Jens Eckhardt, Rudi Kramer

Auftragsdatenverarbeitung

Datenschutzrechtliches Gestaltungselement zwischen Recht und Technik

Die Auftragsdatenverarbeitung stellt in der Praxis ein wesentliches Element dar, um die Datenverarbeitung im Unternehmen rechtskonform zu gestalten. Gerade mit Blick auf die Unwägbarkeiten der Wirksamkeit einer Einwilligung – auch unter dem Aspekt der Transparenz bei komplexeren Vorgängen – und der Unwägbarkeit der nachträglichen Überprüfung von Interessenabwägungen im Rahmen langfristiger Projekte, stellt die Auftragsdatenverarbeitung eine nicht zu vernachlässigende weitere Möglichkeit der datenschutzkonformen Gestaltung von Datenverarbeitungsvorgängen dar. Der Vorteil einer Auftragsdatenverarbeitung wird durch das Datenschutzrecht „gewährt", indem die Umsetzung der Auftragsdatenverarbeitung strikter und enger Vorgaben folgt, rechtlich- insbesondere nach § 11 Abs. 2 S. 2 Nr. 1 bis 10 BDSG und technisch vor allem nach § 11 Abs. 4 S. 1, 4 und 5 BDSG. Diese Vorgaben werden im Lichte des deutschen (nachfolgend Ziffer 1) und europäischen Datenschutzrechts (nachfolgend Ziffer 2) beleuchtet.

1 Auftragsdatenverarbeitung nach deutschem Recht (§ 11 BDSG)

Die Anforderungen an eine Auftragsdatenverarbeitung sind zunächst einmal in § 11 BDSG geregelt. Die sog. Privilegierungswirkung der Auftragsdatenverarbeitung ergibt sich hingegen aus § 3 Abs. 8 S. 2 BDSG, wonach Dritte nicht Stellen sind, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen. Da die Auftragsdatenverarbeiter danach nicht Dritte sind, ist die Übertragung von personenbezogenen Daten an diese keine Übermittlung im Sinne von § 3 Abs. 4 Nr. 3 BDSG und somit kein Vorgang, welcher nach § 4 Abs. 1 BDSG der Einwilligung oder der gesetzlichen Zulässigkeit bedarf.[2] Die Crux der Auftragsdatenverarbeitung ist, dass sich die Vertragspartner ihre Rechtsgrundlage für die datenschutzkonforme Übertragung von personenbezogenen Daten „selbst" schaffen – vorausgesetzt sie halten die nachfolgenden Vorgaben ein:

1 Im Beitrag wird ausschließlich die Meinung des Autors wiedergegeben.

Dr. Jens Eckhardt

RA und FA IT-Recht
JUCONOMY Rechtsanwälte

E-Mail: eckhardt@juconomy.de

Rudi Kramer

Vorstand Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.[1]

E-Mail: rudi.kramer@bvdnet.de

1.1 Inhalt und formale Anforderungen (§ 11 Abs. 1 und Abs. 2 S. 2 BDSG)

Die Auftragsdatenverarbeitung ist durch zwei „Elemente" der Verantwortung des Auftraggebers gekennzeichnet:

1. Den Auftraggeber trifft – trotz der „Auslagerung" der Tätigkeit an einen anderen – weiterhin die Verantwortung für die Zulässigkeit der Erhebung und/oder Verwendung der personenbezogenen Daten (§ 11 Abs. 1 BDSG).
2. Der Auftraggeber ist für die Zulässigkeit der „Auslagerung" verantwortlich – also die Einhaltung der Vorgaben des § 11 BDSG; rechtlich ist dieser Pflicht durch die Vertragsgestaltung

2 *Eckhardt*, DuD 2013, 585 ff.; *Plath/Schreiber*, in: Plath, BDSG, 2013, § 3 BDSG, Rn. 41; *Redeker*, in: Redeker, IT-Recht, 5. Aufl. 2012, Kap. D, Rn. 953; *Bergt*, DSRITB 2013, 37, 38; *Moser*, DSRITB 2010, 595, 602.

nach Maßgabe des § 11 BDSG – einschließlich der Sicherstellung der Weisungsgebundenheit des Auftragnehmers – und in tatsächlicher Hinsicht durch das Überzeugen von der Einhaltung der technischen und organisatorischen Maßnahmen beim Dienstleister Rechnung zu tragen.[3]

Der Auslagernde ist aber nicht verpflichtet, den Vertrag selbst vorzugeben oder selbst die technisch-organisatorischen Maßnahmen „am grünen Tisch" zu definieren. Er muss jedoch beides darauf hin prüfen, ob die datenschutzrechtlichen Vorgaben situationsgerecht eingehalten sind, denn der Auslagernde trägt die Beweislast für die datenschutzrechtliche Zulässigkeit der Auslagerung, also der Einhaltung der Vorgaben des § 11 BDSG (Stichwort: keine Pflicht zur eigenständigen Gestaltung, aber Pflicht zur individuellen Prüfung und Bewertung).[4]

Nach § 11 Abs. 2 S. 2 BDSG muss der Vertrag über die Auftragsdatenverarbeitung – so der Wortlaut des Gesetzes – „schriftlich" geschlossen werden. Die herrschende Meinung in Deutschland legt dies, entgegen Art. 17 Abs. 4 RiLi 95/46/EG, als Schriftformerfordernis i.S.d. § 126 BGB aus.[5]

1.2 Inhaltliche Anforderungen an die Vereinbarung (§ 11 Abs. 2 S. 2 BDSG)

Nach der Maßgabe des § 11 BDSG sind zwei inhaltliche Anforderungen für die Ausgestaltung des Vertrags über die Auftragsdatenverarbeitung wesentlich.

Wesentlicher Bestandteil der Auftragsdatenverarbeitung ist, dass der Auftragnehmer weisungsgebunden handelt. Vereinfacht gesagt: der Auftragnehmer muss stets eine Vorgabe haben, wie er mit den Daten umzugehen hat. Die Pflicht zur Weisungsgebundenheit beschränkt sich nach § 11 BDSG jedoch auf die Erhebung und Verwendung der personenbezogenen Daten und geht nicht darüber hinaus.[6] Der Auftraggeber hat also insbesondere kein umfassendes Weisungsrecht in Bezug auf die Leistungserbringung durch den Auftragnehmer.[7]

Ein weiterer wesentlicher Bestandteil des Vertrags über die Auftragsdatenverarbeitung ist die Umsetzung des sog. 10-Punkte-Katalogs in Nr. 1 bis 10 des § 11 Abs. 2 S. 2 BDSG.[8] Für die vertragliche Ausgestaltung – also insbesondere die Umsetzung des § 11 Abs. 2 S. 2 BDSG – lassen sich eine Vielzahl von Muster und Textvorschläge finden.[9] Besonders hilfreich sind hierbei die Mustervorschläge der Datenschutzaufsichtsbehörden; zuletzt wurde ein aktualisiertes Muster durch das LDA Bayern veröffentlicht.[10] Allerdings sind nicht alle in Mustern der Auftragsdatenverarbeitung anzutreffende Regelungen auch zugleich Vorgaben des § 11 BDSG. Beispielsweise wird durch die Aufsichtsbehörden in deren Mustern eine Regelung zur Vertragsstrafe für den Verstoß gegen Datenschutzpflichten vorgeschlagen. Diese Regelung ist allerdings nicht Voraussetzung für eine rechtlich wirksame Auftragsdatenverarbeitung nach § 11 BDSG. Zudem birgt die Verwendung einer entsprechenden Regelung häufig das Risiko, dass eine rechtlich, vor allem AGB-rechtlich, unwirksame Regelung getroffen wird. Dies hat zur Folge, dass die Vertragsstrafe nicht durchsetzbar ist. Insofern kann es den rechtlich sicheren Weg darstellen auf solche Klauseln zu verzichten. Das gleiche gilt typischerweise für Regelungen über die Haftung (-sbegrenzung) und Regelungen für den Insolvenzfall. Diese Regelungen müssen sich innerhalb rechtlicher Grenzen halten, die bei Gestaltung solcher Vereinbarungen gekannt und beachtet werden müssen. Die Verwendung eines Musters eines Verbands oder einer Datenschutzaufsichtsbehörde „befreit" die Regelungen nicht von den rechtlichen, insbesondere AGB-rechtlichen, Beschränkungen.

Vor allem die Regelungspflichten nach Nr. 3, Nr. 6 und Nr. 7 (auch Nr. 10[11]) des § 11 Abs. 2 S. 2 BDSG sind eine Schnittmenge zwischen Recht und Technik: Einerseits zwingt § 11 Abs. 2 S. 2 BDSG dazu, diese Aspekte vertraglich zu regeln, andererseits sind die technisch-organisatorischen Themen aus der konkreten Sachlage heraus festzulegen.

- In dem Vertrag über die Auftragsdatenverarbeitung sind nach § 11 Abs. 2 S. 2 Nr. 3 BDSG die nach § 9 BDSG zu treffenden technisch-organisatorischen Maßnahmen festzulegen. Die Vertragsparteien sind damit verpflichtet, eine konkrete Leistungsbeschreibung der Maßnahmen zur „Datensicherheit" vorzunehmen. Dies muss nicht zwingend in dem ADV-Vertrag geschehen, sondern kann auch durch Verweis auf eine entsprechende Anlage zum Vertrag erfolgen. Obgleich der Auftraggeber nach §§ 9, 11 Abs. 1 BDSG dafür verantwortlich ist, dass dem § 9 BDSG entsprechende Maßnahmen beim Auftragnehmer und dessen Subunternehmern (siehe unten) vertraglich vereinbart sind, ist er nicht verpflichtet, die Ausgestaltung der technisch-organisatorischen Maßnahmen „aus der eigenen Feder" vorzunehmen. Er kann – nach entsprechender Prüfung – auch durch den Auftragnehmer vorgeschlagene bzw. vorgesehene Maßnahmen als Vertragsinhalt akzeptieren.[12] Gerade bei Angeboten gegenüber einer Vielzahl von Kunden durch einen Dienstleister (bspw. Cloud-Service, Dokumentenentsorgung/-vernichtung) werden die Maßnahmen durch den Dienstleister entwickelt, da individuelle Besonderheiten – gerne auch als „Sonderlocken" bezeichnet – eine andere Preis- und Organisationsstruktur erfordern würden. Notfalls muss sich ein Auftraggeber dann gegen eine Auslagerung im Wege der Auftragsdatenverarbeitung entscheiden oder die höheren Kosten für eine individuelle Gestaltung akzeptieren.

3 *Eckhardt*, DuD 2013, 585, 586 f. (mit Vertiefung hierzu); *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 11 BDSG, Rn. 21 f.; vgl. hierzu ferner *Bergt*, DSRITB 2013, 37, 40.

4 *Eckhardt*, DuD 2013, 585, 586 f.; *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 11 BDSG, Rn. 21a; zudem weiterführend unten im Kontext von § 11 Abs. 2 S. 2 Nr. 3 BDSG.

5 Nach der Art. 17 Abs. 4 RiLi 95/46/EG genügt auch eine Dokumentation in einer anderen Form neben der Schriftform. Diesem kann unterhalb der „Schwelle" des Schriftformerfordernisses genügt werden. Das Schriftformerfordernis ist mit Blick auf die Wirkungen des § 125 BGB kritisch zu hinterfragen: Die in der ADV geregelten Pflichten des Auftragnehmers bestehen überhaupt nicht, was als Sanktion inter partes sinnvoll sein mag, aber die Betroffenen schutzloser stellt, als es erforderlich wäre. Darüber hinaus könnte über § 139 BGB der Vertrag insgesamt und nicht nur ADV unwirksam sein.

6 Zu Sonderregelungen bei Steuerberatern, vgl. *Kramer*, DuD 2013, 658, 659.

7 Insoweit gelten die allgemeinen zivilrechtlichen Grundsätze über die Festlegung der Leistungserbringung und –beschreibung, welche dem Auftragnehmer erhebliche Freiheiten einräumen kann.

8 *Eckhardt*, DuD 2013, 585, 588; *Funke/Wittmann*, ZD 2013, 221, 225.

9 Beispielsweise, aber nicht nur unter [http://www.bitkom.org/files/documents/140109_Mustervertragsanlage.pdf], [https://www.gdd.de/aktuelles/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg, jeweils letzter Abruf 15.1.2014.

10 Vgl. Bayerisches Landesamt für die Datenschutzaufsicht, in: „ Auftragsdatenverarbeitung nach § 11 BDSG, Gesetzestext und Erläuterungen", Stand Januar 2014, S. 3, veröffentlicht unter http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/BayLDA_Auftragsdatenverarbeitung.pdf, letzter Abruf 15.1.2014.

11 Hierzu *Eckhardt*, DuD 2013, 585, 587 ff.; *Bergt*, DSRITB 2013, 37, 39 ff.

12 Vgl. die Checkliste in Bergmann/Möhrle/Herb, BDSG, 46. EL, April 2013, in der Anlage zu § 9 BDSG.

- Die Problematik der Anpassung an technische Veränderungen bei längerfristigen Verträgen kann dadurch gelöst werden, dass der Auftraggeber eine Anpassung zur Aufrechterhaltung des Schutzniveaus verlangen kann, wobei dabei auch an eine Kostenregelung zu denken ist[13]. Letztendlich wird eine Anpassung der vertraglichen Formulierungen auf Wunsch eines Vertragspartners im Rahmen einer Vertragsanpassung erfolgen, die in komplexeren Verträgen unter der Bezeichnung „Change Request" abgebildet wird. Das gleiche wird gelten, wenn der Auftraggeber weitere Weisungsrechte wahrnehmen will, als durch die Leistungsbeschreibung vorgesehen sind.[14] Dies wird in der Praxis nur bei größeren Outsourcingprojekten der Fall sein, wenn der Dienstleister sich nach den Individualinteressen des Auftraggebers richten kann. Im Massengeschäft wird der Dienstleister von sich aus eine standardisierte Leistung anbieten, welche die erforderlichen technischen und organisatorischen Maßnahmen bereits berücksichtigt. Über eine Verpflichtung des Auftragnehmers, die technischen und organisatorischen Maßnahmen anzupassen, um das Gesamt-Schutzniveau nicht zu verringern oder dem Dienstleister zu erlauben, die technischen und organisatorischen Maßnahmen zu ändern, ohne das Schutzniveau zu verringern, kann eine jeweilige Änderung der Vertragsurkunde bei technisch bedingten Änderungen vermieden werden.[15]
- Nach § 11 Abs. 2 S. 2 Nr. 7 BDSG sind in dem Vertrag die Kontrollrechte des Auftraggebers und die korrespondierenden Mitwirkungs- und Duldungspflichten des Auftragnehmers zu regeln. Dieses Kontrollrecht steht in engem Zusammenhang mit der Überzeugungsbildung nach § 11 Abs. 2 S. 4 BDSG. Der Auftraggeber muss sich nach § 11 Abs. 2 S. 2 Nr. 7 BDSG ein „Recht zur Kontrolle vor Ort" vertraglich sichern. Dies gilt, obwohl und selbst dann, wenn er die Kontrolle vor Ort nach § 11 Abs. 2 S. 4 BDSG nicht selbst ausübt.
- Die Thematik Subunternehmer, welche nach Nr. 6 des § 11 Abs. 2 S. 2 BDSG expliziter Vertragsinhalt sein muss, wird im Kontext der technisch-organisatorischen Maßnahmen relevant, weil diese auch bei Subunternehmern des Auftragnehmers sichergestellt und kontrolliert werden müssen; der Auftraggeber haftet auch für „Schwachstellen" bei diesen.[16] Die Einbindung von Subunternehmern für die Hauptleistung stellt daher vor allem bei der Zertifizierung und Auditierung zur Vergabe von Siegeln zugunsten des Auftragnehmers eine Herausforderung dar.

1.3 Technisch-organisatorische Maßnahmen (§ 11 Abs. 4 S. 1, 4 und 5 BDSG)

Der Auftraggeber hat nach § 9 BDSG angemessene technisch-organisatorische Maßnahmen zum Schutz der durch ihn erhobenen und verwendeten personenbezogenen Daten zu treffen. Dies hat er gemäß § 11 Abs. 2 S. 1, 2 Nr. 3, S. 4 BDSG auch beim Auftrag-

13 *Bergt*, DSRITB 2013, 37, 41.

14 So § 2 Abs. 2 in Mustervertrag ADV des BITKOM Version 4.0, http://www.bitkom.org/files/documents/140109_Mustervertragsanlage.pdf, letzter Abruf 15.1.2014

15 So § 3 Abs. 2 letzter Satz in Mustervertrag ADV des BITKOM Version 4.0, http://www.bitkom.org/files/documents/140109_Mustervertragsanlage.pdf, letzter Abruf 15.1.2014

16 Zur Gestaltung von Vertragsregelungen zur Einbindung und Wechsel von Subunternehmern bei *Eckhardt*, DuD 2013, 585, 587; *Bergt*, DSRITB 2013, 37, 43 f.

nehmer sicherzustellen und nach § 11 Abs. 2 S. 5 BDSG zu dokumentieren. Den Auftragnehmer trifft die Pflicht zu technisch-organisatorischen Maßnahmen nicht nur als „abgeleitete" vertragliche Pflicht aufgrund der Vertragsausgestaltung nach Maßgabe des § 11 Abs. 2 S. 2 Nr. 3 BDSG, sondern als „originäre" eigene gesetzliche Pflicht nach § 9 BDSG („*… Stellen, die … im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen …*"), § 11 Abs. 4 BDSG („*Für den Auftraggeber gelten neben den §§ 5, 9, …*").

Der Auftraggeber hat sich nach § 11 Abs. 2 S. 4 BDSG die Überzeugung von ausreichenden technisch organisatorischen Maßnahmen bei dem Auftragnehmer zu bilden. Nach dem eindeutigen Gesetzeswortlaut besteht zwar die Pflicht zur Überzeugungsbildung, jedoch nicht die zur eigenständigen Kontrolle vor Ort durch den Auftraggeber.[17] Es kann vielmehr auch eine Kontrolle durch Dritte erfolgen oder bereits erfolgt sein. Bestätigt wird dies durch die Entwurfsbegründungen im Gesetzgebungsverfahren im Jahr 2009.[18] Auch die Orientierungshilfe Cloud Computing des Düsseldorfer Kreises vom 26.09.2011 nimmt diesen Standpunkt ein.[19] Dieser ist zu entnehmen, dass eine solche Kontrolle dann durch eine unabhängige und kompetente Stelle stattzufinden hat. Das Working Paper 196 der Art. 29 Gruppe vom 1.7.2012 fordert (darüber hinaus), dass sich der Auftraggeber in diesen Fällen die Kontrollberichte vorlegen lässt und diese prüft. Dabei ist zu beachten, dass gerade bei Auftragnehmern, die für eine Vielzahl von Auftraggebern tätig sind, der gegenteilige Effekt eines „Kontrolltourismus" mit Blick auf die Effektivität der technisch-organisatorischen Maßnahmen geradezu kontraproduktiv sein könnte.[20]

Aufgrund der notwendigen technisch-organisatorischen Maßnahmen im Rahmen einer Auftragsdatenverarbeitung hat sich der Auftraggeber weiterhin stets die Frage zu stellen, welches Schutzniveau er im eigenen Interesse fordern sollte. Darüber hinaus unterliegt der Auftraggeber häufig in Bezug auf Dritte, mit denen er vertragliche Beziehungen unterhält, Geheimhaltungspflichten, denen er durch die Ausgestaltung der ADV – insbesondere der technisch-organisatorischen Maßnahmen – Rechnung tragen muss.[21]

Gerade bei Angeboten, welche sich an eine Vielzahl von Nachfragern und damit Auftraggebern im Sinne des § 11 BDSG richten, lässt sich diese Herausforderung mithilfe von „Siegeln" und „Zertifizierungen" durch unabhängige, befähigte Dritte lösen. Die Anforderungen der Datenschutzaufsichtsbehörden und die Praxis legen nahe, dass der Auftraggeber nicht jedem beliebigen „Siegel" oder „Zertifikat" vertrauen kann, denn auch in diesen Fällen bleibt es bei seiner Verantwortung und Haftung für die Auswahl. Das Fehlverhalten bestünde dann jedoch nicht in der unzureichenden Überzeugungsbildung und Kontrolle, sondern in einem Vertrauen auf das „falsche" „Siegel" oder „Zertifikat".[22]

2 Europäische Vorgaben (Art. 17 RiLi 95/46/EG)

Zur Auftragsdatenverarbeitung finden sich aber nicht nur im deutschen Recht Regelungen, sondern auch im europäischen Recht, und das nicht erst durch eine eventuell zukünftig anzuwendende EU-Datenschutzgrundverordnung (im Folgenden: EU-DSGVO-E)[23]. Art. 17 der Datenschutzrichtlinie 95/46/EG enthält Vorgaben zu den inhaltlichen Anforderungen an eine Auftragsdatenverarbeitung. Die Ausgestaltung der Auftragsdatenverarbeitung steht damit nicht allein zur Disposition des nationalen Gesetzgebers. Gerade die Rechtsprechung des EuGH hat aktuell deutlich gemacht, dass diese Richtlinie sowohl das Mindestmaß als auch das Höchstmaß (sog. Vollharmonisierung) der Ausgestaltung darstellt.[24] Eine breite Auseinandersetzung in der Literatur – insbesondere in Veröffentlichungen zu einzelnen Regelungen des BDSG – mit den daraus folgenden Konsequenzen für das BDSG, hat bislang allerdings nicht stattgefunden, wohl auch deswegen, weil sich die Fachwelt auf die Interpretation des Entwurfes der EU-DSGVO-E konzentriert, die bereits im November 2011 in einer Vorversion „geleakt" und kurz darauf am 25.1.2012 offiziell veröffentlicht wurde.[25]

2.1 Inhalt und formale Anforderungen (Art. 16 und 17 Abs. 2 RiLi 95/46/EG)

Die RL 95/46/EG widmet der Auftragsdatenverarbeitung keinen eigenen Artikel. Doch bereits in den Definitionen in Art. 2 lit. f RL 95/46/EG wird der – so die Terminologie der Richtlinie im Unterschied zum BDSG – Auftragsverarbeiter von der Definition des Dritten ausgenommen und der Auftraggeber daher insoweit privilegiert, dass er keine weitere Zulässigkeitsgrundlage benötigt, um personenbezogene Daten an einen Dienstleister zur Verarbeitung zu übertragen. Dies entspricht damit der Vorgehensweise im deutschen Recht.[26]

Die weiteren Regelungen zur Auftragsverarbeitung sind in Art. 16 „Vertraulichkeit der Vereinbarung" und in Art. 17 RL 95/46/EG „Sicherheit der Verarbeitung" integriert. Hiernach hat der

17 Von dieser Pflicht zur Überzeugungsbildung ist – wie bereits oben dargelegt – das Recht zur Kontrolle nach § 11 Abs. 2 Nr. 7 BDSG zu unterscheiden – mit anderen Worten: Der Auftraggeber ist zwar nicht verpflichtet, sich seine Überzeugung selbst vor Ort zu bilden, sondern kann sich hier auf geeignete Prüfungen Dritter verlassen; er muss sich aber gleichwohl das Recht vorbehalten, sich seine Überzeugung im Zweifelsfall doch selbst vor Ort bilden zu dürfen, vgl. *Eckhardt*, DuD 2013, 585, 589; *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 11 BDSG, Rn. 21a.

18 Siehe hierzu Beschlussempfehlung und Bericht des Innenausschusses vom 1.7.2009 im Rahmen des Gesetzgebungsverfahrens der BDSG-Novelle II, BT-Drs. 16/13657, S. 18.

19 Siehe auch unten Ziffer 3und insbesondere Fn. 34.Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Version 1.0, Stand 26.09.2011, Seite 9 (http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf; letzter Abruf 21.1.2014).

20 *Eckhardt*, DuD 2013, 585, 588; ausweislich der Entwurfsbegründung hat der Gesetzgeber aus Gründen der Angemessenheit und Flexibilität von der Verpflichtung zu einer vor-Ort-Begehung abgesehen, BT-Drs. 16/13657, S. 18.

21 Vgl. § 1 Abs. 3 Satz 2 BDSG; *Eckhardt*, DuD 2013, 585, 589; zum Beispiel Patientendaten vgl. *Becker*, DSRITB 2013, 343, 347.

22 Dabei ist haftungsrechtlich auch zwischen Pflichtverstoß und dessen Verschulden zu unterscheiden. Vertraut der Auftraggeber einem für den Verwendungskontext anerkannten oder anerkennenswerten „Siegel" und „Zertifikat", erweist sich dessen Aussage(kraft) jedoch nicht als zutreffend, dann liegt möglicherweise objektiv ein Fehlverhalten vor, mangels Verschulden würde der Auftraggeber hierfür jedoch nicht haften.

23 Hierzu neben anderen: *Eckhardt/Kramer*, DuD 2013, 287 ff.; *Eckhardt/Kramer/Mester*, DuD 2013, 623 ff.; *Hornung*, ZD 2012, 99, 101.

24 EuGH, Urt. v. 24.11.2011 – C-468/10; C-469/10. Weiterführend zu dieser Entscheidung des EuGH unter dem Aspekt der Vollharmonisierung: Freund CR 2012, 32 ff.; *Diederich*, CR 2013, 408 ff.

25 Vorschlag für VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, letzter Abruf am 15.1.2014

26 Siehe oben Ziffer 1.

Auftraggeber einen Auftragsverarbeiter auszuwählen, der hinsichtlich der für die Verarbeitung zu treffenden technischen und organisatorischen Vorkehrungen ausreichende Gewähr bietet (Art. 17 Abs. 2 1. HS RL 95/46/EU). Der für die Verarbeitung Verantwortliche hat sich davon zu überzeugen (Art. 17 Abs. 2 2. HS RL 95/46/EU). Die Weisungsgebundenheit der Verarbeitung personenbezogener Daten gegenüber dem für die Verarbeitung Verantwortlichen ergibt sich für den Auftragsverarbeiter allein aus Art. 16 RL 95/46/EU.

Eine gesonderte Verpflichtung auf die Vertraulichkeit der Mitarbeiter des Dienstleisters muss in Art. 17 nicht geregelt werden, da sich dies bereits aus Art. 16 RL 95/46/EU ergibt.

Die Grundlage für Sanktionsmöglichkeiten wegen Verstößen gegen diese Vorgaben erhalten die Mitgliedsstaaten in Art. 24 RL 95/46/EG. Der Bundestag hat in der BDSG-Novelle II im Jahr 2009 mit der Umsetzung in § 43 Abs. 1 lit. 2b letzte Alternative i. V. m. § 43 Abs. 3 1. Satz BDSG neben der unzureichenden Beauftragung die vor Beginn der Datenverarbeitung unterlassene Überzeugung von der Einhaltung der technischen und organisatorischen Maßnahmen beim Auftragnehmer mit Bußgeld bis 50.000 Euro sanktioniert.

Ein strenges Schriftformerfordernis (vgl. § 11 Abs. 2 S. 2 BDSG, mit den rechtlichen Konsequenzen der Unwirksamkeit des Vertrags nach § 125 BGB und dem Fehlen einer wirksamen Auftragsdatenverarbeitung), gibt die Richtlinie aber nicht vor. Sie verlangt in Art. 17 Abs. 4 RL 95/46/EG allein zum Zwecke der Beweissicherung, dass die datenschutzrelevanten Elemente des Vertrages und die Anforderungen an die technischen und organisatorischen Maßnahmen schriftlich oder in anderer Form dokumentiert werden. Das Dokumentationserfordernis nach der Richtlinie geht daher nicht so weit wie die Umsetzung im BDSG, nach welcher die fehlende gesetzliche Schriftform zu den Diskussionen über die Unwirksamkeit der gesamten Beauftragung führt.[27]

An dieser Stelle ist die Richtlinie hinsichtlich der formellen Anforderungen an die Beauftragung von EDV-Dienstleistungen zukunftstauglicher als das BDSG in sämtlichen seitherigen Novellierungen. Umständliche Beauftragungsformalien, wie das Ausdrucken von Vertragstexten, händische Unterschrift und Versendung per Briefpost, wie dies in Deutschland bei Reichweitenmessungen im Internet als Clouddienstleistungen in Umsetzung der Vorgaben des BDSG empfohlen wird[28], werden durch den Europäischen Gesetzgeber nicht verlangt. Diese deutsche Umsetzung ist mit Blick auf den Wortlaut der Richtlinie und mit Blick auch auf die Entscheidung des EuGH vom 24.11.2011, die von einer Vollharmonisierung[29] ausgeht, nicht zwingend.

2.2 Inhaltliche Anforderungen an die Vereinbarung (Art. 17 Abs. 3, 4 RiLi 95/46/EG)

Die Richtlinie gibt in Art. 17 Abs. 3 RL/95/46/EG für die vertragliche Gestaltung einer Verarbeitung im Auftrag weniger Inhaltliches vor, als der deutsche Gesetzgeber in § 11 Abs. 2 BDSG, gleichwohl ist die Aufzählung in beiden Regelwerken nicht abschließend. In der Richtlinie werden explizit nur die Weisungsgebundenheit des Auftragsverarbeiters und die Verpflichtung, technische und organisatorische Maßnahmen unter Verweis auf Art. 17 Abs. 1 RL 95/46/EG vorzusehen, formuliert.

Die weiteren, aus dem in § 11 Abs. 2 BDSG nicht abschließenden Katalog der Vertragsinhalte bekannten Merkmale wie Regelungen über Subunternehmer, Art der Daten, Kreis der Betroffenen, Hinweispflicht des Auftragnehmers auf datenschutzwidrige Weisungen etc., haben ihre Grundlage nicht in einer entsprechend formulierten Vorgabe der Richtlinie. Gleichwohl erscheint dies nicht richtlinienwidrig, da die Vorgaben der Richtlinie in Art. 17 Abs. 3 nicht abschließend aufgeführt („insbesondere") sind.

2.3 Technisch-organisatorische Maßnahme (Art. 17 Abs. 1 RiLi 95/46/EG)

In der Richtlinie gibt es keine der Anlage zu § 9 BDSG entsprechende Ergänzung des Regelwerkes, es finden sich jedoch in Art. 17 Abs. 1 Satz 1 RL 95/46/EG bei den technischen und organisatorischen Maßnahmen die Vorgaben, welche Ziele diese Maßnahmen zu erfüllen haben. Dabei geht es darum, durch geeignete technische und organisatorische Maßnahmen, die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten zu verhindern. Die Angemessenheitsregelung wird unter Berücksichtigung des Stands der Technik und der bei der Durchführung entstehenden Kosten in Art. 17 Abs. 1 Satz 2 RL 95/46/EG in Abhängigkeit der bei der Verarbeitung ausgehenden Risiken bezogen auf die Art der schützenden Daten berücksichtigt.

Bei der Überzeugungsbildung, inwieweit durch den Dienstleister die technischen und organisatorischen Maßnahmen eingehalten werden, ist die Richtlinie 95/46/EG aus dem Jahr 1995 bereits realitätsnaher an den technischen Möglichkeiten des Internets, als das BDSG nach der Novelle von 2009. Denn bereits in Art. 17 Abs. 3 2. Spiegelstrich, 2. HS RL 95/46/EG wird berücksichtigt, dass die Vorgaben in den jeweiligen Mitgliedsstaaten der EU zu den technischen und organisatorischen Maßnahmen voneinander abweichen können. Im grenzüberschreitenden Dienstleistungsbereich muss ein deutscher Auftraggeber beispielweise sich davon überzeugen, ob der Dienstleister mit Sitz in den Niederlanden die dortigen gesetzlichen Regelungen zu den technischen und organisatorischen Maßnahmen einhält. Oder deutlicher: ein europaweit tätiger Dienstleister muss sich nicht nach den gesetzlichen Vorgaben anderer 27 Mitgliedsstaaten der Europäischen Union richten, sondern nur diejenigen seines Sitzlandes berücksichtigen.

Im BDSG wird diese europarechtlich maßgebliche Vorgabe im Kontext der Auftragsdatenverarbeitung – und damit auch entgegen § 1 Abs. 5 BDSG (Sitzlandprinzip) – nicht berücksichtigt, da die Handhabung nach dem BDSG von einem „Export des deutschen Datenschutzrechts durch die Auftragsdatenverarbeitung" ausgeht. Gerade im innereuropäischen Leistungsaustausch beginnen erst die Diskussionen über die Konsequenzen aus der Ent-

27 Vgl. zur Diskussion über die Rechtsfolgen *Spoerr*, in: Wolff/Brink, BDSG, 2013, § 11 Rn. 87.

28 Hinweise des BayLDA zur Beauftragung einer Reichweitenmessung mittels Google Analytics,
http://www.lda.bayern.de/onlinepruefung/allgemeine_Hinweise_googleanalytics.html, letzter Abruf am 5.1.2014; vgl. Hinweise von Google Ltd. Irland zum Einsatz und zur Beauftragung von Google Analytics unter http://static.googleusercontent.com/media/www.google.com/de//analytics/terms/de.pdf, letzter Abruf am 5.1.2014.

29 Siehe hierzu oben Fußnote 22.

scheidung des EuGH vom 24.11.2011 und die Auslegungen, die sich dadurch für die Richtlinie ergeben.[30]

Dabei wird gegenüber dem bisher in Deutschland verbreiteten Ansatz, in der weiteren Diskussion unter dem Blickwinkel der Vollharmonisierung durch die Entscheidung des EuGH vom 24.11.2011, auch die Zielsetzung eines innereuropäischen freien Datenverkehrs[31] oder einer ebenfalls vollharmonisierend wirkenden[32] EU-Datenschutz-Grundverordnung zu vertiefen sein.

3 Ausgestaltung der tatsächlichen Prüfung

Wie die Überzeugung des Auftraggebers zu bilden ist, bleibt sowohl in der RL 95/46/EG als auch in § 11 Abs. 2 Satz 4 BDSG offen. In der Entwurfsbegründung im Rahmen der BDSG-Novelle II im Jahr 2009 wird allerdings ausgeführt, dass eigene Vor-Ort-Kontrollen des jeweiligen Auftraggebers nicht erforderlich sind.[33] Damit kann eine Vor-Ort-Kontrolle auch durch Dritte – entweder im individuellen Auftrag des jeweiligen Auftraggebers oder generell für alle (potentiellen) Auftraggeber im Auftrag des Auftragnehmers – vorgenommen werden.

Diese Möglichkeit findet sich auch in den – aktuell veröffentlichten – Empfehlungen des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) wieder[34], wonach das BayLDA ein durch den Dienstleister vorgelegtes schlüssiges Datenschutzkonzept oder ein extern durchgeführtes externes Audit ebenfalls als ausreichend betrachtet. Für Cloud-Services wird dies durch die Aufsichtsbehörden differenzierter gesehen, so dass eine reine Selbsterklärung des Auftragsdatenverarbeiters – selbst wenn sie von dessen betrieblichen Datenschutzbeauftragten stammt – im Rahmen von Cloud Services typischerweise nicht genügen soll.[35]

Es besteht damit ein Spielraum für – und ein praktisches Bedürfnis nach – entsprechenden, standardisierten Audits, Siegeln oder Zertifikaten. Diese müssen die gesetzlichen und aufsichtsrechtlichen Anforderungen sachangemessen ausfüllen und für den Auftraggeber die Gewähr bieten, seinen Pflichten mit dem Vertrauen auf Audits, Siegel oder Zertifikate zu genügen.

4 Fazit

Das Thema Datenschutzaudit beschäftigt in Deutschland datenschutzrelevante Bereiche seit dem letzten Jahrtausend. Der Gesetzgeber kündigte in 2001 ein Datenschutzauditgesetz in § 9a Satz 2 BDSG an. Ein solches Gesetz wurde aber bisher nicht verabschiedet, obgleich es in Form eines Artikelgesetzes ursprünglich Bestandteil der BDSG-Novelle II war,[36] die im Jahr 2009 dann ohne diese Regelungen in Kraft trat. Diesem Gesetzentwurf für ein Datenschutzauditgesetz wurden konzeptionelle Schwächen und hoher bürokratischer Aufwand vorgeworfen,[37] so dass es nie beschlossen wurde. In der abgelaufenen 17. Legislaturperiode wurde sodann im Koalitionsvertrag im Oktober 2009 die Errichtung einer Stiftung Datenschutz beschlossen, die den Auftrag hat, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung zu verbessern und ein Datenschutzaudit zu entwickeln. Die Umsetzung erfolgte aber erst Anfang 2013 mit der Gründung der Stiftung Datenschutz.[38]

In der Konsequenz müssen sich Anbieter und Auftraggeber der Verarbeitung personenbezogener Daten verständigen, wie der Auftraggeber als verantwortliche Stelle seiner Überzeugungspflicht nachkommen kann. Die in der Entwurfsbegründung der BDSG-Novelle II zu § 11 BDSG angedeutete Möglichkeit eines Testats eines externen Sachverständigen hat der Gesetzgeber dem Markt überlassen, ohne konkrete Vorgaben zu machen.

Bei standardisierten Leistungen, die einer Mehrzahl von Auftraggebern angeboten werden, kann es auch im eigenen Interesse des einzelnen Aufraggebers liegen, dass andere Kunden sich nicht verpflichtet fühlen, selbst den Dienstleister für Datenschutzkontrollen aufzusuchen, stellt doch jeder Betriebsfremde ein potentielles Sicherheitsrisiko dar. Der Bedarf hierfür besteht außerhalb der klassischen Datenverarbeitungen hinaus, insbesondere bei Cloud Computing. Gerade im Bereich des Cloud Computing, bei denen Hauptleistungen auch durch Subunternehmer – im Ausland – ausgeführt werden können, stellen vertrauensvolle Zertifizierungslösungen eine Herausforderung dar.[39]

In den weiteren Beiträgen dieser DuD-Ausgabe werden verschiedene Ansätze vorgestellt die Überzeugungsbildung des Auftraggebers zu unterstützen und so die durch fehlende gesetzliche Vorgaben entstehende Lücke zu schließen.

30 Vgl. Erwägungsgründe 1 und 3 der RL 95/46/EG.

31 Vgl. Erwägungsgründe 1 und 3 der RL 95/46/EG.

32 Zur Wirkung einer EU-Verordnung *Eckhardt/Kramer/Mester*, DuD 2013, 623, 624.

33 Siehe hierzu Beschlussempfehlung und Bericht des Innenausschusses vom 1.7.2009 im Rahmen des Gesetzgebungsverfahrens der BDSG-Novelle II, BT-Drs. 16/13657, S. 18.

34 Bayerisches Landesamt für Datenschutzaufsicht, Auftragsdatenverarbeitung nach § 11 – Gesetzestext mit Erläuterungen, Stand Januar 2014, Seite 8, http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/BayLDA_Auftragsdatenverarbeitung.pdf , letzter Abruf am 11.1.2014.

35 *„Dem Cloud-Anwender wird es dabei nicht immer möglich sein, eine Vor-Ort-Prüfung durchzuführen. Allerdings darf er sich nicht auf bloße Zusicherungen des Cloud-Anbieters verlassen, sondern er muss eigene Recherchen betreiben, um sich Gewissheit darüber zu verschaffen, dass gesetzlich normierte oder vertraglich vereinbarte Sicherheitsstandards eingehalten werden.15 Die Lösung kann darin bestehen, dass der Cloud-Anbieter sich einem Zertifizierungs- bzw. Gütesiegelverfahren zu Fragen des Datenschutzes und der Datensicherheit bei einer unabhängigen und kompetenten Prüfstelle unterwirft.16 Das Vorliegen von Zertifikaten entbindet den Cloud-Anwender nicht von seinen Kontrollpflichten nach § 11 Abs. 2 Satz 4 BDSG."* (Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Version 1.0, Stand 26.9.2011, Seite 9 (http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf); zuletzt abgerufen: 21.1.2014.

36 BT Drs 16/12011.

37 So *Schantz*, in: Plath, BDSG 2013, § 9a Rn. 1 m.w.Nw.

38 http://stiftungdatenschutz.org/, letzter Abruf am 5.1.2014.

39 Hier sei ein Hinweis auf das Kompetenzzentrum „Trusted-Cloud" des Bundesministeriums für Wirtschaft und Energie gestattet: eine Projektgruppe hat sich eine Pilot-Zertifizierung von Cloud-Diensten unter Datenschutzgesichtspunkten vorgenommen: http://trusted-cloud.de/de/2008.php, letzter Abruf am 15.1.2014.