Matthias Bergt

Rechtskonforme Auftragsdatenverarbeitung im Massengeschäft[1]

Auftragsdatenverarbeitung im Sinne von § 11 BDSG ist im unternehmerischen Alltag Massenphänomen. Doch trotz Bußgeldbewehrung werden regelmäßig weder die vorgeschriebenen Verträge abgeschlossen noch der Auftragnehmer kontrolliert. Dabei ermöglicht es das Gesetz, jedenfalls Standard-Dienstleistungen mit geringem administrativem Aufwand rechtskonform anzubieten – was auch ein Werbe-Argument für entsprechend vorbereitete Provider sein könnte.

1 Begriff der Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG liegt vor, wenn eine verantwortliche Stelle bestimmte Datenverarbeitungsvorgänge nicht selbst ausführt, sondern diese auf eine andere Stelle auslagert. Diese Auslagerung kann zivilrechtlich beliebiger Rechtsnatur sein. Nach § 11 Abs. 5 BDSG sind die Regelungen über die Auftragsdatenverarbeitung zudem entsprechend anzuwenden, wenn Wartungsarbeiten ausgelagert werden und dabei ein Zugriff auf personenbezogene Daten nicht auszuschließen ist. Umfasst vom Begriff der Auftragsdatenverarbeitung sind somit nicht nur klassische IT-Outsourcing-Projekte, sondern auch der E-Mail-Account, die Reparatur des PCs, die Software-as-a-Service-Lösung für die Unternehmensbuchhaltung oder die Entsorgung von Schriftstücken durch fremdes Reinigungspersonal.

Von der Auftragsdatenverarbeitung abzugrenzen ist nach h. M.[2] die so genannte Funktionsübertragung, die vorliegen soll, wenn sich der Auftrag nicht nur auf Hilfs- bzw. Unterstützungstätigkeiten beschränkt. Im Bereich des klassischen IT-Outsourcings wie auch moderner Formen wie Software as a Service wird jedoch in aller Regel nach beiden Ansichten eine Auftragsdatenverarbeitung vorliegen, weil der Auftragnehmer nur nach den Weisungen des Auftraggebers mit den Daten verfahren soll.

Eine Erheblichkeitsschwelle kennt § 11 BDSG nicht, so dass die Regelungen zur Auftragsdatenverarbeitung auch dann zur Anwendung kommen, wenn nur gelegentlich, kurzzeitig oder in geringem Umfang personenbezogene Daten im Auftrag verarbeitet werden,[3] beispielsweise im Rahmen einer kurzzeitigen Cloud-Nutzung zur Abdeckung von Lastspitzen. Dies ist auch der Bedrohungslage angemessen, da sich im Zeitalter der elektronischen Datenverarbeitung vertrauliche Datenbestände praktisch ohne Zeitverlust kopieren oder verändern lassen.

Dogmatisch handelt es sich bei den Regelungen zur Auftragsdatenverarbeitung nicht um einen Erlaubnistatbestand im Sinne von § 4 Abs. 1 BDSG, sondern um eine gesetzliche Fiktion: Denn eine gemäß § 4 Abs. 1 BDSG rechtfertigungsbedürftige Übermittlung liegt nach § 3 Abs. 4 Nr. 3 BDSG nur bei der Bekanntgabe personenbezogener Daten an Dritte vor; der Auftragsdatenverarbeiter, der in der EU oder im EWR tätig wird (auf den Sitz kommt es nicht an), ist allerdings durch § 3 Abs. 8 Satz 3 BDSG aus dem Begriff des „Dritten“ ausgenommen.

Die Datenweitergabe zwischen Auftraggeber und Auftragnehmer stellt somit „nur“ eine Nutzung der Daten dar. Beide werden insoweit als rechtliche Einheit behandelt.[4] § 11 Abs. 1 BDSG regelt, dass der Auftraggeber für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich bleibt. Auch die Betroffenenrechte etwa auf Auskunft, Löschung und Schadensersatz sind nach § 11 Abs. 1 Satz 2 BDSG gegenüber dem Auftragge-

1 Der Beitrag geht – leicht gekürzt und bearbeitet – auf einen Vortrag bei der DSRI-Herbstakademie 2013 zurück, der im Tagungsband Jürgen Taeger (Hrsg.), Law as a Service (LaaS) – Recht im Internet- und Cloud-Zeitalter, Edewecht 2013, dokumentiert ist.

2 Vgl. Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 20 ff.; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 9; Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 10, 11 ff.; Schaffland/Wiltfang, BDSG, Stand Lfg. 1/13, 2013, § 11, Rn. 7. Zum Meinungsstreit und insbesondere zu den beachtlichen Argumenten der Mindermeinung Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 14 ff; kritisch auch Plath, in: Plath, BDSG, 2013, § 11, Rn. 27 ff.

3 Plath, in: Plath, BDSG, 2013, § 11, Rn. 23; a. A. Schaffland/Wiltfang, BDSG, Stand Lfg. 1/13, 2013, § 11, Rn. 3.

4 Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 2; Plath, in: Plath, BDSG, 2013, § 11, Rn. 2; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 4; Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 11 BDSG, Rn. 3.

Matthias Bergt

ist Rechtsanwalt bei v. Boetticher Hasse Lohmann in Berlin.

E-Mail: mbergt@boetticher.com

ber geltend zu machen. Der Auftragsdatenverarbeiter darf deshalb beispielsweise eine Auskunft an Betroffene (§ 34 BDSG) nur auf ausdrückliche Weisung und eindeutig im Namen des Auftraggebers erteilen.[5]

Eine eigene Haftung des Auftragnehmers kommt allerdings in Betracht, wenn er die Daten weisungswidrig verwendet.[6] Nach *Plath*[7] kann der Auftragnehmer dem Betroffenen auch dann haften, wenn kein (form)wirksamer Auftragsdatenverarbeitungsvertrag abgeschlossen worden ist. Der Auftragnehmer könne sich bezüglich der durch ihn verarbeiteten Daten in einem solchen Fall nicht auf die Privilegierung des § 11 BDSG berufen. Ein ordnungsgemäßer Vertragsschluss wäre nach dieser Ansicht auch im Interesse des Auftragnehmers.

2 Anforderungen an die Vertragsgestaltung

Die „Privilegierung der Auftragsdatenverarbeitung" verbindet das Gesetz mit einem umfassenden Anforderungskatalog an die Auswahl und Kontrolle des Auftragnehmers durch den Auftraggeber und die Vertragsgestaltung. Die Auswahl des Auftragnehmers hat nach § 11 Abs. 2 Satz 1 BDSG „unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig" zu erfolgen. Der bei der Auswahl festgestellte Schutzstandard wird regelmäßig Vertragsbestandteil werden. § 11 Abs. 2 Satz 2 BDSG regelt in zehn Nummern nicht abschließend verpflichtende Mindest-Inhalte eines Auftragsdatenverarbeitungsvertrags, darunter auch die Schutzmaßnahmen. Der Vertrag muss jedenfalls im Hinblick auf die Bußgeldandrohung in § 43 Abs. 1 Nr. 2b BDSG zwingend in Schriftform (§ 126 BGB) abgeschlossen werden,[8] auch wenn zweifelhaft ist, ob es sich dabei um ein konstitutives Schriftformerfordernis handelt.[9]

Während der größte Teil der Liste des § 11 Abs. 2 Satz 2 BDSG keine Schwierigkeiten bereitet und oft auf Verfahrensverzeichnis oder Musterformulierungen zurückgegriffen werden kann, stellen die Regelungen über die erforderlichen technischen und organisatorischen Maßnahmen der Datensicherheit und deren Kontrolle durch den Auftraggeber in der Praxis vielfach ein Problem dar.

2.1 Maßnahmen der Datensicherheit

Das Gesetz verlangt Festlegungen zu den technisch-organisatorischen Maßnahmen der Datensicherheit „im Einzelnen". Wenn auch die Festlegungen nicht bis ins kleinste Detail gehen müssen, so verbietet es sich doch, nur die abstrakten gesetzlichen Regelungen abzuschreiben.[10] Vielmehr müssen konkret erforderliche Sicherheitsmaßnahmen vereinbart werden, deren Vorhandensein sodann überprüft werden kann.

2.1.1 Ermittlung des erforderlichen Sicherheitsniveaus

Die fortbestehende Verantwortlichkeit des Auftraggebers für den Auftragnehmer wie der Zweck des Gesetzes, den Schutz des Betroffenen nicht durch Auslagerung von Datenverarbeitungsprozessen zu verringern, erfordern, dass der Auftraggeber sich zunächst darüber Klarheit verschafft, welches Schutzniveau für die auszulagernden Daten erforderlich wäre, wenn die Verarbeitung bei ihm selbst erfolgen würde.[11] Dieses Schutzniveau wird regelmäßig den Mindeststandard darstellen, den der Auftragnehmer einhalten muss.[12]

Welche technisch-organisatorischen Maßnahmen der Datensicherheit letztlich erforderlich sind, ist eine Frage der Abwägung (§ 9 Satz 2 BDSG) im Einzelfall und hängt sowohl von der Schutzbedürftigkeit der Daten ab,[13] als auch davon, ob es sich um eine Auftragsdatenverarbeitung im herkömmlichen Sinne handelt oder „nur" um Wartungsverträge im Sinne von § 11 Abs. 5 BDSG, bei denen je nach Ausgestaltung (Vor-Ort-Service oder Fernwartung) ein großer Teil der technisch-organisatorischen Maßnahmen keiner Regelung bedarf, da sie nur den Auftraggeber betreffen.

2.1.2 Besondere regelungsbedürftige Sicherheits-Aspekte

Gesondert hingewiesen sei an dieser Stelle auf die Erforderlichkeit von Regelungen über die sichere Löschung – auch aus dem Backup –, Rückgabe oder Vernichtung der Datenträger und die Sicherheit der Datenübertragung und -speicherung.

Verschlüsselung kann in diesem Zusammenhang eine herausragende Rolle spielen, denn eine nach dem Stand der Technik verschlüsselte Festplatte lässt sich durch reines Löschen des Schlüssels sicher löschen und kann auch problemlos im Rahmen von Garantie oder Gewährleistung ausgetauscht werden[14] – anderenfalls muss auf die Garantie oder Gewährleistung verzichtet werden, wenn (wie meist) eine vorherige sichere Löschung des defekten Laufwerks nicht möglich ist und der Anbieter (wie meist) Ersatz nur im Austausch gegen das defekte Gerät liefert.

Auch bei der Übertragung von Daten über unsichere Netze wie das Internet ist auf eine lückenlose Verschlüsselung zu achten. In der Praxis beschränkt sich der Einsatz von Verschlüsselungstechnik allzu oft auf den Bereich, der für Endkunden sichtbar ist, beispielsweise die Bestellung im Webshop – während hingegen die Daten danach beispielsweise per unverschlüsselter E-Mail weitergeleitet werden[15].

2.1.3 Sicherheitsniveau des Anbieters

Da bereits die Auswahl des Auftragnehmers „unter besonderer Berücksichtigung der Eignung der von ihm getroffenen techni-

5 Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 50; vgl. auch Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 11 BDSG, Rn. 3.

6 Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 28; Plath, in: Plath, BDSG, 2013, § 11, Rn. 40; Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 11 BDSG, Rn. 23.

7 Plath, in: Plath, BDSG, 2013, § 11, Rn. 40.

8 Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 54; Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 64.

9 Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 54.

10 Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 52; Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 65.

11 Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 58; Bergt, ITRB 2012, 45; vgl. auch Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 31.

12 Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 58; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 20; Bergt, ITRB 2012, 45; vgl. auch Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 33.

13 Schultze-Melling, in: Taeger/Gabel, BDSG, 2010, § 9, Rn. 20; Bergt, ITRB 2012, 45; Bergt, NJW 2011, 2752 (2754); Gola/Schomerus, BDSG, 11. Aufl. 2012, § 9, Rn. 9.

14 Vgl. zur Löschung bei Verschlüsselung Stiemerling/Hartung, CR 2012, 60 (65); allgemein zur Wartung bei verschlüsselten Daten Plath, in: Plath, BDSG, 2013, § 11, Rn. 122.

15 Zu den Risiken des unverschlüsselten Versands von E-Mails vgl. Bergt, NJW 2011, 3752 (3753).

schen und organisatorischen Maßnahmen" zu erfolgen hat (§ 11 Abs. 1 Satz 1 BDSG), kann ggf. auf in diesem Zusammenhang vorgelegte Sicherheitskonzepte, Zertifizierungen und Aufstellungen der technisch-organisatorischen Maßnahmen zurückgegriffen werden, die zum Vertragsbestandteil gemacht werden können. Ebenso kommt die Übersendung einer umfassenden Liste möglicher technisch-organisatorischer Maßnahmen an den künftigen Auftragnehmer in Betracht, aus der die vorhandenen Sicherheitsmaßnahmen in den Vertrag übernommen werden. Selbstverständlich ist stets zu prüfen, ob die getroffenen Maßnahmen das erforderliche Schutzniveau erfüllen; ggf. ist die Einführung zusätzlicher Sicherheitsmaßnahmen mit dem Auftragnehmer zu vereinbaren.[16]

Da sich die Bedrohungslage aufgrund technologischer wie politischer Entwicklungen ständig ändern kann – aber auch aufgrund von Änderungen der verarbeiteten Daten deren Schutzbedürftigkeit –, sollten jedenfalls längerfristige Verträge unbedingt Regelungen darüber enthalten, dass die zu treffenden technisch-organisatorischen Maßnahmen ggf. anzupassen sind, um den erforderlichen Sicherheitsstandard zu halten, und wie ggf. anfallende Zusatzkosten von den Parteien zu tragen sind.

2.2 Weiterer Regelungsbedarf

Die Liste des § 11 Abs. 2 Satz 2 BDSG ist nicht abschließend (Wortlaut „insbesondere"). Nur beispielhaft seien folgende mögliche weitere Vertragsinhalte angesprochen:

Ein Zurückbehaltungsrecht des Auftragnehmers an Daten – einschließlich Datenträgern, die personenbezogene Daten enthalten – ist zwingend auszuschließen.[17] Anderenfalls kann der Auftraggeber seinen gesetzlichen Pflichten (z. B. Auskunft, Löschung, Berichtigung) ggf. nicht nachkommen.

Bei der Regelung der Kontrollrechte des Auftraggebers sollte zu Klarstellungszwecken ausdrücklich vereinbart werden, dass den Auftragnehmer entsprechende Duldungs- und Mitwirkungspflichten – insbesondere auch zur Auskunftserteilung und zur Vorlage relevanter Unterlagen[18] – treffen.[19] Auch wenn seitens der Auftragnehmer wegen der mit Kontrollen verbundenen Belästigungen regelmäßig versucht wird, die Kontrollrechte des Auftraggebers möglichst restriktiv zu fassen, darf sich der Auftraggeber keinesfalls darauf einlassen, weniger Kontrollrechte zu vereinbaren als die Schutzbedürftigkeit der zu verarbeitenden Daten erfordert. Berichte und Zertifizierungen vertrauenswürdiger Stellen können eigene Kontrollen des Auftraggebers zwar vom Grundsatz her erübrigen;[20] im Hinblick auf die Schutzbedürftigkeit der Daten und für den Fall, dass die vorgelegten Unterlagen nicht ausreichend sind, sollte sich der Auftraggeber aber ggf. ergänzende Kontrollrechte vorbehalten.[21] Die Kontrollrechte des betrieblichen Datenschutzbeauftragten und des Betriebsrats des Auftraggebers sollten ausdrücklich in den Vertrag aufgenommen werden.[22]

Wenn der Vertrag bereits vor Abschluss der Erstkontrolle verbindlich geschlossen werden soll, sollte unbedingt ein Rücktrittsrecht für den Fall vereinbart werden, dass bei der Erstkontrolle nicht behebbare Mängel festgestellt werden oder diese nicht umgehend behoben werden, oder die Auftragserteilung sollte aufschiebend bedingt durch eine beanstandungsfreie Erstkontrolle erfolgen.[23]

Soweit der Einsatz von Subunternehmern überhaupt gestattet werden soll, sollte jede Einschaltung von Subunternehmern von der schriftlichen Zustimmung des Auftraggebers abhängig gemacht werden.[24] Notfalls kommt eine Information des Auftraggebers über die beabsichtigte Einschaltung eines Subunternehmers mit Widerspruchsmöglichkeit in Betracht, wobei eine konkrete Benennung des Subunternehmers verpflichtend sein sollte. In jedem Fall muss sichergestellt sein, dass das erforderliche Schutzniveau auch beim Subunternehmer eingehalten wird, dass der Auftraggeber seine Kontrollrechte auch beim Subunternehmer voll ausüben kann und auch dem Subunternehmer keine Zurückbehaltungsrechte zustehen. Zu berücksichtigen bleibt, dass Unterauftragsverhältnisse auch bei Wartung nach § 11 Abs. 5 BDSG vorliegen.[25]

Auch wenn die Erstellung des Verfahrensverzeichnisses und die Benachrichtigung der Aufsichtsbehörde und der Betroffenen bei Abhandenkommen von Daten Sache des Auftraggebers sind, wird er hierfür häufig Unterstützung des Auftragnehmers benötigen. Entsprechende Pflichten des Auftragnehmers sollten daher noch über die Mindestanforderungen des § 11 Abs. 2 Satz 2 Nr. 8 BDSG hinaus vereinbart werden.[26] Ebenso sollte nicht nur eine Informationspflicht über sicher festgestellte schwerwiegende Datenverluste i. S. d. § 42a BDSG vereinbart werden, sondern auch über nur mögliche, und zwar unabhängig von ihrer Schwere.[27]

Empfehlenswert sind zudem Festlegungen, welche Verstöße des Auftragnehmers einen wichtigen Grund im Sinne des § 314 BGB für eine außerordentliche Kündigung darstellen, in welchen Fällen eine Abmahnung entbehrlich ist und im Fall von Rahmenverträgen, ob nur der jeweils einzelne betroffene Vertrag gekündigt werden kann oder sämtliche Vereinbarungen unter dem Rahmenvertrag.[28] Klare Vereinbarungen schaffen angesichts des offenen Wortlauts der §§ 314 Abs. 1 Satz 2 und 323 Abs. 2 Nr. 3 BGB für beide Parteien Rechtssicherheit. Zur Sicherstellung ordnungsgemäßer Auftragserfüllung sehr hilfreich – wenn auch praktisch oft schwer durchsetzbar – sind Vertragsstrafen bei Datenschutzverstößen.[29]

16 Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 42.

17 Als möglicher weiterer Vertragsinhalt genannt bei Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 53; eine derartige Klausel findet sich auch im Mustervertrag in Bayerisches Landesamt für Datenschutzaufsicht, Auftragsdatenverarbeitung nach § 11 BDSG – Gesetzestext mit Erläuterungen, Stand Mai 2013, 17.

18 Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 78.

19 Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 48.

20 Dazu sogleich unter 3.

21 Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 48; EuroCloud Deutschland_eco e.V., Leitfaden Cloud Computing – Recht, Datenschutz & Compliance, 2010, 13.

22 Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 79; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 21a, 22.

23 Bergt, ITRB 2012, 45 (46); ähnlich auch Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 57.

24 Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 76; vgl. auch Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 18e.

25 Vgl. Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 43a; unklar und zweifelhaft dagegen Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 18e, die als Unterauftragsverhältnisse nur solche Dienstleistungen von Subunternehmern ansehen wollen, die unmittelbar der Erfüllung des Ursprungauftrags dienen; zur Widerlegung dieser Ansicht vgl. das Beispiel bei Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 44.

26 Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 80; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 18g; Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 53.

27 Vgl. Plath, in: Plath, BDSG, 2013, § 11, Rn. 109.

28 Vgl. eine ähnliche Klausel im Mustervertrag in Bayerisches Landesamt für Datenschutzaufsicht, Auftragsdatenverarbeitung nach § 11 BDSG – Gesetzestext mit Erläuterungen, Stand Mai 2013, 10.

29 Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 46; vgl. auch Ziff. VII des Musters bei Schaffland/Wiltfang, BDSG, Stand Lfg. 1/13, 2013, § 11,

Da § 7 BDSG für das Verhältnis zwischen Auftraggeber und Betroffenem eine Beweislastumkehr vorsieht, sollte auch der Auftragsdatenverarbeitungsvertrag eine entsprechende Regelung enthalten.[30]

2.3 Verfahren und Vertragstechnik

Im Fall von Ausschreibungen für Auftragsdatenverarbeitung ist zu beachten, ob eine vorherige Kontaktaufnahme zum Bieter zulässig ist; ggf. ist die Ausschreibung so zu gestalten, dass Angaben zu den technisch-organisatorischen Maßnahmen beim Bieter bereits mit dem Angebot eingereicht werden müssen.[31]

Vertragstechnisch hilfreich ist ein modularer Aufbau, bei dem Bestandteile, die sich öfter ändern oder die unübersichtlich sind, in Anlagen ausgelagert werden, beispielsweise über Gegenstand und Dauer des Auftrags, über namentlich benannte Subunternehmer, deren Einsatz gestattet wird, oder über die zu treffenden technisch-organisatorischen Maßnahmen.

2.4 Vorgehen bei Massenverträgen

Die Konzeption der gesetzlichen Regelungen zur Auftragsdatenverarbeitung stammt aus Zeiten, in denen Auftragsdatenverarbeitung nur im Rahmen großer IT-Projekte denkbar war, die ohnehin mit einem organisatorischen und finanziellen Aufwand verbunden waren, bei dem die Anforderungen des § 11 BDSG kaum messbare Auswirkungen auf die Gesamtkosten hatten. Auftragsdatenverarbeitung ist heute allerdings ubiquitär geworden, wie nur das Beispiel E-Mail-Account zeigt. Das heutige Wirtschaftsleben ist von einer Vielzahl kleiner und kleinster Auftragsdatenverarbeitungen geprägt, bis hin zum extremst flexibilisierten Cloud Computing. Der administrative Aufwand zur Erfüllung der gesetzlichen Pflichten kann die Gesamtkosten der eigentlichen Leistung hier schnell übersteigen, so dass die Praxis die Vorschrift des § 11 BDSG trotz Bußgeldbewehrung weiterhin schlicht oftmals ignoriert.

Um die Kostenvorteile nicht zu verspielen, sollte die Initiative für rechtskonforme Auftragsdatenverarbeitungsverträge vom jeweiligen Anbieter ausgehen. Dieser kann sich einmalig ein Vertragsmuster erstellen lassen, das er all seinen Kunden zum Abschluss anbietet.[32] Für den Anbieter kann dies – gerade in Zeiten zunehmender Sensibilisierung für Datenschutz – ein erhebliches Werbeargument sein, das ihm nur geringe Kosten verursacht. Auch wenn ein solches Verfahren dem Anbieter erhebliche Möglichkeiten gewährt, die vertraglichen Vereinbarungen zu seinen Gunsten zu gestalten, sollte der Anbieter sich nicht dazu verleiten lassen, allzu schwache und allzu einseitige Regelungen vorzusehen. Denn das formale Verfahren ist nur dann sinnvoll, wenn die vertraglichen Regelungen auch inhaltlich für eine Auftragsdatenverarbeitung ausreichen.

Da die erforderlichen technisch-organisatorischen Maßnahmen von der Schutzbedürftigkeit der verarbeiteten Daten abhängen,[33] wird ein derartiger Standard-Auftragsdatenverarbeitungsvertrag typischerweise nur für normal vertrauliche personenbezogene Daten ausreichende Sicherheitsmaßnahmen vorsehen. Wollte man einen Standard-Vertrag für sämtliche Arten von Daten nutzen wollen, müsste auch für die wenig schutzbedürftigen Daten ein besonders hohes Schutzniveau eingehalten werden, was wirtschaftlich nicht sinnvoll erscheint. Der Anbieter sollte daher deutlich darauf hinweisen, für welchen Schutzbedarf das Angebot aus seiner Ansicht geeignet ist, und ggf. für besonders vertrauliche Daten ein weiteres Angebot, ggf. mit Aufpreis, bereitstellen.

Im Massenverkehr scheiden individuelle Prüfungen durch jeden einzelnen Auftraggeber aus. Daher müssen bereits im Vertrag Regelungen zum Ersatz der Kontrolle des Auftraggebers durch Zertifizierungen durch unabhängige Dritte[34] getroffen werden.

3 Anforderungen an die Kontrolle des Auftragnehmers

§ 11 Abs. 2 Satz 4 und 5 BDSG verpflichten den Auftraggeber, „sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen“ und das Ergebnis zu dokumentieren. Wie bereits bei der Auftragserteilung ist ein Verstoß gegen die Verpflichtung zur Erstkontrolle vor Beginn der Datenverarbeitung nach § 43 Abs. 1 Nr. 2b BDSG bußgeldbedroht. Nicht geregelt ist, wie die Überzeugungsbildung auszusehen hat.

Zweck der Verpflichtung zur Erstkontrolle ist es, zu gewährleisten, dass alle erforderlichen technisch-organisatorischen Maßnahmen durch den Auftragnehmer getroffen worden sind, bevor durch den Beginn der Datenverarbeitung Betroffenenrechte beeinträchtigt werden können. Die Erstkontrolle muss daher sicherstellen, dass alle Maßnahmen ordnungsgemäß implementiert sind und eventuelle Mängel gefunden und rechtzeitig beseitigt werden und aus diesem Grund besonders umfassend erfolgen.[35] Die genaue Intensität der Prüfung ergibt sich dabei letztlich aus Umfang und Komplexität der Datenverarbeitung und der Schutzbedürftigkeit der verarbeiteten Daten.[36]

3.1 Kontrolle durch Dritte

Eine Vor-Ort-Kontrolle hat der Gesetzgeber bewusst nicht vorgeschrieben.[37] Vielmehr kann der Auftraggeber auch ein Testat eines Sachverständigen einholen, oder es kann im Einzelfall eine schriftliche Auskunft des Auftragnehmers genügen.[38] Über die Gesetzesbegründung hinaus muss es auch nicht der Auftraggeber sein, der einen vertrauenswürdigen und sachkundigen Dritten mit der Überprüfung des Auftragnehmers beauftragt, sondern es kann auch der Auftragnehmer sein, der sich zertifizieren lässt.[39] Diese Auffassung wird zwischenzeitlich auch von Auf-

Anh. 1.

30 Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 21, 45.

31 Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 48e.

32 EuroCloud Deutschland_eco e.V., Leitfaden Cloud Computing – Recht, Datenschutz & Compliance, 2010, 10. Aus der Praxis sei auf das von Google für Analytics verwendete Verfahren verwiesen, bei dem der Auftraggeber zwei Exemplare des Vertrages nebst frankiertem Rückumschlag und Erklärung, dass er die Vordrucke nicht verändert hat, an Google senden muss, siehe http://www.google.com/analytics/terms/de.pdf (Abruf am 13. Juli 2013).

33 Siehe unter 2.1.1.

34 Dazu sogleich unter 3.1.

35 Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 36.

36 Bergt, ITRB 2012, 45 (46).

37 BT-Drs. 16/13657, 18.

38 So die Gesetzesbegründung des Innenausschusses, BT-Drs. 16/13657, 18; vgl. auch Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 59; Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 33, 39; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 21; Bergt, ITRB 2012, 45 (46).

39 Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 48b; Bergt, ITRB 2012, 45 (46); vgl. auch Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 21: „Anforderung von Prüfergebnissen oder Zertifikaten“; Petri, in: Simitis, BDSG,

sichtsbehörden geteilt.[40] Hinsichtlich des Google-Dienstes „Analytics" hat der Hamburgische Datenschutzbeauftragte ausdrücklich ein Verfahren akzeptiert, in dem Google selbst seine Zertifizierung beauftragt.[41]

3.2 Kontrolle ausschließlich durch Zertifizierung?

Unklar ist, ob es den gesetzlichen Anforderungen genügt, wenn der Nachweis der Umsetzung der technisch-organisatorischen Maßnahmen ausschließlich durch Vorlage von Prüfberichten und Zertifikaten Dritter erfolgt. Bisher gab es bei den Aufsichtsbehörden die Tendenz, dass der Auftraggeber zumindest das Recht haben müsse, trotz Zertifizierung selbst die Kontrolle vorzunehmen.[42]

Richtigerweise wird man allerdings differenzieren und eine vollständige Ersetzung der eigenen Kontrolle des Auftraggebers durch Zertifikate unabhängiger und sachkundiger Dritter grundsätzlich zulassen müssen.[43] Hinsichtlich „Google Analytics" hat der Hamburgische Datenschutzbeauftragte ein Verfahren akzeptiert, in dem die Kontrollrechte des Auftraggebers sich ausschließlich auf die Einsicht in den Prüfbericht eines Wirtschaftsprüfers beschränken.[44]

3.3 Anforderungen an Zertifizierungen

Die grundsätzliche Zulässigkeit, die gebotene Kontrolle des Auftragnehmers durch Zertifizierungen durch sachkundige und vertrauenswürdige Dritte zu ersetzen, hat allerdings keine Auswirkungen auf den Umfang der Prüfung. Die Nutzung von Testaten statt eigener Kontrolle darf insbesondere nicht zu einer Verringerung der Kontrollintensität führen. Folgerichtig weisen die Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder völlig zu Recht darauf hin, dass „das Vorliegen von Zertifikaten [...] den Cloud-Anwender nicht von seinen Kontrollpflichten" entbindet.[45] Der Auftraggeber muss daher einerseits überprüfen, ob die zertifizierende Stelle tatsächlich sachkundig und unabhängig ist, und andererseits kontrollieren, dass der Prüfbericht tatsächlich das Vorhandensein sämtlicher vereinbarten technisch-organisatorischen Maßnahmen bestätigt.[46] Ist das vorgelegte Testat nicht in jeder Hinsicht „überzeugend", muss der Auftraggeber ergänzende Kontrollen vornehmen.[47]

Um die administrativen Kosten gering zu halten, ist daher eine genaue Abstimmung des Prüfberichts auf den Vertrag erforderlich. Auch die Gestaltung des Berichts sollte sich an der Gliederung der vertraglichen Vereinbarungen zu den technisch-organisatorischen Maßnahmen orientieren. Um die Eignung des Dritten bewerten zu können, sollte dieser selbst von einer vertrauenswürdigen Stelle zertifiziert sein, beispielsweise vom Bundesamt für Sicherheit in der Informationstechnik (BSI).[48]

Auch hinsichtlich der Intensität der Zertifizierung sollte der Auftragnehmer – wie bereits bei der Vertragsgestaltung – die Interessen seiner Kunden nicht aus dem Auge lassen. Denn nur wenn die Auditierung durch den Dritten so eingehend ist, dass sie eine Überzeugung von der Einhaltung der Sicherheitsmaßnahmen gestattet, können die Kunden ihren gesetzlichen Verpflichtungen als Auftraggeber nachkommen.

3.4 Dokumentation der Kontrolle

Auch eine Kontrolle anhand von Zertifikaten Dritter ist zu dokumentieren, § 11 Abs. 2 Satz 5 BDSG. Die Dokumentation kann allerdings im Hinblick auf den bereits vorliegenden Bericht erheblich kürzer ausfallen als bei einer selbst durchgeführten Kontrolle, sollte aber erkennen lassen, dass der Auftraggeber den Prüfbericht dahingehend durchgesehen hat, dass er eine Einhaltung der vereinbarten technisch-organisatorischen Maßnahmen bestätigt. In jedem Fall genügt ein Ergebnisprotokoll der Kontrolle.[49] Die Dokumentationspflicht ist nicht bußgeldbewehrt, und es ist auch keine Form vorgeschrieben. Eine sicher aufzubewahrende Dokumentation ist jedoch dringend anzuraten, da dieser im Hinblick auf ein drohendes Bußgeld wegen unterlassener Erstkontrolle (§ 43 Abs. 1 Nr. 2b BDSG) große Bedeutung zukommen kann.[50]

4 Gesetzgeberischer Handlungsbedarf

Zwar kann mit den vorstehend dargestellten Maßnahmen der Aufwand einer ordnungsgemäßen Auftragsdatenverarbeitung extrem verringert werden, so dass rechtskonformes Handeln auch im Massenverkehr möglich wird. Probleme stellen allerdings insbesondere der wegen des Schriftformerfordernisses nötige Medienbruch sowie die Kontrolle des Auftragnehmers dar.

7. Aufl. 2011, § 11, Rn. 59: ausreichend, wenn der Auftragnehmer Zertifizierungen „vorweist".

40 Bayerisches Landesamt für Datenschutzaufsicht, Auftragsdatenverarbeitung nach § 11 BDSG – Gesetzestext mit Erläuterungen, Stand Mai 2013, 8; Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, 2011, 9.

41 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Hinweise für Webseitenbetreiber mit Sitz in Hamburg, die Google Analytics einsetzen, Stand März 2013, http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_01.pdf (Abruf: 13. Juli 2013).

42 EuroCloud Deutschland_eco e.V., Leitfaden Cloud Computing – Recht, Datenschutz & Compliance, 2010, 13. Erhebliche Rechtsunsicherheit sieht auch die Arbeitsgruppe „Rechtsrahmen des Cloud Computing" im Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, 2012, 13.

43 Bergt, ITRB 2012, 45 (46); vgl. auch Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 21: „kann im Einzelfall (...) genügen"; Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 48: je nach Schutzbedürftigkeit ggf. Ergänzungsprüfungen. Das Bundesamt für Sicherheit in der Informationstechnik – insoweit unter Beteiligung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – bejaht im Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestanforderungen in der Informationssicherheit –, 2012, 74, pauschal die Ersetzbarkeit von Vor-Ort-Kontrollen durch Zertifizierungen.

44 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Hinweise für Webseitenbetreiber mit Sitz in Hamburg, die Google Analytics einsetzen, Stand März 2013, http://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_01.pdf (Abruf: 13. Juli 2013). Vgl. Anlage 1 Nr. 5 des Vertrags, http://www.google.com/analytics/terms/de.pdf (Abruf am 13. Juli 2013).

45 Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, 2011, 9.

46 Gola/Schomerus, BDSG, 11. Aufl. 2012, § 11, Rn. 21; Bergt, ITRB 2012, 45 (46).

47 Bergt, ITRB 2012, 45 (46); vgl. auch Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 48; Plath, in: Plath, BDSG, 2013, § 11, Rn. 108.

48 Vgl. hierzu https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzZertifikat/Auditoren/auditoren_node.html (Abruf: 13. Juli 2013).

49 Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, Rn. 39.

50 Petri, in: Simitis, BDSG, 7. Aufl. 2011, § 11, Rn. 63; Gabel, in: Taeger/Gabel, BDSG, 2010, § 11, 39; Plath, in: Plath, BDSG, 2013, § 11, Rn. 114; Bergmann/Möhrle/Herb, BDSG, Stand 45. EL, 2012, § 11, Rn. 48c.

Der Dokumentationszweck des Auftragsdatenverarbeitungsvertrags erfordert de lege ferenda keine Schriftform im Sinne von § 126 BGB.[51] Dies hat der Entwurf einer Datenschutz-Grundverordnung aufgenommen und verlangt nur eine Dokumentation ohne nähere Anforderungen an die Form.[52]

Auch wenn angesichts des weiten Spektrums an personenbezogenen Daten und des damit verbundenen äußerst unterschiedlichen Schutzbedarfs die erforderlichen technisch-organisatorischen Maßnahmen der Datensicherheit nicht allgemeingültig festgelegt werden können, so ließen sich doch für bestimmte Standard-Anwendungsfälle Anforderungsprofile definieren, die sowohl der Vertragsgestaltung als auch der Auditierung durch den vertrauenswürdigen Dritten zu Grunde gelegt werden könnten. Da das Gesetz nicht verbietet, über die gebotenen Mindestanforderungen der Datensicherheit hinauszugehen, ließe sich eine weitere Vereinfachung dadurch erreichen, dass für die Zertifizierung ein einheitlicher höherer Sicherheitsstandard zu Grunde gelegt wird, der eine Vielzahl von Anwendungsfällen abdeckt.[53] Aus Kostengründen wird es sich allerdings verbieten, generell von einem hohen Sicherheitsstandard auszugehen.[54] Jedoch ließen sich einige wenige Sicherheitsstufen mit den jeweils erforderlichen technisch-organisatorischen Maßnahmen definieren, für die jeweils spezifische Testate erstellt werden könnten.[55]

Um Rechtssicherheit zu erreichen, spricht vieles dafür, diese Anforderungsprofile europaweit einheitlich festzulegen, wobei ein hoher Sicherheitsstandard jederzeit gewährleistet sein muss, so dass eine schnelle Reaktion auf politische und technische Entwicklungen möglich sein muss.[56]

5 Fazit

Auftragsdatenverarbeitung kann auch im Massengeschäft rechtskonform gestaltet werden, indem die Anbieter standardisierte Verträge anbieten und sich standardisiert von sachkundigen und vertrauenswürdigen Dritten zertifizieren lassen. Die Anbieter sollten den mit einer Datenschutz-Zertifizierung verbundenen Werbeeffekt vermehrt nutzen. Zur Beseitigung der verbleibenden Probleme – Schriftformerfordernis und Kontrolle des Auftragnehmers – ist allerdings der Gesetzgeber gefordert.

51 Arbeitsgruppe „Rechtsrahmen des Cloud Computing" im Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, 2012, S. 10.

52 Art. 26 Abs. 3 des Vorschlags der Europäischen Kommission einer Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig.

53 Arbeitsgruppe „Rechtsrahmen des Cloud Computing" im Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, 2012, S. 14.

54 Bundesamt für Sicherheit in der Informationstechnik, Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestanforderungen in der Informationssicherheit –, 2012, S. 11.

55 Vgl. auch Arbeitsgruppe „Rechtsrahmen des Cloud Computing" im Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, 2012, S. 14.

56 Verschiedene Gestaltungsmöglichkeiten des Verfahrens zeigt die Arbeitsgruppe „Rechtsrahmen des Cloud Computing" im Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, 2012, S. 15 f., auf.