



Mustervertragsanlage zur Auftragsdatenverarbeitung

Version 3.0
Mit englischer Übersetzungshilfe!

■ Impressum

Herausgeber: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Dr. Tobias Stadler
Tel.: 030.27576-224
t.stadler@bitkom.org

Redaktion: Dr. Tobias Stadler

Redaktionsassistentz: Karen Schlaberg

Gestaltung / Layout: Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)

Copyright: BITKOM 2009

Mustervertragsanlage zur Auftragsdatenverarbeitung

Version 3.0

Mit englischer Übersetzungshilfe!



- Bitte beachten Sie, dass der englische Text in der rechten Spalte nicht zur Verwendung als Vertragsinhalt gedacht ist, sondern lediglich eine Übersetzungshilfe zu der deutschen Mustervertragsanlage darstellt!

- Please note that the following text is not intended to be used as a contract template. The text is intended to be used as a translation assistance corresponding to the German contract template in the left column.

Translation

Anlage [XXX] zum Vertrag vom [xxx] Auftragsdatenverarbeitung

Annex [XXX] to the Agreement dated [xxx] Contract Data Processing on Behalf

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im **Dienstvertrag/ Werkvertrag (Hauptvertrag)** in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem **Dienstvertrag/ Werkvertrag (Hauptvertrag)** in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

§ 1 Definitionen:

(1) Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

(2) Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

Preamble

This annex specifies the data protection obligations of the parties which arise from contract data processing on behalf, as stipulated in the **Service/Work and Services Contract (the "Main Contract")**. It applies to all activities performed in connection with the **Main Contract** in which the staff of the contract data processor on behalf ("Processor") or a third party acting on behalf of the Processor may come into contact with personal data of the principal ("Controller"). The term of this annex shall follow the term of the Main Contract.

§ 1 Definitions:

(1) "Personal Data"

Personal Data means any individual element of information concerning the personal or material circumstances of an identified or identifiable individual.

(2) "Processing"

Processing means processing of Personal Data on behalf, encompassing the storage, amendment, transfer, blocking or erasure of personal data by the processor acting on behalf of the Controller.

(3) Weisung*

Weisung ist die auf einen bestimmten datenschutz-mäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG).

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen.

(3) Die Inhalte dieser Vertragsanlage gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird, und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

(3) “Instruction”

Instruction means the written instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalising, blocking, deletion, making available). Instructions shall initially be specified in the Main Contract and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (individual instructions).

§ 2 Scope and Responsibility

(1) Processor shall process Personal Data on behalf of Controller. Processing shall include such actions as may be specified in the Main Contract and in the scope of work. Within the scope of the Main Contract, Controller shall be solely responsible for complying with the statutory requirements relating to data protection, in particular regarding the transfer of Personal Data to the Processor and the Processing of Personal Data (acting as “responsible body” as defined in § 3 para. 7 BDSG”).

(2) Based on this responsibility, Controller shall be entitled to demanding the rectification, deletion, blocking and making available of Personal Data during and after the term of the Main Contract.

(3) The regulations of this annex shall equally apply if testing or maintenance of automatic processes or of Processing equipment is performed on behalf of Controller, and access to Personal Data in such context cannot be excluded.

§ 3 Obligations of Processor

(1) Processor shall collect, process and use Personal Data only within the scope of Controller’s Instructions.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen des Bundesdatenschutzgesetzes (§ 9 BDSG) entsprechen. Dies beinhaltet insbesondere

a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),

b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

c) dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

d) dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

e) dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

(2) Within Processor's area of responsibility, Processor shall structure Processor's internal corporate organisation to ensure compliance with the specific requirements of the protection of Personal Data. Processor shall take the appropriate technical and organisational measures to adequately protect Controller's Personal Data against misuse and loss in accordance with the requirements of the German Federal Data Protection Act (§ 9 BDSG). Such measures hereunder shall include, but not be limited to,

a) the prevention of unauthorised persons from gaining access to Personal Data Processing systems (physical access control),

b) the prevention of Personal Data Processing systems from being used without authorisation (logical access control),

c) ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation (data access control),

d) ensuring that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),

e) ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems, (entry control),

f) dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

g) dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

h) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

Eine Maßnahme nach b bis d ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird Anhang zu dieser Anlage.

Opt. (3) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsdatenverarbeitung zur Verfügung.

(4) Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Angaben zur Verfügung.

(5) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 Bundesdatenschutzgesetz (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

(6) Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit.

f) ensuring that Personal Data Processed are Processed solely in accordance with the Instructions (control of instructions),

g) ensuring that Personal Data are protected against accidental destruction or loss (availability control),

h) ensuring that Personal Data collected for different purposes can be processed separately (separation control).

A measure as referred to in lit. b to d above shall be in particular, but shall not be limited to, the use of state-of-the-art encryption technology.

An overview of the above-entitled technical and organisational measures shall be attached to this annex as an exhibit.

Opt. (3) Upon Controller's request, Processor shall provide a comprehensive and current Personal Data protection and security programme covering Processing hereunder.

(4) Upon Controller's request, Processor shall provide all information necessary for compiling the overview defined by § 4g para. 2 sentence 1 BDSG.

(5) Processor shall ensure that any personnel entrusted with Processing Controller's Personal Data have undertaken to comply with the principle of data secrecy in accordance with § 5 BDSG and have been duly instructed on the protective regulations of the BDSG. The undertaking to secrecy shall continue after the termination of the above-entitled activities.

(6) Processor shall notify to Controller the contact details of the Processor's data protection official.

(7) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.

(8) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(9) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses (Jedermannverzeichnis) gem. § 4g Abs. 2 S. 2 BDSG liegt beim Auftraggeber*.

(4) Dem Auftraggeber obliegen die aus § 42a BDSG resultierenden Informationspflichten.

(7) Processor shall, without undue delay, inform Controller in case of a serious interruption of operations, suspicion of breaches of Personal Data protection, and any other irregularity in Processing Controller's Personal Data.

(8) Controller shall retain title as to any carrier media provided to Processor as well as any copies or reproductions thereof. Processor shall store such media safely and protect them against unauthorised access by third parties. Processor shall, upon Controller's request, provide to Controller all information on Controller's Personal Data and information. Processor shall be obliged to securely delete any test and scrap material based on an Instruction issued by Controller on a case-by-case basis. Where Controller so decides, Processor shall hand over such material to Controller or store it on Controller's behalf.

(9) Processor shall be obliged to audit and verify the fulfilment of the above-entitled obligations and shall maintain an adequate documentation of such verification.

§ 4 Obligations of Controller

(1) Controller and Processor shall be separately responsible for conforming with such statutory data protection regulations as are applicable to them.

(2) Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data detected during a verification of the results of such Processing.

(3) Controller shall be obliged to maintain the publicly available register as defined in § 4g para. 2 sentence 2 of the Germany Federal Data Protection Act.

(4) Controller shall be responsible for fulfilling the duties to inform resulting from § 42a BDSG.

(5) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

Opt. (6) Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber*.

Opt. (7) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

§ 5 Anfragen Betroffener an den Auftraggeber*

Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen, vorausgesetzt:

- der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert und
- der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten.

§ 6 Kontrollpflichten*

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig [alternativ ist ein Zeitraum festzulegen] von den technischen und organisatorischen Maßnahmen des Auftragnehmers und dokumentiert das Ergebnis.

Hierfür kann er...

Alt. 1

...Selbstauskünfte des Auftragnehmers einholen.

(5) Controller shall, upon termination or expiration of the Main Contract and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the measures to return data carrier media or to delete stored data.

Opt. (6) Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Main Contract shall be borne by Controller.

Opt. (7) Any cost arising out of Processor's performance under Instructions outside the Main Contract's scope of work shall be borne by Controller.

§ 5 Enquiries by Data Subjects to Controller

Where Controller, based upon applicable data protection law, is obliged to provide information to an individual about the collection, processing or use of its Personal Data, Processor shall assist Controller in making this information available, provided that:

- Controller has instructed Processor in writing to do so, and
- Controller reimburses Processor for the costs arising from this assistance.

§ 6 Audit Obligations

(1) Controller shall, prior to the commencement of Processing, and in regular intervals thereafter [alternatively, define an interval], audit the technical and organisational measures taken by Processor, and shall document the resulting findings.

For such purpose, Controller may...

Alt. 1

...collect voluntary disclosures from Processor.

Alt. 2

...sich ein Testat eines Sachverständigen vorlegen lassen.

Alt. 3

...sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich überzeugen.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

§ 7 Subunternehmer*

(1) Die Weitergabe von Aufträgen im Rahmen der in § 2 Abs. 1 S. 2 konkretisierten Tätigkeiten an Subunternehmer durch den Auftragnehmer bedarf der schriftlichen Zustimmung* des Auftraggebers.

Alt. 1

(2) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt.

Alt. 2

(2) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Leistungsteile werden unter Einschaltung eines Subunternehmers durchgeführt, nämlich

(Name und Anschrift des Subunternehmers)

Alt. 2

...have an expert provide a testimonial or expert's opinion.

Alt. 3

...during regular business hours, without disrupting Processor's business operations, and after a reasonable prior notice, personally audit Processor.

(2) Processor shall, upon Company's written request and within a reasonable period of time, provide Controller with all information necessary for such audit.

§ 7 Subcontractors

(1) Processor shall be entitled to subcontract Processor's obligations defined in § 2 para. 1 sentence 2 to third parties only with Controller's written consent.

Alt. 1

(2) Controller consents to Processor's subcontracting to Processor's affiliated companies and/or third parties of Processor's contractual obligations hereunder.

Alt. 2

(2) Controller acknowledges that Processor's contractual obligations hereunder, or the parts of the deliverables defined below, will be performed by a subcontractor, namely

(name and address of the subcontractor)

(3)*Erteilt der Auftragnehmer Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages.

***optional** Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend § 6 einzuräumen. Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl*

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Es gilt deutsches Recht.

(3) Where Processor engages subcontractors, Processor shall be obliged to pass on Processor's contractual obligations hereunder to such subcontractors. Sentence 1 shall apply in particular, but shall not be limited to, the contractual requirements for confidentiality, data protection and data security stipulated between the parties of the Main Contract.

***optional** Processor shall be obliged to secure audit and inspection rights as defined in § 6 for Controller's benefit. Controller shall also be entitled, upon written request, to information about the essential content of the subcontract and the implementation of the data protection obligations by the subcontractor, and shall further be entitled to reasonably inspect the relevant contract documentation.

§ 8 Duties to Inform, Mandatory Written Form, Choice of Law

(1) Where Controller's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed, Processor shall inform Controller without undue delay. Processor shall, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in Controller's sole property and area of responsibility, that Personal Data is at Controller's sole disposition, and that Controller is the responsible body in the sense of the BDSG.

(2) No change of or amendment to this annex and all of its components, including any commitment issued by Processor, shall be valid and binding unless made in writing and unless they make express reference to being a change or amendment to these regulations. The foregoing shall also apply to the waiver of this mandatory written form.

(3) This annex is governed by the laws of the Federal Republic of Germany.

■ Anhang 1 / Attachment 1

Auflistung der personbezogenen Daten und Zweck ihrer Verarbeitung durch den Auftragnehmer im Auftrag des Auftraggebers. Hierbei ist der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen zu nennen.

A list of Personal Data elements and the purpose of their Processing by Processor on behalf of Controller. The list shall state the extent, the nature and purpose of any contemplated collection, processing and use of data, the type of data, and the circle of data subjects.

■ Anhang 2 / Attachment 2

Darstellung der technischen und organisatorischen Maßnahmen des Auftragnehmers.

An overview of the technical and organisational measures taken by Processor.

! Bitte beachten Sie:

In einigen Teilen der Anlage sind alternative Formulierungen, Optionen und durch den Anwender auszufüllende Felder enthalten. Im Text sind diese Stellen optisch hervorgehoben. Die alternativen Formulierungen sind durch die Abkürzung „Alt.“ gekennzeichnet, Optionen sind grau, Formulierungen mit Raum für individuelle Angaben sind gelb hinterlegt.

Um den Hintergrund der jeweils möglichen Formulierungen oder auch die Gründe für eine vorgegebene Erwägung zu erläutern, finden sich in den „Begleitenden Hinweisen“ zu vielen Regelungen Ausführungen. Textpassagen in der Anlage, zu denen sich in den „Begleitenden Hinweisen“ solche Erläuterungen finden, sind mit einem hochgestellten, roten Sternchen (*) gekennzeichnet. Dem Anwender wird empfohlen, bei der Verwendung der Anlage immer auch die begleitenden Hinweise zu lesen.

! Please note:

Some parts of the Annex contain alternative wording and clauses, options and fields to be completed by the user. These are emphasised in the text. Alternative wording is denoted by the abbreviation “Alt.“, options are shaded grey, and clauses with space for individual entries have a yellow background.

The accompanying information contains background information and explanations on the reasons underlying many of the clauses. Wording and clauses which have accompanying information in this section are marked with a red asterisk (*). We recommend the users to always consult the accompanying information when implementing the annex template.

Begleitende Hinweise zur der Anlage Auftragsdatenverarbeitung

■ Wann liegt eine Auftragsdatenverarbeitung vor?

Die Auslagerung von Datenverarbeitungsprozessen oder deren Übertragung auf eine unternehmensfremde Stelle ist für viele Unternehmen eine wichtige Möglichkeit, externes Know-how nutzen und gleichzeitig Kosten sparen zu können. Nicht jede Konstellation, in der ein Unternehmen sich eines Dritten zur Datenverarbeitung bedient, stellt zugleich eine Auftragsdatenverarbeitung dar. Die Frage, ob eine solche vorliegt, ist jedoch von erheblicher Bedeutung, denn das Bundesdatenschutzgesetz stellt an die Parteien einer Auftragsdatenverarbeitung (Auftraggeber und Auftragnehmer) sowie an die Datenverarbeitung besondere Anforderungen.

Immer dann, wenn von der Übertragung einer Aufgabe auf eine andere, rechtliche Einheit auch personenbezogene Daten betroffen sind, sind daher die Fragen zu stellen: Ist die Verarbeitung personenbezogener Daten das wesentliche Element der Aufgabenübertragung auf eine andere rechtliche Einheit? Hat die datenverarbeitende Stelle eine Hilfs- oder Unterstützungsfunktion?

Sind diese Fragen zu bejahen, wird eine Auftragsdatenverarbeitung vorliegen. Spielt die Datenverarbeitung

Auftragsdatenverarbeitung ist auch zwischen den verschiedenen rechtlichen Einheiten innerhalb eines Konzerns möglich.

hingegen nur eine untergeordnete Rolle bei der Aufgabenübertragung, kann z.B. eine Funktionsübertragung vorliegen. Bei der Auftragsdatenverarbeitung werden Datenerhebung, -verarbeitung oder -nutzung für die

Erfüllung der Aufgaben und Geschäftszwecke der verantwortlichen Stelle ausgelagert. Der Auftragnehmer hat dementsprechend eine Hilfsfunktion, er leistet dem Auftraggeber in einer oder mehreren Phasen der Datenerhebung, -verarbeitung oder -nutzung weisungsgebundene Unterstützung. Er wird gleichsam als „verlängerter Arm“ des Auftraggebers tätig, weil keine Aufgabe in ihrer Vollständigkeit, sondern lediglich ihre technische Ausführung übertragen wird. Werden die den Verarbeitungsvorgängen zugrunde liegenden Aufgaben oder Geschäftszwecke ganz oder teilweise (mit) abgegeben oder erfüllt der Datenverarbeiter überwiegend eigene Geschäftszwecke, dann liegt eine Funktionsübertragung vor und der Datenverarbeiter wird selbst zur verantwortlichen Stelle.

Bei der Beantwortung der Frage, ob der Auftragnehmer lediglich eine Hilfsfunktion und daher eine Auftragsdatenverarbeitung vorliegt, können die folgenden Kriterien helfen. Für das Vorliegen einer Auftragsdatenverarbeitung spricht es, wenn

- dem Datenverarbeitenden die Entscheidungsbefugnis über die Daten fehlt.
- der Datenverarbeitende mit der Datenverarbeitung ganz oder teilweise fremde Geschäftszwecke verfolgt.
- der Datenverarbeitende einem ausdrücklichen Nutzungsverbot unterliegt.
- der Datenverarbeitende nur mit Daten umgeht, die ihm der Auftraggeber zur Verfügung stellt.
- der Auftrag auf die praktisch-technische Durchführung einer Datenverarbeitung gerichtet ist, die aber nach außen hin vom Auftraggeber vertreten wird.
- der Auftrag so ausgestaltet ist, dass der Datenverarbeitende nicht zu den von der Datenverarbeitung Betroffenen in Kontakt tritt.
- der Datenverarbeitende in keinerlei vertraglichen Beziehungen zu den von der Datenverarbeitung Betroffenen steht.

- es für den Datenverarbeitenden schwierig oder unmöglich ist, einen Bezug der Daten zu den von der Verarbeitung betroffenen Personen herzustellen (Pseudonymisierung durch Kontonummer, Personalnummer etc.)

Eine Auftragsdatenverarbeitung liegt zum Beispiel regelmäßig vor bei:

- externer Datenhaltung, insbesondere beim teilweisen oder gesamten Outsourcing eines Rechenzentrums.
- Zugriff auf personenbezogene Daten vor Ort beim Auftraggeber.
- Papier-/Aktenvernichtung, Vernichtung von Datenträgern.
- manueller oder elektronischer Archivierungsservice.
- Kundenservice, Telefonmarketing und anderen Formen des Direktmarketings, soweit nicht vom Unternehmen selbst durchgeführt.

Diese Mustervertragsanlage und die Erläuterungen richten sich an den Erfordernissen des § 11 BDSG aus. Sie müssen jedoch prüfen, ob Sie ggf. einem Gesetz mit anderen bzw. weitergehenden Vorschriften unterliegen. Weitergehende Vorschriften enthalten beispielsweise die Regelungen zur Auftragsdatenverarbeitung im § 80 des SGB (Sozialgesetzbuch) X für Sozialdaten und einige Landesdatenschutzgesetze. Dabei ist vor allem zu beachten, dass einige dieser Gesetze im Gegensatz zum BDSG bei der Auftragsdatenverarbeitung eine Anzeigepflicht des Auftraggebers gegenüber seiner Aufsichtsbehörde vorsehen. Zudem enthalten § 80 SGB X und einige der Landesdatenschutzgesetze ein Weisungsrecht des Auftraggebers auch bezüglich der technisch-organisatorischen Maßnahmen, wie es das BDSG nicht kennt.

Eine Auftragsdatenverarbeitung kann im Rechtssinn aber auch vorliegen, ohne dass die Parteien die externe Verarbeitung von Daten vereinbaren oder eine solche Verarbeitung überhaupt wollen. Denn das BDSG legt in § 11 Abs. 5 BDSG fest, dass die Vorschriften zur Auftragsdatenverarbeitung auch dann entsprechend zur Anwendung kommen, 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.

In der Konsequenz führt das dazu, dass bei vielen Dienstleistungen der ITK-Branche die gesetzlichen Anforderungen an eine Auftragsdatenverarbeitung zu beachten sind. Betroffen sind zum Beispiel

- Installation und Wartung von Netzwerken, Hardware (incl. Telekommunikationsanlagen) sowie Pflege von Software u.a. (Betriebssysteme, Middleware, Anwendungen),
- Parametrisieren von Software,
- Programmentwicklungen, Programmanpassungen bzw. -umstellungen, Fehlersuche und Tests,

Ohne Belang ist, ob die Wartungsmaßnahmen vor Ort oder per Fernwartung durchgeführt werden (Remote - Zugriff des Auftragnehmers auf personenbezogene Daten beim Auftraggeber)

- Durchführung von Migrationen im Produktivsystem, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Das BDSG ordnet allerdings lediglich die „entsprechende“ Anwendung der Vorschriften zur Auftragsdatenverarbeitung an. Bei der Anwendung der Vorschriften müssen etwaige Besonderheiten, die für die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen charakteristisch sind, daher Berücksichtigung finden.

Beispiel Wartung: Die technischen und organisatorischen Maßnahmen der Datensicherung sind wartungsspezifisch zu treffen.

Wenn Sie Zweifel haben, wie die Aufgabenübertragung richtig einzuordnen ist, sollten Sie sich unbedingt an den Datenschutzbeauftragten Ihres Unternehmens wenden.

■ Konsequenzen einer Auftragsdatenverarbeitung

Liegt eine Auftragsdatenverarbeitung vor, so ist nicht der Auftragnehmer für die Einhaltung der gesetzlichen Datenschutzvorschriften verantwortlich, diese Verantwortlichkeit verbleibt vielmehr beim Auftraggeber, § 11 BDSG. Dementsprechend ist der Auftraggeber nicht nur verpflichtet, den Auftragnehmer sorgfältig auszuwählen, sondern er hat sich auch selber von der Einhaltung

Die Voraussetzungen der Datenübermittlung in ein Drittland sind ausführlich dargestellt in der BITKOM Publikation „Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer“. (Download möglich auf der BITKOM Website www.bitkom.org)

der Datenschutzbestimmungen (§§ 5, 9, 11 BDSG) zu überzeugen. Der Auftragnehmer muss seinerseits intern sicherstellen, dass die Datenerhebung, -verarbeitung bzw. -nutzung nur nach den durch den Auftraggeber festgelegten Weisungen erfolgt und die technischen und

Beachten Sie bitte den Grundsatz der Datenvermeidung und Datensparsamkeit. Die Planung, Gestaltung und Auswahl informations-technischer Produkte und Verfahren haben sich an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und weiter zu verarbeiten, § 3a BDSG.

organisatorischen Maßnahmen (gemäß der Anlage zu § 9 BDSG) eingehalten werden. Seine Mitarbeiter sind auf das Datengeheimnis zu verpflichten.

Der Umsetzung dieser Anforderungen soll die vorliegende Anlage dienen, die zugleich noch weitere, im Zusammenhang der Auftragsdatenverarbeitung häufig auftauchende Fragen, regelt.

■ Erläuterungen zu den Regelungen der Anlage

Anwendungsbereich

Die Anlage kann im Zusammenhang mit allen Verträgen Verwendung finden, die innerhalb Deutschlands oder zwischen einem deutschen Unternehmen und einem Unternehmen der Mitgliedsstaaten der Europäischen Union bzw. des Europäischen Wirtschaftsraums geschlossen werden. Aufgrund der Umsetzung der EU-Richtlinie zum Datenschutz (95/46/EG) wird keine Unterscheidung mehr getroffen zwischen einer Datenverarbeitung in Deutschland oder in einem Staat innerhalb der EU bzw. des EWR. In allen anderen Fällen liegt aber eine Datenübermittlung in ein sog. Drittland vor, die nur unter bestimmten, engen Voraussetzungen erlaubt ist.

Hauptvertrag und Anlage (§ 1 Abs. 3)

Im Hauptvertrag, der in aller Regel ein Dienst- oder Werkvertrag sein wird, ist in allen Einzelheiten die Leistung des Auftragnehmers beschrieben, aus der sich das Vorliegen einer Auftragsdatenverarbeitung ergibt. Der Hauptvertrag und insbesondere die dortige Leistungsbeschreibung stellen auch den Rahmen bzw. die Grundlage für die Weisungen des Auftraggebers dar. Die Weisungen des Auftraggebers an den Auftragnehmer dienen der Sicherstellung der ordnungsgemäßen und datenschutzgerechten Erfüllung der vertraglich geschuldeten Leistung.

In § 11 Abs. 3 BDSG ist festgelegt, dass der Auftragnehmer die Daten „nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen“ darf. Das korrespondiert mit der rechtlichen Wertung des BDSG (vgl. § 11 Abs. 1), dass der Auftraggeber bei der Auftragsdatenverarbeitung verantwortlich für den Datenschutz bleibt.

Der Auftragnehmer muss dementsprechend sicherstellen, dass die Datenerhebung, -verarbeitung bzw. -nutzung nur nach den festgelegten Weisungen erfolgt und die technischen und organisatorischen Maßnahmen gemäß der Anlage eingehalten werden.

§ 3 Abs. 3, § 4 Abs. 5, 6 Kosten

Im Hauptvertrag sollte unbedingt eine Regelung enthalten sein, die die grundsätzliche Kostenverteilung zwischen Auftraggeber und Auftragnehmer klärt. Diese Regelung könnte zum Beispiel die Kosten, die für ein umfassendes Datenschutz- und Datensicherheitskonzept oder für eine über die gesetzlichen Anforderungen (BDSG, vgl. auch § 3 Abs. 2 der Anlage) hinausgehende Weisung anfallen, dem Auftraggeber auferlegen. Regelt der Hauptvertrag diese Fragen, sind die Klauseln überflüssig (aber nicht schädlich). Für den Fall, dass der Hauptvertrag dies nicht regelt, sollten die vorgeschlagenen Formulierungen jedoch in der Anlage bleiben und § 3 Abs. 3 um die Worte ergänzt werden „...und dessen Kosten...“.

§ 4 Abs. 3, Verfahrensverzeichnis

Die Anforderungen des BDSG an Verarbeitungsübersicht und Verfahrensverzeichnis sind ausführlich dargestellt in der BITKOM Publikation „Verfahrensverzeichnis und Verarbeitungsübersicht nach BDSG - Ein Praxisleitfaden- (Version 2.0)“. (Download möglich auf der BITKOM Website www.bitkom.org)

§ 5 Anfragen Betroffener

Die Person, deren Daten verarbeitet werden (sog. Betroffener, § 3 Abs. 1 BDSG), kann seine Rechte (Auskunft, Berichtigung, Löschung und Sperrung, vgl. §§ 6, 19 f, 34 f BDSG) gegenüber seinem Vertragspartner oder gegenüber dem Unternehmen geltend machen, mit dem er in Beziehung steht. Bei einer Auftragsdatenverarbeitung bleibt daher der Auftraggeber Adressat dieser Ansprüche. Dies hat zur Folge, dass ein Verfahren zwischen Auftraggeber und Auftragnehmer festgelegt werden muss, das sicherstellt, den Rechten der Betroffenen nachkommen zu können. Die Verantwortung hierfür und auch die entstehenden Kosten trägt der Auftraggeber.

Der Vertrag ist im Einzelfall aufgabenspezifisch anzupassen. Soweit spezialgesetzliche Regelungen für die Daten, die im Auftrag verarbeitet werden, Anwendung finden, ist zunächst zu prüfen, ob eine Auftragsdatenverarbeitung zulässig ist. Ggf. sind die spezialgesetzlichen Regelungen bei der Vertragsgestaltung (z.B. Beihilfe-, Personal-, Sozial- und Gesundheitsdaten) zu berücksichtigen.

§ 6 Kontrollrecht

In § 3 Absatz 2 der vorliegenden Anlage sind die gesetzlich geforderten Maßnahmen nach § 9 BDSG wiedergegeben. Diese Maßnahmen unterliegen dem Kontrollrecht des Auftraggebers im Rahmen der Auftragskontrolle durch den betrieblichen Datenschutzbeauftragten (oder sonstige Vertreter des Auftraggebers).

Bitte berücksichtigen Sie, dass sich der Auftraggeber vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat. Ein Verstoß gegen diese Pflicht ist bußgeldbewehrt.

Es ist grundsätzlich nicht erforderlich, daß sich der Auftraggeber unmittelbar beim Auftragnehmer vor Ort oder selbst in Person überzeugt. Zur Erfüllung der gesetzlichen Kontrollpflicht kann es je nach Einzelfall auch genügen, Selbstauskünfte des Auftragnehmers einzuholen oder sich ein Testat eines Sachverständigen vorlegen zu lassen. Maßgeblich wird hier stets die Sensitivität der auftragsbezogenen Daten, deren Menge sowie Gefährdungspotential sein. Orientiert hieran ist eine der dargestellten Alternativen zu wählen. Das Ergebnis der Untersuchung ist sachgerecht zu dokumentieren. Der Gesetzgeber selbst macht keine Vorgaben hinsichtlich der Ausgestaltung und Art dieser Dokumentation.

Die regelmäßige Kontrolle ist im Gesetz vorgeschrieben, aber nicht bußgeldbewehrt. Die geforderte Regelmäßigkeit ist daher im Einzelfall abhängig vom Gefährungsgrad der verarbeiteten Daten und dem möglichen Schadenspotential festzulegen. Der Gesetzgeber hat bewusst auf eine feste, beispielsweise jährliche Kontrollpflicht für sämtliche Fallgestaltungen verzichtet.

§ 7 Subunternehmer

§ 7 Abs. 1

Die „Zustimmung“ ist der Oberbegriff für die Einwilligung (=vorherige Zustimmung) und die Genehmigung (=nachträgliche Zustimmung), vgl. § 182 ff BGB.

§ 7 Absatz 2

Für einzelne Tätigkeitsbereiche der Erhebung, Verarbeitung bzw. Nutzung kann es notwendig sein, Unterauftragnehmer einzuschalten (z. B. Delegation von Arbeiten auf Ausweichrechenzentren in Fällen von Überkapazitäten oder Zusammenbrüchen). Zwischen Auftraggeber und Auftragnehmer sollte daher die Zulässigkeit oder Nichtzulässigkeit bestehender und zukünftiger Unterauftragsverhältnisse geregelt werden. Daneben ist ggf. festzulegen, ob dem Auftragnehmer grundsätzlich das Recht zugesprochen werden soll, künftige Unterauftragsverhältnisse abzuschließen und welche Auswirkungen das auf die Beteiligten der Auftragsdatenverarbeitung haben wird. Die in § 7 vorgeschlagene Regelung ist daher

optional. Sie steht im Zusammenhang mit § 3 der Anlage und bietet zwei alternative Regelungsvorschläge. Möglichkeit 1 gewährleistet eine umfassende Abdeckung der erforderlichen Zustimmung; Möglichkeit 2 sollte daher nur dann verwendet werden, wenn der Auftraggeber dies ausdrücklich wünscht.

§ 7 Absatz 3

Absatz 3 ist für beide Alternativen anzufügen, d.h. für Möglichkeit 1 und 2.

Laufzeit und Kündigungsregelung

Diese ergeben sich regelmäßig aus den entsprechenden Regelungen des Hauptvertrags. Zu beachten ist, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht, vgl. § 5 BDSG.

Schadensersatz

Regelungen zum Schadensersatz wird regelmäßig der Hauptvertrag enthalten. Unter Beachtung und Abwägung der Interessen der Vertragspartner können Höchstgrenzen einzelfallbezogen aufgenommen werden, die sich auch auf die Haftung aus § 7 BDSG beziehen. Soll gleichwohl auch in die Anlage eine Regelung zur Haftung aufgenommen werden, sollte diese sich an der Regelung des Hauptvertrages orientieren.

§ 7 BDSG Satz 1 bestimmt:

„Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet.“

Satz 2 dieser Vorschrift sieht aber eine Entlastungsmöglichkeit vor:

„Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.“

Verantwortliche Stelle ist bei der Auftragsdatenverarbeitung der Auftraggeber, vgl. oben. Der Auftraggeber muss also nachweisen, dass er seinen Pflichten aus der Auftragsdatenverarbeitung nachgekommen ist. Die Beschreibungen der Maßnahmen nach § 9 BDSG (vgl. § 3 Abs. 2) und der Nachweis ihrer Erfüllung kann für den Auftraggeber bei der Beweisführung gegenüber dem Betroffenen hilfreich sein, da diese Maßnahmen eine Art gesetzlichen Mindeststandard der gebotenen Sorgfalt darstellen.

Als weitere Publikationen des Arbeitskreises Datenschutz sind erhältlich:

- Leitfaden zur Nutzung von Email und Internet im Unternehmen (Version 1.5)
- Verzeichnisverfahren und Verarbeitungsübersicht nach BDSG - Ein Praxisleitfaden- (Version 2.0)
- Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.300 Unternehmen, davon 950 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein..



Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org