Konzerndatenschutz

Rechtshandbuch

von

Axel Bussche, Freiherr von dem, Paul Voigt, Monika Egle, Nils Hullen, Meike Kamp, Dr. Flemming Moos, Hannes Oenning, Jana Oenning, Dr. Kai-Uwe Plath, Dr. Axel Spies, Prof. Dr. Peter Wedde, Andreas Zeller

1. Auflage

Konzerndatenschutz – Bussche, Freiherr von dem / Voigt / Egle / et al.

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

Thematische Gliederung:

Datenschutz- und Melderecht

Verlag C.H. Beck München 2014

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 66113 6

Inhaltsverzeichnis: Konzerndatenschutz – Bussche, Freiherr von dem / Voigt / Egle / et al.

und wohl auch auf Primärebene eine Rechtfertigung für die Datenweitergabe bieten können.[176] So macht es für die betroffene Person keinen Unterschied, wo die personenbezogenen Daten im Auftrag verarbeitet werden, solange das Schutzniveau angemessen und mit dem innerhalb der EU/des EWR vergleichbar ist. Auch für Auftraggeber und Auftragnehmer besteht eine vergleichbare Interessenlage. Der Auftragnehmer ist ohnehin nach § 11 Abs. 2 Satz 2 BDSG vertraglich zu binden, sodass sich die Anforderungen an den nationalen Auftragnehmer sowie an den Auftragnehmer im Drittland nicht unterscheiden; für den deutschen Auftraggeber ist bei der nationalen und internationalen Weitergabe ohnehin stets das BDSG anwendbar.

Ist der Datentransfer somit gemäß §§ 4b, 4c BDSG durch entsprechende Maß- **88**
nahmen wie beispielsweise den Abschluss von Standardvertragsklauseln,[177] die Unterwerfung des Datenempfängers unter die Safe Harbor-Principles[178] oder den Abschluss von Binding Corporate Rules[179] gerechtfertigt, oder hat der Drittstaat gar ein Datenschutzniveau nach europäischem Standard und ist somit nach Ansicht der EU-Kommission ein „sicheres Drittland",[180] so ist nach hier vertretener Ansicht **analog § 3 Abs. 8 Satz 3 BDSG** davon auszugehen, dass bei Zugrundelegung von § 11 Abs. 2 BDSG entsprechenden Auftragsdatenverarbeitungsvereinbarungen auch **Auftragsdatenverarbeitungen in Drittstaaten ohne gesonderte Rechtfertigung** gemäß § 4 Abs. 1 BDSG zulässig sind.[181]

Dies wird zumindest im Ergebnis beim Abschluss der EU-Standardvertragsklau- **89**
seln zur Auftragsdatenverarbeitung **auch von den Datenschutzaufsichtsbehörden so akzeptiert.**[182] Diese gehen zwar weiterhin davon aus, dass die Datenweitergabe zweistufig zu rechtfertigen sei.[183] Sie vertreten jedoch die Ansicht, dass auf der Primärebene die Weitergabe der zu verarbeitenden Daten an den Auftragsdatenverarbeiter nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG – vorausgesetzt, dass der intendierte Datenverarbeitungsvorgang an sich gemäß § 4 Abs. 1 BDSG zulässig ist – gerechtfertigt sei, wenn die EU-Standardvertragsklauseln um den Katalog aus § 11 Abs. 2 Satz 2 BDSG ergänzt wurden.[184] Folglich gehen die Aufsichtsbehörden bei der Ver-

---

[176] *Weber/Voigt,* ZD 2011, 74 (77); Plath/*Plath,* § 11 BDSG Rn. 14, 53; *Räther,* DuD 2005, 465; *Nielen/Thum*, K&R 2006, 171 (174).

[177] Vgl. hierzu *von dem Bussche/Voigt,* Teil 4 Kapitel 3. sowie speziell zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter Moos/*von dem Bussche,* Teil 5 III.

[178] Vgl. hierzu *Kamp,* Teil 4 Kapitel 4.; auf die Safe-Harbor-Registrierung muss sich der Datenexporteur nach Ansicht der ITA (International Trade Administration) des US-Handelsministeriums verlassen können, vgl. auch den Aufsatz von *Spies/Schröder,* ZD-Aktuell 2013, 03566.

[179] Vgl. hierzu *Kamp,* Teil 4 Kapitel 5.

[180] Vgl. hierzu *von dem Bussche/Voigt,* Teil 4 Kapitel 2. Rn. 9.

[181] *Weber/Voigt,* ZD 2011, 74 (77); Plath/*Plath,* § 11 BDSG Rn. 14, 53; *Räther,* DuD 2005, 465; *Nielen/Thum,* K&R 2006, 171 (174); Moos/*von dem Bussche,* Teil 5 III. Rn. 20.

[182] *Bay. LDA,* Umsetzung des § 11 BDSG bei Auftragsdatenverarbeitung in Drittstaaten, http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_11bdsg_drittstaaten.htm (Stand: September 2013); vgl. auch Beschluss der *Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich* (Düsseldorfer Kreis am 11./12. September 2013): Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen.

[183] Siehe hierzu Rn. 85 f.

[184] Ausführlich hierzu siehe Rn. 91; vgl. auch *Rittweger/Schmidl,* DuD 2004, 617 (620); vgl. Simitis/*Dammann,* § 3 BDSG Rn. 246; *Bay. LDA,* Umsetzung des § 11 BDSG bei Auftragsdatenverarbeitung in Drittstaaten, http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_11bdsg_drittstaa

wendung der EU-Standardvertragsklauseln nicht von einer Privilegierung der Auftragsdatenverarbeitung in Drittstaaten aus. Jedoch fließe im Rahmen der nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG vorzunehmenden Interessenabwägung bei der Weitergabe der Daten an den Auftragnehmer die enge vertragliche Bindung des Auftragnehmers mit ein, so dass die Interessen des Auftraggebers an der Weitergabe der Daten im Rahmen der Quasi-Auftragsdatenverarbeitung gegenüber den schutzwürdigen Interessen der Betroffenen an dem Ausschluss der Verarbeitung regelmäßig überwiegen würden und somit die Weitergabe der personenbezogenen Daten an den Auftragnehmer gerechtfertigt sei.

90 Lediglich bei **besonderen Arten personenbezogener Daten** iSd § 3 Abs. 9 BDSG sowie gegebenenfalls bei **Beschäftigtendaten** kann es aufgrund der Vorgaben von § 28 Abs. 6 bis 9 BDSG sowie § 32 BDSG zu unterschiedlichen Ergebnissen kommen, da § 28 Abs. 1 Satz 1 Nr. 2 BDSG in diesen Fällen regelmäßig keine Anwendung findet. Die Art.-29-Datenschutzgruppe scheint grundsätzlich von der Zulässigkeit der Auftragsdatenverarbeitung von besonderen personenbezogenen Daten in Drittländern auszugehen.[185] Zumindest bei der Auftragsdatenverarbeitung durch andere Konzerngesellschaften ist aber auch nach Ansicht verschiedener deutscher Aufsichtsbehörden eine Verarbeitung von besonderen Arten personenbezogener Daten zulässig.[186]

91 Bei Verwendung der **EU-Standardvertragsklauseln** zur Auftragsdatenverarbeitung sind diese allerdings in jedem Fall um die **Anforderungen aus § 11 Abs. 2 Satz 2 BDSG zu ergänzen,**[187] da die EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung nicht den deutschen datenschutzrechtlichen Anforderungen an die Auftragsdatenverarbeitung gemäß § 11 BDSG genügen.[188] Solche Ergänzungen können im Anhang, teilweise durch geschäftsbezogene Klauseln oder durch eine Nebenvereinbarung vorgenommen werden, ohne dass dadurch eine bei sonstigen Änderungen erforderliche Genehmigungspflicht ausgelöst wird.[189]

92 So können beispielsweise im Anhang 1 der EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung unter anderem ergänzende Angaben über Gegenstand und Dauer des Auftrags sowie Art, Umfang und Zweck der Datenverarbeitung sowie der betroffenen Daten und Personen (§ 11 Abs. 2 Satz 2 Nr. 1 und 2 BDSG) gemacht werden; ferner können Regelungen bezüglich einer etwaigen Unterauftragsvergabe (Nr. 6) sowie bestehender Weisungsbefugnisse (Nr. 9) sowie Rückgabe- und Löschungspflichten (Nr. 10) vereinbart werden. Anhang 2 kann um die gemäß § 11

---

ten.htm (Stand: September 2013); *Konferenz der Datenschutzbeauftragten des Bundes und der Länder,* Orientierungshilfe – Cloud Computing v. 30.8.2011, S. 11; Hess. LT-Drs. 18/2942, 18.

[185] *Art.-29-Datenschutzgruppe,* WP 176, 6; WP 161, 4.

[186] Dies ergibt sich im Umkehrschluss aus *Regierungspräsidium Darmstadt,* Konzerninterner Datentransfer, 9 ff., wonach die Übermittlung besonderer Arten personenbezogener Daten im Konzern nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ausnahmsweise zulässig sein soll.

[187] Moos/*von dem Bussche,* Teil 5 III. Rn. 17.

[188] *Elbel,* RDV 2010, 203 (207 f.); *Bay. LDA,* Umsetzung des § 11 BDSG bei Auftragsdatenverarbeitung in Drittstaaten, http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_11bdsg_drittstaaten.htm (Stand: September 2013).

[189] *Bay. LDA,* Tätigkeitsbericht 2009/2010, S. 72 f., http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/dsa_Taetigkeitsbericht_2010.pdf (Stand: September 2013); *Bay. LDA,* Umsetzung des § 11 BDSG bei Auftragsdatenverarbeitung in Drittstaaten, http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_11bdsg_drittstaaten.htm (Stand: September 2013); Aufsichtsbehörden setzen hohe Anforderungen an Cloud-Nutzung, ZD-Aktuell 2011, 48.

Abs. 2 Satz 2 Nr. 3 iVm § 9 sowie der Anlage zu § 9 Satz 1 BDSG zu ergreifenden technischen und organisatorischen Maßnahmen erweitert werden. Diese sind dem Datenimporteur im Ausland vertraglich aufzuerlegen, obwohl dieser eigentlich nicht dem Regelungsregime des BDSG – und somit auch nicht dem des § 9 BDSG – unterfällt.[190] Die Anforderungen des § 11 Abs. 2 Satz 2 Nr. 5 iVm Abs. 4 BDSG, also beispielsweise die Verpflichtung zur Bestellung eines Datenschutzbeauftragten, müssen hingegen nicht in die Ergänzung der EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung aufgenommen werden.[191]

Im Ergebnis ist somit zumindest bei Verwendung von entsprechend § 11 BDSG **93** ergänzter EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung im Regelfall von einer **genehmigungsfreien Zulässigkeit der Auftragsdatenverarbeitung in Drittstaaten** auszugehen.[192] Nichts anderes sollte für die Fälle gelten, in denen ein der Europäischen Union vergleichbares Datenschutzniveau durch andere Maßnahmen als die EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung hergestellt wird.[193]

III. USA PATRIOT Act

Offen ist, inwieweit Auftragsdatenverarbeitungen mit ausländischen Auftragneh- **94** mern, die in ihrer Jurisdiktion behördlichen Herausgabeansprüchen unterliegen, nach deutschem Datenschutzrecht zulässig sind. Schließlich können die Pflichten des Auftragnehmers, insbesondere die strenge Weisungsgebundenheit[194], möglicherweise im Widerspruch zu etwaigen Herausgabeansprüchen der ausländischen Behörden in Bezug auf personenbezogene Daten stehen. Kommt ein Auftragsdatenverarbeitungsdienstleister einem entsprechenden Herausgabeverlangen nach, kann dies einen Verstoß gegen die Auftragsdatenverarbeitungsvereinbarung sowie gegen deutsches Datenschutzrecht zur Folge haben. Der Abschluss einer Auftragsdatenverarbeitungsvereinbarung mit einem solchen ausländischen Auftragnehmer kann beim Auftraggeber zu einer bewussten Inkaufnahme eines möglichen Eingriffs in deutsches Datenschutzrecht und somit möglicherweise zu einer datenschutzrechtlichen Unzulässigkeit der Auftragsdatenverarbeitungsvereinbarung an sich führen.[195] Virulent wurde das Problem in letzter Zeit insbesondere im Zusammenhang mit dem USA PATRIOT Act.[196]

Der USA PATRIOT Act selbst ist kein Eingriffs-, sondern ein **Änderungsgesetz,** **95** welches nach den Anschlägen im Jahr 2001 diverse US-amerikanische Regelungen modifiziert hat.[197] Datenschutzrechtlich relevant ist insbesondere die durch den USA PATRIOT Act vorgenommene Änderung des Foreign Intelligence Surveyance Act (**FISA**), wonach von einem unbegrenzten Adressatenkreis sämtliche Unterla-

[190] *Voigt,* ZD 2012, 546 (546, 548 f.); Hess. LT-Drs. 15/4659, 20; Moos/*von dem Bussche,* Teil 5 III. Rn. 127 f.
[191] *Voigt,* ZD 2012, 546 (547 f.); Moos/*von dem Bussche,* Teil 5 III. Rn. 129.
[192] Plath/*von dem Bussche,* § 4b BDSG Rn. 19; Moos/*von dem Bussche,* Teil 5 III. Rn. 21.
[193] Vgl. zu diesen Maßnahmen *von dem Bussche/Voigt,* Teil 4 Kapitel 2. Rn. 23 ff.
[194] Siehe oben Rn. 7, 15.
[195] Vgl. hierzu *Voigt/Klein,* ZD 2013, 16.
[196] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.
[197] *Becker/Nikolaeva,* CR 2012, 170 (171).

gen[198] ohne jegliche Beschränkungen, also auch personenbezogene Daten, herausverlangt werden können, die relevant für eine Terrorismus- oder Spionageermittlung sein könnten.[199] Zwar ergeht solch eine **Herausgabeermächtigung** regelmäßig nur aufgrund einer gerichtlichen Anordnung bzw. ist eine behördliche Anordnung gerichtlich überprüfbar.[200] Die **territoriale Reichweite** der Regelungen hingegen wird von den US-Gerichten **sehr weit** ausgelegt. Obwohl die US-Behörden grundsätzlich nur Informationen in ihrem Staatsgebiet bzw. zu ihren Staatsangehörigen verlangen können, werden gerade bei **verbundenen Unternehmen** schlicht die in den USA ansässigen Konzernunternehmen aufgefordert, auf das möglicherweise im Ausland befindliche Tochter-/Schwesterunternehmen einzuwirken, von dem die Informationen gewünscht werden.[201] Auf diese Weise erstreckt sich die Reichweite der Herausgabeermächtigung zumindest theoretisch auf alle Unternehmen, die sich in einem Konzernverbund befinden und bei denen mindestens ein Konzernunternehmen eine Niederlassung in den USA hat. Darüber hinaus bestehen Zugriffsrechte auf in den USA belegene Server.[202]

96 Diese auf Anfrage der US-Behörden bestehende **Herausgabepflicht** alleine dürfte jedoch nicht bereits zur datenschutzrechtlichen Unzulässigkeit des zugrundeliegenden Auftragsdatenverarbeitungsverhältnisses führen. Selbst bei Vorliegen eines Herausgabeverlangens ist die Herausgabe durch den Auftragsdatenverarbeiter nämlich keinesfalls zwingend. So kann sich der Auftragsdatenverarbeiter (wenngleich nicht immer mit herausragendem Erfolg) gegen entsprechende Anordnungen **gerichtlich zur Wehr setzen bzw. sich entsprechenden Herausgabeverlangen widersetzen** und die hieraus resultierenden Konsequenzen in Kauf nehmen; inwieweit dies realistisch ist, wird in der Praxis von einer Abwägung zwischen den zu erwartenden Konsequenzen der Nichtbefolgung des Herausgabeverlangens auf der einen Seite und eines Verstoßes gegen europäisches Datenschutzrecht auf der anderen Seite abhängen.

97 Es ist überdies festzustellen, dass eine vollständige Vermeidung des Zugriffs von US-Behörden durch die extensiv ausgelegte territoriale Reichweite der Eingriffsermächtigungen (trotz bestehender Abwehrmöglichkeiten) schlicht nicht möglich erscheint.[203] Da es kaum Auftragsdatenverarbeiter gibt, die nicht zumindest über den Standort der Server oder eine konzernrechtliche Verbindung dem USA PATRIOT Act unterliegen, wäre folglich bei zu enger Ansicht im Ergebnis jede Auftragsdatenverarbeitungstätigkeit rechtlich unzulässig.[204]

98 Darüber hinaus gibt es **vergleichbare Eingriffsregelungen** für Behörden durchaus auch im **deutschen Recht.** So können gemäß §§ 94 ff. StPO personenbezogene Daten beschlagnahmt oder herausverlangt werden; auch §§ 111 ff. TKG sehen eine Auskunftspflicht von Telekommunikationsanbietern im Falle von Ersuchen der Sicherheitsbehörden vor.

---

[198] Information and Privacy Commissioner for British Columbia, Privacy and the PATRIOT Act: Implications for British Columbia Public Sector Outsourcing, October 2004, 71, http://www.steptoe.com/assets/attachments/400.pdf (Stand: September 2013).

[199] *Pallasky,* DuD 2002, 221 (225); *Becker/Nikolaeva,* CR 2012, 170 (171).

[200] *Voigt/Klein,* ZD 2013, 16 (17).

[201] *Barnitzke,* MMR-Aktuell 2011, 321103; *Becker/Nikolaeva,* CR 2012, 170 (172).

[202] *Voigt/Klein,* ZD 2013, 16 (17).

[203] Vgl. auch die Dimensionen der Datenerhebung durch das Prism-Programm, http://de.wikipedia.org/wiki/Prism (Stand: September 2013).

[204] *Voigt/Klein,* ZD 2013, 16 (17, 20).

Inwieweit eine Datenübermittlung von Auftragsdatenverarbeitern in die USA zur Herausgabe von personenbezogenen Daten an US-Behörden nach deutschem Datenschutzrecht **zulässig** ist, ist noch **nicht abschließend geklärt.** Da eine Übermittlung durch einen Auftragsdatenverarbeiter an eine US-Behörde eine Übermittlung in einen Drittstaat darstellt, müssen an dieser Stelle wiederum **zweistufig** erstens die allgemeine Zulässigkeit des Verarbeitungsvorgangs und zweitens die Übermittlungen in die USA betrachtet werden.[205] **99**

1. Grundsätzliche Zulässigkeit der Weitergabe. Auf erster Stufe ist eine Rechtfertigung für die konkrete Übermittlung (unabhängig vom Empfängerland) schwierig. Als Rechtsgrundlage kommt hier **§ 28 Abs. 2 Nr. 2b BDSG** in Betracht, wonach personenbezogene Daten an Sicherheitsbehörden **„zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten"** übermittelt werden dürfen, wenn „kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat". Ein schutzwürdiges Interesse des Betroffenen, welches der Übermittlung entgegensteht, dürfte regelmäßig nicht vorliegen. Gerade bei dem nach dem USA PATRIOT Act zulässigen Auskunftsersuchen wird dieses Interesse fehlen, denn das Interesse, nicht der Strafverfolgung ausgesetzt zu sein, ist nicht schutzwürdig im Sinne der Norm.[206] **100**

Fraglich ist jedoch, ob die Übermittlung den Anforderungen für eine „Abwehr der Gefahren für die staatliche und öffentliche Sicherheit oder zur Verfolgung von Straftaten" genügt, da hier eine restriktive Sichtweise anzulegen ist und eine hinreichend konkrete Gefahr vorausgesetzt wird. Des Weiteren soll § 28 Abs. 2 Nr. 2b BDSG nicht ermöglichen, dass staatliche Behörden bei Fehlen einer Ermächtigungsgrundlage Daten von der verarbeitenden Stelle herausverlangen können.[207] Dies kann jedoch bei einer Anforderung nach dem USA PATRIOT Act gerade der Fall sein. Der Erlaubnisnorm des § 28 Abs. 2 Nr. 2b BDSG stünde nämlich – im Gegensatz zu einem Herausgabeverlangen deutscher Behörden – keine deutsche Ermächtigungsgrundlage gegenüber. Die Erlaubnisgrundlage würde somit – zumindest faktisch – selbst zu einer „Quasi-Ermächtigungsgrundlage".[208] **101**

2. Zulässigkeit der Übermittlung in die USA. Eine Zulässigkeit der Übermittlung in die USA gemäß **§ 4b Abs. 1, Abs. 2 Satz 1 BDSG** dürfte regelmäßig ausscheiden. Die Behörde im unsicheren Drittland USA könnte weder ein angemessenes Datenschutzniveau durch die Safe Harbor-Grundsätze sicherstellen, noch erscheint der Abschluss eines EU-Standardvertrags mit der Behörde wahrscheinlich. Eine solche Übermittlung in die USA könnte regelmäßig nur dann gemäß § 4b Abs. 1, Abs. 2 BDSG gerechtfertigt werden, wenn der Auftragsdatenverarbeiter die personenbezogenen Daten zunächst an ein Konzernunternehmen in den USA übermittelt, damit letzteres die Daten an die US-Behörden herausgeben kann.[209] **102**

Eher in Betracht kommt eine Zulässigkeit nach **§ 4c Abs. 1 Satz 1 Nr. 4 BDSG.** Hiernach kann „im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwen- **103**

---

[205] Siehe *von dem Bussche/Voigt,* Teil 4 Kapitel 2. Rn. 1 ff.; Moos/*von dem Bussche,* Teil 5 III. Rn. 3 ff.; *Eckhardt,* DuD 2013, 585 (590).

[206] Taeger/Gabel/*Taeger,* § 28 BDSG Rn. 147.

[207] Däubler/Klebe/Wedde/Weichert/*Wedde,* § 28 BDSG Rn. 77; Simitis/*Simitis,* § 28 BDSG Rn. 192; Taeger/Gabel/*Taeger,* § 28 BDSG Rn. 146.

[208] *Voigt/Klein,* ZD 2013, 16 (17, 19).

[209] *Voigt/Klein,* ZD 2013, 16 (17, 19).

dungsbereich des Rechts der Europäischen Gemeinschaft fallen", eine grenzüberschreitende Übermittlung von Daten in ein unsicheres Drittland wie die USA erfolgen, wenn **„die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses"** erforderlich ist. Die Übermittlung dürfte jedoch bereits nicht in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen. In jedem Fall müsste das „wichtige öffentliche Interesse" nach wohl herrschender Ansicht nicht nur beim Empfänger (den US-Behörden), sondern auch beim übermittelnden Auftragsdatenverarbeiter bestehen.[210] Solch ein qualifiziertes öffentliches Interesse wird bei diesem jedoch regelmäßig nicht vorliegen; allein das generelle Interesse, mögliche Straftaten zu verhindern, dürfte in Bezug auf die nicht-öffentliche Übermittlerstelle nicht ausreichend sein.

104 Trotz der bestehenden rechtlichen Bedenken einer Übermittlung personenbezogener Daten an US-Behörden gibt es bislang keine explizite Äußerung der **Datenschutzbehörden** dahingehend, Auftragsdatenverarbeitungsbeziehungen aufgrund des USA PATRIOT Acts mit US-Dienstleistern zu unterlassen. Lediglich das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat bisher konkret zur datenschutzrechtlichen Relevanz des USA PATRIOT Acts Stellung genommen.[211] Das ULD weist jedoch lediglich auf die bisher **nicht eindeutige Rechtslage** hin und schlägt vor, entsprechende vertragliche Regelungen, insbesondere das explizite Verbot der Herausgabe von personenbezogenen Daten an US-Behörden, in den Vertrag aufzunehmen.

105 Im Rahmen der **PRISM-Affäre** und der Snowden-Enthüllungen zu den weitreichenden Zugriffen der NSA auf personenbezogene Daten europäischer Bürger haben sich die deutschen Datenschutzbehörden jedoch allgemein dahingehend geäußert, dass Datenweitergaben in die USA und andere Drittländer außerhalb der EU und des EWR generell als datenschutzrechtswidrig anzusehen seien und dass **keine Genehmigungen** für entsprechende Drittlandsübermittlungen **mehr erteilt** würden; auch solle die **Aussetzung von** Datenübermittlungen auf Grundlage der **EU-Standardvertragsklauseln und Safe Harbor** überprüft werden.[212] Eine tatsächliche rechtliche Unzulässigkeit aller Drittlandübermittlungen dürfte dennoch nicht anzunehmen sein; vielmehr ist im Einzelfall zu beurteilen, ob entsprechend (insbesondere durch Standardvertragsklauseln oder Safe Harbor) gerechtfertigte Drittlandübermittlungen im Einzelfall unzulässig sein können.[213]

106 **3. Das BDSG als Verbotsgesetz zur Verhinderung der Datenweitergabe.** Wenn man die Übermittlung personenbezogener Daten durch einen Auftragsdatenverarbeitungsdienstleister an US-Behörden nicht für nach deutschem Datenschutzrecht gerechtfertigt hält, macht dies jedoch lediglich den konkreten Übermittlungsvorgang, nicht auch das zugrundeliegende Vertragsverhältnis rechtswidrig. Der Auf-

[210] Plath/*von dem Bussche,* § 4c BDSG Rn. 12; Spindler/Schuster/*Spindler,* § 4c BDSG Rn. 13; vgl. *Gola/Schomerus,* § 4c BDSG Rn. 4.

[211] Pressemitteilung des *ULD Schleswig-Holstein* v. 15.11.2011, „Inanspruchnahme des Patriot Act und anderer US-rechtlicher Regelungen zur Beschaffung von personenbezogenen Daten aus dem Raum der Europäischen Union durch US-Behörden", https://www.datenschutzzentrum.de/internationales/20111115-patriot-act.html (Stand: September 2013).

[212] Pressemitteilung des Bundesbeauftragten für Datenschutz vom 24.7.2013 zur möglichen allgemeinen Unzulässigkeit von Datenweitergaben in Drittländer, http://www.bfdi.bund.de/DE/Home/homepage_Kurzmeldungen2013/PMDerDSK_SafeHarbor.html (Stand: September 2013); *Voigt,* ZD-Aktuell 2013, 03165; *Spies,* ZD-Aktuell 2013, 03691.

[213] Vgl. *Voigt,* ZD-Aktuell 2013, 03165; *Spies,* ZD 2013, 535 (536 ff.).

tragsdatenverarbeitungsdienstleister könnte den US-Behörden sogar das BDSG als die Übermittlung verbietendes Gesetz entgegenhalten, wenn er um die Übermittlung personenbezogener Daten ersucht wird. So wird vom **US-Justizministerium** ausdrücklich anerkannt, dass es entsprechende Verbotsgesetze gibt, die an der Herausgabe personenbezogener Daten hindern können.[214] Deutschland wird explizit als ein solches Land mit entsprechenden Verbotsgesetzen genannt,[215] auch wenn im Ergebnis die Erfolgsaussichten eines solchen Berufens auf das BDSG als Verbotsgesetz eher beschränkt sein dürften.[216]

4. Handlungsempfehlungen. Auch wenn es in einer Vielzahl von Jurisdiktionen ähnlich weite Zugriffsrechte von Behörden gibt, die sich bisher lediglich der allgemeinen Kenntnis entziehen,[217] kann es **bei besonders sensiblen Daten** im Einzelfall möglicherweise angezeigt sein, spezielle Vorkehrungen sowie **vertragliche Abreden** mit den Auftragsdatenverarbeitungsdienstleistern zum Schutz vor dem Zugriff ausländischer Behörden zu treffen.[218] **107**

Beispielsweise kann **lediglich mit europäischen Auftragsdatenverarbeitungsdienstleistern kontrahiert** werden, die selbst nicht dem Zugriff durch US-Behörden unterliegen. Mit diesen kann vereinbart werden, dass personenbezogene Daten erst nach **Rücksprache** mit dem Auftraggeber an die US-Behörden herausgegeben werden dürfen und dass etwaigen **Herausgabeverlangen notfalls gerichtlich entgegenzutreten** ist. Daneben kann verlangt werden, dass sich ausdrücklich auf das deutsche BDSG als Verbotsgesetz berufen wird. In diese Abreden kann auch die **US-Mutter-/Schwestergesellschaft als Vertragspartei** miteinbezogen werden. Somit kann der in den USA niedergelassenen Konzerngesellschaft der Einfluss auf die Herausgabe von Daten der europäischen Konzerngesellschaft entzogen werden. **108**

Soweit verhandelbar können die unerlaubte Verwendung von Daten von möglichen bestehenden Haftungsbeschränkungen für **Schadensersatzansprüche** explizit ausgenommen und sogar **Vertragsstrafen** für den Fall eingefordert werden, dass Daten an US-Behörden rechtswidrig herausgegeben bzw. die vereinbarten Informationspflichten diesbezüglich anbieterseitig nicht eingehalten werden. Um überdies zu verhindern, dass die getroffenen Vereinbarungen durch einen **„Change of Control"** umgangen werden können, kann für diesen Fall ein **Kündigungsrecht** vorgesehen werden. Auch ein **Serverstandort außerhalb der USA** erschwert zumindest faktisch den Zugriff durch US-Behörden.[219] **109**

---

[214] *Information and Privacy Commissioner for British Columbia,* Privacy and the PATRIOT Act: Implications for British Columbia Public Sector Outsourcing, October 2004, 120, http://www.steptoe.com/assets/attachments/400.pdf (Stand: September 2013).

[215] *Voigt/Klein,* ZD 2013, 16 (17, 20).

[216] So werden beispielsweise nur 0,03 % der Abhöranträge vor dem sog. Foreign Intelligence Surveillance Court abgelehnt, vgl. *Pitzke,* http://www.spiegel.de/netzwelt/netzpolitik/geheimes-fisa-gericht-segnet-nsa-ueberwachung-ab-a-907036.html (Stand: September 2013); vgl. für das Jahr 2002 den Jahresbericht zum FISA: http://www.fas.org/irp/agency/doj/fisa/2002rept.html (Stand: September 2013), demnach allen Anträgen stattgegeben wurde.

[217] Vgl. hierzu beispielsweise die umfangreiche Überwachung des weltweiten E-Mail-Verkehrs „Tempora" durch den britischen Geheimdienst Government Communications Headquarters, *Reißmann,* http://www.spiegel.de/netzwelt/netzpolitik/internetueberwachung-tempora-geheimdienst-zapft-glasfaserkabel-an-a-907283.html (Stand: September 2013).

[218] Zu alledem *Voigt/Klein,* ZD 2013, 16 (17, 20).

[219] Rechtlicher Schutz wird damit eher nicht erreicht, vgl. *Schuppert/von Reden,* ZD 2013, 210 (220).

Kapitel 4. Verträge für den konzerninternen Datentransfer

Übersicht