Mustervertragsanlage zur Auftragsdatenverarbeitung

Version 4.0

Mit englischer Übersetzungshilfe!

BITKOM

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
Autoren: (Überarbeitung Version 4.0)	Kramer, Rudi (Datev eG) | Kripko, Lars Marten (Bitkom Servicegesellschaft mbH) | Lindemann, Ilona (gkv informatik GbR) | Peter, Catrin (Ricoh Deutschland GmbH) | Schwab, Hermann-Josef (SAP AG) | Wagner, Christian (Nokia Solutions and Networks GmbH & Co. KG) | Weinert, Stephan (Computacenter AG & Co. oHG)
Übersetzung:	Markus Stamm (Alcatel-Lucent Deutschland AG)
Redaktion:	Susanne Dehmel, Carmen Kulpe, Oliver Lowin
Ansprechpartner:	Susanne Dehmel, Tel.: 030.27576-223, s.dehmel@bitkom.org
Copyright:	BITKOM 2013
Verantwortliches Gremium:	Arbeitskreis Datenschutz
Grafik/Layout:	Design Bureau kokliko/Astrid Scheibe (BITKOM)
Titelbild:	Daniela Stanek (BITKOM)

Mustervertragsanlage zur Auftragsdatenverarbeitung

Version 4.0

Mit englischer Übersetzungshilfe!

BITKOM

Nutzungshinweise:

In einigen Teilen der Anlage sind alternative Formulierungen, Optionen und durch den Anwender auszufüllende Felder enthalten. Im Text sind diese Stellen optisch hervorgehoben.

- Alternative Formulierungen sind durch die Abkürzung »Alt.« oder »Var. « (Variante) gekennzeichnet und jeweils grau hinterlegt,
- Optionale Formulierungen sind durch die Abkürzung »Opt.« gekennzeichnet und blau hinterlegt,
- 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 im Vertragstext, zu denen sich in den »Begleitenden Hinweisen« solche Erläuterungen finden, sind mit einem hochgestellten, blauen Sternchen (*) gekennzeichnet.

Dem Anwender wird empfohlen, bei der Verwendung der Anlage immer auch die begleitenden Hinweise zu lesen.

Anlage [XXX] zum Vertrag vom [xxx]

Zwischen XXX

-Auftraggeber-

und XXX

-Auftragnehmer-

über Auftragsdatenverarbeitung i.S.d. §11 Abs. 2 Bundesdatenschutzgesetz (BDSG)

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag vom XXX in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsdatenverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenerhebung, -verarbeitung oder -nutzung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung (Anmerkung: Bitte ausfüllen, sofern noch nicht im Vertrag geregelt, andernfalls streichen):

Art der Daten	Zweck der Datenerhebung, -verarbeitung oder -nutzung	Kreis der Betroffenen

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.«, or »Var. « (Variation) and shaded grey,
- Optional wording is denoted by the abbreviation »Opt. « and shaded blue,
- Clauses with space for individual entries have a yellow background.

The accompanying information contains background information and explanations on the reasons under¬lying many of the clauses.

- Wording and clauses which have accompanying information in this section are marked with a blue asterisk (*).

We recommend the users to always consult the accompanying information when implementing the annex template.

Annex [XXX] to the agreement dated [xxx] (hereinafter, the »Agreement«) concluded by and between XXX -hereinafter, the »Company«- and XXX -hereinafter, the »Supplier«-

- both Company and Supplier hereinafter individually referred to as a »Party«, and jointly referred to as the »Parties« - on contract data processing on behalf as referred to by section 11 paragraph 2 of the German federal data protection act (»Bundesdatenschutzgesetz«, hereinafter »BDSG«)

Preamble

This annex details the obligations of the Parties related to the protection of data resulting from the scope of the processing of personal data on behalf as defined in detail in the Agreement XXX. It shall apply to all activity within the scope of and related to the Agreement, and in whose context the Supplier's employees or subcontractors may come into contact with Company's personal data.

§ 1 Scope, Duration and Specification as to Contract Data Processing on Behalf

The scope and duration as well as the extent and nature of the collection, processing and use of personal data shall be as defined in the Agreement. Processing on behalf shall include in particular, but not be limited to, the categories of personal data listed in the table below: (Note: If the information to be documented in the following table is already contained in the Agreement itself, remove the second sentence of this paragraph and the table, otherwise, fill in the table.)

Category of data	Purpose of collection, processing or use of data	Category of data subjects the data relates to

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag 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) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

§ 3 Pflichten des Auftragnehmers

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

(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 zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Bundesdatenschutzgesetzes (Anlage zu § 9 BDSG) genügen. Diese Maßnahmen werden wie folgt festgelegt (Anmerkung: Bitte ausfüllen, sofern nicht als Anhang zu dieser Anlage vereinbart):

a) Zutrittskontrolle
b) Zugangskontrolle
c) Zugriffskontrolle
d) Weitergabekontrolle
e) Eingabekontrolle
f) Auftragskontrolle
g) Verfügbarkeitskontrolle
h) Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Informationen zur Verfügung, sofern er sie sich nicht selbst beschaffen kann.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu

Except where this annex expressly stipulates any surviving obligation, the term of this annex shall follow the term of the Agreement.

§ 2 Scope of Application and Distribution of Responsibilities

(1) Supplier shall process personal data on behalf of Company. The foregoing shall include the activities enumerated and detailed in the Agreement and its scope of work. Within the scope of the Agreement, Company shall be solely responsible for complying with the statutory data privacy and protection regulations, including, but not limited to, the lawfulness of the transmission to the Supplier and the lawfulness of processing; Company shall be the responsible body (»verantwortliche Stelle«) as defined in section 3 paragraph 7 BDSG.

(2) Any instruction by Company to Supplier related to processing (hereinafter, a »Processing Instruction«) shall, initially, be defined in the Agreement, and Company shall be entitled to issuing changes and amendments to Processing Instructions and to issue new Processing Instructions. Parties shall treat any Processing Instruction exceeding the scope of work defined in the Agreement as a change request.

§ 3 Supplier's Obligations and Responsibilities

(1) Supplier shall collect, process, and use data related to data subjects only within the scope of work and the Processing Instructions issued by Company.

(2) Supplier shall, within Supplier's scope of responsibility, structure Supplier's internal organisation so it complies with the specific requirements of the protection of personal data. Supplier shall implement and maintain technical and organisational measures to adequately protect Company's data in accordance with and satisfying the requirements of the BDSG (annex to section 9 BDSG). These measures shall be implemented as defined in the following list: (Note: Either fill in the technical and organisational measures directly into the list below, or include the items in an exhibit to this annex.)

a) physical access control
b) logical access control
c) data access control
d) data transfer control
e) data entry control
f) control of Processing Instructions
g) availability control
h) separation control

Supplier shall be entitled to modifying the security measures agreed upon, provided, however, that no modification shall be permissible if it derogates from the level of protection contractually agreed upon.

(3) Upon Company's request, and except where Company is able to obtain such information directly, Supplier shall provide all information necessary for compiling the overview defined by § 4g paragraph 2 sentence 1 BDSG.

erheben, zu verarbeiten oder zu nutzen (Datengeheimnis entsprechend § 5 BDSG). Das Datengeheimnis besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder die im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten nach § 42a BDSG.

(6) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach §§ 4f, 4g BDSG nachzukommen (§ 11 Abs. 2 Nr. 5 i.V.m. § 11 Abs. 4 BDSG), wie z. B. seiner Pflicht, einen Datenschutzbeauftragen zu bestellen, soweit vom Gesetz vorgeschrieben.

(8) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung.

(9) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

(10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

Opt.: Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich.

Opt.: Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber. *

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

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

(4) Supplier shall ensure that any personnel entrusted with processing Company's 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.

(5) Supplier shall, without undue delay, inform Company of any material breach of the regulations for the protection of Company's personal data, committed by Supplier or Supplier's personnel. Supplier shall implement the measures necessary to secure the data and to mitigate potential adverse effects on the data subjects and shall agree upon the same with Company without undue delay. Supplier shall support Company in fulfilling Company's disclosure obligations under section 42a BDSG.

(6) Supplier shall notify to Company the point of contact for all issues related to data privacy and protection within the scope of the Agreement.

(7) Supplier represents and warrants that Supplier complies with Supplier's obligations under sections 4f and 4g BDSG (section 11 paragraph 2 no. 5 in connection with section 11 paragraph 4 BDSG). The foregoing shall include in particular, but not be limited to, Supplier's obligations to appoint a data protection official where required by law.

(8) Supplier shall not use data transmitted to Supplier for any purpose other than to fulfil Supplier's obligations under the Agreement.

(9) Where Company so instructs Supplier, Supplier shall correct, delete or block data in the scope of this Agreement. Unless stipulated differently in the Agreement, Supplier shall, at Company's individual request, destroy data carrier media and other related material securely and beyond recovery of the data it contains. Where Company so instructs Supplier, Supplier shall archive and/or provide to Company, such carrier media and other related material.

(10) Supplier shall, upon Company's order, provide to Company or delete any data, data carrier media and other related materials after the termination or expiration of the Agreement.

Opt.: In case of testing and reject materials, no individual order by Company shall be required.

Opt.: Where Company's requests exceed the scope of work of the Agreement, Company shall reimburse Supplier for any expenses incurred through Supplier's compliance with Company's instructions to transfer or delete the data.*

§ 4 Company's Obligations

(1) Company shall, without undue delay and in a comprehensive fashion, inform Supplier of any defect Company may detect in Supplier's work results and of any irregularity in the implementation of statutory regulations on data privacy.

(2) Company shall be obliged to maintain the public register of processing in accordance with section 4g paragraph 2 sentence 2 BDSG.

§ 5 Anfragen Betroffener

(1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu erteilen, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen. Dies setzt voraus, dass der Auftraggeber den Auftragnehmer hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten erstattet. Der Auftragnehmer wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.

(2) Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen.

§ 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 z. B. Auskünfte des Auftragnehmers einholen,
- sich ein ggf. vorhandenes Testat eines Sachverständigen vorlegen lassen
- oder nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

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

§ 7 Subunternehmer

Alt. 1 von Abs. 1

(1) Eine Weitergabe von Aufträgen im Rahmen der in dem Vertrag vereinbarten Tätigkeiten an Subunternehmer durch den Auftragnehmer erfolgt nicht.

Alt. 2 von Abs. 1

(1) Die Weitergabe von Aufträgen im Rahmen der in dem Vertrag vereinbarten Tätigkeiten an Subunternehmer durch den Auftragnehmer bedarf der schriftlichen Zustimmung* des Auftraggebers. Der Auftragnehmer wird Subunternehmer nach deren Eignung sorgfältig auswählen.

Var. 1 von Abs. 2

(2) Zum Zeitpunkt des Abschlusses dieser Vereinbarung sind die in der Anlage aufgeführten Unternehmen als Subunternehmer für Teilleistungen für den den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem

§ 5 Enquiries by Data Subjects

(1) Where, in accordance with applicable data privacy laws, Company is obliged to answer a data subject's enquiry related to the collection, processing or use of such data subject's data, Supplier shall support Company in providing the required information. The foregoing shall be apply only where Company has so instructed Supplier in writing or in text form, and where Company reimburses Supplier for the cost and expenses incurred in providing such support. Supplier shall not directly respond to any enquiries of data subjects and shall refer such data subjects to Company.

(2) Where a data subject requests Supplier correct, delete or block data, Supplier shall refer such data subject to Company.

§ 6 Audit Obligations

(1) Company shall, prior to the commencement of the processing of data and at regular intervals thereafter [alternatively, an interval may be expressly stipulated], audit the technical and organisational measures implemented by Supplier and shall document the result of such audit.
In the course of such audit, Company may, in particular, conduct the following measures, but shall not be limited to the same:

- Company may obtain information from Supplier.
- Company may request Supplier to submit to Company an existing attestation or certificate by an independent professional expert.
- Company may, upon reasonable and timely advance agreement, during regular business hours and without interrupting Supplier's business operations, conduct an on-site inspection of Supplier's business operations or have the same conducted by a qualified third party which shall not be a competitor of Supplier.

(2) Supplier shall, at Company's written request and within a reasonable period of time, submit to Company any and all information, documentation and other means of factual proof necessary for the conduction of an audit.

§ 7 Subcontractors

Alt. 1 for paragraph 1

(1) Supplier shall not subcontract any part of the scope of work defined in the Agreement to any subcontractor.

Alt. 2 for paragraph 1

(1) Supplier shall not subcontract any part of the scope of work defined in the Agreement to a subcontractor except with Company's prior written approval* for each individual act of subcontracting. Supplier shall diligently select any subcontractor, duly taking into account their qualification.

Var. 1 for paragraph 2

(2) As of the effective date of this annex, the Supplier has subcontracted certain parts of the scope of work defined in the Agreement to the subcontractors enumerated in the attachment hereto. Within the subcontracted parts of the scope of

Zusammenhang auch unmittelbar die Daten des Auftraggebers. Für diese Subunternehmer gilt die Einwilligung für das Tätigwerden als erteilt.

Var. 2 von Abs. 2

(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 den aufgeführten Leistungen unterbeauftragt.

Var. 3 von Abs. 2

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

Name und Anschrift des Subunternehmers	Beschreibung welche Teilleistungen
XXX	XXX

(3) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages. Eine etwaige Prüfung durch den Auftraggeber beim Subunternehmer erfolgt nur in Abstimmung mit dem Auftragnehmer.*

Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Subunternehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

(4) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung.

Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

§ 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.

work, these subcontractors directly process and/or use Company's data. Company's approval of Supplier's use of these subcontractors shall be deemed given.

Var. 2 for paragraph 2

(2) Company hereby permits Supplier to use Supplier's affiliated legal entities as subcontractors for the scope of work defined in the Agreement, in whole or in part, and to subcontract to said affiliated legal entities the parts of the scope of work enumerated below.

Var. 3 for paragraph 2

(2) Company consents to Supplier's subcontracting, to the subcontractors enumerated in the following table, the scope of work defined in the Agreement, and/or the individual deliverables enumerated below, as the case may be:

Subcontractor name and address	Description of the individual deliverables
XXX	XXX

(3) Where Supplier subcontracts deliverables to subcontractors, Supplier shall be obliged to extend any and all of Supplier's obligations under the Agreement to all subcontractors. Sentence 1 shall apply in particular, but not be limited to, the requirements on the confidentiality and protection of data as well as data security, each as agreed upon between the Parties. Company shall be entitled to auditing Supplier's subcontractors only upon prior agreement with Supplier to that effect.*

At Company's written request, Supplier shall be required to provide to Company comprehensive information on the obligations of all subcontractors as they relate to data privacy and protection; this information shall, where necessary, include Company's right to inspect the relevant contract documents.

(4) The approval requirements for subcontracting shall not apply in cases where Company subcontracts ancillary deliverables to third parties; such ancillary deliverables shall include, but not be limited to, the provision of external contractors, mail, shipping and receiving services, and maintenance services.

Supplier shall conclude, with such third parties, any agreement necessary to ensure the adequate protection of data.

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

(1) Where Company's 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 in Supplier's control, Supplier shall notify Company of such action without undue delay. Supplier shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Company's sole property and area of responsibility, that data is at Company's sole disposition, and that Company is the responsible body in the sense of the BDSG.

(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) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

ggf. Anhang über technische und organisatorische Maßnahmen nach § 9 BDSG (vgl. auch § 3 Abs. 2 der Mustervertragsanlage)

(2) No modification of this annex and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing and then only if such modification expressly states that such modification applies to the regulations of this annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.

(3) In case of any conflict, the regulations of this annex shall take precedence over the regulations of the Agreement. Where individual regulations of this annex are invalid or unenforceable, the validity and enforceability of the other regulations of this annex shall not be affected.

(4) This annex is subject to the laws of the Federal Republic of Germany.

Attachment on technical and organisational measures pursuant to section 9 BDSG (also compare § 3 paragraph 2 of Annex)

Begleitende Hinweise zur der Anlage Auftragsdatenverarbeitung

Die Auslagerung von Datenverarbeitungsprozessen oder deren Übertragung auf einen Dienstleister, eine unternehmensfremde Stelle, ist für viele Unternehmen eine wichtige Möglichkeit, externes Spezialwissen zu nutzen, höhere Sicherheitsstandards zu erreichen und effektiver und flexibler zu wirtschaften.

Das Datenschutzrecht erlaubt prinzipiell nur die Verarbeitung personenbezogener Daten innerhalb eines Unternehmens (verantwortliche Stelle). Eine privilegierte Einbindung von Dienstleistern bei der Verarbeitung personenbezogener Daten bietet § 11 BDSG über die Auftragsdatenverarbeitung.

Die Auftragsdatenverarbeitung verlangt eine vertragliche Regelung zwischen Auftraggeber und Auftragnehmer. Im Gegenzug darf das Unternehmen die Daten vom Auftragnehmer verarbeiten lassen, ohne dass es einer weiteren Rechtsgrundlage für die ansonsten vorliegende »Übermittlung« der Daten an den Auftragnehmer bedarf. Es ist dann also weder die Zustimmung des Betroffenen erforderlich noch besteht das Erfordernis einer Interessensabwägung.

Wann liegt eine Auftragsdatenverarbeitung vor?

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

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.

Immer dann, wenn von der Übertragung einer Aufgabe auf eine andere, rechtliche Einheit auch personenbezogene Daten betroffen sind, sind daher die folgenden Fragen zu stellen:

- Ist die Verarbeitung personenbezogener Daten das wesentliche Element der Aufgabenübertragung auf eine andere rechtliche Einheit?
- Hat die datenverarbeitende Stelle ausschließlich eine Hilfs- oder Unterstützungsfunktion?

Sind diese Fragen zu bejahen, wird eine Auftragsdatenverarbeitung vorliegen. Spielt die Datenverarbeitung hingegen nur eine untergeordnete Rolle bei der Aufgabenübertragung, kann z. B. eine vollkommen anders zu handhabende Funktionsübertragung vorliegen (wie beispielsweise bei der Finanzbuchführung oder Gehaltsabrechnung durch einen Steuerberater).

Annotations to the Annex on Contract Data Processing on Behalf

Many corporations see the out-sourcing of processes related to the processing of data, to an external service provider or otherwise to an entity outside the corporation, as an important possibility to make use of specialised external expertise and know-how, to attain enhanced security standards and to operate more efficiently and more flexibly.

By design, the applicable data protection laws permit the processing of personal data solely within the boundaries of each legal entity (the »responsible body« as defined in the German BDSG). Through its regulations on contract data processing on behalf, section 11 BDSG affords the possibility of a privileged incorporation of service providers into the process of processing personal data.

Contract data processing on behalf, which is sometimes also referred to as commissioned data processing, requires a contractual agreement between the service provider and the responsible body. Pursuant to such an agreement, the responsible body may have data processed by a service provider without the need for a specific justification. Such a justification would otherwise be needed as a basis for »transferring« the data to the service provider which would otherwise occur. Provided that such an agreement exists, no consent by a data subject and no balancing of interest are required..

When is contract data processing deemed applicable?

Contract data processing on behalf is possible also between legal entities of the same group of companies.

There are transactions where a legal entity uses a third party in order to have data processed, but wherein, nonetheless, contract data processing on behalf is not deemed to exist. Ascertaining whether a certain transaction is contract data processing on behalf is therefore of paramount importance.

In all cases where the transfer or out-sourcing of a task to another legal entity also affects personal data, the following questions must be answered:

- Does processing personal data constitute the key element of the transfer of the affected task to another legal entity?
- Does the entity that will process data solely fulfil an auxiliary or a support function?

Where both questions are to be answered in the affirmative, contract data processing will typically be deemed to occur. Where, however, the processing of data is only circumstantial in transferring a task, there may occur a »functional transfer« which requires an entirely different approach (cases where this may apply are, for instance, accounting and payroll services conducted by a tax professional).

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)

Bei der Auftragsdatenverarbeitung können Datenerhebung, -verarbeitung oder -nutzung für die Erfüllung der Aufgaben und Geschäftszwecke der verantwortlichen Stelle ausgelagert werden. Der Auftragnehmer hat dementsprechend nur 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.

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

Werden die den Verarbeitungsvorgängen zugrunde liegenden Aufgaben 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 ausübt und daher eine Auftragsdatenverarbeitung vorliegt, können die folgenden Kriterien helfen. Für das Vorliegen einer Auftragsdatenverarbeitung spricht es, wenn

- dem Auftragnehmer die Entscheidungsbefugnis über die Daten fehlt.
- der Auftragnehmer mit der Datenverarbeitung keine eigenen Geschäftszwecke verfolgt.
- der Auftragnehmer einem ausdrücklichen Nutzungsverbot in Bezug auf die zu verarbeitenden Daten unterliegt.
- der Auftragnehmer mit Daten umgeht, die ihm der Auftraggeber zur Verfügung stellt oder Daten nach Weisung des Auftraggebers erhebt und damit umgeht.
- der Auftrag auf die Durchführung einer Datenverarbeitung gerichtet ist, die aber nach außen hin vom Auftraggeber verantwortet wird.
- der Auftragnehmer im Zusammenhang mit der Auftragsdatenverarbeitung in keinerlei vertraglichen Beziehungen zu den von der Datenverarbeitung Betroffenen steht.

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, bspw. bei der Implementierung neuer IT-Systeme mit Migration bestehender Daten durch den Auftragnehmer.
- Aktenvernichtung, Vernichtung von Datenträgern.
- manuellem oder elektronischem Archivierungsservice.
- Telefonmarketing und anderen Formen des Direktmarketings, soweit nicht vom Unternehmen selbst durchgeführt.

The prerequisites for transmitting data to third countries are discussed, at length, in the BITKOM guideline »Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer« which may be downloaded from the web site www.bitkom.org.

In cases where contract data processing on behalf occurs, the gathering, processing and use of data for the purpose of fulfilling the obligations and business purposes of the responsible body may be out-sourced. Consequently, the service provider will perform only an auxiliary or a support function in asmuch as it will provide support to the responsible body in one or more phases of gathering, processing or using data to the responsible body, and then only pursuant to the instructions given by the responsible body. The service provider will, in effect, become the extended workbench of the responsible body as no task is transferred in its entirety, and the service provider is limited to its technical execution.

If you are in doubt as to how the out-sourcing of certain tasks is to be assessed correctly, you should not hesitate to contact your company's data protection official under any circumstance.

Where the obligations and duties underlying the acts of processing are also transferred, in whole or in part, or where the data processor fulfils mostly its own business purposes, a functional transfer exists, and the data processor itself becomes a responsible body. The following criteria may be of assistance in ascertaining whether a service provider only performs supporting functions, and therefore contract data processing on behalf is carried out. The following circumstances support the assumption that contract data processing on behalf exists:

- The service provider is not entitled to decide on the use of data.
- The service provider does not pursue its own business purposes in processing the data.
- The use of the data to be processed by the service provider is expressly forbidden.
- The service provider handles data provided by the controller, or the service provider collects and handles data in accordance with the controller's instructions.
- The scope of work is targeted at the performance of data processing, but the controller is responsible for the processing vis-à-vis third parties.
- There are no contractual relationships between the data subjects affected by the processing of data and the service provider.

As a rule, and by way of example, contract data processing on behalf is regularly deemed to be carried out in the following cases:

- the external storage of data, including especially the partial or full outsourcing of a computing or data centre;
- the access to personal data at the controller's premises, for instance, during the implementation of new IT systems involving the migration of existing data by the service provider;
- the destruction of files and data carrier media;
- the performance of manual or electronic archival services;
- the performance telemarketing or other forms of direct marketing, where not conducted by the controller itself.

Wartung und Prüfung

Aufträge über Wartung oder Prüfung von IT-Systemen stellen keine Auftragsdatenverarbeitung dar. Allerdings gelten nach § 11 Abs. 5 BDSG die gleichen Regelungen wie bei einer Auftragsdatenverarbeitung, soweit der Zugriff der prüfenden bzw. wartenden Dienstleister auf personenbezogene Daten nicht ausgeschlossen werden kann. Diese scheinbar unbedeutende Unterscheidung führt in der praktischen Umsetzung zu einigen Abweichungen.

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

Ziel einer Vereinbarung nach § 11 Abs. 5 BDSG ist, für einen tatsächlichen Zugriff des Auftragnehmers auf personenbezogene Daten des Auftraggebers vorsorglich angemessene Regelungen zu treffen. In der Praxis sind diese Einzelfälle des tatsächlichen Zugriffs sehr gut durch Weisungen auf Grundlage einer, im Übrigen weitgehend dem allgemeinen Muster einer Vereinbarung zur Auftragsdatenverarbeitung entsprechenden, Vereinbarung lösbar.

Zu den Besonderheiten zählt, dass der Auftragnehmer die personenbezogenen Daten des Auftraggebers gerade nicht planmäßig verarbeitet oder nutzt. Die Art der Daten und der betroffene Personenkreis kann damit in aller Regel nicht im Voraus definiert werden. Häufig verlassen die personenbezogenen Daten auch nicht die IT-Systeme des Auftraggebers. Im Einzelfall müssen deshalb die einzelnen Regelungen der Mustervertragsanlage auf die tatsächlichen Gegebenheiten des Auftrages abgestimmt werden. Die Darstellung der technischen und organisatorischen Sicherheitsmaßnahmen ist nur sinnvoll, wenn die personenbezogenen Daten des Auftraggebers in IT-Systemen des Auftragnehmers verarbeitet werden könnten. Erst dann wird man auch Regelungen über die Rückgabe und Löschung der Daten zwischen den Parteien vereinbaren müssen. Selbst wenn personenbezogene Daten im Rahmen der Wartung in IT-Systemen des Auftragnehmers zu verarbeiten sind (bspw. Auswertung von Verbrauchshistorien eines Druckers), können wenige Maßnahmen bereits ausreichend Sicherheit bieten (bspw. die Daten dort umgehend löschen).

Im Rahmen der Dienstleistungserbringung muss darauf geachtet werden, dass der Rahmen der Tätigkeiten Wartung oder Prüfung nicht verlassen wird. Entwickelt sich die Dienstleistung dagegen zu einer Auftragsdatenverarbeitung gem. § 11 Abs. 2 BDSG, ist eine gesonderte Vereinbarung zu treffen.

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 (inkl. Telekommunikationsanlagen) sowie Pflege von Software u.a. (Betriebssysteme, Middleware, Anwendungen),
- Parametrisieren von Software,
- Programmanpassungen bzw. -umstellungen, Fehlersuche und Tests, 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.

Maintenance and Testing

Agreements and assignments to maintain and text IT systems are not contract data processing on behalf. However, section 11 paragraph 5 BDSG declares the same regulations applicable to maintenance and testing that would apply to contract data processing on behalf, unless any access to personal data by the service provider conducting such maintenance and testing can be excluded. This seemingly insignificant distinction leads to several deviations in the actual implementation.

Whether the maintenance (and thus the potential access to personal data by the service provider) is performed on-site or remotely, is irrelevant.

The aim of an agreement pursuant to section 11 paragraph 5 BDSG is to establish adequate regulations, by way of precaution, for an actual access of the controller's personal data by the service provider. In practice, such individual cases of actual access can be regulated quite well by instructions issued on the basis of an agreement which otherwise mostly resembles the standard template for an agreement on contract data processing on behalf.

The characteristics of note in this case include the fact that the service provider does not methodically process or use the controller's personal data. As a result, it will not normally be possible to define the types of data and the circle of the affected data subjects in advance. In many cases, personal data will never leave the IT systems of the controller. The regulations of the agreement template for contract data processing on behalf must therefore be adapted to the actual circumstances underlying the service agreement. The documentation of technical and organisational security measures will be useful only where the controller's personal data might be processed in IT systems of the service provider. Also, the regulation of the return and deletion of personal data by and between the parties will be required only in such cases. Even where, within the scope of maintenance, personal data is to be processed in the service provider's IT systems (e.g. where the usage history of consumable supplies or a printer is to be analysed), certain select measures may already provide for an adequate level of security (e.g. the deletion of data as early as is reasonable).

When rendering such services, it is necessary to ensure that the boundaries of maintenance and testing are not exceeded. Where the services provided do evolve into contract data processing on behalf pursuant to section 11 paragraph 2 BDSG, a separate agreement must be concluded

Based on the foregoing, the statutory requirements for contract data processing on behalf must be observed in many services provided in the IT and telecommunications sector. Examples of transactions covered by these requirements include:

- the installation and maintenance of computer networks and hardware (including private branch exchanges) as well as the maintenance of software (operating systems, middle ware, application software);
- the parametrisation of software;
- the development and adaptation as well as conversion and transcoding of software, including fault analysis and testing;
- all of which is relevant where an access to personal data cannot be excluded.

The BDSG stipulates only the »analogous« application of the regulations on contract data processing on behalf. In applying these regulations, the characteristics relevant to the testing or maintenance of automated processes or of data processing facilities must therefore be considered.

For example, in case of maintenance, the technical and organisational measures of securing and backing up data must be specific to the maintenance operations.

Nebenleistungen

Eine Auftragsdatenverarbeitung liegt nicht vor, wenn

- die Dienstleistung in speziellen Gesetzen geregelt ist, z. B. Telekommunikationsdienstleistungen oder Postdienstleistungen,

- fremd in Anspruch genommene Tätigkeiten beauftragt werden, die im eigentlichen Kern nicht den Umgang (Erhebung, Verarbeitung, Nutzung) mit personenbezogenen Daten betreffen, sondern in denen andere Dienstleistungsschwerpunkte im Vordergrund stehen und der dabei notwendigerweise verbundene Umgang mit personenbezogenen Daten nur ein unvermeidliches »Beiwerk« darstellt (z. B. Pförtnerdienstleistungen, Wachschutz, Reinigungsdienstleistungen, Handwerkereinsätze in Unternehmen, Hauspostverteilung).

Verantwortung und Umsetzung

Liegt eine Auftragsdatenverarbeitung vor, so ist der Auftraggeber für die Einhaltung der gesetzlichen Datenschutzvorschriften allein verantwortlich. Dementsprechend ist der Auftraggeber verpflichtet, den Auftragnehmer sorgfältig auszuwählen und er hat sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zum Schutz der betroffenen personenbezogenen Daten zu überzeugen.

Der Umsetzung dieser Anforderungen soll die vorliegende »Mustervertragsanlage ADV« als Anlage zum Vertrag dienen, die zugleich noch weitere im Zusammenhang mit der Auftragsdatenverarbeitung häufig auftauchende Fragen regelt.

Der Auftragnehmer muss seinerseits sicherstellen, dass die Datenerhebung, -verarbeitung bzw. -nutzung nach den, durch den Auftraggeber erteilten, Weisungen erfolgt. Er hat außerdem in seinem Verantwortungsbereich die technischen und organisatorischen Maßnahmen (bei deutschen Auftragnehmern gemäß der Anlage zu § 9 BDSG) selbständig umzusetzen und einzuhalten, die für den Schutz der betroffenen personenbezogenen Daten angemessen sind und die mit dem Auftraggeber vereinbart wurden. Seine Mitarbeiter sind von ihm auf das Datengeheimnis zu verpflichten. Verweise auf Rechtsvorschriften in der Vereinbarung sind an das jeweils geltende nationale Recht anzupassen.

Die nachfolgend beschriebenen Maßnahmen führen beispielhaft die Mindestanforderungen an die zu treffenden Sicherheitsvorkehrungen im Rahmen einer Auftragsdatenverarbeitung auf. Sie sind für den konkreten Fall entsprechend anzupassen und soweit nicht bereits im Vertrag (zum Beispiel in der Anlage zur Leistungsbeschreibung) festgelegt, in der »Mustervertragsanlage ADV« in § 3 Abs. 2 aufzuführen und damit zu vereinbaren.

Sicherheitsmaßnahmen gemäß § 9 BDSG

Die vom Auftragnehmer zu treffenden Maßnahmen können Folgendes umfassen:

1. Zutrittskontrolle:
   Elektronische Zutrittskontrolle (z. B. durch Ausweisleser) zu Betriebsstätten des Auftragnehmers

2. Zugangskontrolle:
   Autorisierte Benutzerkennungen und individuelle Passwörter für den Zugang zu Datenverarbeitungssystemen

3. Zugriffskontrolle:
   Abgestufte Zugriffskonzepte mit unterschiedlichen Kennungen und Passwörtern für den Zugriff auf Datenverarbeitungssysteme

4. Weitergabekontrolle:
   Einrichtung technischer Maßnahmen, um zu verhindern, dass Kundendaten bei der elektronischen Übertragung oder während ihres Transports unbefugt verarbeitet oder genutzt werden können (z. B. durch Verschlüsselung oder Schutz durch Passwörter)

Ancillary Services

Contract data processing does not exist where

- the services provided are regulated by specific statute, for instance in case of telecommunications and postal services,
- the services provided externally do not, in their actual nature, encompass the handling (collection, processing, and use) of personal data, but focus on other service elements, and the handling of personal data necessary in the course of the provision of the services is considered only an unavoidable and ancillary subordinate element (e.g. in case of desk officer, security, cleaning, janitorial and craftspeople, and internal mail services).

Responsibility and Implementation

In cases of contract data processing on behalf, the controller is solely responsible for compliance with the statutory regulations on data protection. Consequently, the controller is required to diligently select the service provider, and to audit the service provider in order to satisfy itself of the technical and organisational measures implemented by the service provider to protect the controller's personal data affected by processing.

The template agreement for contract data processing on behalf, as an annex to the agreement on the provision of services, is designed to implement the statutory requirements and to regulate several additional issues commonly in need of regulation in connection with contract data processing on behalf.

The service provider itself must ensure that the collection, processing, and use of data is performed in accordance with the instructions issued by the controller. The service provider must itself, in addition, implement and adhere to the technical and organisational measures (for German service providers, these shall be in accordance with the annex to section 9 BDSG) which are adequate to the protection of the personal data affected, and that have been agreed upon with the controller. The service provider must instruct its employees to the secrecy of data. References to the statute contained in the template must be adapted to the applicable statute of the pertinent jurisdiction.

The following description of measures enumerates, by way of example, the minimum requirements of the security measures to be adopted in the framework of contract data processing on behalf. They are to be adapted to the individual case and, unless already stipulated in the agreement itself (e.g. in an annex detailing the scope of work), must be agreed upon by listing them in section 3 paragraph 2 of the template.

Security Measures pursuant to section 9 BDSG

The measures to be implemented by the service provider may include the following:

1. Physical access control:
   Electronic physical access control (e.g. by badge or card readers) to sites of the service provider.

2. Logical access control:
   Authorised user names and individual passwords for accessing data processing systems.

3. Data access control:
   Hierarchical access control concepts using separate user names and passwords for accessing data processing systems.

4. Data transfer control:
   Implementation of technical measures that prevent customer data from being processed or used without authorisation during electronic transmission or during transport (e.g. by encryption or password protection).

5. Eingabekontrolle:
   Aufzeichnung von Zugriffen der Mitarbeiter des Auftragnehmers auf Daten des Auftraggebers in Logfiles bei Verarbeitung auf Systemen des Auftragnehmers

6. Auftragskontrolle:
   Anweisung an Mitarbeiter des Auftragnehmers über Umfang und Inhalt der vom Kunden erteilten Weisungen

7. Verfügbarkeitskontrolle:
   Maßnahmen zum Brandschutz und bei Stromausfällen in den Rechenzentren des Auftragnehmers. »Back-up« entsprechend der Vereinbarung mit dem Auftraggeber.

8. Trennungskontrolle:
   Personenbezogene Daten unterschiedlicher Auftraggeber werden physikalisch oder logisch getrennt gespeichert.

Mögliche zusätzliche Kostenregelungen

Sollten nach Vertragsabschluss Änderungswünsche des Auftraggebers an den technischen und organisatorischen Maßnahmen entstehen, wird empfohlen, diese im Rahmen eines Change-Verfahrens zum Hauptvertrag zu regeln. Dies gilt auch für Vergütungsregelungen für Unterstützung bei Kontrollmaßnahmen.

Erläuterungen zu den Regelungen der Anlage

Das Muster 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.

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.

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

5. Data entry control:
   Auditing and recording of the access transactions performed by the service provider's employees to the controller's data, using log files, in case of processing on the service provider's systems.

6. Control of processing instructions:
   Instructions to the service provider's employees on the scope and content of the instructions issued by the customer.

7. Availability control:
   Protection against fire and measures in case of power outages in the data processing centres of the service provider. Creating back-ups in accordance with the agreement with the controller.

8. Separation control:
   Personal data of different controllers are separated physically or logically when stored.

Possible additional Regulations on the Remuneration

Where the controller requests changes to the technical and organisational measures after the conclusion of the agreement, it is recommended to regulate these within the scope of a change management procedure applicable to the agreement itself. This applies also to regulations on the remuneration of support services in case of audits.

Annotations to the Regulations contained in the Template Annex

The template must be adapted so it is aligned with the tasks and duties of the individual case. Where special statutory provisions apply to the data processed on behalf, it is therefore necessary to ascertain, first, whether contract data processing on behalf is permissible. Where applicable, the specific statutory provisions need to be incorporated when drafting the agreement (examples include civil servants' health benefits, personnel, social and health data)..

The template annex and the annotations are aligned with the requirements of section 11 BDSG. You need to verify, however, whether you are subject to statutory provisions stipulating other or additional requirements. Such additional requirements are, for instance, stipulated in the regulations on contract data processing on behalf in section 80 of the tenth book of the code of social law (SGB X), which apply to social data, and in several state data protection laws. It is necessary to observe, in this context, that some of these statutory requirements deviate from the BDSG in that they stipulate a duty for the controller to notify any contract data processing on behalf to its supervisory authority. In addition, section 80 SGB X and several state data protection laws stipulate the controller's right to issue instructions also with regard to technical and organisational measures; such an instrument is not contained in the BDSG.

Scope of Application

The annex may be used in connection with all agreements concluded within Germany or by and between a German legal entity and a legal entity in a member state of the European Union or the European Economic Area. Due to the implementation of the EU directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC), no distinction is made between processing of

in ein sog. Drittland vor, die nur unter bestimmten, engen Voraussetzungen erlaubt ist.

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)

Hauptvertrag und Anlage

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

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.

§ 4 Abs. 2 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 ihre 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 sollte, das sicherstellt, den Rechten der Betroffenen nachkommen zu können. Die Verantwortung hierfür und auch die entstehenden Kosten trägt der Auftraggeber.

§ 6 Kontrollpflichten

In § 3 Abs. 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

data in Germany and in a member state of the EU or the EEA. In all other cases, however, a transfer of data into a so-called third country exists, which is permissible only if defined and strict requirements are observed.

The requirements for transferring data into third countries are discussed, at length, in the BITKOM guideline »Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer«. This publication is available in German only and may be downloaded from the BITKOM Website at www.bitkom.org).

Main Agreement and Annex

Do observe the principles of data avoidance and data minimisation. Any planning, design and selection of IT products must be aligned with the goal of collecting and processing as little personal data as possible, see section 3a BDSG.

The main agreement, referred to in the annex as the »Agreement«, will normally be an agreement for the provision of professional services (»Dienstvertrag«) or work and services (»Werkvertrag«), and it is expected to contain the detailed definition of the deliverables to be provided by the service provider to the controller (referred to in the annex as »Company«), which result in contract data processing being effected. The Agreement, and in particular the scope of work it contains, also establish the framework and form the basis for the instructions issued by the controller. The instructions issued by the controller to the service provider serve to ensure that the contractual deliverables are rendered in a fashion compliant with the scope of work and the data protection requirements. Section 11 paragraph 3 BDSG stipulates that »the service provider may collect, process and use data only within the framework of the controller's instructions«. This corresponds to the legal concept of the BDSG (see section 11 paragraph 1), namely that the controller remains responsible for the protection of data in contract data processing on behalf.

Consequently, the service provider must ensure that the collection, processing and use of data is effected only in accordance with the instructions issued by the controller, and that the technical and organisational measures defined in the annex are observed and implemented.

Section 4 paragraph 2 Register of Processing

The requirements stipulated by the BDSG with regard to the overview and register of processing are discussed, at length, in the BITKOM guideline »Verfahrensverzeichnis und Verarbeitungsübersicht nach BDSG – Ein Praxisleitfaden (Version 2.0)«. This publication is available in German only and may be downloaded from the BITKOM Website at www.bitkom.org).

Section 5 Enquiries by Data Subjects

All natural persons whose data are being processed (the »data subject«, see section 3 paragraph 1 BDSG) may assert their rights (as to disclosure, correction, deletion, and blocking, see sections 6, 19 et seq., 34 et seq. BDSG) vis-à-vis their contract partners or the corporations with whom they have a relationship. In case of contract data processing on behalf, therefore, the controller remains the addressee of such rights. In consequence, a process should be agreed upon by and between the controller and the service provider which ensures that the data subjects' rights can be complied with. The responsibility for this compliance and the resulting expenses are borne by the controller.

Section 6 Audit Obligations

Section 3 paragraph 2 of the annex enumerates that measures required by law and stipulated in section 9 BDSG. These measures are subject to the controller's right to audit within the scope of the order control, either through the data protection official or through representatives of the controller.

It must be remembered that the controller must satisfy itself of the processor's compliance with the technical and

sich ein Testat eines Sachverständigen vorlegen zu lassen. Maßgeblich wird hier stets die Sensitivität der auftragsbezogenen Daten, deren Menge sowie Gefährdungspotential sein. Orientiert an diesen Kriterien 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 Gefährdungsgrad der verarbeiteten Daten und dem möglichen Schadenspotential festzulegen. Der Gesetzgeber hat bewusst auf eine feste, beispielsweise jährliche Kontrollpflicht für sämtliche Fallgestaltungen verzichtet.

§ 7 Subunternehmer

Subunternehmer ist jedes im Rahmen des Auftrages tätig werdende Unternehmen, das nicht mit dem Auftragnehmer identisch ist. Auch konzernverbundene Unternehmen des Auftragnehmers können in diesem Sinne Subunternehmer sein.

Beauftragt der Auftraggeber selbst eine Teilleistung direkt bei einem anderen Unternehmen, wird dieses Unternehmen nicht Subunternehmer im Sinne dieser Vereinbarung. Allerdings sollten die Verantwortlichkeiten in diesem Fall dokumentiert werden.

§ 7 Abs. 1

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

§ 7 Abs. 2

Für einzelne Tätigkeitsbereiche der Erhebung, Verarbeitung bzw. Nutzung kann es notwendig sein, Subunternehmer, also Unterauftragnehmer einzuschalten (z. B. Delegierung von Arbeiten auf Ausweichrechenzentren in Fällen von Überlastung). 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 Abs. 7 der Anlage und bietet zwei alternative Regelungsvorschläge. Alternative 1 gewährleistet eine umfassende Abdeckung der erforderlichen Zustimmung; Alternative 2 sollte daher nur dann verwendet werden, wenn der Auftraggeber dies ausdrücklich wünscht.

§ 7 Abs. 3

Absatz 3 ist für alle Alternativen des Abs. 2 anzufügen.

organisational measures implemented by the processor before processing of data commences. Any breach of this obligation is punishable by administrative fine.

As a rule, the controller does not need to satisfy itself of the processor's compliance physically at the processor's place of business, or that the controller conducts the audits directly and in person. Based on the characteristics of the individual case, the controller may be able to fulfil its audit obligation by obtaining questionnaire audit responses from the service provider, or by having the service provider produce an attestation or certificate issued by an independent professional expert. The sensitivity of the data affected by processing, their volume, and the risk potential, are criteria that will determine the audit methodology and the choice of one of the alternatives laid out above. The results of the audit must be documented appropriately. The statute does not stipulate the design and nature of this documentation.

The law requires recurring audits, but a breach of this obligation is not punishable by administrative fine. The required recurrence will therefore, in each individual case, depend on the risk potential with regard to the data processed, and the potential exposure associated with this processing. The statute, on purpose, does not stipulate fixed time intervals (e.g. a yearly recurrence) for the recurring audits for all cases.

§ 7 Subcontractors

Any legal entity not identical with the service provider and working within the scope of work or contributing thereto is considered a subcontractor. Even group legal entities belonging to the same group of legal entities the service provider itself belongs to may therefore be subcontractors.

Where the controller directly contracts another legal entity for a part of the deliverables, this legal entity does not become a subcontractor within the scope of the annex. However, the delineation of responsibilities should be documented in such a case.

Section 7 paragraph 1

The term »approval« (»Zustimmung«) is the collective term for prior consent (»vorherige Zustimmung«) and approval in arrears (»nachträgliche Zustimmung«). See section 182 et seq. of the German civil code (»BGB«).

Section 7 paragraph 2

It may be necessary to involve subcontractors for individual parts of the collection, processing and use (e.g. the overflow and delegation of work to substitute data centres in case of processing overload). The controller and the service provider should therefore regulate whether, and under what circumstances, existing and subcontracting relationships are permissible. In addition, it should be regulated whether the service provider should, as a rule, be entitled to conclude subcontracting agreements in the future, and what effects those agreement should have on the parties to the contract data processing relationship. The regulations proposed in section 7 are therefore optional. They are linked to section 3 paragraph 7 of the annex and propose two alternative regulations. Alternative 1 secures a comprehensive approval requirement. Alternative 2 should be used only where the controller expressly so desires.

Section 7 paragraph 3

Paragraph 3 must be added to all alternatives suggested for paragraph 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 können 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)
- Verfahrensverzeichnis und Verarbeitungsübersicht nach BDSG -Ein Praxisleitfaden- (Version 2.0)
- Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer

Term and Termination

These will regularly result from and be associated with the regulations of the Agreement. It should be noted, however, that the requirements of data secrecy will survive any termination of the processing operations, see section 5 BDSG.

Damages

The Agreement is typically expected to contain regulations on damages. Damage liability caps may be introduced on a per-case basis, and duly observing and taking into account the interests of the parties to the agreement, and these may also extend to the liability established by section 7 BDSG. Where the parties to the agreement desire to introduce a regulation on the liability into the annex, this regulation should be aligned with the regulation contained in the Agreement.

Section 7 sentence 1 BDSG stipulates: »Where a responsible body causes any damage to a data subject through an illegal or incorrect act of collection, processing, or use of the data subject's personal data, the responsible body or its legal entity shall be obliged to compensate the data subject for such damage.«

Sentence 2 of this section, however, stipulates a regulation to mitigate this liability: »DThe obligation to compensate [the data subject] shall not apply where the responsible body has observed the required level of diligence deemed necessary under the circumstances of the individual case.«

As explained above, in cases of contract data processing on behalf, the controller is the responsible body; consequently, the controller must prove that it has fulfilled its obligations resulting from the act of contract data processing on behalf. The documentation of the measures under section 9 BDSG (see section 3 paragraph 2) and the proof that they have been complied with, may therefore be beneficial to the controller in proving its case vis-à-vis the data subject, as these measures form a sort of statutory minimum standard for the adequate level of diligence.

The Data Protection Working Group has published the following further guidelines, all of which are currently available in German only:

- Leitfaden zur Nutzung von Email und Internet im Unternehmen (Version 1.5)
- Verfahrensverzeichnis 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 2.000 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 140 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

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