

Elmar Brunsch

Sachverständiger für Informationstechnik und Datenschutz
Eper Str. 20, 48599 Gronau, www.dbc.de

Die Auftragsdatenverarbeitung gem. §11 des
Bundesdatenschutzgesetzes 2009 im nicht-öffentlichen Bereich.
Änderungen, Entscheidungshilfen, Beispiele

Bearbeitungsstand 25.08.2009

Mit der im Juli 2009 erfolgten und vom Bundesrat verabschiedeten Novelle¹ des Bundesdatenschutzgesetzes (BDSG) erfolgte auch eine Überarbeitung des §11, der die Auftragsdatenverarbeitung² (ADV) behandelt. Im Folgenden sollen die Änderungen bezogen auf nicht-öffentliche Stellen erläutert werden. Diese sind angehalten, ihre Geschäftsprozesse zeitnah an die novellierten Regelungen anzupassen, zumal fehlerhafte oder unvollständige Verträge für die ADV bereits als Ordnungswidrigkeit geahndet werden können. Zur Vereinfachung und aus Gründen der Lesbarkeit werden die bereits bekannten und unveränderten Abschnitte des Paragraphen aus den vorangegangenen Fassungen ebenfalls behandelt.

Alle Kommentare sollen die Details und Konsequenzen der Regelungen verdeutlichen und als Anhaltspunkt für eine datenschutzkonforme Auftragsvergabe dienen. Sie spiegeln die persönliche Auffassung des Verfassers wieder und stellen keine Rechtsberatung dar. Kritik, Anregungen und Verbesserungsvorschläge nimmt der Verfasser gerne entgegen. Eine Veröffentlichung ist mit Quellenangabe erlaubt.

Wurden in der alten Fassung des Bundesdatenschutzgesetzes³ noch eher allgemeine Anforderungen an die Vergabe des Auftrags gestellt, sind nun deutlich präzisere Ausführungen in den Gesetzestext eingeflossen. Diese Ausführungen können auch als „10-Punkte-Katalog“ gemäß BDSG bezeichnet werden. Sie müssen Bestandteil eines jeden Vertrags zur ADV sein.

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

Der Auftraggeber wird weiterhin explizit in die Pflicht genommen. Er alleine trägt zunächst die Verantwortung für die korrekte Datenverarbeitung, auch wenn er die Verarbeitung an sich mit der ADV an ein anderes Unternehmen vergibt. Auch im Hinblick auf die genannten §§ 6,7 und 8⁴, erfolgt keine unmittelbare Pflichtverlagerung an den Auftragnehmer. Die Rechte des Betroffenen werden weiterhin gegenüber dem Auftraggeber geltend gemacht.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen.

Vergibt die „verarbeitende Stelle“⁵ den Auftrag, so ist sie verpflichtet, den Auftragnehmer dahingehend zu überprüfen, ob dieser den Auftrag überhaupt ordnungsgemäß ausführen kann. Dabei genügt es nicht, eine allgemeine Beurteilung des Auftragnehmers durchzuführen, da im Gesetzestext die Wortwahl „besondere Berücksichtigung der Eignung“ erfolgt. Für die Beurteilung der technischen und organisatorischen Maßnahmen ist es notwendig, den Auftragnehmer auch in dieser Hinsicht auszuwählen. Es ist die dort vorhandene technische Ausstattung zu prüfen, was im Einzelnen die Kontrolle von Zutritt, Zugang, Zugriff, Weitergabe, Eingabe, Auftrag und Verfügbarkeit sowie das Trennungsgebot betrifft.⁶ Vorteilhaft dürften gleichfalls vorhandene Zertifizierungen gemäß ISO900x, ISO2700x und BSI-Grundschutz sein.

Als weitere Neuerung wurde in der Novelle eine detaillierte Auflistung der zu dokumentierenden Punkte erstellt, welche in der bisherigen Form so nicht gefordert wurde:

Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

Die Erfordernis der Schriftform bestand bereits vor der Novelle. Die neue Formulierung „...wobei insbesondere im Einzelnen festzulegen sind...“, gibt dem Auftraggeber Definitionen und gleichzeitig

¹ BDSG Novelle II lt. BT-Drucksache 16/12011 mit Änderung 16/13657, am 01.09.2009 in Kraft

² Wortlaut: „Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag“

³ BDSG geänderte Fassung vom 22. August 2006

⁴ u.a. „Rechte des Betroffenen“ und „Schadensersatz“

⁵ der spätere „Auftraggeber“

⁶ vgl. Anlage zu §9 Satz 1 BDSG

ein Vorgehensschema an die Hand. Dieses Schema dient im Beispiel (Anhang) auch als Orientierungshilfe für die Formulierung des Vertrags zur ADV.

1. der Gegenstand und die Dauer des Auftrags,

Zu Beginn der Auflistung erfolgt zunächst eine allgemeinere Beschreibung des Gegenstands und der zeitliche Rahmen für die Verarbeitung. In Bezug auf den Zeitraum sind verschiedene Varianten denkbar. Es kann sich sowohl um eine Eingrenzung im Sinne eines Kalendermonats (Kundenzufriedenheitsstudie im Monat Dezember 2009), als auch um einen Zeitraum beginnend und endend mit einem festgelegten Datum handeln. Entscheidend ist hier bereits, daß der Auftragnehmer davon in Kenntnis gesetzt wird, daß es ihm darüber hinaus nicht gestattet ist, eine weitere Verarbeitung durchzuführen. Damit soll verhindert werden, daß der Auftragnehmer sich auch nach Beendigung des eigentlichen Auftrags auf die ursprüngliche Fassung stützt und unter dem Deckmantel der ursprünglich erteilten ADV eine eigene Verarbeitung weiterführt.

2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,

Hier ist festzuhalten zu welchem Zweck die ADV vergeben wird. Unter Berücksichtigung der Sorgfaltspflicht hat eine genaue Beschreibung zu erfolgen, wie genau der Auftragnehmer mit den zu verarbeitenden Daten verfahren soll. Eine Abweichung von diesem Zweck darf durch den Auftragnehmer eigenwillig nicht erfolgen. Hier muß ein neuer Auftrag erteilt werden, wenn der Zweck nicht genau genug definiert wurde oder sich im Nachhinein eine erweiterte Anforderung ergibt. Es empfiehlt sich auch, die einzelnen Projektschritte zu formulieren zumal die Begriffe Erhebung, Verarbeitung und Nutzung getrennt werden⁷. Da sowohl die Art der Daten als auch der Kreis der Betroffenen genannt werden müssen, entfällt für den Auftragnehmer jeglicher Spielraum für weitere Interpretationen. Gleichzeitig muß sich der Auftragnehmer darüber im Klaren sein, daß eine möglichst genaue Beschreibung ihn unter Umständen vor Schadensersatzforderungen stellt. Werden diese Angaben nicht mit der erforderlichen Sorgfalt erstellt, werden Fehler berechtigter Weise dem Auftraggeber zufallen. An dieser Stelle muß auch an die Grundsätze zur Datenvermeidung und Datensparsamkeit⁸ hingewiesen werden. Selbstverständlich dürfen dem Auftragnehmer nur die Daten übergeben werden, die er für die Erledigung des Auftrags zwingend benötigt.

3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,

Verwiesen wird hier besonders auf die Anlage zu §9, welche sich unverändert ganz am Ende des BDSG-Textes findet. Da es nicht erforderlich ist, unverhältnismäßig hohe Anforderungen zu stellen, gleichzeitig aber zwingende Kriterien des Datenschutzes und der Datensicherheit notwendig sind, sollte schon im eigenen Interesse die besonders detaillierte Beschreibung des Punktes 2 durchgeführt werden, um die notwendigen Maßnahmen beurteilen zu können. Für eine solche Beurteilung kann auf die IT-Grundschutz-Kataloge des BSI⁹ zurückgegriffen werden. Diese beinhalten auch entsprechende Handlungsweisen für die Feststellung des Schutzbedarfs¹⁰. Der Schutzbedarf wird bei besonderen Daten¹¹ sicher höher ausfallen, als bei Adresslisten.

4. die Berichtigung, Löschung und Sperrung von Daten,

Falsche Daten sind zu berichtigen, zu löschen oder zu sperren. Stellt der Auftragnehmer fest, daß Daten offensichtlich falsch sind, so hat auch dieser entsprechende Maßnahmen einzuleiten. Dies setzt im Umkehrschluß entsprechende Kenntnisse beim Auftragnehmer voraus. Er hat schon aus diesen Gründen die Pflicht, entsprechend fachkundiges Personal für den Auftrag auszuwählen.

5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,

⁷ vgl. §3 Abs. 3 bis 5 BDSG

⁸ §3a BDSG

⁹ Bundesamt für Sicherheit in der Informationstechnik

¹⁰ Baustein B1.5 Datenschutz (mit Kreuzreferenztabellen)

¹¹ §3 Abs 9 BDSG

Gemeinst ist hier nicht die Beschreibung des vorangegangenen Absatzes 4 (Berichtigung, Löschung, Sperrung), sondern §11 Abs 4 mit den dort genannten Pflichten aus weiteren Paragrafen des BDSG. Dieser Querverweis ist schematisch etwas verwirrend und enthält besonders in Abs. (4) 2 die Pflicht zur Bestellung eines Datenschutzbeauftragten beim Auftragnehmer!¹²

Ausserdem auch seine Kontrollpflichten. Der Auftragnehmer kann sich daher nicht auf den schriftlichen Auftrag verlassen. Ihm obliegt die Mitwirkungs- und Prüfpflicht.

6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,

Es kann durchaus der Fall sein, daß der Auftragnehmer weitere Unterauftragsverhältnisse bereits führt. Besonders in Bezug auf beim Auftragnehmer eingesetzte Softwarewartung kann dies möglich sein. Wird eine Datenbank des Auftraggebers in einer Software des Auftragnehmers bearbeitet, kann für diese Software z.B. ein Wartungsvertrag bestehen. Somit erhalte der Softwarehersteller in diesem Rahmen u.U. ebenfalls Kenntnis vom Datenbestand. Da dies nur schwer auszuschließen ist, sollten diese Umstände bekannt sein. Weitere Unterauftragsvergaben, z.B. wegen Überlastung des Auftragnehmers dürften hiermit allerdings nicht begründet sein. Dies sollte bereits während der Auswahl des Auftragnehmers geklärt und ausgeschlossen werden. Nötigenfalls wäre der Auftrag an einen anderen Auftragnehmer zu vergeben.

7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

Da der Auftraggeber weiterhin auch bei der ADV alle Pflichten behält, muß er sich die Kontrollbefugnisse explizit bestätigen lassen. Der Auftragnehmer duldet diese Kontrollpflicht und nimmt unterstützend daran teil.

8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

In der Praxis wird es nicht möglich sein, die Datenverarbeitung permanent zu überwachen. Andererseits können auch zwischen den einzelnen Überwachungsterminen Fehler auftreten, die bis hin zu Verletzungen des BDSG führen. Dies hat der Auftragnehmer dem Auftraggeber unverzüglich mitzuteilen. Dabei bezieht sich die Mitteilungspflicht nicht nur auf den Datenbestand des Auftraggebers, sondern darüber hinaus. Wird der Auftragnehmer oder die bei ihm beschäftigten Personen auffällig gegenüber anderen Kunden, so kann durchaus angenommen werden, daß er nicht in der Lage ist, eine korrekte Auftragsbearbeitung durchzuführen. Ähnlich wie die neu geschaffene Anzeigepflicht für Datenschutzverletzungen in §42a BDSG¹³ hat eine Unterrichtung des Auftraggebers zu erfolgen. Dieser hat dann die notwendigen Maßnahmen – u.U. auch den Entzug des Auftrags – durchzuführen.

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

Weisungen des Auftraggebers können sich z.B. auf das Trennungsgebot beziehen. Nimmt der Auftragnehmer eine Vielzahl von Datenverarbeitungen auch für weitere Auftraggeber vor, so gilt natürlich auch hier das Trennungsgebot. Es ist also durchaus im Sinne des Auftraggebers, sich derartige Weisungsbefugnisse vorzubehalten.

10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Eine erhebliche Anzahl der erfolgten Datenschutzverstöße wurde durch das Fehlen entsprechender Überlassungs- und Rückgabeerklärungen erst möglich. Ganze Datenbanken wurden nach Beendigung des Auftrags zweckentfremdet und gewinnbringend an weitere Unternehmen verkauft. Daher wird nun gefordert, den Auftragnehmer auf die Rückgabe oder Löschung der Daten nach Beendigung des Auftrags zu verpflichten.

¹² §§4f, 4g und 38 BDSG

¹³ BDSG Novelle II lt. Bundestags-Drucksache 16/12011, tritt am 01.09.2009 in Kraft

Für die schriftliche Dokumentation der ADV müssen sich Auftraggeber und Auftragnehmer mindestens an den oben genannten zehn Punkten orientieren.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.
Dieser Satz gilt wie beschrieben nur für öffentliche Stellen.

Ein entscheidender Diskussionspunkt nach der Novellierung begründet sich sodann aus folgendem Abschnitt des geänderten §11 BDSG:

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.

Eine eingehende Prüfung des Auftragnehmers wird ausdrücklich bereits vor Vergabe des Auftrags verlangt. Der Auftraggeber ist verpflichtet, alle Maßnahmen vorher und „sodann regelmäßig“ zu prüfen und zu dokumentieren. Vereinzelt wird angenommen, daß eine solche Prüfung immer vor Ort beim (potenziellen) Auftragnehmer durchgeführt werden soll, was nach dem Wortlaut des Gesetzes so nicht zwingend interpretiert werden muß.

Es ist alternativ möglich, eine Prüfung durch einen Sachverständigen mit Hilfe eines entsprechenden Gutachtens bzw. einer Einschätzung einzuholen. Dies hat für beide Parteien den Vorteil, daß nicht jeder Auftraggeber eine weitere, gleichartige Prüfung durchführen muß. Ein solches Gutachten ist daher auch aus wirtschaftlichen Aspekten sinnvoll.

Es ist durchaus vorstellbar, daß die nötigen Informationen durch einen qualifizierten Datenschutzbeauftragten des Auftragnehmers zu Verfügung gestellt werden können. Gleichzeitig darf angenommen werden, daß durch diese Art der Formulierung speziell die viel gescholtenen Callcenter die per Gesetz geforderte Bestellung eines Datenschutzbeauftragten nun endlich vornehmen. Der Auftraggeber muß in der Folge wohl eher dem Kandidaten mit ordnungsgemäß bestelltem Datenschutzbeauftragten und sorgfältiger technischer und organisatorischer Dokumentation den Vorzug geben. Dies ganz besonders, da das Ergebnis der Prüfung „zu dokumentieren“ ist. Hier wird der Spielraum für all zu freizügige Interpretationen eng.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

Es erfolgt die Quasi-Definition einer anspruchsvollen Wechselbeziehung. Beide Partner – sowohl Auftraggeber als auch Auftragnehmer – müssen sich über die Tragweite und Pflichten der getroffenen Vereinbarungen im Klaren sein. Zum einen wird schriftlich exakt festgehalten wie der Auftrag genau aussieht, was an die Definition der datenschutzrechtlichen Zweckbindung angelehnt ist. Gleichzeitig steht der Auftragnehmer jedoch in der Pflicht, die Weisungen des Auftraggebers zu prüfen und gegebenenfalls auf Defizite oder rechtliche Unzulänglichkeiten hinzuweisen. Dies dürfte ebenfalls nur dann möglich sein, wenn der Auftragnehmer einen Datenschutzbeauftragten bestellt hat und dieser der gesetzlichen Anforderung an Fachkunde und Zuverlässigkeit nachkommt.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1) a) öffentliche Stellen,

b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist, die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2) die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

Eine andere Formulierung bzw. eine für nicht-öffentliche Stellen:

Für den Auftragnehmer gelten neben den Vorschriften zum Datengeheimnis (§5), den technischen und organisatorischen Maßnahmen (§9), Bußgeld- (§43) und Strafvorschriften (§44) nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, die Vorschriften zum Beauftragten (§4g), dessen Aufgaben (§4f) und die Aufsichtsbehörde (§38).

Das Wort „nur“ birgt die Gefahr, daß der Auftragnehmer die Pflichten unterschätzt. Alleine die Tragweite der genannten Paragraphen ist erheblich. Jeder Auftragnehmer ist gut beraten, sich eingehend mit ihnen zu beschäftigen.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Die vorgenannten Ausführungen gelten nicht nur für den klassischen Auftragsdatenverarbeiter, sondern auch für die Unternehmen, welche mit den Wartungsarbeiten an Datenverarbeitungsanlagen und der eingesetzten Software der verantwortlichen Stelle beauftragt werden. Es ist zu beachten, daß auch weitere Dienstleister unter die Vorschriften fallen und auch für diese ein schriftlicher Auftrag erteilt werden muß. Betroffen hiervon sind z.B. IT-Dienstleister, Systemhäuser, Wartungsunternehmen für Büromaschinen, Aktenvernichter, Programmierer, Steuerberater etc.

Fazit:

Es wird interessant sein, wie viele Auftragsdatenverarbeiter nach Inkrafttreten der neuen Regelungen noch in der Lage sind, diese zu erfüllen. Alle genannten Punkte beruhen auf einer ständigen Wechselwirkung zwischen Auftraggeber und Auftragnehmer. Die Rechte und Pflichten werden nicht verschoben, sondern im Konstrukt eines besonderen Kunden-Lieferantenverhältnisses gemeinsam erarbeitet, ohne das eine Seite in unzumutbarer Weise für den Betroffenen aus der Pflicht genommen wird. Dies alles dient dem Zweck der ordnungsgemäßen Datenverarbeitung und hiermit direkt dem Schutz der personenbezogenen Daten des Betroffenen. Eine Vereinbarung für die Durchführung der ADV gründet auch immer auf einem Geschäftsbesorgungsvertrag gem. §675 BGB. Es muß berücksichtigt werden, daß eine Differenzierung zwischen ADV und einer Funktionsübertragung (auch „Outsourcing“) stattfinden muß. Eine solche Funktionsübertragung tritt dann an Stelle einer ADV, wenn über die eigentliche Datenverarbeitung hinaus eigenverantwortlich Funktionen durch den Auftragnehmer übernommen werden. Bei der ADV besitzt der Auftragnehmer keinen Ermessensspielraum!

Zusätzlich gilt es zu prüfen, ob eine ADV in Deutschland oder in einem Drittland durchgeführt wird. Besonders bei einer Auftragsvergabe in ein Land ausserhalb der EU kann es sich dann schnell um ein Land mit „nicht angemessenem Datenschutzniveau“ handeln. Dazu gehören u.U. auch die USA, wenn sich der Auftragnehmer nicht den „Safe-Harbor-Principles“¹⁴ unterworfen hat.

Durch die neue, sehr klare Definition der ADV in Bezug auf die schriftlich zu klärenden Punkte, müssen sich beide Parteien der Tragweite und Verantwortung bewusst sein. De facto stellen die neuen Regeln auch erhöhte Anforderungen an die eingesetzte Hard- und Software. Computersysteme sollten ein bereits auf Systemebene einsetzende Verschlüsselung und entsprechenden Zugriffsschutz bieten. Software muß vor allem für Trennungsgebot, Datenvermeidung, Datensparsamkeit und Eingabekontrolle entsprechende Möglichkeiten bieten. Was zur Zeit am Markt vorhanden ist genügt vielfach nicht den Anforderungen. Ganz zu schweigen von den Unternehmen, die sich nun schnellstmöglich auf diese einzustellen haben. Andererseits besteht für alle Partner, die sich diesen Herausforderungen ernsthaft stellen ein erhebliches Entwicklungspotenzial mit erstklassigen Chancen.

Als Ergebnis wird die Sensibilität der ADV definiert. Beiden Seiten wird nun unmißverständlich dargelegt, daß sie in hohem Maße Verantwortung für die Verarbeitung personenbezogener Daten tragen. In der Folge wird sich bereits an der Form des Auftrags erkennen lassen, ob sich die Parteien im geforderten Umfang mit ihren Aufgaben befasst haben.

¹⁴ <http://www.export.gov/safeharbor/>

Gronau im August 2009

Elmar Brunsch / dbc.de
Sachverständiger für Informationstechnik und Datenschutz

Quellenangaben und Literaturverzeichnis:

BDSG Bundesdatenschutzgesetz vom 22.08.2006
BDSG Bundesdatenschutzgesetz mit Novelle II, Juli 2009
Bundestag Drucksache 16/12011 mit Änderungen 16/13657
BGB Bürgerliches Gesetzbuch
Script Internetrecht, Stand September 2009, Prof. Dr. Thomas Hoeren, Universität Münster
U.S. - EU Safe Harbor Framework, U.S. Department of Commerce

Anlage:
Beispiel zur Regelung der Auftragsdatenverarbeitung im nicht-öffentlichen Bereich

Vereinbarung zur Auftragsdatenverarbeitung gem. §11 Bundesdatenschutzgesetz (BDSG)

Der Auftraggeber
Max Muster GmbH, Musterstr. 10, 10178 Berlin

beauftragt hiermit den Auftragnehmer
Hans Glück GbR, Freudeweg, 25348 Glückstadt

mit der ordnungsgemäßen und datenschutzgerechten Erledigung folgender Arbeiten:

1. Gegenstand und Dauer des Auftrags

- Pflege von Adressdatenbeständen

Die Auftragsdatenverarbeitung wird erteilt im Zeitraum: 14.09.2009 bis 16.10.2009

Die Auswahl des Auftragnehmers erfolgte durch den Auftraggeber nach vorheriger Kontrolle der technischen und organisatorischen Maßnahmen vor Ort beim Auftragnehmer am 01.09.2009. Der Auftragnehmer erklärt, daß er in der Lage ist, die aufgetragenen Arbeiten nach Maßgabe des §11 Bundesdatenschutzgesetz ordnungsgemäß und gewissenhaft durchzuführen.

Die technischen und organisatorischen Maßnahmen unterliegen der Kontrolle des Sachverständigen für Informationstechnik Klaus Kenner, 10178 Berlin. Ein entsprechendes Gutachten liegt vor.

Datenschutzbeauftragter im Hause des Auftraggebers ist Dieter Sparsam
Datenschutzbeauftragter im Hause des Auftragnehmers ist Günter Gebot

2. Umfang, Art und Zweck der Auftragsdatenverarbeitung und Kreis der Betroffenen

Der Umfang der durchzuführenden Arbeiten erstreckt sich auf die unter (1) angegebenen Tätigkeiten zu Zweck der:

- Bestandspflege
- Datenkorrektur

Art der Daten:

- Kundenname, Kundennummer, Adresse, Telefonnummer, Datum des letzten Kontakts

Der Kreis der Betroffenen umfasst:

- Kunden des Auftraggebers

3. Folgende technischen und organisatorischen Maßnahmen zur Datensicherung im Sinne von § 9 BDSG nebst Anlage sind beim Auftragnehmer getroffen worden:

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind:

(Zutrittskontrolle)

Die Zutrittskontrolle wird im Empfang durch das Sekretariat sicher gestellt. Nicht berechnigte Personen haben keinen Zutritt.

(Zugangskontrolle)

Der Zugang zu den DV-Anlagen erfolgt nur für die berechtigten Personen unter Aufsicht der Abteilungsleitung.

(Zugriffskontrolle)

Der Zugriff wird administrativ mittels Benutzerauthentifizierung über die Domänenrichtlinien geregelt. Die USB-Anschlüsse der PC sind deaktiviert, Brennerlaufwerke sind nicht vorhanden.

(Weitergabekontrolle)

Eine Maßnahme ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren. Nach erfolgtem Auftrag werden die Daten mittels Axcrypt verschlüsselt und per DVD an den Auftraggeber transportiert.

(Eingabekontrolle)

Die veränderten bzw. korrigierten Datensätze erhalten in einem Datenbankfeld ein Namenszeichen des Bearbeiters.

(Auftragskontrolle)

Der Auftraggeber erhält alle 2 Wochen einen Statusbericht des Datenschutzbeauftragten des Auftragnehmers über die ordnungsgemäß durchgeführte Verarbeitung.

(Verfügbarkeitskontrolle)

Die Daten werden beim Auftragnehmer regelmäßig gesichert und auf einem redundanten Plattensystem bearbeitet.

4. Berichtigung, Sperrung, Löschung personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten achtet der Auftragnehmer insbesondere darauf, daß im Sinne des BDSG eine ggf. nötige Berichtigung, Sperrung und Löschung personenbezogener Daten durchgeführt wird. Im Zweifelsfall wird der Auftragnehmer den Auftraggeber informieren.

5. Pflichten des Auftragnehmers und dessen Kontrollen

Die Pflichten des Auftragnehmers ergeben sich aus § 11 Abs. 4 BDSG, insbesondere die durch den Auftragnehmer durchzuführenden Kontrollen. Die bei der Datenverarbeitung eingesetzten Mitarbeiter des Auftragnehmers sind schriftlich auf das Datengeheimnis nach § 5 BDSG verpflichtet. Sofern gemäß BDSG beim Auftragnehmer ein Datenschutzbeauftragter zu bestellen ist, erklärt der Auftragnehmer diesen bestellt und über die Auftragsdatenverarbeitung zu informieren zu haben.

6. Berechtigung zur Begründung von Unterauftragsverhältnissen

Der Auftragnehmer verpflichtet sich, die ihm übergebenen personenbezogenen Daten grundsätzlich nur in seinen eigenen Geschäftsräumen und ohne Einschaltung von Subunternehmen / Unterauftragnehmern zu verarbeiten. Vor einer dennoch erforderlichen Einschaltung eines Subunternehmens / Unterauftragnehmers (z. B. bei technischen Störungen an der EDV-Anlage bzw. an der Vernichtungsanlage des Auftragnehmers) ist unbedingt das Einverständnis des Auftraggebers einzuholen.

Unterauftragsverhältnisse zum Zweck der Wartung der DV-Anlage bestehen mit:

- Firma IT-Service Müller, Ansprechpartner Markus Müller, 25348 Glückstadt

7. Kontrollrechte des Auftraggebers, Duldungs- und Mitwirkungspflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, die Kontrolle der Datenverarbeitung durch den Auftraggeber jederzeit zu dulden und zu unterstützen. Der Auftragnehmer ist zur Duldung und Mitwirkung bei der Kontrolle verpflichtet. Auch die Dokumentation des Kontrollergebnisses vor Beginn und während des Auftrags wird vom Auftragnehmer geduldet und unterstützt.

8. Mitzuteilende Verstöße des Auftragnehmers

Verstößt der Auftragnehmer oder die bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die in diesem Auftrag getroffenen Festlegungen ist dies dem Auftraggeber unverzüglich schriftlich mitzuteilen.

9. Umfang der Weisungsbefugnisse des Auftraggebers

Der Auftragnehmer verpflichtet sich, die Verarbeitung der ihm übergebenen personenbezogenen Daten ausschließlich im Rahmen der vertraglich festgelegten Weisungen des Auftraggebers durchzuführen (§11 Abs. 2, Nr.1-10 BDSG). Ist der Auftragnehmer der Ansicht, daß eine Weisung des Auftraggebers gegen das Bundesdatenschutzgesetz oder andere Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit die Daten und Unterlagen des Auftraggebers betroffen sind.

10. Rückgabe der Datenträger und Löschung nach Beendigung des Auftrags

Nicht mehr erforderliche Daten sind beim Auftragnehmer unverzüglich zu löschen. Bei Beendigung des Auftragsverhältnisses verpflichtet sich der Auftragnehmer, alle ihm im Zusammenhang mit dem Auftrag übergebenen und bis dahin noch nicht verarbeiteten bzw. gelöschten personenbezogenen Daten an den Auftraggeber zurückzugeben, bzw. den Nachweis einer ordnungsgemäßen Verarbeitung darüber zu führen. Es wird gewährleistet, dass zur Verarbeitung/Löschung bestimmte Datenträger während ihres Transportes gegen unberechtigte Einsichtnahme und Verlust geschützt sind. Eine notwendige endgültige Löschung der verbliebenen personenbezogenen Daten wird vom Auftragnehmer unmittelbar nach Beendigung des Auftrags durchgeführt.

Berlin, 01.09.2009

[Auftragnehmer / Unterschrift]

[Auftraggeber / Unterschrift]