Datenschutz in der Bankpraxis

von
Dr. Markus Deutsch, Dr. Andreas Fillmann, Paul Gürtler, Dr. Wulf Kamlah, Peter Suhren, Wolfgang Vahldiek, Dr. Thomas Winzer

1. 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 63924 1

Inhaltsverzeichnis: Datenschutz in der Bankpraxis – Deutsch / Fillmann / Gürtler / et al.

- Abschluss verbindlicher Unternehmensregelungen, oder
- Abschluss von Individualverträgen.

6. Besondere Umstände der Datenübermittlung in einer Unternehmensgruppe

Für die Übermittlung von Daten zwischen den Unternehmen eines Konzerns ergeben sich im Hinblick auf den Datenschutz sowie auf die Datensicherheit einige Besonderheiten: **20**

- Vermeintlich als anonymisiert angesehene Daten gemäß § 3 Abs. 6 BDSG können durch ihre Verarbeitung im Konzern eventuell wieder bestimmt oder bestimmbar werden, weil verschiedene Stellen im Konzern möglicherweise über weiteres Wissen verfügen, wodurch eine Bestimmbarkeit der Daten möglich wird;
- Die verantwortliche Stelle hat die Rechtmäßigkeit der gesamten Datenverarbeitung zu gewährleisten, insbesondere muss sie Daten gemäß § 35 Abs. 2 Satz 2 BDSG löschen, unrichtige Daten gemäß § 35 Abs. 1 BDSG berichtigen, Daten gemäß § 35 Abs. 3 BDSG sperren und dem Betroffenen unter Umständen gemäß § 34 Abs. 1 BDSG Auskünfte über die zu seiner Person gespeicherten Daten – auch soweit sie sich auf die Herkunft dieser Daten beziehen – gemäß § 34 Abs. 1 BDSG erteilen; und
- Aus technisch-organisatorischer Sicht müssen vor allem besondere Vorkehrungen für die ordnungsgemäße Löschung und Trennung von Daten sowie für die Sicherstellung von Transparenz, Integrität und Revisionsfähigkeit der Datenverarbeitung getroffen werden.

Zu beachten ist auch, dass das Thema einer globalen Datenvernetzung im Konzern weder in der Datenschutzrichtlinie noch im BDSG reguliert oder definiert worden ist. Das bedeutet, dass die jeweiligen gesetzlichen Regelungen im BDSG vom Normalfall der Datenübermittlung an nur „einen" Dritten ausgehen, wobei der Dritte von vornherein bestimmt ist. **21**

III. Internationale Anwendbarkeit des BDSG

Die internationale Anwendbarkeit des BDSG ist in dessen § 1 Abs. 5 als spezialgesetzliche Kollisionsnorm geregelt[41], die den allgemeinen Kollisionsnormen vorgeht. Diese Regelung gilt bei grenzüberschreitendem Datenverkehr innerhalb der EU oder mit einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum („EWR"). Dabei ist das bis zum Jahre 2001 geltende Territorialprinzip des BDSG durch das (modifizierte) Sitzstaatprinzip abgelöst worden. Danach gilt für alle verantwortlichen Stellen mit Sitz in Deutschland sowie für die hiesigen Niederlassungen ausländischer Banken und Finanzinstitute deutsches Datenschutzrecht gemäß § 1 Abs. 2 BDSG. Hat die verantwortliche Stelle ihren Sitz in einem Mitgliedsstaat der EU oder dem EWR, gilt für diese bei der Datenverarbeitung in Deutschland das Recht des Sitzstaates. Entsprechend unterliegen **22**

[41] Vgl. Artikel 4 Abs. 1 lit (a) Datenschutzrichtlinie.

Banken mit Sitz in Deutschland bei der Verarbeitung in der EU nur deutschem Recht. Dies gilt auch dann, wenn die Leistung über das Internet angeboten wird und selbst wenn sich der Server in einem anderen EU- oder EWR-Staat befindet. Falls sowohl die Niederlassung in Deutschland als auch eine Niederlassung in einem EU- oder EWR-Staat datenschutzrechtlich relevante Handlungen vornehmen, müssen sowohl das BDSG als auch das Recht der anderen nationalen EU- oder EWR-Rechtsordnungen beachtet werden[42].

23 § 1 Abs. 5 Satz 2 BDSG regelt die Voraussetzungen, die von Kredit- und Finanzinstituten in ihrer Eigenschaft als verantwortliche Stellen zu beachten sind, die in einem Drittstaat außerhalb der EU und des EWR gelegen sind und in Deutschland personenbezogene Daten erheben, verarbeiten oder nutzen. Aufgrund des aus europäischer Sicht geringen Datenschutzniveaus in den meisten Staaten außerhalb der EU oder des EWR (einschließlich den USA), ist die entscheidende Frage stets, ob eine Datenverarbeitung in Deutschland vorgenommen wird, da nach dem Territorialprinzip das BDSG dann Anwendung findet, wenn datenschutzrechtlich relevante Handlungen von einer Bank oder einem Finanzinstitut mit Sitz in einem Drittstaat in Deutschland durchgeführt werden. Demgegenüber findet im Falle eines reinen Transits der personenbezogenen Daten durch Deutschland das BDSG gemäß § 1 Abs. 5 Satz 4 keine Anwendung (z. B. bei einer Zwischenspeicherung der Daten auf Routern oder Servern)[43]. Eine Abgrenzung diesbezüglich erfolgt danach, ob die personenbezogenen Daten in Deutschland erhoben werden. In § 3 Abs. 3 BDSG ist das Erheben definiert als das Beschaffen von Daten bei dem Betroffenen[44], so dass aufgedrängte Informationen erst dann dem BDSG unterliegen, wenn der Empfänger auf den Computer der Nutzer zugreift, insbesondere wenn die Daten vom Empfänger gespeichert und genutzt werden[45].

24 Im Hinblick auf das entscheidende Kriterium der Datenverarbeitung in Deutschland gibt es derzeit zahlreiche kontroverse und auch weitgehend ungeklärte Fragen. So wird beispielsweise diskutiert, ob eine solche Datenerhebung auch dann erfolgt, wenn auf den Computer des Nutzers zugegriffen wird (z. B. mithilfe von Cookies)[46]. Ob Cookies personenbezogene Daten sind oder solche beinhalten, muss jeweils anhand der konkreten Umstände bestimmt werden. Wenn diese, wie etwa beim Webtracking, eine Identifikationsnummer des Webseitenbesuchers beinhalten, sind diese als personenbezogene Daten anzusehen[47].

---

[42] Vgl. Simitis/*Dammann*, § 1 Rdn. 199; *Gola/Schomerus*, § 1 Rdn. 28.

[43] So auch Simitis/*Dammann*, § 1 Rdn. 238.

[44] Vgl. Simitis/*Dammann*, § 3 Rdn. 102.

[45] Vgl. dazu Simitis/*Dammann*, § 1 Rdn. 223.

[46] Siehe Art. 5 Abs. 3 und Erwägungsgrund 25 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), zuletzt geändert durch Art. 2 Änderungsrichtlinie 2009/136/EG vom 25. 11. 2009 (auch bezeichnet als „Cookie-Richtlinie"), dort Erwägungsgrund 66; vgl. auch Hoeren/Sieber/*Wolff*, Multimedia-Recht, Teil 11 Rdn. 100.

[47] Zum ganzen siehe Hoeren/Sieber/*Helfrich*, Multimedia-Recht, Teil 16.1 Rdn. 34; *Voigt* MMR 2009, S. 377, 380; Simitis/*Dammann*, § 3 Rdn. 65.

Zu beachten ist außerdem, dass das BDSG für Persönlichkeitsverletzungen durch Übermittlung von personenbezogenen Daten kein eigenständiges Sanktionssystem enthält, sodass die allgemeinen deliktischen Ansprüche gemäß § 823 Abs. 1, 2 BGB und § 1004 BGB nicht durch das BDSG verdrängt werden[48]. Für sämtliche privatrechtlichen Ansprüche, die aus dem widerrechtlichen Umgang mit personenbezogenen Daten als unerlaubter Handlung folgen, richtet sich das anwendbare Recht auch nicht nach § 1 Abs. 5, sondern nach dem allgemeinen Deliktstatut gemäß Artikel 40 Abs. 1 Satz 1 EGBGB[49]. Demgemäß richtet sich das anwendbare Recht nach dem Ort, an dem die spezielle Verletzungshandlung stattgefunden hat. Dies ist grundsätzlich der Geschäftssitz der datenverarbeitenden Stelle. Abweichend hiervon kann der in seinem Persönlichkeitsrecht Verletzte auch verlangen, dass das Recht desjenigen Staates anzuwenden ist, in dem der Verletzungserfolg eingetreten ist[50]. Dies ist oft der Ort in dem der Betroffene seinen gewöhnlichen Aufenthalt hat. **25**

IV. Datenübermittlung im Konzern

1. Rechtliche Einordnung

Die Anwendung des BDSG auf Konzerne[51] als „nicht-öffentliche Stellen" wird in § 1 Abs. 2 Nr. 3 i.V. m. § 2 Abs. 4 BDSG geregelt. Das Datenschutzrecht definiert diese als „natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, die nicht unter die Absätze 1 bis 3 fallen" (§ 2 Abs. 4 BDSG)[52]. Des Weiteren dient der Begriff der „verantwortlichen Stelle" der Bezeichnung des Normadressaten des Datenschutzrechtes, also grundsätzlich der Stelle, die die Daten erhebt, verarbeitet und nutzt (§ 3 Abs. 7 BDSG)[53]. Dies ist entweder die Daten verarbeitende Organisationseinheit innerhalb der juristischen Person (z. B. Aktiengesellschaft, GmbH, Verein) oder die juristische Person selbst. Es existieren somit keine gesetzliche Datenschutzregelungen für in einem Konzern verbundene Unternehmen, so dass in einem Konzern verbundene selbständige Unternehmen daher untereinander datenschutzrechtlich wie Dritte (siehe oben) zu behandeln sind, mit der Folge, dass die Übermittlungsvorschriften des BDSG auch zwischen Unternehmen eines Konzerns gelten[54]. Der Düsseldorfer Kreis, eine informelle Vereinigung der obersten deutschen Aufsichtsbehör- **26**

---

[48] So auch *Giesen* JZ 2007, S. 918, 924.

[49] *Jotzo* MMR 2009, S. 232, 233.

[50] Artikel 40 Abs. 1 Satz 2 EGBGB.

[51] Die folgenden Ausführungen betreffen privatrechtlich gegründete Banken und Finanzinstitute, die in eiern Unternehmensgruppe verbunden sind.

[52] Vgl. Simitis/*Dammann*, § 3 Rdn.136.

[53] Vgl. Simitis/*Dammann*, § 3 Rdn. 223 f.; *Gola/Schomerus*, BDSG,§ 3 Rdn. 48.

[54] Nach Meinung von Simitis/*Simitis*, § 3 Rdn. 233 und *Gola/Schomerus*, § 3 Rdn. 52 f. sind unselbstständige Zweigstellen eines Unternehmens, sofern sie im Inland belegen sind, untereinander nicht Dritte, mit der Folge, dass die Übermittlungsvorschriften nicht zur Anwendung kommen. Sofern die unselbstständige Zweigstelle jedoch in der EU oder EWR belegen ist, sei sie Dritte und unterliege dem Recht des EU-Mitgliedstaates.

den, hat in seinem Positionspapier zum internationalen Datentransfer im Februar 2007[55] klargestellt, dass sogar unselbständige Niederlassungen übermittelnde Stellen im Sinne der §§ 4b, 4c BDSG sein können.

27 Im Rahmen von datenschutzrechtlichen Aspekten haben Bankkonzerne typischerweise mit personenbezogenen Daten in Form von Kunden- und Mitarbeiterdaten zu tun, wenn z. B. der Kunde ein neues Konto bei einer Bank eröffnet oder ein neuer Mitarbeiter angestellt wird. Diese Kunden- und Mitarbeiterdaten werden häufig an andere Konzerngesellschaften weitergegeben, da das internationale Bankgeschäft ohne einen grenzüberschreitenden Datenfluss zwischen den jeweiligen Instituten kaum realisierbar ist[56]. Als Datenübermittlung gilt auch, wenn ein Datenzugriff der Muttergesellschaft auf Kunden- oder Mitarbeiterdaten erfolgt, die auf Computern der Tochtergesellschaft gespeichert sind. Analog gilt dies für die Einrichtung einer zentralen Kundendatei, die auf Rechnern der Muttergesellschaft betrieben wird und in der die Kundendaten sämtlicher Tochtergesellschaften gespeichert werden. Eine diesbezügliche gesetzliche Privilegierung gibt es nicht, da das BDSG keinen Unterschied zwischen einem Konzernunternehmen und einem beliebigen externen Unternehmen macht[57].

2. Analyse der Rolle der beteiligten Unternehmen

28 Zur Überprüfung der Rechtmäßigkeit der Datenübermittlung im Konzern bedarf es auf der der ersten und zweiten Prüfungsstufe einer eingehenden Analyse der Datenströme, der Feststellung der verantwortlichen Stelle und der Herstellung eines angemessenen Datenschutzniveaus.

29 Zunächst ist von Bedeutung, welche personenbezogenen Daten von welcher Bank oder von welchem Finanzinstitut an welche andere Konzerngesellschaft oder andere Konzerngesellschaften mit Sitz in einem oder mehreren Drittstatten übermittelt werden oder übermittelt werden sollen. Daran anschließend muss analysiert werden, welche Rollen die einzelnen Unternehmen im Konzern beim Umgang mit diesen Daten haben. Die Prüfung sollte die folgenden Umstände und Fragen umfassen:

- Werden Daten von natürlichen Person erhoben (z. B. von Kunden, Mitarbeitern, Bewerbern, Interessenten, Webseiten-Besucher);
- Um welche Daten handelt es sich dabei konkret (z. B. Name, Einkommen, Familienstand, Position, Gehalt bei Mitarbeitern, Adresse),
- An welches oder welche Konzernunternehmen werden diese personenbezogenen Daten übermittelt, bzw. von welchen Konzernunternehmen können Mitarbeiter auf diese personenbezogenen Daten zugreifen;

---

[55] https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2007/20070419_Internationaler_Datenverkehr/Positionspapier.pdf.

[56] *Weniger,* Grenzüberschreitende Datenübermittlung international tätiger Unternehmen, S. 51 ff.

[57] Kein Konzernprivileg, vgl. *Gola/Schomerus*, § 27 Rdn. 4; Simitis/*Seifert*, § 32 Rdn. 116; Simitis/*Simitis*, § 2 Rdn. 142 ff.; *Schulz* BB 2011, S. 2552; *Kilian/Scheja* BB 2002 Beil. 3, S. 19, 21 f., 27 ff.; *Schild/Tinnefeld* DuD 2011, S. 629 ff.

- Was ist der Sinn und Zweck der Datenübermittlung (z. B. zentrale Lohnbuchhaltung, zentrale Kundendatenverwaltung, Erbringung von Kundendienstleistungen); und
- Werden die personenbezogenen Daten vom empfangenden Konzernunternehmen auch Dritten zur Verfügung gestellt oder haben Dritte darauf Zugriff (z. B. Wartungsunternehmen, Cloud-Anbieter, Softwareanbieter, externe Auftragsdatenverarbeiter).

Im Rahmen dieser Analyse ergibt sich oft, dass personenbezogene Daten bei einzelnen Konzernunternehmen zusammen geführt werden oder Daten von einer Vielzahl von Unternehmen an andere Konzernunternehmen übermittelt oder diesen zur Verfügung gestellt werden. **30**

3. Verantwortliche Stelle im Konzern

Für die Prüfung der rechtlichen Zulässigkeit der Datenübermittlung ist von Bedeutung, welches Institut im Konzern die verantwortliche Stelle für die Datenverarbeitung ist und welche Rolle die anderen Konzernunternehmen dabei haben. Die Begriffsdefinition im § 3 Abs. 7 BDSG bezeichnet als verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Diese Legaldefinition steht in direktem Zusammenhang mit dem Begriff der Übermittlung gemäß § 3 Abs. 4 Nr. 3 BDSG. Nach der Datenschutzrichtlinie wird die verantwortliche Stelle als die Stelle definiert: „(...) die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“[58]. Demgegenüber wird der Auftragsdatenverarbeiter als die Stelle bezeichnet, die „... im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet“[59]. **31**

Eine Hilfe zur Abgrenzung der Rollen der beteiligten Stellen bietet auch die Stellungnahme 1/2010[60] der Artikel-29-Datenschutzgruppe[61]. Die Artikel-29-Datenschutzgruppe ist der Auffassung, dass die Stelle, die den Zweck und die wesentlichen Mittel der Verarbeitung bestimmt, verantwortliche Stelle ist. Maßgeblich ist somit, welche Stelle faktisch befugt ist, über den Zweck der Datenverarbeitung zu bestimmen[62]. In Bezug auf die Mittel der Datenverarbeitung können technische und organisatorische Fragen an den Auftragsdatenverarbeiter delegiert werden. Falls der Auftragsdatenverarbeiter auch über die wesentlichen Elemente des Mittels der Datenverarbeitung mitentscheidet, wird er dadurch ebenfalls, d. h. neben der den Auftrag vergebenden Bank, zur verantwortlichen Stelle. **32**

---

[58] Artikel 2 lit. (d) Datenschutzrichtlinie.

[59] Artikel 2 lit. (e) Datenschutzrichtlinie.

[60] Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ (WP 169), abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation.

[61] Die Artikel-29-Datenschutzgruppe wurde gemäß Artikel 29 der Datenschutzrichtlinie eingesetzt und ist ein unabhängiges Beratungsgremium der EU in Datenschutzfragen in der auch die nationalen Datenschutzbehörden vertreten sind.

[62] Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 (WP 169), S. 38 f.

a) Modalitäten der Datenübermittlung

33 Wie oben dargestellt, ist Datenübermittlung nach der Legaldefinition des § 3 Abs. 4 Nr. 3 BDSG die Weitergabe von Daten an Dritte[63]. Das Übermitteln selbst betrifft hierbei das Bekanntgeben gespeicherter Daten an einen Dritten (Empfänger) in der Weise, dass die Daten an den Empfänger weitergegeben werden oder der Empfänger zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Die Datenübermittlung im Konzern lässt sich somit in zwei Gruppen einteilen:

- Exporteur ist verantwortliche Stelle
  - Importeur ist verantwortliche Stelle (Funktionsübertragung),
  - Importeur ist Auftragsdatenverarbeiter (Auftragsdatenverarbeitung)
- Exporteur ist Auftragsdatenverarbeiter
  - Importeur ist verantwortliche Stelle,
  - Importeur ist Auftragsdatenverarbeiter (Unterauftragsdatenverarbeitung)

34 Es ist daher zu unterscheiden, ob die verantwortliche Stelle die personenbezogenen Daten als Exporteur an einen Dritten als Auftragsdatenverarbeiter übermittelt (sogenannte „*Controller to Processor*"-Übermittlung) oder an eine andere verantwortliche Stelle (sogenannte „*Controller to Controller*"-Übermittlung). Es geht bei den Alternativen im Wesentlichen um die Abgrenzung und Unterscheidung von Auftragsdatenverarbeitung und Funktionsübertragung[64]. Schaltet hingegen ein Auftragsdatenverarbeiter seinerseits einen Auftragsdatenverarbeiter ein, so liegt eine Unterauftragsdatenverarbeitung vor (sogenannte „*Processor to Processor*"-Übermittlung).

b) Abgrenzung der Funktionen

35 Die Unterscheidung der Funktion als verantwortliche Stelle, Auftragsdatenverarbeiter und Unterauftragsdatenverarbeiter und Datenexporteur ist in mehrerer Hinsicht von wesentlicher Bedeutung:

- Es findet grundsätzlich das Recht des EU-Staates Anwendung, in dem die verantwortliche Stelle ihren Sitz hat[65];
- Die verantwortliche Stelle ist für die Einhaltung der nationalen datenschutzrechtlichen Vorschriften verantwortlich; und
- Bei einer Auftragsdatenverarbeitung müssen im Vertrag insbesondere die Aspekte geregelt werden, die sicherstellen, dass der Datenimporteur die Daten tatsächlich nur nach den Weisungen der verantwortlichen Stelle verarbeitet[66].

36 Vor dem Hintergrund dieser mit der Einordnung der verantwortlichen Stelle oder Auftragsdatenverarbeiter verbundenen Implikationen kann eine Einstufung

---

[63] Dritter ist hierbei jede Person oder Stelle außerhalb der verantwortlichen Stelle und den Betroffenen.

[64] Vgl. zur Abgrenzung: *Gola/Schomerus*, § 11 Rdn. 9; Simitis/*Petri*, BDSG, § 11 Rdn. 22 ff.

[65] Vgl. § 1 Abs. 5 Satz 1 BDSG; Art. 4 Datenschutzrichtlinie; *Steding/Meyer* BB 2001, S. 1693, 1698 speziell zur Abgrenzung bei Ausgliederung von Bankdienstleistungen.

[66] § 11 BDSG; in § 11 BDSG finden sich detaillierte Regelungen, wohingegen die Datenschutzrichtlinie „nur" einen schriftlichen Vertrag für die Datenübertragung verlangt.

im Einzelfall schwierig sein, so dass die Prüfung eine umfassende Berücksichtigung der konkreten Umstände erfordert. Bei der Feststellung der verantwortlichen Stellen und der konzerninternen Auftragsdatenverarbeitungen gilt zunächst als Regel: Verantwortliche Stelle für die Kundendaten ist die Bank oder das Finanzinstitut, welche(s) die Kontoeröffnung oder den Dienstleistungsvertrag (z. B. Geschäftsbesorgungsvertrag, Garantievertrag) mit dem Kunden geschlossen hat. Bei Mitarbeiterdaten ist es die Bank, mit der der Mitarbeiter den Arbeitsvertrag geschlossen hat.

Zunächst ist die Datenübermittlung von der Datenweitergabe an einen Auftragsdatenverarbeiter innerhalb der EU oder dem EWR abzugrenzen, da die Auftragsdatenverarbeitung innerhalb der EU bereits gesetzlich durch § 11 BDSG geregelt wird. Wird ein rechtlich selbstständiges Konzernunternehmen als Auftragsdatenverarbeiter nach § 11 BDSG für ein oder mehrere Konzernunternehmen tätig, so sind Auftraggeber und Auftragnehmer im Verhältnis zueinander nicht Dritte und die Weitergabe stellt keine Übermittlung dar[67]. Erfolgt die Auftragsdatenverarbeitung in der EU oder im EWR, ist im Hinblick auf diesbezügliche Vereinbarungen auf die Muster zu § 11 BDSG zurückzugreifen und es sind keine EU-Standardvertragsklauseln zu vereinbaren[68]. In diesem Sinne sind auch Rechendienstleistungen durch Auftragsdatenverarbeiter mit Sitz in der EU oder im EWR im Rahmen von Outsourcing gemäß § 25a Abs. 2 KWG als eine Auftragsdatenverarbeitung zu betrachten[69]. Dies ist jedoch zu relativieren, falls keine Auftragsdatenverarbeitung, sondern eine Funktionsübertragung vorgenommen wird, da in diesem Fall eine Übermittlung an Dritte gegeben ist. Als Rechtsgrundlage ist dafür entweder eine Einwilligung nach § 4a BDSG nötig, oder die Übermittlung wird legitimiert durch § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Zusätzlich zu dem Auftragsdatenverarbeitungsvertrag sollte jedoch zwischen der verantwortlichen Stelle und dem Auftragsdatenverarbeiter noch ein Rahmenvertrag geschlossen werden, der die zivilrechtliche Seite des Auftrages regelt. **37**

Bei einer Auftragsdatenverarbeitung außerhalb der EU oder dem EWR gilt die Regelung des § 11 BDSG nicht – aus § 3 Abs. 8 Satz 3 BDSG ergibt sich, dass Auftragnehmer in Drittstaaten immer „Dritte" und damit kein Auftragsdatenverarbeiter sind[70]. **38**

4. Sicherstellung eines angemessenen Datenschutzniveaus

Gemäß Art. 25 der Datenschutzrichtlinie und § 4b Abs. 2 Satz 2 BDSG ist die Sicherstellung eines angemessenen Datenschutzniveaus beim Datenimporteur zu gewährleisten. Nach den genannten Vorschriften darf eine Datenübermittlung in einen Drittstaat nicht stattfinden, wenn das angemessene Datenschutzniveau nicht sichergestellt werden kann. Es drohen dann Maßnahmen der Aufsichtsbehörde und Bußgelder sowie gegebenenfalls ein Strafverfahren gemäß §§ 43, 44 **39**

[67] § 3 Abs. 8 Satz 3 § 3 Abs. 4 Nr. 3 so auch *Graf von Westphalen* WM 1999, S. 1800, 1814.

[68] Vgl. *Wybitul/Patzak* RDV 2011, S. 11, 17.

[69] *Steding/Meyer* BB 2001, S. 1693 ff.; *Kahler/Werner*, Die Zulässigkeit der Verarbeitung von Kundendaten gemäß Bankgeheimnis und Datenschutz, S. 199f.; zu den entsprechenden Anforderungen an die IST-Sicherheit: *Gackern/Karger* MMR 2011, S. 3, 7.

[70] Vgl. *Gola/Schomerus*, § 11 Rdn. 16.

BDSG. Zur Sicherstellung eines angemessenen Datenschutzniveaus stehen die bereits oben erwähnten Möglichkeiten zur Verfügung[71]:

- **EU-Standardvertragsklauseln**: Abschluss von Verträgen zwischen Datenexporteur und Datenimporteur mit bestimmten Standardvertragsklauseln[72].
- **Safe-Harbor-Abkommen**: Unterwerfung unter die Safe-Harbor-Grundsätze für Unternehmen in den USA[73].
- **Binding Corporate Rules**: Rechtlich verbindliche Implementierung von Unternehmensregelungen zum Umgang mit personenbezogenen Daten im Konzern[74].
- **Individualverträge**: Genehmigung durch die zuständige Aufsichtsbehörde erforderlich.

a) EU-Standardvertragsklauseln

40 **aa) Anforderungen.** Falls im Drittstaat kein angemessenes Datenschutzniveau existiert, muss die Bank oder das Finanzinstitut als verantwortliche Stelle ausreichende Garantien zum Schutz des allgemeinen Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweisen. Ein angemessenes Datenschutzniveau kann dadurch sichergestellt werden, dass die Vertragsregelungen gewählt werden, die die Europäische Kommission als ausreichende Garantien für den Datenschutz entworfen hat. In Deutschland kommt es auf die Praxis im jeweiligen Bundesland an, ob ein formales Genehmigungsverfahren für die Benutzung dieser Standardvertragsklauseln erforderlich ist oder nicht[75]. Es wird aber teilweise als ausreichend erachtet, wenn die Standardvertragsklauseln der Behörde auf Anfrage vorgelegt werden[76]. Sobald aber selbst gestaltete oder modifizierte Standardvertragsklauseln verwendet werden, kann ein angemessenes Datenschutzniveau nicht ohne weiteres angenommen werden. Eine individuelle Genehmigung bei der zuständigen Datenaufsichtsbehörde muss dann eingeholt werden. Zu beachten ist, dass die vertraglichen Regelungen in den Standvertragsklauseln die sonstigen Vertragsbedingungen über die eigentliche Leistungserbringung hinsichtlich der datenschutzrechtlich geforderten Mindeststandards ergänzen. Schließen die Daten exportierende Bank in der EU und das importierende Institut außerhalb der EU oder des EWR einen Vertrag ab, in den die Standard-

---

[71] Siehe dazu schon Ziffer 5.2.

[72] Vgl. *Räther/Seitz* MMR 2002, S. 520 ff.; zu den aktuellen Standardvertragsklauseln *Spies* MMR-Aktuell 2010, 298882; *Scholz/Lutz* CR 2011, S. 424 ff.; *Moos* CR 2010, S. 281 ff.; *Plenzdorf* CR 2010, S. 735 f..

[73] *Räther/Seitz* MMR 2002, S. 425 ff.; *Erd* K&R 2010, S. 624 ff.; zum Inhalt der „Safe Harbor Privacy Principles" *Engel*, Reichweite und Umsetzung des Datenschutzes gemäß der Richtlinie 94/46/EG für aus der Europäischen Union in Drittländer exportierte Daten am Beispiel der USA, S. 143 ff.

[74] *Dix/Gardain* DuD 2006, S. 343 f.; speziell zu Haftung und BCR: *Grapentin* CR 2011, S. 102 ff.; *Büllesbach*, Transnationalität und Datenschutz; *Schröder*, Die Haftung für Verstöße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht, S. 198.

[75] *Räther/Seitz* MMR 2002, S. 520 ff.

[76] *Gola/Schomerus*, § 4 c Rdn. 14; Simitis/*Simitis*, § 4c Rdn. 37: Aufsichtsbehörden müssten sich nach der den Standardvertragsklauseln innewohnenden Entscheidung der Kommission „richten".