Thomas Hoeren

Das neue BDSG und die Auftragsdatenverarbeitung

Im Sommer 2009 wurden – bedingt durch sog. Datenschutzskandale – zwei größere Änderungsentwürfe zum BDSG verabschiedet. In der BDSG-Novelle II wurde versucht, den Fällen des unberechtigten Datenhandels zu begegnen. Am 10. Dezember 2008 hat die Bundesregierung den vom Bundesinnenminister vorgelegten Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Regelung datenschutzrechtlicher Vorschriften beschlossen. Der heftig diskutierte Entwurf wurde am 3. Juli 2009 vom Bundestag verabschiedet.[1] Neben neuen Regelungen zum Direktmarketing wurde auch der Bereich der Auftragsdatenverarbeitung neu strukturiert.

Die Neuregelungen des § 11 BDSG beruhen auf einer Bundesratsinitiative.[2] Kritisiert wurde vom Bundesrat, dass die Call-Center mit den Auftraggebern in zu losen Verbindungen stünden und eine hinreichende Kontrolle der Einhaltung des BDSG nicht gewährleistet sei. Es sei stattdessen hilfreich, wenn einige besonders wichtige Bestandteile einer solchen Festlegung im Gesetz beispielhaft aufgeführt würden. Wichtig sind hier vor allem die Ergänzungen in § 11 Abs. 2 S. 2 BDSG. Hier findet sich eine ausführliche Checkliste für die Auftragserteilung. Die entsprechende Checkliste ist nicht abschließend („insbesondere"). Die einzelnen Eckpunkte sind allerdings verbindlich, wie sich insbesondere aus den Bußgeldvorschriften des § 43 BDSG ergibt. Fehlen entsprechende Festlegungen, ist dies mit Bußgeld bewehrt.

Schon nach altem Recht bestanden viele der genannten Vertragspflichten aufgrund der Entscheidungspraxis der Aufsichtsbehörden. So regelte z.B. die Aufsichtsbehörde Baden-Württemberg schon 1980: „Dem betrieblichen Datenschutzbeauftragten des Auftraggebers obliegt es nach § 37 BDSG [jetzt § 4g BDSG], auch insoweit die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz sicherzustellen. Das bedeutet, daß er bei der Auswahl eines Auftragnehmers und bei der Auftragsvergabe regelmäßig unter Datensicherungsgesichtspunkten zu beteiligen ist und über eine Aufstellung der verschiedenen Auftragsdatenverarbeitungsverträge seines Unternehmens verfügen bzw. davon in anderer Weise unmittelbar Kenntnis erlangen können muss."[3]

Im Einzelnen war es nach der ständigen Entscheidungspraxis der Datenschutzbehörden erforderlich, im Vertrag mit dem Auftragnehmer festzulegen, welche Sicherungsmaßnahmen hinsichtlich der Zuverlässigkeit des Auftragnehmers getroffen worden sind. Der Auftragnehmer hat sich zu verpflichten, die für den konkreten Auftrag tätigen Mitarbeiter sorgfältigst, gerade im Hinblick auf den vertraulichen Umgang mit sensiblen Daten, auszuwählen. Die Zuverlässigkeit der Mitarbeiter muss regelmäßig vom Auftragnehmer überwacht werden; auch der Auftraggeber muss die Möglichkeit haben, die Zuverlässigkeit der Mitarbeiter zu testen. Ferner ist der Auftragnehmer zu verpflichten, nur sichere Programme zu verwenden, die besonders die Vertraulichkeit und Integrität der Daten gewährleisten und eine Verknüpfung mit anderen Datenbeständen verhindern.

Unklar bleiben die Abgrenzung der Auftragsdatenverarbeitung zur Funktionsübertragung und die damit verbundenen Konsequenzen. Die Auftragsverarbeitung ist von der Funktionsübertragung abzugrenzen, für die § 11 BDSG nicht zum Tragen kommen soll.[4] Allerdings irritiert bei dieser gängigen Auffassung immer noch, dass die Funktionsübertragung dann in einem liberaleren datenschutzrechtlichen Umfeld stattfinden könnte, als die in § 11 BDSG eng gefasste Auftragsdatenverarbeitung. Im Fall der Funktionsübertragung würde die Weitergabe von Daten an den Funktionsnehmer als Datenübermittlung an einen Dritten anzusehen sein, so dass (nur) die Voraussetzungen für eine zulässige Datenübermittlung nach § 29 BDSG vorliegen müssten. Ein solches Outsourcing (i.S.e. Funktionsübertragung) soll anzunehmen sein, wenn der Dritte über die reine Datenverarbeitung hinaus weitere Funktionen übernimmt.[5] Entscheidend ist dabei der Handlungsspielraum des Dritten. Sofern dieser eigenverantwortlich tätig sein kann, liegt keine Auftragsdatenverarbeitung vor. Für eine Eigenverantwort-

Prof. Dr. Thomas Hoeren

ist Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster.
E-Mail: hoeren@uni-muenster.de

1 BT-Drs. 16/12011 und BT-Drs. 16/13657.
2 BT-Drs. 16/12011, S. 40.
3 Hinweis zum BDSG Nr. 5, Staatsanz. 1980, Nr. 5, S. 6.
4 Gola/Schomerus, BDSG, 9. Auflage 2007, § 11 Rn. 9; Bergmann/Möhrle/Herb, Datenschutzrecht, 30. Ergänzungslieferung, Stand: Dezember 2004, § 11 Rn. 10.
5 Gola/Schomerus, BDSG, 9. Auflage 2007, § 11 Rn. 9.

Anzeige

DATENSCHUTZ UND INFORMATIONSSICHERHEIT
KOMPETENT UND UNABHÄNGIG

DATENSCHUTZ *gestalten wir interdisziplinär und lösungsorientiert*
- betrieblicher Datenschutzbeauftragter
- behördlicher Datenschutzbeauftragter
- Erstellung von Datenschutzkonzepten
- Durchführung von Schulungen

INFORMATIONSSICHERHEIT *analysieren wir umfassend konform zu ISO 27001 und IT-Grundschutz*
- IT-Sicherheitsbeauftragter
- IT-Sicherheit kompakt
- IT-Sicherheitsmanagement nach ITIL
- Durchführung von Penetrationstests
- SAP-Revision

www.datenschutz-nord.de

datenschutz nord

DATENSCHUTZ NORD JETZT AUCH IM SÜDEN

datenschutz süd

lichkeit spräche vor allem, wenn nicht die Datenverarbeitung oder -nutzung als solche Vertragsgegenstand sei, sondern eine konkrete Aufgabenerfüllung, für deren Erfüllung die überlassenen Daten als Hilfsmittel dienten.[6] Für ein Outsourcing im o.g. Sinne soll vor allem sprechen, dass der Outsourcing-Geber auf einzelne Phasen der Verarbeitung keinen Einfluss nehmen kann oder die Haftung für die Zulässigkeit und Richtigkeit der Daten auf den Verarbeiter abgewälzt wird.[7]

Die Regelung über Auftragsdatenverarbeitung gilt auch für die Wartung von DV-Unternehmen und den Fernzugriff (§ 11 Abs. 5 BDSG). Die Gesellschaft für Datenschutz und Datensicherheit (GDD) hat in ihrem Vertragsmuster[8] darüber hinaus vorgeschlagen, den Anwendungsbereich des § 11 BDSG auf die Fälle zu beschränken, in denen die Datenverarbeitung den Hauptzweck des Vertrages ausmacht. Daher sollen die Bestimmungen nicht zur Anwendung kommen im Verhältnis zu Reinigungsunternehmen oder Datenentsorgungsunternehmen. Dies ist meines Erachtens sehr fragwürdig, da dieser Einschränkungsvorschlag mit dem Wortlaut des § 11 BDSG nicht in Einklang steht.

6 Müthlein, RDV 1993, 165, 167.

7 Bergmann/Möhrle/Herb, Datenschutzrecht, 30. Ergänzungslieferung, Stand: Dezember 2004, § 11 Rn. 11.

8 https://www.gdd.de/nachrichten/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg.

1 Der Mustervertrag

§ 11 Abs. 2 BDSG regelt eine Art Mustervertrag, dessen Beachtung allerdings wegen der Bußgeldandrohungen nicht ganz unfreiwillig ist. Im Folgenden werden die einzelnen Kriterien des Modellvertrages erläutert.

1.1 Gegenstand und Dauer des Auftrags

Zu vereinbaren sind als Erstes der Gegenstand und die Dauer des Auftrages. Diese Verpflichtung scheint insofern überflüssig, als bei einer Auftragserteilung Gegenstand und Dauer des Auftrages ohnehin regelmäßig spezifiziert werden. Zu beachten ist, dass es sich bei Auftragsverhältnissen typischerweise um Dauerschuldverhältnisse handelt, die zeitlich begrenzt sind und entsprechende Kündigungsregeln vorsehen. Insofern ist mit einer Auftragserteilung in der Regel eine Befristung verbunden.

1.2 Umfang der Datenverarbeitung

Als Zweites sind der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen festzulegen. Insofern ist eine genaue Spezifizierung des Datenschutzanteils eines IT-Projektes notwendig. Dies macht vor allem deshalb Probleme, weil auch Auftragsverträge typischerweise komplexe Langzeitverträge sind, deren Umfang und Konkretisierung erst im Laufe des entsprechenden Projektes bestimmt bzw. vorgenommen werden kann. Daher werden die entsprechenden Datenmodelle zunächst nur abstrakt festgelegt, um dann später genauer spezifiziert zu werden. Diesbezüglich bietet es sich an, in einem ersten Schritt nur allgemein die entsprechenden Datenarten und Nutzungsformen festzulegen, um dann im Rahmen späterer Service Level Agreements (SLA) Änderungen und Erweiterungen zu spezifizieren.

1.3 Datensicherheit

Als Drittes festzulegen sind die Datensicherheitsmaßnahmen nach § 9 BDSG. Die entsprechende Datensicherheitsliste ist damit bußgeldbewehrt in einem eigenen Katalog festzulegen. Auch hier wird darauf zu achten sein, dass Datensicherheitsstandards sich verändern und auch insofern im langen Verlauf einer Auftragsdatenverarbeitung weitere Konkretisierungen erfolgen müssen.

1.4 Berichtigung und Löschung

Nach § 11 Abs. 2 S. 2 Nr. 4 BDSG ist die Berichtigung, Löschung und Sperrung von Daten festzulegen. Gemeint ist hiermit nicht die Berichtigung als solche, sondern das Verfahren, mit dem die Berichtigungs-, Löschungs- und Sperrungsansprüche der Betroffenen umgesetzt werden können. Insofern verweist die Vorschrift auf § 35 BDSG und die dort gere-

gelten Voraussetzungen für die Geltendmachung entsprechender Rechte seitens der Betroffenen. Ansprechpartner für die entsprechenden Rechte ist der Auftraggeber selbst, wie sich aus § 11 Abs. 4 BDSG ergibt. Insofern geht es hier darum, intern zwischen Auftraggeber und Auftragnehmer festzulegen, wie der Auftragnehmer auf entsprechende Weisungen des Auftraggebers im Hinblick auf die Berichtigung, Löschung und Sperrung solcher Daten zu reagieren hat.

1.5 Pflichten des Auftragnehmers

Als Fünftes ist zu spezifizieren, wie die Einhaltung der Pflichten des Auftragnehmers nach § 11 Abs. 4 BDSG sichergestellt werden soll. § 11 Abs. 4 Nr. 2 BDSG verweist für die nicht-öffentlichen Stellen der Auftragsdatenverarbeitung auf §§ 4f, 4g und § 38 BDSG. Nach § 4f BDSG ist ein Beauftragter für den Datenschutz zu bestellen, wenn das Unternehmen eine bestimmte Größe erreicht hat. Dieser hat ein besonderes Aufgabenprofil nach §§ 4f, 4g BDSG. Er ist im Übrigen mit einer besonderen Stellenbeschreibung versehen, die insbesondere auf die Unabhängigkeit und Weisungsfreiheit des Datenschutzbeauftragten abstellt (§ 4f Abs. 3 BDSG). Zu beachten ist vor allem auch die Regelung des § 4f Abs. 2 S. 1 BDSG, nach der zum Datenschutzbeauftragten nur bestellt werden darf, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Insofern hat also der Auftraggeber zu spezifizieren und zu kontrollieren, ob ein entsprechender Datenschutzbeauftragter beim Auftragnehmer bestellt wird und ob dieser die entsprechende Fachkunde, Zuverlässigkeit und Unabhängigkeit aufweist. Im Übrigen ist der Auftragnehmer zur Gewährleistung der Datensicherungsmaßnahmen nach § 9 BDSG verpflichtet. Das Datengeheimnis (§ 5 BDSG) gilt auch für seine Mitarbeiter. Unbefugte Verarbeitungen stellen auch für ihn ggf. strafbare Handlungen nach § 44 BDSG dar.

Ferner unterliegt auch der Auftragnehmer der Datenschutzaufsicht. Etwas rätselhaft ist allerdings der Verweis auf § 38 BDSG, da dort nur die entsprechenden Kontrollbefugnisse der Aufsichtsbehörden geregelt sind. Gemeint sind hiermit aber vor allem die Anordnungsbefugnisse und Kontrollrechte der Behörden nach § 38 Abs. 4 und 5 BDSG sowie die Auskunftspflichten nach § 38 Abs. 3 BDSG, die entsprechende Pflichten der verarbeitenden Stelle auslösen. § 38 Abs. 3 BDSG spricht insofern auch davon, dass die der Kontrolle unterliegenden Stellen sowie die mit ihrer Leitung beauftragten Personen entsprechende Auskünfte zu erteilen haben.

1.6 Unteraufträge

Nach § 11 Abs. 2 S. 2 Nr. 6 BDSG ist zu regeln, ob Unterauftragsverhältnisse begründet werden dürfen. Das Gesetz schließt die Begründung solcher Unteraufträge nicht aus, verlangt aber eine Regelung darüber, ob der Auftragnehmer überhaupt zur Erteilung von Unteraufträgen berechtigt ist. Bei einem solchen Unterauftragsverhältnis wären dann wieder die Regelungen des § 11 BDSG einzuhalten. Auf diese Weise können Vertragsketten entstehen, in denen der Auftraggeber den Auftragnehmer kontrolliert, dieser aber wiederum vertraglich seine Unterauftragnehmer überwacht. Zu beachten ist hier vor allem auch, dass die Begründung von Unterauftragsverhältnissen nach § 613 BGB problematisch sein kann. Diese Bestimmung sieht vor, dass eine Übertragung von Dienstverhältnissen auf Dritte im Zweifel nicht vorgenommen werden kann.

1.7 Kontrollrechte

In § 11 Abs. 2 S. 2 Nr. 7 BDSG findet sich der Kern der erforderlichen Festlegungen, nämlich die Verpflichtung zur Einführung von Kontrollrechten des Auftraggebers und entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmers. Diese Bestimmung entspricht der bisherigen Entscheidungspraxis der Aufsichtsbehörden, die eine Auftragsdatenverarbeitung nur dann angenommen haben, wenn entsprechende Kontrollrechte des Auftraggebers vorgesehen waren. Erstaunlicherweise werden die Kontrollrechte nicht weiter bestimmt, sondern nur als solche in § 11 Abs. 2 S. 2 Nr. 7 BDSG erwähnt. Der Auftragnehmer muss durch die Kontrollrechte in eine solche Beziehung zum Auftraggeber gebracht werden, dass er diesem in Sachen Datenschutz und Datensicherheit vollständig unterliegt.

Zu beachten ist hier allerdings, dass die Kontrollrechte nur dann vereinbart werden können, wenn die Vorgaben des § 307 Abs. 2 Nr. 1 BGB eingehalten werden. Insbesondere sieht es die Rechtsprechung als problematisch an, wenn entsprechende Audit-Rechte des Auftraggebers vor Ort vorgesehen werden. Denn auf diese Weise kann der Auftraggeber Betriebsgeheimnisse des Auftragnehmers erfahren, was wiederum datenschutzrechtlich bedenklich ist. Dies gilt insbesondere dann, wenn der Auftraggeber im Rahmen einer Selbstkontrolle auch die Daten anderer Auftraggeber einsehen könnte. Eine derartige Regelung wäre im unternehmerischen Verkehr bei einem Softwarevertrag so ungewöhnlich, dass der Kunde mit ihr nicht zu rechnen braucht. Insofern geht also die im Rahmen von § 307 Abs. 2 Nr. 1 BGB notwendige Güterabwägung zugunsten des Kunden aus. Zu beachten sind auch die denkbaren Folgen einer weit gefassten Auditierung. Das auditierende Unternehmen kann auf diese Weise in das betriebliche Know-how des Nutzers eingreifen. Das Prüfunternehmen erfährt von zahlreichen Details des Innenlebens eines Unternehmens und bekommt so auch eine Vorstellung davon, wann, wo, wie und an welchen Projekten innerhalb eines Unternehmens gearbeitet wird. Insofern berührt die Auditierung den Schutz von Geschäfts- und Betriebsgeheimnissen im Rahmen des § 17 UWG. Zu berücksichtigen ist in diesem Zusammenhang auch die neuere Tendenz der Rechtsprechung zur Bejahung eines Persönlichkeitsrechts für juristische Personen.[9] Ferner ist eine Auditierung in Fällen des § 203 StGB problematisch, etwa wenn es sich bei dem zu überprüfenden Unternehmen um ein Unternehmen aus dem medizinischen oder anwaltlichen Bereich handelt.[10] Sollte das prüfende Unternehmen von medizinischen Daten Kenntnis erlangen, wäre vorab eine Einwilligung der Betroffenen einzuholen. Insofern ähnelt die Sach- und Rechtslage der Frage der Drittwartung von IT-Diensten im medizinischen Bereich.[11] Selbst wenn jedoch kein Fall des § 203 StGB vorliegt, müssen die datenschutzrechtlichen Vorgaben eingehalten werden. Ein Audit-Unternehmen erfährt einiges, was in den Bereich der personenbezogenen Daten fällt, etwa über den Datenzugriff einzelner Mitarbeiter und deren IT-Nutzungsverhalten. Somit könnte eine Kenntnisgabe von Daten mit Personenbezug nur im Rahmen von § 28 Abs. 1 BDSG legitimiert werden. Zur

9 BVerfG, NJW 2005, 883; BVerfG, DuD 2003, 170.
10 Vgl. Heghmanns/Niehaus, NStZ 2008, 57.
11 Ehmann, CR 1991, 294; Otto, wistra 1999, 203.

Anwendung käme dann allerdings nur der Tatbestand des § 28 Abs. 1 S. 1 Nr. 2 BDSG, der eine umfassende Güterabwägung zwischen dem Übermittlungsinteresse des Kunden und den Schutzinteressen der Betroffenen verlangt. Der Kunde könnte zwar als Übermittlungsinteresse geltend machen, dass er sich vertraglich gegenüber dem IT-Unternehmen zur Auditierung verpflichtet hat. Er müsste dann aber begründen können, warum dieses vertragliche Interesse den Vorrang vor den Schutzinteressen der Betroffenen haben soll. Dies dürfte ihm insofern schwer fallen, als er gar keinen Einfluss auf den extern vorgenommenen Auditierungsprozess hat. Er weiß also gar nicht, welche personenbezogenen Daten unter Umständen bei der Auditierung mit offenbart werden. Damit gerät er in eine gefährliche Zwickmühle: Er soll zwar seine vertraglichen Auditierungspflichten erfüllen, steht aber gleichzeitig den Betroffenen in Bezug auf die Einhaltung datenschutzrechtlicher Vorgaben in obligo. Die unkonturierte Auditierungsverpflichtung kann den IT-Kunden zu einem permanenten Rechtsbruch verleiten und ist daher schon aus diesem Grund nicht als sachangemessen anzusehen.

1.8 Mitteilungspflichten

§ 11 Abs. 2 S. 2 Nr. 8 BDSG sieht Mitteilungspflichten vor, falls der Auftragnehmer oder bei ihm beschäftigte Personen gegen Vorschriften des BDSG oder vertragliche Festlegungen zum Schutz der personenbezogenen Daten verstoßen. Insofern korrespondiert § 11 Abs. 2 S. 2 Nr. 8 BDSG mit § 42a BDSG und den dort geregelten Mitteilungspflichten nach außen hin. Der Auftragnehmer soll entsprechende Verstöße mitteilen müssen, damit der Auftraggeber hierauf entsprechend reagieren kann. Bei den Mitteilungspflichten i.S.v. § 11 Abs. 2 S. 2 Nr. 8 BDSG ist zu berücksichtigen, dass die Form der Mitteilung ebenso zu regeln ist wie das Prüfungsrisiko und die Reaktionsgeschwindigkeiten.

Im Übrigen war nach § 11 Abs. 3 S. 2 BDSG a.F. der Auftragnehmer verpflichtet, unverzüglich zu warnen, wenn Weisungen bzw. die im Auftrag vorgesehenen Erhebungen, Verarbeitungen oder Nutzungen von Daten nach seiner Ansicht ganz oder teilweise gegen Datenschutzvorschriften verstoßen. Es handelte sich hierbei um eine Hinweispflicht, d.h. der Auftraggeber brauchte dem Hinweis nicht zu folgen und der Auftragnehmer durfte – und war je nach der Ausgestaltung des dem Auftrag zugrunde liegenden Rechtsverhältnisses auch verpflichtet – den „beanstandeten" Auftrag gleichwohl auszuführen. Die Treuepflicht des Auftragnehmers basiert auf § 280 BGB und wird trotz fehlender ausdrücklicher Regelung auch nach neuem BDSG anzunehmen sein.

1.9 Weisungsrechte

§ 11 Abs. 2 S. 2 Nr. 9 BDSG kann, gerade im Verhältnis zu § 11 Abs. 2 S. 2 Nr. 7 BDSG und den dort geregelten Kontrollrechten, als eine eigenartige Regelung bezeichnet werden. Hiernach ist der Umfang der Weisungsbefugnisse festzulegen, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält. Ein Vorbehalt von Weisungsbefugnissen ist sprachlich jedoch kaum möglich. Gemeint ist, dass der Umfang der Weisungsbefugnisse genauer geregelt werden soll. Dies ergibt sich aber bereits aus § 11 Abs. 2 S. 2 Nr. 7 BDSG.

1.10 Löschung und Rückgabe

Neu ist auch § 11 Abs. 2 S. 2 Nr. 10 BDSG, der eine Rückgabepflicht überlassener Datenträger und vertragliche Regelungen zur Löschung von Daten nach Beendigung des Auftrags vorsieht. Hier ist zu beachten, dass sich zahlreiche professionelle Auftragsdatenbearbeiter die Datenherrschaft vertraglich zusichern lassen. Solche Klauseln sind regelmäßig nach § 307 Abs. 2 Nr. 1 BGB unwirksam. Die Datenherrschaft liegt beim Auftraggeber, der sich diese durch entsprechende Rückgabepflichten und Löschungspflichten sichern muss. Zu beachten ist, dass die rein vertragliche Regelung zur Löschung nicht ausreicht. Vielmehr ist zu verlangen, dass der Auftragnehmer die entsprechende Löschung bestätigt und gegebenenfalls auch eidesstattlich versichert. Die Rückgabepflicht erfordert eine genaue Bezeichnung der zurückzugebenden Datenträger. Sinnvoll ist hier die Vereinbarung von Besitzkonstituten i.S.v. § 868 BGB.

2 Auswahl und Vorabkontrolle

§ 11 Abs. 2 S. 1 BDSG gebietet eine sorgfältige Auswahl des Auftragsunternehmens nach Maßgabe deren Datensicherheitskonzeptes. Diese Vorschrift hat vor allem einen vergaberechtlichen Hintergrund, ist aber ansonsten nicht sanktioniert. Insbesondere fehlt es an einer Bußgeldvorschrift, wie § 43 Abs. 1 Nr. 2b BDSG zeigt.

§ 11 Abs. 2 S. 4 BDSG sieht ferner vor, dass der Auftraggeber sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat. Dies ist eine neue Formulierung gegenüber dem alten § 11 Abs. 2 BDSG. Dort war nur allgemein von der Pflicht die Rede, dass der Auftraggeber sich von der Einhaltung entsprechender Maßnahmen überzeugen muss. Hier wird nun der Zeitpunkt der Kontrollpflicht konkretisiert, nämlich einmal vor Beginn der Datenverarbeitung und sodann regelmäßig.

Zu beachten ist, dass nach § 43 Abs. 1 Nr. 2b BDSG die Pflicht zur Kontrolle der entsprechenden Maßnahmen vor Beginn der Datenverarbeitung bußgeldbewehrt ist. Die regelmäßige Kontrollpflicht ist allerdings nicht bußgeldbewehrt. Insofern stellt sich hier die Frage, wie man die Phase vor Beginn der Datenverarbeitung von der regelmäßigen Überwachung abgrenzt. Zu beachten ist ferner, dass die Kontrollpflicht nicht zwangläufig dazu führt, dass der Auftraggeber vor Ort kontrollieren muss. Neu ist auch § 11 Abs. 2 S. 5 BDSG, wonach das Ergebnis der Kontrolle zu dokumentieren ist. Auf Grund der Tatsache, dass die Kontrollpflicht vor Beginn der Datenverarbeitung und dann regelmäßig einsetzt, besteht insofern auch eine korrespondierende kontinuierliche Dokumentationspflicht.

3 Fazit

Die neuen Regelungen zur Auftragsdatenverarbeitung sind nicht ganz neu, aber sie gewinnen durch die Bußgeldandrohung des § 43 Abs. 1 BDSG an Brisanz. Die Unternehmen tun gut daran, alsbald ihre Vertragsbeziehungen zu IT-Dienstleistern zu überdenken und anzupassen.