



eCompliance

by TÜV[®]

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Jörg Schlißke / Peter Kattner



Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Literatur

- Abel, Horst G. (Hrsg.): Praxiskommentar Bundesdatenschutzgesetz, 5. Aufl., Kissing 2009
- Abel, Ralf B.: Auftragsdatenverarbeitung in der Praxis, Datenschutz Praxis, Ausgabe 04/2011
- Bergmann, Lutz; Möhrle, Roland; Herb, Armin (Hrsg.): Datenschutzrecht, Kommentar, Stuttgart 2009
- Däubler, Wolfgang; Klebe, Thomas; Wedde, Peter; et.al.: Bundesdatenschutzgesetz, Basiskommentar zum BDSG, 3. Aufl., Frankfurt/Main 2009
- Göhner, Reinhart: Bundesvereinigung der Deutschen Arbeitgeberverbände, Geschäftsbericht 2009
- Gola, Peter; Schomerus, Rudolf: BDSG - Bundesdatenschutzgesetz, Kommentar - 10. Aufl., München 2010
- Görtz, Birte; Fechte, Tim: Daten schützen: Eine Studie zum aktuellen Stand des Datenschutzes in Großunternehmen 2011, PricewaterhouseCoopers, Frankfurt 2011
- Gemeinsam für spürbare Entlastung-12 Vorschläge von BDA, BDI, DIHK, ZDH und ZKA zum Abbau bürokratischer Hemmnisse, Berlin 2010
- Schaar, Peter: Bundesbeauftragter für den Datenschutz und die Informationssicherheit, Tätigkeitsbericht für die Jahre 2009 und 2010 – 23. Tätigkeitsbericht, 23. Tätigkeitsbericht, Berlin 2011
- Simitis, Spiros: Bundesdatenschutzgesetz, Kommentar, 7. neu bearb. Aufl., Baden-Baden 20
- Sommer, Imke: Landesbeauftragte f. d. Datenschutz Bremen, 33. Jahresbericht für das Jahr 2010
- von Bose, Harald: Landesbeauftragter f. d. Datenschutz Sachsen-Anhalt, VIII. Tätigkeitbericht 2007

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

- Inhalte
 - **Definitionsansatz Rechtsdogma**
 - **Regelungsziele des § 11 BDSG**
 - **Kernpunkte der Auftragsdatenverarbeitung**
 - **Hintergründe zur Neuregelung des § 11**
 - **Die Novelle des § 11 im Jahre 2009**
 - **Erfordernis einer Neuregelung des § 11:**
 - *Stellungnahme des Bundesrates*
 - *Stellungnahme der Aufsichtsbehörden*
 - *Stellungnahme der Wirtschaftsverbände*
 - *Tätigkeitsbericht des LfD Sachsen-Anhalt*
 - *“Typische Outsourcingfehler“*
 - **Beispiele für eingeleitete Bußgeldverfahren**
 - **Handlungsempfehlung für die Umsetzung einer ADV**
 - **Auslegungshinweise, LDI-NW Fragen an die Aufsichtsbehörde**

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Definitionsansatz Rechtsdogma

„Die *Rechtsdogmatik* interpretiert das geltende Recht einer bestimmten Rechtsordnung aus einer *internen* Anwenderperspektive, also aus der Perspektive von Richtern und Verwaltungsbeamten. Dabei integriert sie theoretische Analyse und empirische Beschreibung. Aber ihr eigentlicher Charakter ist der einer "Normwissenschaft", ihr eigentlicher Zweck ein normativer: die praktische Ausgestaltung und Anwendung des geltenden Rechts. Auch die meisten Rechtswissenschaftler [...] nehmen diese Anwenderperspektive ein, etwa wenn sie zivilrechtliche, öffentlich-rechtliche oder datenschutzrechtliche Artikel und Kommentare für die Praxis verfassen [...].“¹

¹Vgl., N.N., <http://www.rechtsphilosophie.uni-goettingen.de/info.html>

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Regelungsziele des § 11 BDSG

- Schaffung von Transparenz und Rechtssicherheit, dabei Konkretisierung gesetzlicher Vorgaben.
- Fokussierung der Auftragskontrolle durch „konkrete“ Kontrollpflichten und Ergänzung von Kontrollpflichten.
- Juristische Durchsetzbarkeit gesetzlicher Vorgaben durch Schaffung von Bußgeldtatbeständen. Erhöhung des Bußgeldrahmens sowie Erweiterung von Sanktionsmöglichkeiten.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Kernpunkte der Auftragsdatenverarbeitung nach § 11 BDSG

... beinhalten juristische Komponenten sowie technische- und organisatorische Maßnahmen...

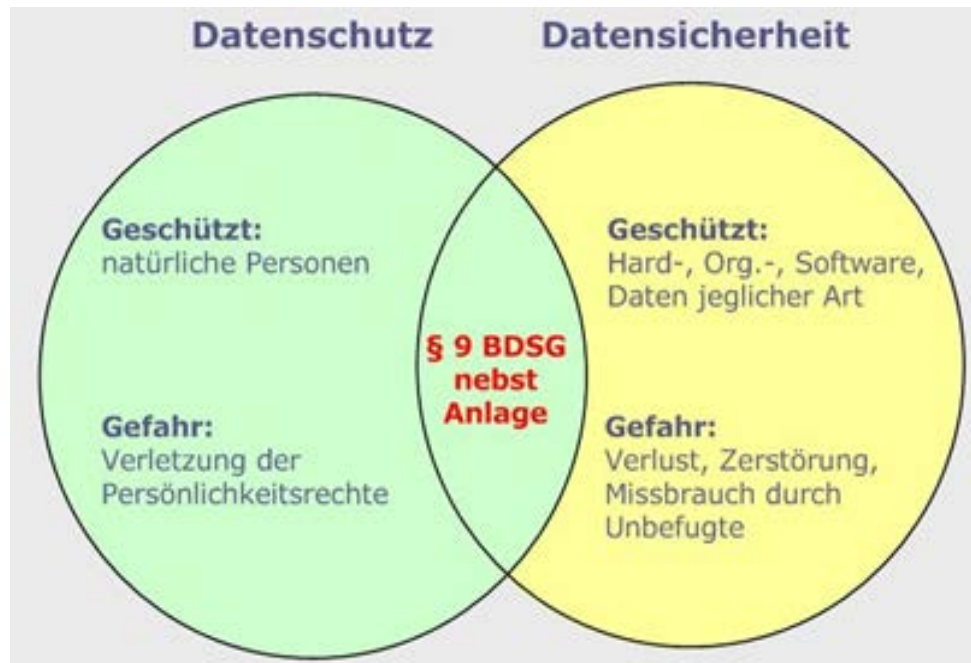


Abb. Entnommen aus: Gola;Jaspers, Das novellierte BDSG im Überblick, Abb. S. 13.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Hintergründe zur Neuregelung des § 11 BDSG

Datenskandale

- Anlass für dieses Gesetzgebungsverfahren war vor allem ein häufig auftretender rechtswidriger Umgang, mit personenbezogenen Daten von Mitarbeitern in Call Centern aber auch Datenschutzskandale bei DB, Telekom sowie LIDL im Rahmen des § 32 BDSG.²

Verträge

- Keine ausreichende Definition des Auftragsgegenstandes
- Unzureichende Festlegung der Verantwortlichkeiten zwischen den Parteien.

Stichwort: Privatautonomie

Sanktionierung

- Verfehlungen haben Bußgeldbewährtheit zur Folge. Handlungsmöglichkeiten durch die Aufsichtsbehörden.

²BR-Drs 4/09, Stellungnahme des Bundesrates. Entwurf eines Gesetzes zur Regelung des DS-Audits und zur Änderung datenschutzrechtlicher Vorschriften

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Die Novelle des § 11 BDSG im Jahre 2009

■ § 11 Abs. 2 Satz 2, 4, 5 BDSG

(+) Mindestanforderungen = 10 Punkte-Katalog
(siehe insbesondere Nr. 3 i. V. m. § 9 und Anlage BDSG = 8 Goldene Regeln)

(+) Kontrolle der toM durch den AG „vor Beginn“ und „sodann regelmäßig“ beim AN „zu überzeugen“ hat.

Fragestellung: Zeitraum und Turnus der Kontrollen?

Fragestellung: Überzeugen, Kontrolle vor Ort? oder vorgelegte Prüfberichte/Zertifikate?

(+) „[...]das Ergebnis ist zu dokumentieren

Fragestellung: dokumentieren, Wie und Was, Umfang? archivieren, Fristen?



Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Die Novelle des § 11 BDSG im Jahre 2009

- § 43 Abs. 1 Nr. 2b³
- Bußgeldvorschriften i. V. m. § 11 Abs. 2 Satz 2 BDSG

1. Bußgeldtatbestand, Rechtsfolge: Ahndung mit Geldbuße bis 50.000,- Euro

(+) „[...] Auftrag nicht richtig, nicht vollständig, nicht in vorgeschriebener Weise erteilt“

- § 43 Abs. 1 Nr. 2b Bußgeldvorschriften i. V. m. § 11 Abs. 2 Satz 4 BDSG

2. Bußgeldtatbestand, Rechtsfolge: Ahndung mit Geldbuße bis 50.000,- Euro

(+) „[...] sich nicht vor Beginn [...]

(-) sodann regelmäßig über die Einhaltung der toM überzeugt.“

h.M.: „Nicht durchgeführte regelmäßige Kontrollen und Dokumentation unterliegen keiner Sanktion“.⁴ So fehlt auch ein konkreter Hinweis im § 43 Abs. 1 Nr. 2b BDSG.

Begründung, unbestimmte Rechtsbegriffe implizieren semantische Unschärfe.

³Normative Wirkung durch Inkrafttreten des § 43 Abs. 1 Nr. 2b ab dem 01.09.2010.

⁴Vgl., Abel, Praxiskommentar BDSG S.283, so auch Gola/Schomerus BDSG Kommentar Rn. 28.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Erfordernis einer Neuregelung des § 11 BDSG

Stellungnahme des Bundesrates vom 12.03.2009, BR- Drs 04/09

- Anlassbezug, häufig auftretender, unsachgemäßer und rechtswidriger, Umgang mit pb Daten von „Mitarbeitern“ in Call Centern.⁵
- Fehlende, unzureichende schriftliche Beschreibung der Auftragsbeziehung zwischen AG und AN aus perspektivischer Betrachtung des Datenschutzes, als Resultat einer nicht vollumfänglichen Durchdringung der Gesetzesnorm.⁶
- Fazit des BR: Eine Konkretisierung durch Mindestanforderungen des § 11 BDSG sind zu begrüßen.

^{5,6}Vgl. BR-Drs 4/09, Stellungnahme des Bundesrates. Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Erfordernis einer Neuregelung des § 11 BDSG

Stellungnahme der Aufsichtsbehörden, BfDI Peter Schaar

- Die angepassten Regelungen führen zu verbesserten in der ADV z.B. in Call Centern. Die Branche sei in den Fokus gerückt da pb Daten ohne eingehende Kontrolle an AN weitergereicht wurden.
- Ausgangslage, dass der AG als „Verantwortliche Stelle [...] gar nicht mehr weiß wo und von wem pb Daten verarbeitet werden“.⁷ Die Datenschutzskandale haben gezeigt, dass Pflichtverletzungen nicht vom AG ausgingen, sondern von AN und wiederum beauftragten Subunternehmen.
- Gründe hierfür sind in einer komplexen Anzahl von Auftragsmodellen und nebulösen Vertragsbeziehungen zu suchen.
- Fazit des BfDI: Durch Mindestinhalte ist die Verantwortung des AG nicht ohne weiteres auf den AN zu delegieren. Der AG als verantwortliche Stelle bleibt „Herr der Daten“ und ist somit verantwortlich für die Verarbeitung von pb Daten.

⁷Vgl, Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationssicherheit, 23. Tätigkeitsbericht, S. 29.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Erfordernis einer Neuregelung des § 11 BDSG

Stellungnahme der Wirtschaftsverbände⁸ Stand 06/2010

- Vorschlag an die Bundesregierung, die „Auftragsdatenverarbeitung unbürokratisch zu ermöglichen“. Eine Gleichbehandlung von Großkonzernen die komplexe Outsourcing Projekte durchführen und KMU „die Lohnbuchhaltung an Dritte übertragen“ stehen in keinem Verhältnis zueinander.
- „Eine spürbare Entlastung sei den kleineren Wirtschaftsbetrieben beizumessen, indem die nach § 11 Abs. 2 Satz 4 BDSG regelmäßigen Kontroll- und Dokumentationspflichten abgeschafft werden. Eine Vorabkontrolle vor Inbetriebnahme der Auftragsdatenverarbeitung ist als ausreichend einzustufen. „Es bietet sich an, die Grenze bei 20 Beschäftigten festzulegen“.
- Insgesamt sieht das Gremium der Wirtschaftsvertreter in einer neuen, unbürokratischeren Fassung des § 11 BDSG einen Hebel für eine adäquate und zielgruppenorientierte Auftragsdatenverarbeitung, als zukünftige Lösung.

⁸Eckpunktepapier „12 Vorschläge von BDA, BDI, DIHK, ZDH und ZKA zum Abbau bürokratischer Hemmnisse“.

BDA | Bundesvereinigung der Deutschen Arbeitgeberverbände; BDI | Bundesverband der Deutschen Industrie e. V.; DIHK | Deutscher Industrie- und Handelskammertag e. V.; ZDH | Zentralverband des Deutschen Handwerks e. V.; ZKA | Zentraler Kreditausschuss

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Erfordernis einer Neuregelung des § 11 BDSG

Tätigkeitsbericht des LfD Sachsen-Anhalt Dr. H. Bose

- Der Landesbeauftragte für Datenschutz für das Land Sachsen-Anhalt *Bose* konstatiert „bekannte Probleme in der Auftragsdatenverarbeitung“. Als Beispiel führt *Bose* eine Auftragsdatenverarbeitung einer öffentlichen Stelle an. Vorausgegangen war ein Vertragsschluss zwischen einer verantwortlichen Stelle, die für die Vernichtung von Festplatten des Justizbereichs Sorge zu tragen hatte und einem privaten Unternehmen. Bei einer planmäßigen Kontrolle durch den LfD wurde festgestellt, dass der Auftragnehmer zuvor nicht auf seine Eignung als Auftragsdatenverarbeiter überprüft wurde.
- Auch bei den umzusetzenden technischen und organisatorischen Maßnahmen würden Mängel festgestellt. Ein Vertrag zur Auftragsverarbeitung wurde nicht schriftlich verfasst.⁹

⁹Vgl., Dr. Harald Bose, Landesbeauftragter für den Datenschutz Sachsen-Anhalt, VIII.Tätigkeitsbericht (4/2005-3/2007)S. 76.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Erfordernis einer Neuregelung des § 11 BDSG

„Typische Outsourcingfehler“, Veröffentlichung des ULD¹⁰ vom 26.04.2005

- In einer Veröffentlichung von typischen Outsourcingfehlern durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, gelten 45% der Auftragsdatenverarbeitungen als fehlerhaft. Die häufigsten Fehlerbilder resultieren aus unzureichenden „Bedarfs- und Leistungsbeschreibungen des Auftraggebers sowie einem ebenfalls unzureichenden Vertragswerk zwischen Auftraggeber und Auftragnehmer.

¹⁰Vgl. Rost, <https://www.datenschutzzentrum.de/systemdatenschutz/backup/meldung/sm105.htm>.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Beispiel eingeleiteter Bußgeldverfahren

- Wie hoch sich der Anteil an eingeleiteten Bußgeldverfahren zu Ordnungswidrigkeiten im Datenschutz insgesamt beziffern lässt, ist über die vorliegenden Quellen wie Tätigkeitsberichten der 16 Landesbeauftragten für Datenschutz (LfD) sowie einschlägiger Zeitschriften und Rechtsliteratur nicht vollumfänglich ermittelbar.
- Das begründet sich daraus, dass nicht alle Aufsichtsbehörden Informationen über erlassene Bußgelder veröffentlichen oder Statistiken darüber führen.
- Die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen Imke *Sommer*, beschreibt in ihrem Jahresbericht aus dem Jahre 2010 folgendes Fallbeispiel: So lagen über einen Softwaredienstleister und eine Werbeagentur – jeweils verantwortliche Stelle – mehrere Beschwerden von Betroffenen in der Form vor, „dass ihrem jeweiligen Auskunftsverlangen, selbst wenn sie das um Auskunft ersuchte Unternehmen wiederholt hieran erinnerten, nicht entsprochen wurde“. Da dieses Verhalten in keinsten Weise nicht mit dem Auskunftsanspruch des § 34 BDSG korrespondiert, „wurden Geldbußen in Höhe von 1.400,- Euro bis 1.600,- Euro verhängt“.¹¹

¹¹Vgl. *Sommer*, 33. Jahresbericht 2010, S. 83.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Beispiel eingeleiteter Bußgeldverfahren

LDI NRW: 60.000 Euro Bußgeld für die Easycash GmbH¹²

- Der Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI NRW) Lepper hat bekannt gegeben, gegen die Easycash GmbH – ein Dienstleistungsunternehmen, das Lastschriftverfahren im Rahmen der EC-Kartenzahlung für Einzelhändler abwickelt – ein Bußgeld in Höhe von 60.000 Euro verhängt und damit die unzulässige Weitergabe von rund 400.000 Kontodaten und Daten über Ort, Zeitpunkt und Höhe von Zahlungsvorgängen sanktioniert zu haben. Diese Daten wurden einem Schwesterunternehmen der Easycash GmbH, das Kunden- und Bonusprogramme anbietet, zur statistischen Auswertung übermittelt. “ Wer Zahlungsvorgänge quasi als Treuhänder für Einzelhandelsunternehmen abwickelt, muss besonders sorgfältig mit diesen Daten umgehen. Er darf so sensible Daten über Zahlungsverhalten und Kontoverbindungen, die durchaus auch Profilbildungen erlauben würden, nicht für andere Zwecke an Dritte übermitteln. Deswegen musste ich hier einschreiten”, kommentierte Lepper sein Vorgehen. Er zeigte sich jedoch erfreut, dass sich das Unternehmen in Datenschutzfragen kooperativ gezeigt und das Bußgeld bereits gezahlt habe. Außerdem habe Easycash nicht nur die Weitergabe von Kontoverbindungsdaten an Dritte umgehend eingestellt, sondern auch die von ihm geforderten Änderungen umgesetzt.

¹²Vgl., <http://www.datenschutzticker.de/index.php/2011/09/ldi-nrw-60-000-euro-bussgeld-fuer-die-easycash-gmbh/>

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

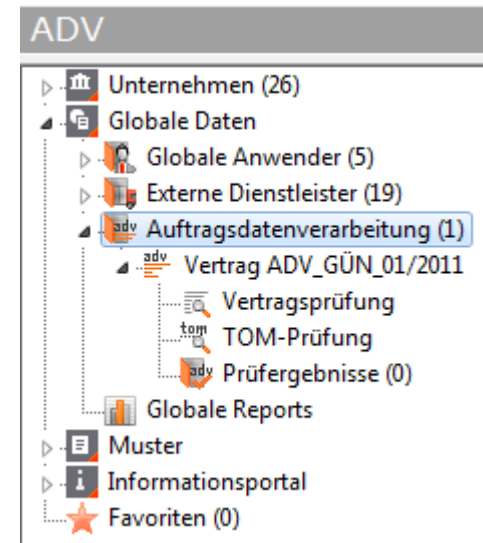
Handlungsempfehlung für die Umsetzung einer ADV

- Detaillierte Festlegung der Regelungsbereiche. Vorsicht bei der Übernahme von Gesetzestexten.
- Legen Sie ein besonderes Augenmerk auf die Berücksichtigung der technischen- und organisatorischen Maßnahmen (§ 9 und Anlage BDSG). Als zu empfehlender Maßstab sollten Sie sich am BSI Grundschutz orientieren.
- Externe Zertifizierungen sind von Vorteil aber nicht zwingend notwendig.
- Als Orientierungsgrundlage für den Vertrag sind grundsätzlich Vertragsmuster wie z.B. die der GDD oder der BITKOM einsetzbar. Diese sind jedoch auf die spezifischen Anforderungen an den Auftrag zu prüfen, anzupassen und vor allem kritisch zu hinterfragen.
- Das gleiche gilt für Checklisten zur Vorabkontrollen, Kontrollroutinen und Durchführung der Auftragsdatenverarbeitung zwischen Auftraggeber und Auftragnehmer.
- Der Einsatz einer Softwarelösung zur Gesamtadministration und Strukturierung in der Auftragsdatenverarbeitung über **privacyGUARD** ermöglicht eine ressourcensparende, effiziente Vertragsdurchführung und versetzt sie jederzeit in die Lage auskunftsfähig bei Anfragen von Mitarbeitern, Geschäftspartnern und Aufsichtsbehörde zu sein.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Modul Auftragsdatenverarbeitung in privacyGUARD...

- Positiver Ansatz auf Grund von Praxiserfahrungen
- Offen für weitere Entwicklung des Moduls
- An der Praxis orientierte „Dreierkette“
 - Vertrag (zentrale Dokumentenablage)
 - Vertragsprüfung (über standardisierte Prüflisten)
 - Dokumentation der techn. und org. Maßnahmen
- Ergebnisdokumentation einzelner ADV-Prüfungen
- Positive Rückmeldung aus der Wirtschaft



Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Auslegungshilfe LDI-NW § 11 BDSG...

... Erhebung, Verarbeitung oder Nutzung pb Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere...

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind...

...Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

Das Ergebnis ist zu dokumentieren.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

Auslegungshinweise, LDI-NW Fragen an die Aufsichtsbehörde...

1. zu den in § 11 Abs. 2 Satz 4 verwiesenen Grundprüfpflichten
2. zu den nach § 11 Abs. 2 Satz 1 "sorgfältigen" Auswahlpflichten
3. zu den nach § 11 Abs. 2 Satz 4 „regelmäßigen“ Prüfpflichten
4. zum § 11 Abs. 5 in Bezug auf die Absätze 1-4 des § 11 BDSG entsprechend im Zusammenhang der Prüfung und Wartung automatisierter Verfahren durch Dritte (Fernwartung etc.)
5. Zum datenschutzkonformen Umgang mit den v. g. Prüfpflichten, wenn der Dienstleister seinen Sitz im Ausland (EU/EWR; Drittland) hat.

Die Geduld ist der Schlüssel zur Freude!?

- Arabisches Sprichwort -

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

1. Auslegungshinweis LDI-NW

§ 11 Abs. 2 Satz 4 zu den Grundprüfpflichten...

Der LDI-NW weist zunächst darauf hin, dass die zu gebenden Antworten kaum so eindeutig sein werden, wie Sie sich das möglicherweise wünschen.

Bei der Gesetzgebung sind unbestimmte Rechtsbegriffe gerade gewählt worden, um die Bandbreite möglicher Auftragsdatenverarbeitungen insgesamt zu erfassen.

Ein evtl. kleinerer Auftrag an einen Lettershop unterliegt anderen Maßstäben als das Outsourcing einer IT-Infrastruktur. Den Maßstab muss letztlich der Auftraggeber selbst setzen, denn er bleibt rechtlich in der Verantwortung für die Datenverarbeitung beim Auftragnehmer.

Er sollte also denselben Maßstab bei der Prüfung eines Auftragnehmers ansetzen, den er für sein eigenes Unternehmen anstrebt.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

2. Auslegungshinweis LDI-NW

§ 11 Abs. 2 Satz 1 zu den Auswahlpflichten...

Mindeststandards können nicht absolut beschrieben werden, weil sie sich immer an den individuellen Anforderungen des Auftrags und den dafür notwendigen Schutzstufen orientieren müssen. Der Auftraggeber muss daher zunächst den eigenen Schutzstandard klar definieren.

Die gebotene Intensität der Überprüfung hängt von Umfang und Komplexität der Verarbeitung und der Schutzwürdigkeit der zu verarbeitenden Daten ab.

Regelmäßig sollte der Auftraggeber das IT-Sicherheitskonzept des Auftragnehmers einsehen. Eine Prüfung vor Ort sollte, wenn möglich, erfolgen.

Eine Zertifizierung des Auftraggebers oder die Prüfung der vom Auftraggeber vorgegebenen Kriterien für die Vertrauenswürdigkeit mittels Fragebogen kann bei entsprechend niedriger Schutzstufe im Einzelfall ausreichen, wenn daraus aussagekräftige Rückschlüsse auf die Vertrauenswürdigkeit möglich sind.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

3. Auslegungshinweis LDI-NW

§ 11 Abs. 2 Satz 4 zu den „regelmäßigen“ Prüfpflichten...

Das Gesetz sieht bewusst keine regelmäßigen Intervalle vor, denn auch hier gilt, dass der Auftraggeber das Verfahren bestimmt und die Häufigkeit von Kontrollen danach „takten“ muss, wie datenschutzkritisch die Datenverarbeitung ist.

Es ist grundsätzlich auch möglich, dass Kontrollen durch Zertifikate unabhängiger Gutachter erfolgen. Entscheidend ist aber, dass ein Zertifikat nicht in einer bloßen Unbedenklichkeitsbescheinigung bestehen darf. Der Auftraggeber muss vielmehr nachvollziehen können, was mit welchem Ergebnis vom Auditor überprüft wurde. Letztlich ist es der Auftraggeber, der sich eine Überzeugung bilden muss, ob seine Datenverarbeitung sicher durchgeführt wird.

Blindes Vertrauen reicht nicht.

Fakt ist, dass der Auftraggeber bestimmt, was er wissen muss, um zu einer schlüssigen Überzeugung zu gelangen.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

4. Auslegungshinweis LDI-NW

§ 11 Abs. 5 Fernwartung, IT-Service, Viren-Update...

Laut LDI-NW gelten die Abs. 2-4 im Zusammenhang des § 11 Abs. 5 bereits dann, wenn ein Zugriff auf personenbezogene Daten durch externe Stellen nicht ausgeschlossen werden kann.

Danach bestimmt sich die Antwort auf die Frage nach der technischen Ausgestaltung der Zugriffsmöglichkeiten der externen Dienstleister.

Hingegen kein Fall von § 11 Abs. 5 BDSG liegt vor, wenn nur auf ein Testsystem mit anonymisierten Daten oder auf künstlich generierte Testdaten zugegriffen wird.

Die Auftragsdatenverarbeitung nach § 11 BDSG, ein juristisches Dogma mit eingeschränkter Praktikabilität?

5. Auslegungshinweis LDI-NW ADV-Auftragnehmer im Ausland...

Hierzu gibt der LDI-NW letztlich keine Auslegungshilfe.

Die Prüfpflichten nach § 11 BDSG sind dieselben, unabhängig davon wo der Auftragnehmer seinen Sitz hat.

Wie der Auftraggeber gegenüber einem "starken" Auftragnehmer agieren kann, ist eine taktische Frage. Aus Sicht der Aufsicht gilt, dass die Beauftragung eines Auftragnehmers ausscheidet, wenn er sich den Kontrollen des Auftraggebers entzieht, oder wenn Kontrollen beim Auftragnehmer faktisch nicht möglich sind, weil er seinen Sitz an einem fernen Ort hat.

Die tatsächlichen Gegebenheiten entbinden den Auftragnehmer nicht von der Verantwortung, Datenverarbeitungen beim Auftragnehmer zu kontrollieren.

Vielen Dank für Ihre Aufmerksamkeit!

TÜV Informationstechnik GmbH

Unternehmensgruppe TÜV NORD

Jörg Schlißke, LL.B
eDSB; Datenschutzauditor (TÜV)
Fachstelle für Datenschutz

Langemarckstr. 20
45141 Essen

Telefon: +49 201 8999 – 533

Telefax: +49 201 8999 – 544

E-Mail: j.schlisske@tuvit.de

URL: www.tuvit.de