Gelbe Erläuterungsbücher

BDSG Bundesdatenschutzgesetz

Kommentar

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

11. Auflage

Thematische Gliederung:

Datenschutz- und Melderecht

Verlag C.H. Beck München 2012

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 63876 3

Inhaltsverzeichnis: BDSG Bundesdatenschutzgesetz – Gola / Klug / Körffer / et al.

mer zum Stillschweigen über bestimmte betriebliche Vorgänge verpflichten soll, dann greift, wenn die Verschwiegenheit das betriebliche Ordnungsverhalten betrifft).

11. Widerspruch gegen die Verarbeitung/Widerruf der Einwilligung

11.1 Das BDSG äußert sich – mit der Ausnahme der Regelung in § 28 Abs. 3, § 29 Abs. 3 sowie dem besonderen Widerspruchsrecht nach § 20 Abs. 5 und § 35 Abs. 5 (vgl. hierzu Gola, DuD 2001, 278) – nicht zu dem Fall, dass der Betroffene einer – ggf. sogar per Einwilligung legitimierten – Verarbeitung später widerspricht. Gleichwohl kann ein solcher **Widerspruch** unter verschiedenen Aspekten für die Zulässigkeit der Verarbeitung relevant werden. **37**

11.2 Zunächst ist insoweit festzuhalten, dass der Betroffene eine einmal erteilte Genehmigung regelmäßig auch wieder zurücknehmen kann (vgl. auch die diesbezügliche Hinweispflicht in § 13 Abs. 2 Nr. 4 TMG). Der mit dem **Widerruf der Einwilligung** zum Ausdruck kommende Widerspruch gegen weitere Verarbeitungen ist von der datenspeichernden Stelle für die Zukunft zu beachten, d. h. der Widerruf der Einwilligung entzieht den Verarbeitungen ex nunc die erforderliche Rechtsgrundlage. Allerdings sollte die Einwilligung nicht willkürlich, sondern entsprechend den Grundsätzen von Treu und Glauben nur dann zurückgenommen werden, wenn für ihre Erteilung maßgebende Gründe entfallen sind, sich wesentlich geändert oder die tatsächlichen Voraussetzungen für die Erteilung sich verändert haben (den Verzicht auf den Widerruf bejaht Wächter, Datenschutz im Unternehmen, Rn. 232; a. A. Schaffland/Wiltfang, BDSG § 4a Rn. 26). Das LG Hamburg (RDV 2006, 77) lässt den Widerruf einer nach § 22 KUG erteilen Einwilligung in die **Veröffentlichung von Filmaufnahmen** im Fernsehen u. a. zu, wenn veränderte Umstände das Festhalten an der Einwilligung unzumutbar machen oder wenn der Betroffene überrumpelt wurde und den Eingriff in sein Persönlichkeitsrecht nicht hinreichend abschätzen konnte (so hier bei unangekündigten Filmaufnahmen eines Kontrollbesuchs des Sozialamts). **38**

11.3 Eine Einwilligung ist zudem dann nicht widerrufbar, wenn sie verbunden ist mit rechtsgeschäftlichen Abreden und die Einwilligung der Abwicklung einer vertraglichen Beziehung dient (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) (vgl. Gola/Wronka, RDV 2007, 51). Werden z. B. personenbezogene Daten gegen Honorar zum Zwecke der **Veröffentlichung verkauft,** so ist die Einwilligung Gegenstand eines Vertrages, der nicht einseitig rückgängig gemacht werden kann (vgl. hierzu insgesamt auch Simitis in: Simitis (Hrsg.), BDSG § 4a Rn. 99). Will ein Arbeitgeber Daten der Beschäftigten an eine zentrale „Überwachungsstelle" (vgl. LAG Hamburg, RDV 1990, 3) oder will ein Arzt **Patientendaten** an eine privatärztliche Verrechnungsstelle (vgl. BGH, NJW 1991, 2955 = RDV 1992, 38; Bongen/Kremer, NJW 1990, 2911) übermitteln, so ist hierfür die Einwilligung des Betroffenen erforderlich; ein Widerruf wird aber nach Vertragsabschluss jedenfalls dann nicht mehr möglich sein, wenn damit die weitere Abwicklung des Vertrages mit dem Betroffenen in Frage gestellt oder unbillig erschwert wird. **39**

11.4 Auch wenn das informationelle Selbstbestimmungsrecht nicht so weit greift, dass der Betroffene der Verarbeitung seiner Daten grundsätzlich widersprechen kann, so ist ein eventueller **Widerspruch** – auch abgesehen von dem besonders geregelten Fall des § 20 Abs. 5 und § 35 Abs. 5 – bzw. die Nichtausübung eines eingeräumten Widerspruchsrechts für die Beurteilung der Zulässigkeit der Verarbeitung gleichwohl relevant. Das BDSG macht die Zulässigkeit mehrfach davon abhängig, dass schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden. Für die verantwortliche Stelle ist es oft schwierig, dies zu beurteilen, insbesondere dann, wenn eine Einzelfallprüfung erforderlich ist (vgl. hierzu § 28 Rn. 27). Hier kann es sinnvoll sein, **40**

zur Sicherheit eine Einwilligung einzuholen (insoweit gegen sog. „Angstklauseln", Wächter, Datenschutz im Unternehmen, Rn. 233). Generell sollte die Einholung der Einwilligung jedoch „ultima ratio" gegenüber anderen Erlaubnistatbeständen sein (vgl. § 4 Anm. 6.2).

41 **11.5** Ggf. ist es aber auch ausreichend, dem Betroffenen die Möglichkeit des Widerspruchs einzuräumen. Diese **Widerspruchsmöglichkeit** ersetzt nicht etwa die Einwilligung. Ist jedoch wegen der Art der zu verarbeitenden Daten oder wegen der beabsichtigten Nutzung davon auszugehen, dass schutzwürdige Interessen im Regelfall nicht beeinträchtigt werden, so kann aus der Tatsache, dass von der ausdrücklich eingeräumten Widerspruchsmöglichkeit kein Gebrauch gemacht wurde, darauf geschlossen werden, dass eventuelle, für die verantwortliche Stelle nicht erkennbare, entgegenstehende Interessen Einzelner nicht vorliegen (so z. B. für die vereinsinterne Veröffentlichung von **Vereinsmitgliederlisten:** Weichert, DuD 1994, 200; für die Übermittlung von Vereinsmitgliederdaten zwecks Abschluss eines günstigen Gruppenversicherungsvertrages: LfDI Bremen, 31. TB (2008) Ziff. 18.11; Veröffentlichungen **betrieblicher Jubilarien:** Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Rn. 470, 672). Dazu ist ebenfalls erforderlich, dem Betroffenen präzise anzugeben, welche Daten zu welchen Zwecken verarbeitet werden sollen, sofern er nicht in der vorgesehenen Form, z. B. durch Ankreuzen eines hierfür vorgesehenen Kästchens, widerspricht. Durch die Widerspruchslösung wird erreicht, dass auch dann, wenn nur in möglichen Einzelfällen eventuelle Zweifel an der Zulässigkeit bestehen, und in denen aus Gründen der Praktikabilität eine ausdrückliche Einwilligung nicht einholbar ist, ein Grund zur Annahme der Verarbeitung entgegenstehender schutzwürdiger Interessen nicht mehr gegeben ist (vgl. auch § 28 Rn. 28 ff).

42 **11.6** Nicht ausreichend ist das Einräumen eines Widerspruchsrechts bei der Weitergabe von Arbeitnehmerdaten an ein Versicherungsunternehmen. Die Aufsichtsbehörde Baden-Württemberg (Hinweis zum BDSG Nr. 32, Staatsanz. Nr. 3 vom 12. 1. 1994) stellt hierzu fest: „**Versicherungsunternehmen** treten häufig mit der Bitte an Betriebe heran, ihnen Namen und Adressen von Mitarbeitern zur Bewerbung mit Versicherungsleistungen zu überlassen. Besonderes Interesse finden dabei regelmäßig die Daten von Berufsanfängern und **Auszubildenden.** Hierzu wird darauf hingewiesen, dass die Übermittlung von Arbeitnehmerdaten zum Zwecke der **Werbung** nur mit schriftlicher Einwilligung des Betroffenen zulässig ist, wobei dieser auf den Zweck der Datenübermittlung und den Empfänger der Daten hinzuweisen ist. Es reicht nicht aus, statt einer Einwilligung dem Arbeitnehmer die beabsichtigte Datenübermittlung nur allgemein (z. B. durch Betriebszeitung oder Aushang am Schwarzen Brett) oder in anderer Form bekannt zugeben und ihm ein Widerspruchsrecht einzuräumen (vgl. zur Unzulässigkeit der Übermittlung der Mitgliederadressen einer Partei an einen Verlag nach nicht ausgeübtem Widerspruchsrecht, 1. TB des Innenm. Baden-Württemberg (2001), S. 153; vgl. im Übrigen § 28 Rn. 29).

43 **11.7** Der Hinweis auf das **Widerspruchsrecht** in Form des Widerrufs der Einwilligung kann ggf. auch die Fortwirkung einer Einwilligung bei der Weitergabe und Nutzung von Kundendaten beim **Unternehmenskauf** (vgl. hierzu Duisberg, RDV 2004, 104) bewirken. Wird z. B. von einer Bank die Einwilligung eingeholt, dass bestimmte Daten an bestimmte, konkret zu benennende Kooperationspartner im Rahmen von **Allfinanzkonzepten** zwecks sog. **Cross Selling** weitergegeben werden dürfen, so stellt sich die Frage, ob bei späteren konzerninternen Veränderungen auch neu hinzugekommene Firmen in den Verbund mit einbezogen werden dürfen. Dabei kann, wenn das neue Unternehmen die Daten im Rahmen der eingewilligten Zweckbestimmungen nutzt, die Weitergabe und Nutzung dann im Rahmen einer Interessenabwägung gem. § 28 Abs. 1 Satz 1 Nr. 2 als zulässig bewertet werden, wenn der Betroffene über den neuen „Datenempfänger" gem. § 33

benachrichtigt wurde und er ausdrücklich auf sein Recht, der Speicherung seiner Daten zu widersprechen, d. h. die erteilte Einwilligung zu widerrufen, hingewiesen wurde (vgl. Däubler in: DKWW, BDSG § 4a Rn. 44 ff.).

11.8 Die **EU-DatSchRL** räumt dem Betroffenen in Art. 14 ein Widerspruchsrecht nicht nur bei unerwünschter Werbung, sondern auch in weiteren Fällen der Interessenabwägung ein (Art. 14 Abs. 1 Satz 1a). Der Widerspruch ist aber auch hier nur zu beachten, wenn er aus „überwiegenden, schutzwürdigen" Gründen, also „berechtigt", erfolgt (vgl. hierzu § 20 Abs. 5 und § 35 Abs. 5 Anm. 9). Eine grundlegende Änderung der Rechtslage bedeutet diese Regelung daher zwar nicht; gleichwohl wird die Rechtsposition des Betroffenen gestärkt (Gola, DuD 2001, 278). **44**

12. Landesrecht

Die Landesdatenschutzgesetze gehen von dem gleichen Prinzip des „Verbots mit Erlaubnisvorbehalt" aus wie das BDSG und sehen als Erlaubnistatbestand auch die – regelmäßig schriftlich zu erteilende – Einwilligung vor. Die Vorgabe der EU-DatSchRL, dass die **Einwilligung** ohne Zwang erfolgen muss, haben von den Landesdatenschutzgesetzen Berlin (§ 6 Abs. 5), Bremen (§ 3 Abs. 3), Hamburg (§ 5 Abs. 2), Niedersachsen (§ 4 Abs. 3), Nordrhein-Westfalen (§ 4 Abs. 1) und Rheinland-Pfalz (§ 5 Abs. 2) übernommen. Die übrigen enthalten die allgemeinen Regelungen zum Inhalt und zur Form der Einwilligung (Art. 15 BayDSG; § 4 Abs. 2–4 LDSG BW; § 6 Abs. 4–6 BlnDSG; § 4 Abs. 2 und 3 BbgDSG; § 5 Abs. 2 HmbDSG; § 7 Abs. 2 HDSG; § 8 DSG M-V; § 4 Abs. 2 NDSG; § 4 Abs. 1 SDSG; § 4 Abs. 3–5 SächsDSG; § 4 Abs. 2 DSG-LSA; § 12 LDSG SH; § 4 Abs. 2 ThürDSG). **45**

§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen

(1) **Für die Übermittlung personenbezogener Daten an Stellen**
1. in anderen Mitgliedstaaten der Europäischen Union,
2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder
3. der Organe und Einrichtungen der Europäischen Gemeinschaften
gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30a nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

(2) [1] **Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder zwischenstaatliche Stellen gilt Absatz 1 entsprechend.** [2] **Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist.** [3] **Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.**

(3) **Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.**

(4) [1] **In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten.** [2] **Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.**

(5) **Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.**

(6) **Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden.**

Literatur: *Backes/Eul/Guthmann/Martwich/Schmidt,* Entscheidungshilfe für die Übermittlung personenbezogener Daten in Drittländer, RDV 2004, 156; *Blume,* Personal Data Transfer: Possibilities and Limitations, CRi 2005, 71; *Breinlinger/Krader,* Whistleblowing – Chancen und Risiken bei der Umsetzung von anonym nutzbaren Hinweisgebersystemen im Rahmen des Compliance-Managements, RDV 2006, 60; *Brisch/Laue,* E-Discovery und Datenschutz, RDV 2010, 1; *Büllesbach,* Überblick über europäische Datenschutzregelungen bezüglich des Datenaustauschs mit Ländern außerhalb der Europäischen Union, RDV 2002, 55; *ders.,* Datenschutz in einem globalen Unternehmen, RDV 2000, 1; *ders.* (Hrsg.), Datenverkehr ohne Datenschutz? Eine globale Herausforderung, 1999; *Büllesbach/Höss-Löw,* Vertragslösung, Safe-Harbor oder Privacy Code of Conduct – Handlungsoptionen globaler Unternehmen, DuD 2001, 135; *Büllesbach, Achim,* Transnationalität und Datenschutz – Die Verbindlichkeit von Unternehmensregelungen, Diss., 2008; *Burianski/Reindl,* Deutsches Datenschutzrecht in internationalen Schieds-

verfahren, RDV 2011, 214; *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; *Erd,* Zehn Jahre Safe Harbor Abkommen – kein Grund zum Feiern, K&R 2010, 624; *Eul/Eul,* Datenschutz International, 2011; *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; *Greer,* Safe Harbor – ein bewährter Rechtsrahmen, RDV 2011, 267; *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; *Lensdorf,* Autragsdatenverarbeitung in der EU/EWR und Unterauftragsdatenverarbeitung in Drittländern: Besonderheiten der neuen EU-Standardvertragsklauseln, CR 2010, 735; *Martin,* Kunden- und Mitarbeiterdaten im weltweiten Fluss, DuD 2007, 126; *Moos,* Die EU-Standardvertragsklauseln für Auftragsverarbeiter 2010, CR 2010, 281; *Moritz/Tinnefeld,* Der Datenschutz im Zeichen einer wachsenden Selbstregulierung, JurPC WebDok. 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 § 4c 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; *Schild/Tinnefeld,* Datenverarbeitung im internationalen Konzern, DuD 2011, 629; *Schmidl,* Datenschutzrechtliche Anforderungen an innereuropäische Personaldatenübermittlungen in Matrixorganisationen, DuD 2009, 364; *ders.,* Übermittlung von Arbeitnehmerdaten auf Grundlage des Standardvertrags Set II, DuD 2008, 258; *ders.,* Die Whistleblowing-Stellungnahme der Artikel-29-Gruppe, DuD 2008, 414; *ders.,* Datenschutz für Whistleblowing Hotlines, DuD 2006, 353; *Scholz/Lutz,* Standardvertragsklauseln für Auftragsverarbeiter und § 11 BDSG, CR 2011, 424; *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; *Wybitul/Patzak,* Neue Anforderungen beim grenzüberschreitenden Datenverkehr, RDV 2011, 11; *von Zimmermann,* Whistleblowing und Datenschutz, RDV 2006, 242; *ders.,* Whistleblowing, Anforderungen des Sarbanes-Oxley-Acts, WM 2007, 1060.

Übersicht

1. Allgemeines

1 § 4b 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 ursprünglichen Drei-Säulen-Konzept vgl. Bergmann/Möhrle/Herb, Datenschutzrecht, § 4b 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 § 4c 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 (zur Lage nach Inkrafttreten des Lissabon-Vertrags vgl. Ronellenfisch, DuD 2009, 451 (460)). Für die Verarbeitung von Daten durch Polizei- und Justizbehörden im strafrechtlichen Bereich gilt derzeit in erster Linie der Rahmenbeschluss 2008/977/JI. Im Rahmen ihres Vorschlags für eine umfassende Reform des europäischen Rechtsrahmens für den Datenschutz (s. Einleitung Rn. 28) strebt die EU-Kommission nun den Erlass einer EU-Richtlinie „zum Schutz natürlicher Personen bei der Verarbeitung perso-

nenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr" – KOM(2012) 10 endg. – an. Durch die Richtlinie sollen allgemeine Datenschutzgrundsätze und -regeln für die polizeiliche und justizielle Zusammenarbeit in Strafsachen eingeführt werden. Die Bestimmungen sollen sowohl für inländische als auch für grenzüberschreitende Datenübermittlungen gelten und machen langfristig gegebenenfalls eine Anpassung von § 4b notwendig (geplantes Inkrafttreten: zwei Jahre nach Annahme der Richtlinie). 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 somit relativieren. Zudem fallen die auf Basis des Lissabon-Vertrags gestärkten Kompetenzen bzw. Mitentscheidungsbefugnisse des Europäischen Parlaments im Rahmen des Abschlusses internationaler Übermittlungsabkommen zunehmend ins Gewicht , was sich bereits frühzeitig an der Notwendigkeit der Nachverhandlung des sog. SWIFT-Abkommens mit den USA hinsichtlich der Übermittlung von Geldüberweisungsdaten (ABl. EU v. 27. 7. 2010, Nr. L 195/5) manifestiert hat.

2. Ungehinderter Datenfluss innerhalb der EU/des EWR

2.1 Wie der vollständige Titel der EU-DatSchRL schon zum Ausdruck bringt, will sie einerseits **Persönlichkeitsrechtsschutz** und andererseits **freien Datenverkehr** 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 Artikel-29-Datenschutzgruppe 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**

2.2 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. § 4c Rn. 5), greifen die Übermittlungstatbestände des zweiten bzw. dritten Abschnitts des BDSG (§§ 15 Abs. 1, 16 Abs. 1 bzw. §§ 28–30a; die unterbliebene Verweisung auf § 32 dürfte auf einem Versehen des Gesetzgebers beruhen; ebenso Seifert, in: Simitis (Hrsg.), BDSG, § 32 Rn. 120; Thüsing, Arbeitnehmerdatenschutz und Compliance, 2010, Rn. 434 sowie Wybitul/Patzak, RDV 2011, 11). 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 **4**

Vertragsklauseln oder verbindlichen Unternehmensregelungen (s. hierzu § 4c Rn. 10 ff.) für verbindlich zu erklären (BlnDSB, Jahresbericht 2002, Ziff. 4.7.3).

5 **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 sowie unter Hinweis auf ein Klarstellungsbegehren des Bundesrates Kort, RDV 2011, 79); 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. § 4c Rn. 13). Die oftmals schwierige Abgrenzung zwischen Auftragsdatenverarbeitung und Datenübermittlung an Dritte ist beispielsweise auch bei der **Serververlagerung** im internationalen Konzern relevant (zur Thematik vgl. Hilber/Knorr/Müller, CR 2011, 417 (421 f.)). 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 §§ 4b, 4c nicht (vgl. § 11 Rn. 16a).

3. Datenübermittlung in Drittländer und an über- oder zwischenstaatliche Stellen

6 **3.1** Nach § 4b **Abs. 2 Satz 1** gilt Abs. 1 für innereuropäische Datenflüsse, die im Rahmen von nicht dem Gemeinschaftsrecht unterfallenden Tätigkeiten erfolgen (s. Rn. 1), sowie beim Datentransfer in **Drittländer** oder an **über- oder zwischenstaatliche Stellen** entsprechend. Mithin sind auch in diesen Fällen zunächst die allgemeinen Zulässigkeitstatbestände relevant (s. Rn. 3).

Die Aufsichtsbehörden prüfen die Zulässigkeit der Datenübermittlung in **Drittstaaten** in einem **zweistufigen Verfahren**.

- 1. Stufe: Zulässigkeit nach nationalen Datenschutzvorschriften (insbesondere § 28; aber wohl auch § 32 – vgl. Rn.3)
- 2. Stufe: Einhaltung der besonderen Anforderungen bzgl. des Drittstaatentransfers nach den §§ 4b, 4c)

Dem liegt die Überlegung zugrunde, dass das nach deutschem Datenschutzrecht gewährleistete Datenschutzniveau gewahrt bleiben soll. Deswegen muss die Übermittlung zunächst durch einen **Erlaubnistatbestand** des deutschen Datenschutzrechts gedeckt sein **(1. Stufe).** Die in der Praxis häufig einschlägige Erlaubnisnorm des § 28 Abs. 1 Satz 1 Nr. 2 setzt eine **Interessenabwägung** voraus. Insofern werden im Prinzip zunächst dieselben Maßstäbe angelegt, wie bei Übermittlungen innerhalb der EU/des EWR.

Erst, wenn das Vorliegen einer grundsätzlichen Übermittlungsbefugnis festgestellt worden ist, werden im Rahmen der **2. Stufe** die besonderen Voraussetzungen nach den §§ 4b, 4c überprüft. § 4b Abs. 2 Satz 2 enthält zunächst die ausdrückliche Feststellung, dass Drittlandsübermittlungen insbesondere bei entgegenstehenden