, d. h. auf Grundlage einer Interessenabwägung (Nr. 2 Satz 1) bzw. bei besonderen Arten von personenbezogenen Daten (§ 3 Abs. 9) nach den für diese geltenden Voraussetzungen (Nr. 2 Satz 2) vornehmen, die Verpflichtung, den Betroffenen über die Übermittlung seiner Daten zu informieren. Die **Unterrichtungspflicht** entfällt, wenn damit zu rechnen ist, dass der Betroffene auf andere Weise Kenntnis erlangt. **17**

7. Verantwortung für die Zulässigkeit der Übermittlung

Gemäß **Absatz 5** ist die übermittelnde Stelle für die Zulässigkeit der Übermittlung verantwortlich (zur Bestimmung der datenexportierenden Stelle auf Basis tatsächlicher Entscheidungsbefugnis bzgl. des Datenexports vgl. Hillenbrand-Beck, RDV 2007, 231 ff.). Dies bedeutet, dass grundsätzlich die **verantwortliche Stelle** (§ 3 Abs. 7) nicht nur auf die Einhaltung der allgemeinen Übermittlungsvoraussetzungen zu achten hat, sie beurteilt im Fall des Drittlandtransfers – vorbehaltlich des Vorliegens einschlägiger Kommissionsentscheidungen (vgl. Rn. 14) – auch das **18**

beck-shop.de

Schutzniveau beim Datenempfänger in eigener Verantwortung (ebenso Bergmann/Möhrle/Herb, BDSG § 4 b Rn. 33). Dies ist sachgerecht, denn die verantwortliche Stelle kennt die Übermittlungsumstände am besten (s. auch Simitis in: Simitis (Hrsg.), BDSG § 4 b Rn. 89). Soweit allerdings besondere Schutzgarantien wie Vertragsklauseln oder verbindliche Unternehmensregelungen das Schutzniveau beim Datenempfänger auf einen angemessenen Standard heben sollen, kann dies nicht gänzlich ohne eine Koordination mit den Aufsichtsbehörden geschehen (s. § 4 c Rn. 14 ff.).

8. Hinweispflicht gegenüber dem Empfänger

19 **8.1** Nach **Absatz 6** besteht für die übermittelnde Stelle die Pflicht, den im Ausland ansässigen Empfänger auf die Zwecke hinzuweisen, zu deren Erfüllung die Daten übermittelt werden. Eine entsprechende Pflicht findet sich aber auch schon anderweitig, da Abs. 1 und Abs. 2 Satz 1 die für die Privatwirtschaft geltenden Übermittlungsbestimmungen der §§ 28 bis 30 a für entsprechend anwendbar erklären und § 28 Abs. 5 Satz 3 bzw. § 29 Abs. 4 eine die **Zweckbindung** noch konkreter betonende **Hinweispflicht** enthalten.

20 **8.2** Inwieweit die Stelle, an die die Daten übermittelt wurden, diese für andere als die ursprünglichen Übermittlungszwecke verarbeiten oder nutzen darf, hängt von den Regelungen ab, die beim Datenempfänger ein angemessenes Datenschutzniveau sicherstellen. Insoweit ist aber eine Orientierung an den Vorgaben der EU-DatSchRL geboten, d. h. eine mit der ursprünglichen, rechtmäßigen Zweckbestimmung nicht zu vereinbarende Erhebung bzw. Verarbeitung ist zu vermeiden.

9. Landesrecht

21 Die Landesdatenschutzgesetze haben die Vorgaben der Richtlinie für die Übermittlung personenbezogener Daten ins Ausland sowie an über- und zwischenstaatliche Stellen ausnahmslos übernommen (Art. 21 BayDSG; § 20 LDSG BW; § 17 BbgDSG; § 18 BremDSG; § 17 HmbDSG; § 17 HDSG; § 16 DSG M-V; § 14 NDSG; § 17 DSG NRW; § 17 LDSG R-P; § 13 DSG-LSA; § 17 SDSG; § 16 LDSG SH; § 17 SächsDSG; § 23 ThürDSG; § 14 BlnDSG mit Ausnahmeregelungen in Absatz 5 für Daten, die nicht automatisiert verarbeitet und nicht in Dateien gespeichert sind oder werden).