A1. Muster: Auftrag gemäß § 11 BDSG

Hinweise: *Der nachstehende Mustertext soll eine Orientierungshilfe bieten. Er ist je nach den Umständen des konkreten Einzelfalls anzupassen. Bei komplexen Auftragsverhältnissen oder der Verarbeitung sensibler personenbezogener Daten im Auftrag werden weitere bzw. ergänzende Vertragsklauseln notwendig sein.*

Die einzelnen schriftlichen Festlegungen nach § 11 Abs. 2 Nr. 1 bis Nr. 10 BDSG sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen.

Vereinbarung

zwischen dem/der

_____

- nachstehend Auftraggeber genannt -

und dem/der

_____

- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/SLA/_____ vom _____, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

_____ (Definition der Aufgaben)

Dauer des Auftrags

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum _____.

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von _____ zum _____ gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

☐ Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom _____.

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Umfang, Art und Zweck der Aufgaben des Auftragnehmers: _____.

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter _____.

oder

☐ Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ _____

Kreis der Betroffenen

☐ Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen ist in der Leistungsvereinbarung konkret beschrieben unter _____.

oder

☐ Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung/Beschreibung der betroffenen Personenkategorien)

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte i. S. d. § 3 Abs. 11 BDSG
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ _____

3. Technisch-organisatorische Maßnahmen

Die im Anhang beschriebenen technischen und organisatorischen Maßnahmen werden zwischen Auftraggeber und Auftragnehmer als verbindlich festgelegt.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen um nicht auftragsspezifische Maßnahmen hinsichtlich der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots, sowie andererseits um auftragsspezifische Maßnahmen, insbesondere im Hinblick auf die Art des Datenaustauschs/Bereitstellung von Daten, Art/Umstände der Verarbeitung/der Datenhaltung sowie Art/Umstände beim Output/Datenversand.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Der Auftragnehmer hat auf Anforderung die Angaben nach § 4g Abs. 2 Satz 1 BDSG dem Auftraggeber zur Verfügung zu stellen.

4. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach § 11 Abs. 4 BDSG folgende Pflichten:

- ⇨ Schriftliche Bestellung - soweit gesetzlich vorgeschrieben - eines Datenschutzbeauftragten, der seine Tätigkeit gem. §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.
- ⇨ Die Wahrung des Datengeheimnisses entsprechend § 5 BDSG. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.
- ⇨ Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend § 9 BDSG und Anlage.
- ⇨ Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde nach § 38 BDSG. Dies gilt auch, soweit eine zuständige Behörde nach §§ 43, 44 BDSG beim Auftragnehmer ermittelt.
- ⇨ Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.
- ⇨ Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

6. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies unter folgenden Bedingungen gestattet:

- ⇨ Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.
- ⇨ Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- ⇨ Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den

wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. [1]

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gem. § 9 BDSG und der Anlage nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) erbracht werden.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet dem Auftraggeber in allen Fällen eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Es ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

9. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers (vgl. § 11 Abs. 3 Satz 1 BDSG). Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind

[1] Die im vorstehenden Absatz getroffene Regelung kann seitens des Auftraggebers im Zuge einer Risikoabwägung optional getroffen werden. Sie erlaubt dem Auftragnehmer im Falle unterstützender Nebenleistungen durch Dritte die Ausgestaltung der datenschutzrechtlichen Vertragsbeziehung mit Dritten ohne Zustimmungserfordernis des Auftraggebers.

Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten benötigt werden.

Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend § 11 Abs. 3 Satz 2 BDSG zu informieren, wenn er der Meinung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder zuvor nach Aufforderung durch den Auftraggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

A2. Template Commission pursuant to Section 11 BDSG

***Notes*: This model text is intended for guidance. It should be amended to reflect the circumstances of any given case. In complex situations or where sensitive personal data are to be processed on behalf of others, additional or expanded clauses may be needed.**

The individual written provisions set out in Section 11(2) Nos 1 to 10 of the Federal Data Protection Act [Bundesdatenschutzgesetz - BDSG] should be used as a checklist and copied into the agreement appropriately. The alternatives applicable to the specific service relationship should be ticked. Gaps (marked _____) should be filled in according to the specific commission.

Agreement

between

_____

- (the “Principal”) -

and

_____

- (the “Agent”) -

1. Subject-matter and duration of the commission

Subject-matter of the commission

☐ The subject-matter of the commission is derived from the Service Agreement/SLA/_____ dated _____, to which reference is made here (the “Service Agreement”).

or

☐ The subject-matter of the data processing commission is the performance of the following tasks by the Agent: _____ (definition of tasks)

Duration of the commission

☐ The duration (term) of this commission is equal to the term of the Service Agreement.

or *(particularly where there is no Service Agreement for a specified term)*

☐ The commission is for a one-off task.

or

☐ The duration (term) of this commission runs until _____.

or

☐ The commission is for an indefinite period and may be terminated by either party giving _____ notice to _____. The right to terminate the commission without notice is unaffected by the above.

2. Details of the substance of the commission

Scope, nature and purpose of the proposed collection, processing or use of data

☐ The scope, nature and purpose of the collection, processing and/or use of personal data by the Agent on behalf of the principal are described in detail in the Service Agreement dated _____.

or

☐ More detailed description of the subject-matter of the commission in terms of the scope, nature and purpose of the tasks to be carried out by the Agent: _____.

The data will be processed and used exclusively within the territory of the Federal Republic of Germany, a Member State of the European Union or another signatory to the Agreement on the European Economic Area. Any movement of data to a third country requires the prior consent of the Principal and is subject to compliance with the special requirements set out in Sections 4b and 4c BDSG.

Nature of the data

☐ The nature of the personal data to be used is described in detail in the Service Agreement under: _____.

or

☐ The subject-matter of the collection, processing and/or use of personal data covers the following types/categories of data (list/description of categories of data)

- ☐ Personal master data
- ☐ Contact details (e.g. telephone, e-mail)
- ☐ Contract master data (contractual relationship, interest in products or contracts)
- ☐ Customer history
- ☐ Billing and payment data
- ☐ Planning and management data
- ☐ Rating data (from third parties, e.g. rating agencies, or from public directories)
- ☐ _____

Persons affected (data subjects)

☐ The group of data subjects affected by the processing of their personal data within this commission is described in detail in the Service Agreement under: _____.

or

☐ The group of data subjects affected by the processing of their personal data within this commission includes (list/description of categories of data subjects concerned):

- ☐ Customers
- ☐ Prospects
- ☐ Subscribers
- ☐ Employees in the meaning of Section 3(11) BDSG
- ☐ Suppliers
- ☐ Commercial representatives
- ☐ Contacts
- ☐ _____

3. Technical/organizational measures

The technical and organizational measures, stipulated in annex x, are binding for the Agent.

Overall, the measures to be taken include actions not specific to the commission in relation to organizational control, access control, disclosure control, input control, job control and availability control, and to the need for a segregation of functions, and commission-specific actions (particularly with regard to the type of data transfer/provision of data, the nature/method of data processing/storage and the nature/method of output/dispatch of the data).

The technical and organizational measures are subject to technical progress and development, and the Agent may implement adequate alternative measures. These must not however fall short of the level of security provided by the specified measures. Any material changes must be documented. The Agent must provide the Principal with the details set out in Section 4g(2) sentence 1 BDSG upon request.

4. Correction, deletion and blockings of data

The Agent may only correct, delete or block the data processed on behalf of the Principal when instructed to do so by the Principal. If a data subject should apply directly to the Agent to request the correction or deletion of his personal data, the Agent must forward this request to the Principal without delay.

5. Controls and other responsibilities of the Agent

In addition to complying with the provisions of this commission, the Agent has the following responsibilities under Section 11(4) BDSG:

- ⇨ Written appointment - where stipulated by law - of a data protection official, able to discharge his duties as set out in Sections 4f and 4g BDSG. The official’s contact details must be supplied to the Principal to enable direct contact to be made.
- ⇨ The maintenance of confidentiality in accordance with Section 5 BDSG. All persons who have access to personal data belonging to the Principal under the terms of this commission must give an undertaking to maintain confidentiality and must be informed of any special data protection requirements arising from this commission, and the limitation of use to specific purposes as instructed.
- ⇨ The implementation and maintenance of all technical and organizational measures required for this commission according to Section 9 BDSG and the Annex thereto.
- ⇨ Immediate notification to the Principal of any monitoring activities and measures undertaken by the supervisory authority pursuant to Section 38 BDSG. This also applies where a competent authority investigates the Agent in accordance with Sections 43 and 44 BDSG.
- ⇨ Monitoring of the commission by way of regular reviews by the Agent concerning the performance and fulfillment of the contract, particularly compliance with and any necessary amendment to provisions and measures laid down to carry out the commission.
- ⇨ Evidence to be provided to the Principal of the technical and organizational measures taken. For this purpose, the Agent may present up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department or quality auditors) or suitable certification by way of an IT security or data protection audit (e.g. ‘IT basic security’ as defined by the Federal Office for Information Security - BSI).

6. Subcommissions

Where sub-contractors are to be engaged for the processing or use of personal data belonging to the Principal, this will be allowed under the following conditions:

- ⇨ The commissioning of sub-contractors is only permitted with the prior written consent of the Principal. The Agent may engage his own affiliated companies or other sub-contractors for the performance of the contract without written consent, provided that he exercises the due care required by law, complies with the monitoring obligation set out in point (5) above, and informs the Principal before starting to process or use the data.
- ⇨ The Agent must set out the contractual agreements with the sub-contractor(s) in such a way that they reflect the data protection provisions agreed between the Principal and the Agent.
- ⇨ Where a sub-contractor is used, the Principal must be granted the right to monitor and inspect the sub-contractor in accordance with this Agreement and Section 11 BDSG in conjunction with item No 6 of the Annex to Section 9 BDSG. This also includes the right of the Principal to obtain information from the Agent, upon written request, on the substance of the contract and the implementation of the data protection obligations within the sub-contract relationship, where necessary by inspecting the relevant contract documents.

Subcommissions in the meaning of this provision do not include ancillary services ordered by the Agent from third parties to assist in the performance of the commission. These may be e.g. telecommunications services, maintenance and user support, cleaning, auditing or the disposal of data media. To safeguard the protection and security of the Principal’s data, even where ancillary services are taken from third parties, the Agent must however conclude adequate and lawful contractual agreements and undertake monitoring activities.

7. Monitoring rights of the Principal

The Principal may carry out the job control stipulated in No. 6 of the Annex to Section 9 BDSG in consultation with the Agent, or appoint auditors to do so. The Principal may carry out sample checks on the Agent’s business premises, generally to be announced in advance, in order to verify compliance with this Agreement by the Agent. The Agent undertakes to provide the Principal with the information required to meet his job control obligation, and make the necessary documentation available.

With regard to the monitoring obligations of the Principal under Section 11(2) sentence 4 BDSG before the start of data processing and throughout the term of the commission, the Agent must ensure that the Principal can confirm adherence to the technical and organizational measures taken. For this purpose, the Agent must provide the Principal upon request with evidence of the implementation of the technical and organizational measures pursuant to Section 9 BDSG and the Annex thereto. Evidence of the implementation of any measures that do not only affect the specific commission may also be presented in the form of up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department or quality auditors) or suitable certification by way of an IT security or data protection audit (e.g. ‘IT basic security’ as defined by the Federal Office for Information Security - BSI).

8. Notification of infringements by the Agent

The Agent must notify the Principal in all cases where the Agent or persons employed by him infringe provisions relating to the protection of personal data belonging to the Principal or any other stipulations set out in the commission.

The Parties are aware that Section 42a BDSG may impose a duty to inform in the event of the loss or unlawful disclosure of personal data or access to it. Such incidents should therefore be notified to the Principal immediately, regardless of their origin. This also applies to serious operational faults or where there is any suspicion of an infringement of provisions relating to the protection of personal data or other irregularities in the handling of personal data belonging to the Principal. In consultation with the Principal, the Agent must take appropriate measures to secure the data and limit any possible detrimental effect on the data subjects. Where obligations are placed in the Principal under Section 42a BDSG, the Agent must assist in meeting them.

9. Principal’s authority to issue instructions

The data may only be handled under the terms of the agreements concluded and the instructions issued by the Principal (see Section 11(3) sentence 1 BDSG). Under the terms of the commission as described in this Agreement, the Principal retains a general right of instruction as to the nature, scope and method of data processing, which may be supplemented with individual instructions. Any changes to the subject-matter of the processing and any changes to procedure must be agreed and documented together. The Agent may only pass on information to third parties or to the data subject with the prior written consent of the Principal.

The Principal must confirm any oral instructions immediately in writing or by e-mail (in text form). The Agent must not use the data for any other purpose and is particularly forbidden to disclose the data to third parties. No copies or duplicates may be produced without the knowledge of the Principal. This does not apply to backup copies where these are required to assure proper data processing, or to any data required to comply with statutory retention rules.

The Agent must inform the principal immediately, in accordance with Section 11(3) sentence 2 BDSG, if he believes that there has been infringement of legal data protection provisions. He may then postpone the execution of the relevant instruction until it is confirmed or changed by the Principal’s representative.

10. Deletion of data and return of data media

Upon completion of the contractual work or when requested by the Principal - and no later than the end-date of the Service Agreement - the Agent must return to the Principal all documents in his possession and all work products and data produced in connection with the commission, or delete them in compliance with data protection law with the prior consent of the Principal. The same applies to any test data and scrap material. The deletion log must be presented upon request.

Documentation intended as proof of proper data processing must be kept by the Agent beyond the end of the Agreement in accordance with relevant retention periods. The Agent may hand such documentation over to the Principal after expiry of the Agreement.

A3. Notes on the production of an Annex to the Agreement pursuant to Section 11 BDSG:

General technical and organizational measures pursuant to Section 9 BDSG and Annex

1. Access control to premises and facilities

Unauthorized access (in the physical sense) must be prevented.

Technical and organizational measures to control access to premises and facilities, particularly to check authorization:

Examples:

- ⇨ Access control system
  ID reader, magnetic card, chip card → see Section 6c BDSG
- ⇨ (Issue of) keys
- ⇨ Door locking (electric door openers etc.)
- ⇨ Security staff, janitors
- ⇨ Surveillance facilities
  Alarm system, video/CCTV monitor → see Section 6b BDSG

2. Access control to systems

Unauthorized access to IT systems must be prevented.

Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

Examples:

- ⇨ Password procedures (incl. special characters, minimum length, change of password)
- ⇨ Automatic blocking (e.g. password or timeout)
- ⇨ Creation of **one** master record per user
- ⇨ Encryption of data media

3. Access control to data

Activities in IT systems not covered by the allocated access rights must be prevented.

Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:

Examples:

- ⇨ Differentiated access rights (profiles, roles, transactions and objects)
- ⇨ Reports
- ⇨ Access
- ⇨ Change
- ⇨ Deletion

4. Disclosure control

Aspects of the disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.

Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

Examples:

- ⇨ Encryption/tunneling (VPN = Virtual Private Network)
- ⇨ Electronic signature
- ⇨ Logging
- ⇨ Transport security

5. Input control

Full documentation of data management and maintenance must be maintained.

Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

Example:

⇨ Logging and reporting systems

6. Job control

Commissioned data processing must be carried out according to instructions.

Measures (technical/organizational) to segregate the responsibilities between the Principal and the Agent:

Examples:

⇨ Unambiguous wording of the contract
⇨ Formal commissioning (request form)
⇨ Criteria for selecting the Agent
⇨ Monitoring of contract performance

7. Availability control

The data must be protected against accidental destruction or loss.

Measures to assure data security (physical/logical):

Examples:

⇨ Backup procedures
⇨ Mirroring of hard disks, e.g. RAID technology
⇨ Uninterruptible power supply (UPS)
⇨ Remote storage
⇨ Anti-virus/firewall systems
⇨ Disaster recovery plan

8. Segregation control

Data collected for different purposes must also be processed separately.

Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

Examples:

⇨ “Internal client” concept/limitation of use
⇨ Segregation of functions (production/testing)

A4. Hinweise zur Erstellung einer Anlage zur Vereinbarung nach § 11 BDSG:

Allgemeine technische und organisatorische Maßnahmen nach § 9 BDSG und Anlage

1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

Beispiele

- ⇨ Zutrittskontrollsystem,
  Ausweisleser, Magnetkarte, Chipkarte → zu beachten: § 6c BDSG
- ⇨ Schlüssel/Schlüsselvergabe
- ⇨ Türsicherung (elektrische Türöffner usw.)
- ⇨ Werkschutz, Pförtner
- ⇨ Überwachungseinrichtung
  Alarmanlage, Video-/Fernsehmonitor → zu beachten: § 6b BDSG

2. Zugangskontrolle

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort-/Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

Beispiele

- ⇨ Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- ⇨ Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- ⇨ Einrichtung eines Benutzerstammsatzes pro User
- ⇨ Verschlüsselung von Datenträgern

3. Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

Beispiele

- ⇨ Differenzierte Berechtigungen
  (Profile, Rollen, Transaktionen und Objekte)
- ⇨ Auswertungen
- ⇨ Kenntnisnahme
- ⇨ Veränderung
- ⇨ Löschung

4. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle...

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

Beispiele

- ⇨ Verschlüsselung/Tunnelverbindung (VPN = Virtual Private Network)
- ⇨ Elektronische Signatur

- ⇨ Protokollierung
- ⇨ Transportsicherung

5. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

Beispiel

- ⇨ Protokollierungs- und Protokollauswertungssysteme

6. Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Maßnahmen (technisch/organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

Beispiele

- ⇨ Eindeutige Vertragsgestaltung
- ⇨ Formalisierte Auftragserteilung (Auftragsformular)
- ⇨ Kriterien zur Auswahl des Auftragnehmers
- ⇨ Kontrolle der Vertragsausführung

7. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch/logisch):

Beispiele

- ⇨ Backup-Verfahren
- ⇨ Spiegeln von Festplatten, z.B. RAID-Verfahren
- ⇨ Unterbrechungsfreie Stromversorgung (USV)
- ⇨ Getrennte Aufbewahrung
- ⇨ Virenschutz/Firewall
- ⇨ Notfallplan

8. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

Beispiele

- ⇨ "Interne Mandantenfähigkeit"/Zweckbindung
- ⇨ Funktionstrennung (Produktion/Test)

A5. Musterformular: Dokumentation der Ergebnisse von Kontrollmaßnahmen

Hinweise: *Gem. § 11 Abs. 2 Satz 4 BDSG hat sich der Auftraggeber vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Nach Satz 5 der Vorschrift ist das Ergebnis zu dokumentieren.*

Das nachstehende Musterformular kann als Orientierungshilfe für eine ordnungsgemäße Dokumentation der Kontrollmaßnahme dienen. Selbstverständlich ist das Muster nach Maßgabe der Umstände des konkreten Einzelfalles anzupassen.

Hilfestellungen hinsichtlich der Ausfüllung des Formulars sind der Anleitung und den Hinweisen zu einzelnen Angaben auf den Seiten 18 ff. zu entnehmen.

Verteiler (Name, Abteilung)

Verfahrensverantwortliche/r	
Datenschutzbeauftragte/r Data Protection Officer	
CIO/GF der Organisationseinheit	
Prüfer/in	

1. Auftragsdaten

Verfahrensbezeichnung	
Kritikalität	
Verantwortliche Stelle	
Auftragnehmer (Hauptauftragnehmer)	
Unterauftragnehmer	
Art der Leistungen	
Vereinbarung zur Auftragsdatenverarbeitung	
Vertrag liegt vor bei	
Beginn der Leistung	
Ggf. Ende der Leistung	

2. Grunddaten der Kontrolle

Datum der Kontrolle	

Prüfer/in Name Organisationseinheit	
Erstkontrolle	

3. Art und Umfang der Kontrolle

☐ vor Ort (beim Auftragnehmer) ☐ schriftlich

☐ vollständig ☐ inkl. Recherchen

☐ ohne IT-Security-Maßnahmen ☐ Schwerpunktprüfung

Anmerkungen (z.B. Art der Recherchen, Schwerpunkte bzw. Begründung der Einschränkung des Kontrollumfangs):

4. Feststellungen

Vertragliche Anforderungen	☐ eingehalten	☐ nicht eingehalten[1]
Gesetzliche Anforderungen	☐ eingehalten	☐ nicht eingehalten[1]
Technisch-organisatorische Maßnahmen (Anlage zu § 9 BDSG)	☐ eingehalten	☐ nicht eingehalten[1]
Vertragsänderungen	☐ nicht erforderlich	☐ erforderlich[1]

[1]Soweit angekreuzt, sind hierzu weitere Angaben zum bestehenden Handlungsbedarf erforderlich:

5. Weitere Maßnahmen

Nachkontrolle erforderlich	☐ nein ☐ ja, am _____ (Datum)
Nächste Kontrolle	Zeitraum: Form:

Sonstige Bemerkungen

Als verantwortliche(r) Prüfer(in) bestätige ich die ordnungsgemäße Durchführung der Kontrolle und die Richtigkeit aller vorstehenden Angaben. Die detaillierten Aufzeichnungen zu meinen Überprüfungen und herangezogene Unterlagen

liegen bei mir/bei dem/der Verfahrensverantwortlichen (Nichtzutreffendes streichen) in geordneter Form zur Einsicht vor.

_____ _____

(Ort, Datum) (Unterschrift)

Anleitung

Vorbemerkung:

Im Rahmen der Änderung des Bundesdatenschutzgesetzes mit Wirkung ab 1. September 2009 hat der Gesetzgeber vorgeschrieben, dass Auftragnehmer (und deren Unterauftragnehmer) im Sinne von § 11 BDSG zu kontrollieren sind.

Diese Verpflichtung gab es im Prinzip auch schon zuvor, sie wurde in der Praxis aber nur unzureichend erfüllt. Nun wurden die Anforderungen konkretisiert; die Nichtvornahme bestimmter Kontrollen ist als Bußgeldtatbestand ausgestaltet worden.

§ 11 BDSG unterscheidet hinsichtlich der durchzuführenden Kontrollmaßnahmen zwischen einer sog. Erstkontrolle, welche vor Beginn der Datenverarbeitung durch den Dienstleister erfolgen muss, und weiteren regelmäßig durchzuführenden Kontrollen. Das Gesetz schreibt nicht vor, dass sich der Auftraggeber stets vor Ort von der Einhaltung aller gesetzlichen und vertraglichen Vorgaben überzeugen muss. Ebenso wenig gibt es einen festen zeitlichen Abstand hierfür. Vielmehr ist von der verantwortlichen Stelle eine angemessen sorgfältige Planung aufzustellen und abzuarbeiten. Diese Planung orientiert sich an Art und Umfang der Auftragsverarbeitung und an den denkbaren Gefährdungen für das Persönlichkeitsrecht der Betroffenen. Bei Auftragsdatenverarbeitungen, die einer hohen Kritikalitätsklasse zugeordnet werden müssen (s. dazu Nr. 1 Auftragsdaten) empfiehlt sich eine jährliche Überprüfung. (vgl. ausführlich Kapitel II Ziff. 4.3).

Verantwortlicher:

Verantwortlich für die Planung, Durchführung und Dokumentation der Kontrollen ist der Verfahrensverantwortliche, d.h. derjenige in einer Organisationseinheit, der die wesentlichen Entscheidungen über Art, Umfang und Zweck der Datenverarbeitung trifft und/oder die Daten für seine fachlichen Aufgaben verarbeiten lässt. Mit der tatsächlichen Durchführung der Kontrollen können auch qualifizierte Dritte beauftragt werden.

Dokumentation:

Die Form der Dokumentation ist vom Gesetz nicht im Einzelnen vorgegeben. Da die Dokumentation die ordnungsgemäße Durchführung der Kontrollen belegen soll und dem Nachweis auch gegenüber Aufsichtsbehörden dient, sollte im Ergebnis die („gewillkürte“) Schriftform sollte gewahrt werden. Ausgefüllte Dokumentationsbögen können auch eingescannt werden.

Aufbewahrungsdauer des Dokumentationsblattes:

Es wird empfohlen das Dokument der Erstprüfung und die weiteren Kontrolldokumente für die gesamte Dauer des Verfahrens aufzubewahren.

Hinweise zu einzelnen Angaben

Verteiler

Namentlich und mit Abteilungsbezeichnung anzugeben sind der Verfahrensverantwortliche, der zuständige Datenschutzbeauftragte/Data Protection Officer und der CIO/GF (Chief Information Officer oder Geschäftsführer) der das Verfahren betreibenden Einheit sowie der Prüfer (die Person, die die Kontrolle tatsächlich verantwortlich durchgeführt hat).

1. Auftragsdaten

Verfahrensbezeichnung ist die unternehmensinterne Bezeichnung des Verfahrens. Sofern es sich um andere Fälle der Kontrolle handelt (Kontrolle von Verarbeitungen ohne Zusammenhang zu einem IT-Verfahren) ist stattdessen eine aussagekräftige Beschreibung erforderlich.

Kritikalität bedeutet die Zuordnung der jeweiligen Auftragsdatenverarbeitung zu einer Risikoklasse. Dabei gilt:

Gering: personenbezogene Daten, keine besonderen personenbezogenen Daten gem. § 3 Nr. 9 BDSG enthalten, geringer Datenbestand, kurze Beauftragungszeit

Mittel: personenbezogene Daten, keine besonderen personenbezogenen Daten gem. § 3 Nr. 9 BDSG enthalten, längerfristige Beauftragung, Auftragsdatenverarbeitung unterstützt oder ist Teil wesentlicher Geschäftsprozesse

Hoch: personenbezogene Daten, besondere personenbezogene Daten gem. § 3 Nr. 9 BDSG enthalten, längerfristige Beauftragung, Auftragsdatenverarbeitung unterstützt oder ist Teil wesentlicher IT-Infrastrukturdienstleistungen oder Teil wesentlicher, für die Aufrechterhaltung des Geschäftsbetriebs notwendiger IT-Applikationen

Die Zuordnung zu einer Kritikalitätsklasse kann außerdem durch weitere, auch externe Faktoren (z.B. mögliche Beschwerdepotenziale, öffentliche Diskussionen über die Zuverlässigkeit des Dienstleisters) beeinflusst und verändert werden.

Verantwortliche Stelle ist die interne fachverantwortliche Stelle bei der X-AG/Tochter/Fremdunternehmen, die das Verfahren betreibt oder in deren Interesse der sonstige Auftrag erteilt worden ist. Das ist in der Regel nicht die IT-Organisation, sondern die Stelle, die die Daten für ihre Geschäftsprozesse benötigt.

Verfahrensverantwortlicher ist der bei der verantwortlichen Stelle persönlich für die wesentlichen Aspekte des Verfahrens/Auftrages zuständige Mitarbeiter, der auch im Verteiler angegeben ist.

Auftragnehmer ist das Unternehmen, das als Dienstleister Daten im Auftrag verarbeitet und daher zu kontrollieren ist. Anzugeben ist die gesamte Bezeichnung inkl. Rechtsform.

Sofern ein **Unterauftragnehmer** kontrolliert wird, ist dieser zusätzlich anzugeben.

Unter **Art der Leistungen** ist kurz zu beschreiben, welche Leistungen tatsächlich erbracht werden (z.B. Hosting, Druckdienste, Applikation Support, Datenbank-Administration …).

Bei **Vereinbarung zur Auftragsdatenverarbeitung** sollte eintragen werden, ob es sich um einen eigenständigen ADV-Vertrag i.S.d. Mustervereinbarung oder eine sonstige, ggf. in einen Dienstleistungsvertrag oder sonstigen Vertrag integrierte Vereinbarung handelt.

Bei **Vertrag liegt vor bei** sollen der Name des Betreffenden und die Organisationseinheit, bei der sich der Vertrag im Original befindet, angegeben werden.

Auch der **Beginn der Leistung** sollte vermerkt werden.

Falls das **Ende der Leistung** schon bekannt ist, z.B. bei einer befristeten Dienstleistung, sollte auch dieses angegeben werden.

2. Grunddaten der Kontrolle

Unter Nummer 2 ist die Kontrollmaßnahme zu bezeichnen; dazu ist das **Datum** der Kontrolle (bei mehrtägigen Kontrollen ggf. das Ende) anzugeben.

Der **Prüfer** ist namentlich und mit Organisationseinheit anzugeben.

Anzukreuzen ist zudem, ob es sich um die **erstmalige Kontrolle** vor dem Beginn der Verarbeitung handelt, die das Gesetz nun ausdrücklich vorsieht, oder um eine **weitere Kontrolle** während der Laufzeit des Vertrages (in diesem Fall ist auch anzugeben, wann die **letzte Kontrolle** vor der aktuellen Prüfung stattgefunden hat).

3. Art und Umfang der Kontrolle

Prüfungsmaßstab sind alle relevanten gesetzlichen und vertraglichen Anforderungen, ggf. in der Form wie sie in Berechtigungs-, Sicherungs-, Löschkonzepten und dgl. konkretisiert worden sind. Kontrollen beziehen sich dabei regelmäßig auf die allgemeine Umgebungssicherheit (z.B. physikalische Schutzmaßnahmen), systemübergreifende Schutzmaßnahmen (z.B. allgemeiner Zugriffsschutz) und applikations- bzw. anwendungsspezifische Schutzmaßnahmen.

Je kritischer ein Verfahren eingestuft ist, desto detaillierter sollte die Prüfung sein. Zunächst ist anzugeben, ob es sich um eine Kontrolle **vor Ort** beim Auftragnehmer handelt, oder ob die Maßnahme im Wesentlichen **schriftlich** (durch Auskünfte des Auftragnehmers, ggf. die Einsichtnahme in Unterlagen, Zertifikate, Audit-Berichte Dritter u.ä.) erfolgte. In einigen Fällen können auch **ergänzende Recherchen** im Internet und dgl. sinnvoll sein und zur Vervollständigung des Eindrucks beitragen, was ebenfalls anzugeben ist.

Die Kontrollen sind in der Regel auf alle wesentlichen Aspekte zu erstrecken (**vollständige Kontrolle**). Es kann aber auch - unter 3. zu dokumentierende - Gestaltungen geben, bei welchen z.B. **IT Security Maßnahmen außer Betracht** bleiben, z.B. wegen einer parallelen Prüfung durch Corporate Audit oder wegen aktueller Zertifizierungen Dritter, etwa entsprechend dem ISO 27001 ff. Standard.

Das Gleiche gilt für die gezielte Setzung von wechselnden **Schwerpunkten** bei relativ häufig geprüften, in sich sehr umfangreichen Verfahren.

Unter **Anmerkungen** sind besondere Einzelheiten (insb. Gründe für eingeschränkte Prüfungsumfänge) knapp zu beschreiben.

4. Feststellungen

Anzukreuzen ist jeweils, ob in der Gesamtbetrachtung nach Ende der Kontrolle alle vertraglichen und gesetzlichen Anforderungen eingehalten sind oder nicht bzw. ob als Ergebnis der Kontrolle ein Bedarf für Anpassungen/Veränderungen (Vertragsänderungen?) besteht. Soweit das der Fall ist (Nichteinhaltung bzw. Erforderlichkeit) sind kurze Angaben zum Handlungsbedarf einzutragen.

5. Weitere Maßnahmen

Hier ist anzugeben, ob im Fall von bestimmten Maßnahmen deren tatsächliche Umsetzung kurzfristig **nachgeprüft** werden muss und ggf. ist ein **Datum** hierfür anzugeben. In diesem Fall sollte die Nachkontrolle in gleicher Weise dokumentiert werden. Ansonsten ist nach Monat und Jahr anzugeben, wann die **nächste turnusmäßige Kontrolle** erfolgen sollte. Es kann auch eine Empfehlung zur **Form** abgegeben werden, also z.B. dass nach einer schriftlichen Kontrolle als nächstes eine Vor-Ort-Kontrolle sinnvoll erscheint.

6. Sonstiges

Das Original des Dokumentationsbogens hat der Verfahrensverantwortliche aufzubewahren. Er sollte grundsätzlich auch die detaillierten Aufzeichnungen zu der Überprüfung aufbewahren, z.B. umfassende Auditreports, Checklisten, herangezogene oder vom Auftragnehmer erhaltene Unterlagen etc.

A6. Template
Inspection of the Commissioned Data Processing - Documentation of the Inspection Measures
(Section 11 Bundesdatenschutzgesetz - BDSG (Federal Data Protection Act))

Notes: *According to Section 11(2) sentence 4 BDSG the controller shall verify compliance with the technical and organizational measures taken by the processor before data processing begins and regularly thereafter. The result shall be documented.*

The following template is intended for guidance. It should be amended to reflect the circumstances of any given case. Explanatory notes on how to fill out the form can be found on page 24.

Distributor (name, department)

Controller/internal unit	
Data Protection Officer	
CIO/MD of organizational unit	
Auditor	

1. Contract data

Process/Order description	
Criticality	
Controller	
Processor (main agent)	
Subcontractor (subagent)	
Type of services	
Controller-Processor Agreement for the commissioned data processing (CPA)	
CPA on file at	
Start date of services	
If applicable, end date of services	

2. Basic data of the inspection

Date of inspection	

Auditor Name Organizational unit	
First audit	☐ yes ☐ no, additional inspections Last inspection on (date)

3. Type and scope of the inspection

☐ *On-site (at the agent's site)* ☐ *in writing*

☐ *complete* ☐ *incl. research*

☐ *without IT security measures* ☐ *Focus of audit*

Comments (e.g., type of research, focus or reasons for a limited scope of the inspection):

4. Findings

Contractual requirements (CPA)	☐ met	☐ not met[1]
Legal requirements	☐ met	☐ not met[1]
Technical-organizational measures (attachment to Section 9 BDSG)	☐ met	☐ not met[1]
Changes to the Agreement (CPA)	☐ not required	☐ required[1]

[1]If checked, additional information is needed in regard to the existing need for action:

5. Additional measures

Subsequent inspection required	☐ no ☐ yes, on (date)
Next inspection	Period: Form:

Other comments

As the responsible auditor I confirm the proper execution of the inspection and the accuracy of all stated information. Detailed notes from my inspections and reviewed documents are on file with me/with the party responsible for the procedure *(Please strike what is not applicable)* in an organized form and are available for review.

_____ _____

(Location, date) (Signature)

Instruction

Preliminary remarks:

Due to a change of the Federal Data Protection Act effective as of September 1, 2009, the legislative body has stipulated that there must be inspections of processors (and their subcontractors) of commissioned data processing (Section 11 BDSG).

This obligation already existed previously, but in practice its fulfilment was rather insufficient. Now, the requirements have become more specific; the non-conducting of controls are met with a penalty element.

In regards to the inspection measures that must be executed, Section 11 BDSG differentiates between a so-called first inspection which must take place prior to the start of the data processing and additional inspections that are to be carried out on a regular basis. The law does not stipulate that the controller must always check the compliance with requirements stipulated in the agreement or the legislation on site. There is also no fixed time interval for this matter. Rather, the responsible party is to set up and follow an appropriate diligent schedule. This plan is based on the type and scope of the commissioned processing and the plausible risks for the personality rights of the data subjects. An annual inspection is recommended for commissioned data processing that must be associated with a high criticality classification (refer to Item 1 Contract data in this matter).

Controller/Responsible Party:

The party responsible for the planning, execution and documentation of the inspections is the party responsible for the procedure = controller (also referred to as "master of data/data owner"), which means the person in an organizational unit who makes the essential decisions with respect to type, scope and purpose of the data processing and/or who commissions data to be processed for his/her specialized tasks. The actual execution of inspections can also be assigned to qualified third parties.

Documentation:

The details of the form of the documentation are not stipulated by law. Since the documentation is to prove the proper execution of the inspections and is used as a proof toward supervisory boards, the result has to be in "arbitrary" written format. Completed documentation forms may also be scanned in.

Storage period of the documentation sheet:

We recommend a storage of the document of the first inspection for the entire duration of the procedure, which should also includes the documents of the review.

Notes for individual information

Distribution list

The *Controller/internal unit*, the Data Protection Officer and the CIO/MD (Chief Information Officer or Managing Director) as well as the Auditor (the person who is actually responsible for executing the inspection) must be listed by name together with the name of the department.

1. Contract data

Order description is the name of the procedure/order typically used within the company. To the extent that those are other inspection cases (processing inspection without a connection to an IT procedure) a meaningful description is required instead.

Criticality means the allocation of a risk classification to the respective commissioned data processing. The following shall apply in this context:

Low: Personal data, no special categories of personal data in accordance with Section 3 No. 9 BDSG included, low data inventory, short contract time

Medium: Personal data, no special categories of personal data in accordance with Section 3 No. 9 BDSG included, longer-term contract, commissioned data processing supports or is part of essential business processes

High: Personal data, special categories of personal data in accordance with Section 3 No. 9 BDSG included, longer-term contract, commissioned data processing supports or is a part of essential IT infrastructure services or is used for maintaining the business operation of essential/necessary IT applications.

The allocation to a criticality classification can also be impacted and changed by additional factors, including external factors (e.g., possible complaint potential, public discussions about the reliability of the service provider).

Controller is the internal unit responsible for this specialized area at the X-AG/subsidiary/third-party company, who operates the procedure **or** in whose interest the remaining contract has been issued. That is usually not the IT organization, but the unit that requires the data for its business processes. The controller is also named in the distribution list.

Processor (Main Agent) is the company who as a service provider processes the data on behalf of another party. The entire name including the legal form has to be listed.

In the event a **subcontractor** is made subject to an inspection, the subcontractor also has to be named.

A brief description is required under **type of services** to indicate which services are actually provided (e.g., hosting, printing services, application support, database administration ...).

Please enter for the controller-processor agreement concerning the commissioned data processing, whether it is an independent controller-processor agreement in the sense of a callable template agreement or an agreement that has been integrated in a service agreement or in an other agreement.

Under Agreement (CPA) **is available** please enter the name and the organizational unit that has the original agreement(CPA).

Please enter the **Start of the service**.

If the **End of the service** is already known, e.g., for a temporary service, please enter it here upon the start of the service.

2. Basic data of the inspection

The control measure is to be named under Item 2; for this, please enter the **Date** of the inspection (potentially the end for inspections that last multiple days).

The **auditor** is to be listed by name together with the organizational unit.

It needs to be indicated with a checkmark whether this is the **first inspection** prior to the beginning of the processing which is now explicitly called for by law, or whether it is an **additional inspection** during the term of the contract (in this case it also needs to be stated, when the **last inspection** prior to the current inspection has taken place).

3. Type and scope of the inspection

Inspection criteria are all relevant legal and contractual requirements, potentially in the form as they have been specified in authorization, security, and erasure concepts and similar. Inspections respectively relate regularly to the general security of the environment (e.g., physical security measures), cross-system protective measures (e.g., general access protection) and application-specific protection measures).

The level of details of the inspection should increase with the level of criticality of the procedure. First of all, it needs to be stated whether it is an **On-site** inspection with the processor or whether the measure mostly took place **in writing** (through information provided by the processor, potentially the review of documentation, certificates, inspection reports of third parties and similar). In some cases, **complementary research** on the Internet and such may be sensible and may contribute to the completeness of the impression, which is also to the indicated.

The inspections usually shall cover all essential aspects (**complete inspection**). However, there may also be cases - to be documented under Item 3 - for which for example **IT security measures are not taken into consideration**, e.g., due to the simultaneous inspection through Corporate Audit or due to current third-party certifications, e.g. corresponding with ISO 27001 ff. standard.

The same applies for the targeted identification of changing focus of audit for in and by themselves very extensive procedures that are inspected on a relatively frequent basis.

Individual facts (especially reason for limited scopes of inspection) must be described briefly under **Comments**.

4. Findings

Please check respectively whether or not all contractual and legal requirements have been maintained overall or whether the result of the inspection indicates a need for adjustments/changes. To the extent that this is the case (non-compliance or requirements) brief comments regarding the need for action have to be entered.

5. Additional measures

Here, it needs to be stated whether the actual implementation of specific measures must be **reviewed** in the near future and if necessary, a respective **Date** needs to be entered. In this case, the subsequent inspection should be documented in the same manner. Otherwise, state the month and the year when the **next cyclical inspection** should take place. There can also be a recommendation concerning the **Format**, e.g., that after a written inspection the next inspection should be an on-site inspection for good measure.

6. Miscellaneous

The party responsible for the procedure has to keep the original documentation sheet on file. As a matter of principle, this person should also keep the detailed notes for the inspection on file, e.g., extensive audit reports, checklists, documentation that was utilized or received from the contractor etc.

A7. Muster: Auftrag gemäß § 11 BDSG zur Vernichtung von Datenträgern nach DIN 66399:2012

Hinweise: *Der nachstehende Mustertext soll eine Orientierungshilfe für den Einzelfall der Vernichtung von Datenträgern nach DIN 66399:2012 bieten. Erfolgt eine Auftragsvergabe zur Vernichtung von Datenträgern unabhängig von den Spezifikationen der DIN 66399:2012, ist der Vertragstext nach den Umständen des konkreten Einzelfalls anzupassen.*

Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sind anzukreuzen. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen.

Auftragsdatenverarbeitung

(Übernahme und Vernichtung von Datenträgern)

zwischen der/dem

_____

- nachstehend Auftraggeber genannt -

und der/dem

_____

- nachstehend Auftragnehmer genannt -

§ 1 Präambel

Diese Vereinbarung (Auftrag im Sinne des § 11 BDSG) zur Verarbeitung personenbezogener Daten (nachfolgend auch „Daten“) im Auftrag nebst ihren Anlagen konkretisiert die zwischen den Parteien bestehende Leistungsvereinbarung:

§ 2 Gegenstand des Vertrages

(1) Der Vertrag regelt die Übernahme und Vernichtung von Datenträgern nach DIN 66399:2012. Der Auftragnehmer verpflichtet sich zur ordnungsgemäßen Übernahme und Vernichtung der Datenträger nach den Weisungen des Auftraggebers.

(2) Vertraulichkeitsgrad[2] und Menge der zu vernichtenden Datenträger, Abholungszeit und -ort werden im Leistungsvertrag _____ vom _____ geregelt.

Angabe der Datenarten und deren Schutzbedarf:

☐ Interne Daten

(normaler Schutzbedarf, Schutzklasse 1)

☐ Nicht allgemein zugängliche personenbezogene und vertrauliche Daten

(hoher Schutzbedarf, Schutzklasse 2)

☐ Geheime Daten

(sehr hoher Schutzbedarf, Schutzklasse 3)

[2] Angabe der Sicherheitsstufe nach DIN 66399-1.

z.B. besondere Arten von Daten nach § 3 Abs. 9 BDSG bzw. § 203 StGB,

(Zutreffendes bitte ankreuzen)

(3) Nach § 11 Abs.2 S.1 Nr.2 BDSG umfasst der Kreis der etwaig Betroffenen folgende Personenkategorien:

- ☐ Kunden
- ☐ Beschäftigte i.S. § 3 Abs. 11 BDSG
- ☐ Lieferanten
- ☐ Berater/Handelsvertreter
- ☐ Ansprechpartner
- ☐ Geschäftspartner
- ☐ Interessent
- ☐ _____
- ☐ _____

(Zutreffendes bitte ankreuzen/ergänzen)

§ 3 Übernahme der Datenträger

Die Abholung erfolgt nach vorheriger Terminvereinbarung. Der Auftragnehmer darf grundsätzlich nur so viele Datenträger abholen, die am gleichen Tag restlos vernichtet werden können. Sollten Störungen im Prozessablauf auftreten und eine taggleiche Vernichtung nicht möglich sein, so sind die unter § 5 Abs. 1 festgelegten Sicherungsmaßnahmen einzuhalten. Der zur Übernahme der Datenträger berechtigte Beauftragte des Auftragnehmers übergibt als Berechtigungsnachweis ein vorgefertigtes Übernahmeprotokoll nach Angaben aus der jeweils gültigen Norm (DIN 66399:2012). Das Übernahmeprotokoll wird von den befugten Mitarbeitern der Vertragspartner abgezeichnet.

§ 4 Transport

Der Transport der Datenträger darf nur in ge- und verschlossenen Fahrzeugen des Auftragnehmers und/oder Sicherheitsbehältnissen mit vom Auftragnehmer verpflichtetem Personal durchgeführt werden. Dabei muss sichergestellt sein, dass keine Datenträger verloren gehen oder entnommen werden können. Dies geschieht durch eine Begleitprotokollierung des Auftragnehmers.

§ 5 Vernichtung

(1) Die übernommenen Datenträger sind vom Auftragnehmer am Tag der Abholung zu vernichten. Nur in Ausnahmefällen (Kapazitäts- oder Personalengpässe, Ausfall der Vernichtungsanlage) dürfen die Datenträger über Nacht zwischengelagert werden. Die Lagerung (bis zur Vernichtung) und Entleerung der Sicherheitsbehälter findet ausschließlich innerhalb eines geschlossenen und überwachten Bereichs statt. Dabei muss sichergestellt werden, dass Unbefugte keinen Zutritt haben und die Datenträger nicht mit denen anderer Auftraggeber vermischt werden. Die Art und Weise der Vernichtung richtet sich nach der Art, der Vertraulichkeit und Beschaffenheit der Datenträger nach dem jeweiligen Stand der Technik unter Beachtung der jeweils gültigen Normen (DIN 66399:2012). Der Auftragnehmer sichert die Vernichtung gem. der in der Leistungsvereinbarung angegebenen Sicherheitsstufe mit anschließender Verwirbelung und Verpressung (soweit dies nach der DIN 66399 noch zulässig ist) zu.

(2) Ein Nachweis, das geeignete Maschinen zur Vernichtung nach der jeweils gültigen Norm (DIN 66399:2012) verwendet werden, wird vom Auftragnehmer erbracht und dokumentiert. Der Auftragnehmer hat über die Vernichtung der Datenträger ein schriftliches Vernichtungsprotokoll nach Angaben aus der jeweils gültigen Norm (DIN 66399:2012) abzugeben.

§ 6 Sorgfaltspflichten des Auftraggebers

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

(2) Sabotage oder Manipulation an den (Sicherheits-) Behältern während der Standzeit beim Auftraggeber sind durch entsprechende organisatorische bzw. sonstige Sicherungsmaßnahmen zu verhindern. Die Anfertigung von Kopien überlassener Schlüssel von Sicherheitsbehältern, z.B. zur Mehrfachbenutzung, ist nicht gestattet. Die Vergabe von Schlüsseln ist zu dokumentieren. Der Verlust eines Schlüssels ist dem Auftragnehmer unverzüglich schriftlich anzuzeigen.

(3) Schäden oder sonstige Veränderungen an den Behältern sind dem Auftragnehmer unverzüglich schriftlich anzuzeigen.

(4) Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, falls ihm Umstände bekannt werden, die eine ordnungsgemäße und sichere Vernichtung irgendwie beeinträchtigen könnten. Dem Auftraggeber obliegt die Verhinderung und sofortige Beseitigung solcher Umstände, soweit sie seinem Einfluss- bzw. Verantwortungsbereich zuzuordnen sind.

§ 7 Sorgfaltspflichten des Auftragnehmers

(1) Der Auftragnehmer sichert zu, beim Transport und bei der Vernichtung der Datenträger nur eigenes Personal einzusetzen, das nach § 5 BDSG auf das Datengeheimnis verpflichtet worden ist. Er untersagt den in seinem Betrieb beschäftigten Personen jedes Beiseiteschaffen von Datenträgern sowie eine Einsichtnahme in diese und überwacht die Einhaltung dieser Anordnung.

(2) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nicht erteilen. Etwaige Auskunftsersuchen sind unverzüglich dem Auftraggeber zu melden.

(3) Beim Auftragnehmer ist als Beauftragter für den Datenschutz Herr/Frau _____ bestellt.

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

§ 8 Verfügungsgewalt

(1) Der Auftragnehmer erwirbt keine Rechte an den in seinen Besitz gelangten Datenträgern und den darauf verzeichneten Daten, schriftlichen oder bildlichen Darstellungen. Die Einsichtnahme in die Datenträger sowie deren Weitergabe oder sonstige Verwendung durch den Auftragnehmer ist untersagt (soweit dies durch die DIN 66399:2012 gefordert wird).

(2) Das durch die Vernichtung gewonnene Abfallgut geht in das Eigentum des Auftragnehmers über.

§ 9 Kontrolle

Der Auftraggeber ist berechtigt, den Transport und die Vernichtung der Datenträger zu überwachen. Der Auftragnehmer verpflichtet sich, die Anwesenheit von Beauftragten des Auftraggebers bei allen mit dem Transport und der Vernichtung zusammenhängenden Dienstleistungen und in allen dabei benutzten Räumen, Fahrzeugen und Betriebseinrichtungen zu dulden. Er gestaltet den Betriebsablauf so, dass die Überwachung durch den Beauftragten des Auftraggebers jederzeit gewährleistet ist. Der Auftragnehmer verpflichtet sich, die von der zuständigen Aufsichtsbehörde bei einer möglichen Überprüfung festgestellten Mängel unverzüglich abzustellen, den Auftraggeber über die Überprüfung zu unterrichten und ihm Einsicht in die Prüfberichte der Aufsichtsbehörde zu gewähren. Sollte der konkrete Auftrag von den festgestellten Mängeln betroffen sein, so ist die für den Auftraggeber zuständige Aufsichtsbehörde mit in den Prozess einzubeziehen.

Werden im Vernichtungsprozess datenschutzrechtliche Verstöße festgestellt (Datenmaterial gelangt in fremde Hände bzw. wird vertragswidrig verwendet), so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren, damit dieser ggf. im Sinne des § 42a BDSG tätig werden kann.

§ 10 Maßnahmen bei Funktionsstörungen

(1) Der Auftragnehmer verpflichtet sich, geeignete Maßnahmen für den Fall von schwerwiegenden Funktionsstörungen in seinem Betriebsablauf zu treffen, um zu verhindern, dass auf die zur Vernichtung vorgesehenen Datenträger unbefugt zugegriffen wird. Der Auftraggeber ist über solche schwerwiegende Funktionsstörungen unverzüglich zu verständigen.

(2) Ansprechpartner für Meldungen von Unregelmäßigkeiten bei der Abwicklung von Arbeiten sowie für die Erteilung und Entgegennahme von weiteren Weisungen des Auftraggebers über Art, Umfang und Verfahren der Datenträgervernichtung sind:

für den Auftraggeber

für den Auftragnehmer

(3) Änderungen in der Person der Ansprechpartner teilen sich die Vertragspartner unverzüglich schriftlich mit. Weitere Weisungen des Auftraggebers bedürfen ebenfalls der Schriftform.

§ 11 Technisch-organisatorische Maßnahmen nach § 9 BDSG nebst Anlage

(1) Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen gem. § 11 Abs. 2 i.V.m. § 9 BDSG zu. Diese ergeben sich im Einzelnen aus der zur Zeit gültigen Norm DIN 66399-3, Tabelle 1, 3, 4 und 5.

(2) Die Einhaltung der technischen und organisatorischen Maßnahmen wird im Rahmen von externen Audits, die von unabhängigen fachkundigen Stellen durchgeführt werden, zertifiziert. Der Auftragnehmer stellt dem Auftraggeber vor Beginn der Beauftragung und sodann in regelmäßigen zeitlichen Abständen, die gemeinsam festzulegen sind, einen entsprechenden Nachweis in Form eines Zertifikates zur Verfügung.

§ 12 Subunternehmen

(1) Die Einschaltung von Subunternehmern ist grundsätzlich ausgeschlossen. Abweichungen von dieser Regelung bedürfen der vorherigen schriftlichen Einwilligung durch den Auftraggeber.

(2) Der Auftragnehmer wird vertraglich sicherstellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmen gelten.

§ 13 Vertragsdauer

Die Vertragsdauer richtet sich nach den Angaben in der Leistungsvereinbarung.

§ 14 Gerichtsstand

Es gilt deutsches Recht. Gerichtsstand ist _____.

§ 15 Sonstiges

(1) Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen der Vereinbarung nicht. Beide Seiten sind in diesem Fall verpflichtet, unverzüglich in eine nachträgliche Zusatzbestimmung einzuwilligen, die nach Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.

(2) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch eine Insolvenz- oder Vergleichsverfahren oder sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

_____ _____

(Unterschrift Auftraggeber) (Unterschrift Auftragnehmer)

_____

(Ort, Datum)

A8. Muster zur Funktionsübertragung

***Hinweise**: Eine gesetzliche Pflicht zum Abschluss einer schriftlichen Vereinbarung besteht im Rahmen der Funktionsübertragung nicht. Allerdings ist es auf Grund haftungsrechtlicher Überlegungen und zum Schutz von Betroffenen im Einzelfall sinnvoll, die in § 11 BDSG aufgeführten Kriterien auch bei der Funktionsübertragung als Maßstab für die Auswahl des Outsourcingnehmers und die Vertragsgestaltung anzuwenden. Der nachstehende Mustertext soll hierbei eine Orientierungshilfe bieten. Er ist je nach den Umständen des konkreten Einzelfalls anzupassen. Bei komplexen Outsourcingverhältnissen oder der Übermittlung sensibler personenbezogener Daten können weitere bzw. ergänzende Vertragsklauseln notwendig sein.*

Vereinbarung zur Funktionsübertragung

zwischen dem/der

_____

- nachstehend Outsourcingnehmer genannt -

und dem/der

_____

- nachstehend Outsourcinggeber genannt -

1. Gegenstand und Dauer der Funktionsübertragung

Gegenstand der Funktionsübertragung

☐ Der Gegenstand der Funktionsübertragung ergibt sich aus der Leistungsvereinbarung/SLA/_____ vom _____, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand der Funktionsübertragung zum Datenumgang ist die Durchführung folgender Tätigkeiten durch den Outsourcingnehmer:

_____ (Definition der Tätigkeiten)

Dauer der Funktionsübertragung

☐ Die Dauer dieser Funktionsübertragung (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Die Funktionsübertragung vollzieht sich im Rahmen einer einmaligen Ausführung.

oder

☐ Die Dauer dieser Funktionsübertragung (Laufzeit) ist befristet bis zum _____.

oder

☐ Die Funktionsübertragung ist unbefristet und kann von beiden Parteien mit einer Frist von _____. zum _____ gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung der Inhalte der Funktionsübertragung

Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

☐ Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Outsourcingnehmer für den Outsourcinggeber sind konkret beschrieben in der Leistungsvereinbarung vom _____.

oder

☐ Nähere Beschreibung des Gegenstands der Funktionsübertragung im Hinblick auf Umfang, Art und Zweck der Aufgaben des Outsourcingnehmers: _____.

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Outsourcinggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der §§ 4b, 4c BDSG erfüllt sind.

Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter _____.

oder

☐ Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ _____

Kreis der Betroffenen

☐ Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieser Funktionsübertragung Betroffenen ist in der Leistungsvereinbarung konkret beschrieben unter _____.

oder

☐ Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieser Funktionsübertragung Betroffenen umfasst (Aufzählung/Beschreibung der betroffenen Personenkategorien)

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte i.S.d. § 3 Abs. 11 BDSG
- ☐ Lieferanten

☐ Handelsvertreter

☐ Ansprechpartner

☐ _____

3. Verantwortlichkeiten

Der Outsourcingnehmer ist in seinem Verantwortungsbereich verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Outsourcingverhältnisses durchgeführten Verarbeitung und Nutzung personenbezogener Daten, die ihm zur Vertragserfüllung durch den Outsourcinggeber zur Verfügung gestellt werden, so im Hinblick auf die Regelungen des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz.

Er hat in eigener Verantwortung die formalen Datenschutzvorschriften (z.B. Bestellung eines betrieblichen Datenschutzbeauftragten, Führung von Dokumentationen) und die Rechte der Betroffenen (z.B. Benachrichtigung über die Speicherung, Auskunftserteilung) wahrzunehmen.

4. Zweckbindung

Die personenbezogenen Daten, die der Outsourcingnehmer vom Outsourcinggeber zur Erfüllung der vertraglichen Verpflichtungen erhält, dürfen gem. § 28 Abs. 5 BDSG nur zu diesen Zwecken verarbeitet oder genutzt werden.

Eine Zweckänderung gem. § 28 Abs. 1 BDSG für Zwecke, die außerhalb dieser Vereinbarung liegen, ist ausgeschlossen.

Zur Durchführung des Vertragsgegenstandes ist der Outsourcingnehmer zur Durchführung aller technisch erforderlichen Verarbeitungen und Nutzungen der Daten (z.B. Duplizieren von Beständen für die Verlustsicherung, Anlegen von Logdateien, Zwischendateien und Arbeitsbereichen etc.), soweit die Verarbeitung nicht zu einer inhaltlichen Umgestaltung führt, berechtigt. Darüber hinaus ist er zur Bereinigung von technisch bedingten Fehlern berechtigt, über die er den Outsourcinggeber umgehend entsprechend zu informieren hat.

Sofern der Outsourcinggeber besondere - über diese vertraglichen Vereinbarungen hinausgehende - Anforderungen bei der technisch bedingten Verarbeitung stellt, sind diese gesondert schriftlich zu vereinbaren und mit den bereits vorhandenen Vereinbarungen abzustimmen.

5. Hinweispflichten

Bei Störungen, Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten des Outsourcinggebers ist dieser unverzüglich zu informieren.

Der Outsourcinggeber seinerseits hat bei der Feststellung von Fehlern oder Unregelmäßigkeiten, die er insbesondere bei der Prüfung von Ergebnissen feststellt, unverzüglich den Outsourcingnehmer zu informieren.

Werden bei einer Untersuchung dieser Vorfälle Störungen festgestellt, die zu Änderungen des Verfahrensablaufes führen, ist die entsprechende Verfahrensänderung vor ihrer Durchführung mit dem Outsourcinggeber abzustimmen. Sie darf nicht ohne dessen schriftlicher Einwilligung vollzogen werden.

6. Geheimhaltungspflichten

Der Outsourcingnehmer ist verpflichtet, bei der Verarbeitung der personenbezogenen Daten, die ihm durch den Outsourcinggeber zur Verfügung gestellt werden, das Datengeheimnis gem. § 5 BDSG zu wahren.

Er hat hierzu bei der Verarbeitung und Nutzung ausschließlich Beschäftigte einzusetzen, die auf das Datengeheimnis verpflichtet sind. Er hat insbesondere mit der gebotenen Sorgfalt darauf hinzuwirken, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung dieses Vertrages betraut sind, die gesetzlichen Bestimmungen über den Datenschutz beachten und die aus dem Bereich des Outsourcinggebers erlangten Informationen nicht an Dritte weitergeben oder sonst verwerten.

Beide Parteien verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebs- und Geschäftsgeheimnissen vertraulich zu behandeln.

7. Datenschutzbeauftragter

Der Outsourcingnehmer hat - soweit gesetzlich vorgeschrieben - einen Datenschutzbeauftragten bestellt, der seine Tätigkeit gem. §§ 4f, 4g BDSG ausüben kann. Dessen Kontaktdaten werden dem Outsourcinggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt.

8. Rechte der Betroffenen

Die Rechte der durch die Datenverarbeitung beim Outsourcingnehmer betroffenen Personen sind ihm gegenüber geltend zu machen. Er ist verantwortlich für die Wahrung dieser Rechte.

9. Technische und organisatorische Maßnahmen

Die im Anhang beschriebenen technischen und organisatorischen Maßnahmen werden zwischen Outsourcinggeber und Outsourcingnehmer als verbindlich festgelegt.

Insgesamt handelt es sich bei den zu treffenden Maßnahmen einerseits um allgemeine Maßnahmen hinsichtlich der erforderlichen technischen und organisatorischen Maßnahmen gem. § 9 BDSG und Anlage, sowie andererseits um spezifische Maßnahmen zur Bewältigung der Funktionsübertragung, insbesondere im Hinblick auf die Art des Datenaustauschs/Bereitstellung von Daten, Art/Umstände der Verarbeitung/der Datenhaltung sowie Art/Umstände beim Output/Datenversand.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Outsourcingnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

10. Prüfungsrechte des Outsourcinggebers

Der Outsourcinggeber hat das Recht, die Kontrolle der Einhaltung der vertraglich vereinbarten Datenschutz- und Datensicherungsmaßnahmen bezüglich der im Rahmen des Outsourcingvertrages überlassenen personenbezogenen Daten im Benehmen mit dem Outsourcingnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Outsourcingnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Outsourcingnehmer verpflichtet sich, dem Outsourcinggeber auf Anforderung die erforderlichen Auskünfte zu geben und Nachweise zu führen.

11. Unterauftragsverhältnisse

Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Outsourcinggebers gestattet.

Der Outsourcingnehmer hat die vertraglichen Vereinbarungen mit dem/den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Outsourcinggeber und Outsourcingnehmer entsprechen.

Bei der Unterbeauftragung sind dem Outsourcinggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Outsourcinggebers, vom Outsourcingnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Outsourcingnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Aufgabenwahrnehmung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Outsourcingnehmer sorgt nichtsdestoweniger zur Gewährleistung des Schutzes und der Sicherheit der Daten des Outsourcinggebers auch bei fremd vergebenen Nebenleistungen für den Abschluss angemessener und gesetzeskonformer vertraglicher Vereinbarungen sowie der Gewährung von Kontrollmaßnahmen.[3]

[3] Die im vorstehenden Absatz getroffene Regelung kann seitens des Outsourcinggebers im Zuge einer Risikoabwägung optional getroffen werden. Sie erlaubt dem Outsourcingnehmer im Falle unterstützender Nebenleistungen durch Dritte die Ausgestaltung der datenschutzrechtlichen Vertragsbeziehung mit Dritten ohne Zustimmungserfordernis des Outsourcinggebers.

12. Nachvertragliche Pflichten

Nach Abschluss der vertraglichen Arbeiten oder zuvor nach Aufforderung durch den Outsourcinggeber - spätestens mit Beendigung der Leistungsvereinbarung - hat der Outsourcingnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Funktionsübertragung stehen, dem Outsourcinggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Outsourcingnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Outsourcinggeber übergeben.

13. Datenschutzrechtliche Haftung

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem Bundesdatenschutzgesetz oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen des Outsourcingverhältnisses im Verantwortungsbereich des Outsourcingnehmers erleidet, ist dieser gegenüber dem Betroffenen verantwortlich.

A9. Muster zur Fernwartung nach § 11 Abs. 5 BDSG

Hinweise: *Dieser Mustervertrag wurde in starker Anlehnung an eine entsprechende Ausarbeitung des Hessischen Datenschutzbeauftragten vom 3. November 2003 erstellt. Er übernimmt die Methodik des Hessischen Datenschutzbeauftragten und wesentliche Inhalte. Gleichzeitig ist eine Anpassung und Ergänzung auf Basis der „Novelle II“ des Bundesdatenschutzgesetzes vorgenommen worden. Diese Mustervereinbarung ist vorrangig für den nicht öffentlichen Bereich relevant. Grundsätzlich kann sie jedoch auch im öffentlichen Bereich des Bundes und mit Anpassungen auch der Länder verwendet werden. Der Mustervertrag für die Fernwartung gem. § 11 Abs. 5 BDSG ist im Einzelfall aufgabenspezifisch anzupassen. Soweit spezialgesetzliche Regelungen für die Daten, die im Auftrag verarbeitet werden sollen, Anwendung finden, ist zunächst zu prüfen, ob eine Auftragsdatenverarbeitung überhaupt zulässig ist (z.B. Regelungen über Berufs- oder besondere Amtsgeheimnisse).*

Vereinbarung

zwischen dem/der

_____

- nachstehend Auftragnehmer genannt -

und dem/der

_____

- nachstehend Auftraggeber genannt -

§ 1 Gegenstand der Vereinbarung

Diese Vereinbarung umfasst folgende, vom Auftragnehmer durchzuführende Fernwartungsarbeiten:

Hardware-Diagnose: für folgende(s) Hardwareprodukt(e)

Software-Wartung: für folgende(s) Softwareprodukt(e)

Hinweis:

Hier sind Art und Umfang der durchzuführenden Fernwartungsarbeiten, die davon betroffenen EDV-Systeme und ggf. einsehbare Datenkategorien sowie der Kreis der Betroffenen genau zu beschreiben. Bspw. könnte eine Hardware-Fehlerdiagnose zur Vorbereitung einer Wartung erfolgen oder die Wartung einer Anwendungssoftware.

Beispiel Software-Wartung:

Behebung von Fehlerzuständen in der Anwendung _____ in der Abteilung _____.

Damit verbunden sind folgende Zugriffe:

Schreibender Zugriff auf die Konfigurationsdateien _____ der Anwendung _____.

Lesender Zugriff auf die anderen Dateien im Programmverzeichnis _____ der Anwendung _____.

Lesender Zugriff auf Kundendaten (Name, Vorname, Anschrift, E-Mail-Adresse, Kreditkartendaten) in den Verzeichnissen _____.

Ein Zugriff auf die Personaldatei wird soweit erforderlich nach Rücksprache ermöglicht.

§ 2 Verfahrensregelungen

(1) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind schriftlich zu vereinbaren.

(2) Mitteilungen der Vertragsparteien über E-Mail oder Internet werden nur akzeptiert, wenn das Schriftstück verschlüsselt übertragen wurde und mit einer digitalen Signatur versehen worden ist.

§ 3 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Fernwartung sowie für die Wahrung der Rechte der Betroffenen bleibt der Auftraggeber verantwortlich.

(2) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Ablauf der Fernwartung zu erteilen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

Weisungsberechtigte Personen des Auftraggebers sind:

_____

Weisungsempfänger beim Auftragnehmer sind:

_____

Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners wird dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitgeteilt.

(3) Im System des Auftraggebers werden alle Zugriffe, die für Wartungsarbeiten erfolgen, protokolliert. Die Protokollierung muss so erfolgen, dass sie in einer Revision nachvollzogen werden kann. Die Protokollierung darf vom Auftragnehmer nicht abgeschaltet werden.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten feststellt, die bei der Fernwartung aufgetreten sind oder die einen Zugriff durch Unbefugte möglich machen.

(5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer führt die Fernwartung ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Er verwendet Daten, die ihm im Rahmen der Erfüllung dieses Vertrags bekannt geworden sind, nur für Zwecke der Fernwartung. Kopien, Dumps, Traces oder Debugger-Protokolle werden ohne Wissen des Auftraggebers nicht erstellt. Soweit möglich, erfolgt die Fernwartung am Bildschirm ohne gleichzeitige Speicherung.

(2) Der Auftragnehmer führt seinerseits regelmäßig Kontrollen zur vertragsgerechten Erfüllung seiner Aufgaben durch.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er Sachverhalte oder Unregelmäßigkeiten feststellt, die gegen das BDSG oder andere Vorschriften über den Datenschutz verstoßen insbesondere solche, die einen Zugriff durch Unbefugte möglich machen.

(4) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen.

(5) Der Auftragnehmer sichert die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden.

(6) Notwendige Datenübertragungen zu Zwecken der Fernwartung müssen in hinreichend verschlüsselter Form erfolgen; Ausnahmen sind besonders zu begründen.

(7) Der Auftragnehmer teilt dem Auftraggeber vor Beginn der Fernwartung schriftlich oder in der Form des § 2 Abs. 2 mit, welche Mitarbeiter er dafür einsetzen wird und wie diese Mitarbeiter sich identifizieren werden. Die Mitarbeiter des Auftragnehmers verwenden hinreichend sichere Identifizierungsverfahren.

(8) Der Beginn der Fernwartung ist telefonisch anzukündigen, um den Beauftragten des Auftraggebers die Möglichkeit zu geben, die Maßnahmen der Fernwartung zu verfolgen.

(9) Fernwartungen dürfen nur von der Wartungszentrale aus vorgenommen werden, deren Sicherheitsmaßnahmen in § 7 Abs. 1 vereinbart worden sind.

(10) Der Auftragnehmer erkennt an, dass der Auftraggeber jederzeit berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften. Ergeben sich Zweifel, so gestattet der Auftragnehmer die Begehung der Räume, von denen aus die Fernwartung durchgeführt wird.

(11) Die Fernwartung von Privatwohnungen aus ist nicht gestattet. Soll im Einzelfall davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers. In diesem Fall ist der Zutritt zur Wohnung durch den Auftraggeber vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

(12) Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial sind unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen.

(13) Nicht mehr benötigte Unterlagen und Dateien dürfen erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet werden.

Hinweis:

Für Beweissicherung, Auskunftsansprüche oder die Revision relevant

(14) Die Einschaltung von Subauftragnehmern ist ausgeschlossen. Soll im Einzelfall davon abgewichen werden, bedarf dies der gesonderten schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer hat in diesem Falle vertraglich sicher zu stellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 5 BDSG erfüllt hat.

(15) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen.

(16) Der Auftraggeber hat das Recht, die Fernwartung zu unterbrechen, insbesondere wenn er den Eindruck gewinnt, dass unbefugt auf Dateien zugegriffen wird. Die Unterbrechung kann erfolgen, wenn eine Fernwartung mit nicht vereinbarten Hard- und Softwarekomponenten festgestellt wird.

§ 5 Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, das Datengeheimnis zu wahren und die im Rahmen dieses Vertrages tätig werdenden Mitarbeiter auf das Datengeheimnis gem. § 5 BDSG schriftlich zu verpflichten. Er verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften; im Fall des § 4 Abs. 13 gilt das auch gegenüber dem Subunternehmer.

(3) Der Auftragnehmer hat Betroffenenwünsche (Auskunft, Berichtigung, Löschung, Sperrung) immer an den Auftraggeber weiterzuleiten. Auskünfte an Dritte darf der Auftragnehmer nicht erteilen, Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen (§ 3 Abs. 2) erteilen.

§ 6 Kontrollrechte der Aufsichtsbehörden

(1) Der Auftragnehmer verpflichtet sich, der für den Auftraggeber zuständigen Kontrollbehörde insbesondere den von dieser eingesetzten Bediensteten Zutritt zu den Arbeitsräumen zu gewähren und unterwirft sich der Kontrolle nach Maßgabe des § 38 BDSG in seiner jeweiligen Fassung.

(2) Soweit Daten in einer Privatwohnung verarbeitet werden, ist das Zugangsrecht für die Mitarbeiter der Aufsichtsbehörde und der von ihr eingesetzten Bediensteten vorher mit dem Auftragnehmer abzustimmen. Der Auftragnehmer stellt sicher, dass die anderen Bewohner dieser Privatwohnung mit dieser Regelung einverstanden sind.

Hinweis:

Bei öffentlichen Auftraggebern ist dieser Paragraf entsprechend des gültigen Bundes- oder Landesdatenschutzgesetzes zu modifizieren.

§ 7 Datensicherungsmaßnahmen

(1) Um die Übertragung der Daten abzusichern und unbefugten Zugang auf die Rechner des Auftraggebers im Rahmen der Fernwartung zu verhindern, legt der Auftraggeber folgende technische und organisatorische Maßnahmen für beide Seiten verbindlich fest:

a) Organisationskontrolle

Maßnahmen, damit die innerbetriebliche (oder innerbehördliche) Organisation den besonderen Anforderungen des Datenschutzes gerecht wird:

_____

Hinweis :

Hier können Schulungsmaßnahmen und die Revision des Verfahrens der Fernwartung festgelegt werden. Vor allem ist die Dokumentation aller wesentlichen Verarbeitungsschritte sowie der zur Fernwartung eingesetzten Hard- und Software zu vereinbaren, damit die Überprüfbarkeit möglich ist.

Die Protokollierung ist hier vor allem als Maßnahme zu nennen. Um die Daten mit einem vertretbaren Aufwand auswerten zu können, müssen in der Regel Tools vorhanden sein.

Beispiele:

Die Bildschirmanzeige des Wartungspersonals wird auf einer Konsole beim Auftraggeber gespiegelt.

Die übertragenen Daten werden protokolliert.

b) Zutrittskontrolle

Maßnahmen, damit Unbefugte keinen Zutritt zu den Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden:

_____

Hinweis:

In den meisten Fällen werden im Zusammenhang mit der Fernwartung keine Maßnahmen zur Zutrittskontrolle getroffen. Es ist aber denkbar, dass der Auftragnehmer die Hardwarekomponenten (Server, Router etc.) installiert und betreut. In diesem Fall sollten hier die Maßnahmen beschrieben werden, wann Wartungspersonal wie Zutritt zur Hardware erhält.

c) Zugangskontrolle

Maßnahmen, damit Unbefugte an der Benutzung der Datenverarbeitungssysteme gehindert werden:

_____

Hinweis:

Hier sind insbesondere die Maßnahmen festzulegen, mit denen sichergestellt wird, dass die Fernwartung nur mit Wissen und Willen des Auftraggebers stattfindet und die Identität des Wartungspersonals festgestellt wird.

Beispiele:

Vor einer Wartung wird das Modem durch einen berechtigten Mitarbeiter des Auftraggebers aktiviert.

Es wird eine Benutzerkennung für das Wartungspersonal eingerichtet. Um die Wartung durchführen zu können, muss die Kennung mit dem Passwort eingegeben werden oder ein Einmalpasswort wird für die bevorstehende Aktion des Auftragnehmers ausgegeben.

Es wird ein durch Chipkarten unterstütztes Challenge-Response-Verfahren zur Identifizierung des Wartungspersonals eingesetzt.

d) Zugriffskontrolle

Maßnahmen, damit die zur Benutzung der Datenverarbeitungssysteme Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass bei der Fernwartung solche Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

_____

Hinweis:

Im § 1 des Vertrags ist der Umfang der Fernwartung festgelegt. Dem Auftrag entsprechend müssen die Zugriffsregeln für das Wartungspersonal definiert werden. Ein Zugriff auf andere Anwendungen oder Daten muss ausgeschlossen werden. Auch sind dem Wartungspersonal grundsätzlich keine Administratorrechte einzuräumen. Änderungen im Betriebssystem oder systemnaher Software sollten nur von Mitarbeitern des Auftraggebers vorgenommen werden, damit der Auftraggeber den Überblick über den Stand des Systems behält. Dies gilt umso mehr, wenn mehrere Anwendungen auf einem Rechner laufen und Änderungen im System während der Fernwartung die anderen Anwendungen beeinflussen würden.

Beispiel:

Dem Auftragsumfang entsprechend werden die Zugriffsrechte des Wartungspersonals vergeben.

e) Weitergabekontrolle

Maßnahmen, die sicherstellen, 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:

_____

Hinweis:

Die vorgesehen Maßnahmen müssen u.a. gewährleisten, dass die Verbindung nur zwischen der Wartungszentrale und den zu wartenden Rechnern aufgebaut werden kann. Außerdem dürfen Dritte die übertragenen Daten nicht zur Kenntnis nehmen können.

Beispiele:

Die Datenübertragung wird verschlüsselt. Es kommt das Verfahren _____ zum Einsatz.

Durch Call-Back-Verfahren wird die Verbindung zur Fernwartungszentrale aufgebaut.

Datenträger dürfen nur von dazu ausdrücklich berechtigten Personen und mittels Datenträgerbegleitschein transportiert werden.

f) Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

_____

Hinweis:

Die Maßnahmen müssen gewährleisten, dass bei schreibenden Zugriffen des Auftragnehmers auf das System des Auftraggebers Fehler, zufälliges Löschen oder Verändern, Funktionalitätsprobleme usw. ausgeglichen werden können, in dem auf den Arbeitsstand vor Beginn der Wartungsarbeiten zurückgegriffen werden kann.

Beispiel:

Unmittelbar vor Beginn der Wartungsarbeiten ist eine Sicherungskopie (differenziertes Backup) der von diesen Arbeiten mittelbar und unmittelbar betroffenen Bestände durch _____ anzufertigen.

g) Trennungsgebot

Die Maßnahmen müssen gewährleisten, dass die zum Test der erfolgten Wartungsarbeiten bestimmten personenbezogenen Daten getrennt von den produktiven Datenbeständen verarbeitet werden können:

_____

Hinweis:

Nur im absoluten Ausnahmefall (nicht immer sind Testdaten für eine bestimmte Konstellation ausreichend!) sollte der Zugriff auf produktive Daten genehmigt werden.

Beispiel:

Beim Auftragnehmer wird eine Testumgebung eingerichtet, die der Realität beim Auftraggeber weitgehend entspricht. Der Auftraggeber stellt dafür eine Testdatenbank zur Verfügung und pflegt diese.

(2) Der Auftragnehmer beachtet die Grundsätze ordnungsmäßiger Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

(3) Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu vereinbaren.

(4) Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen oder unvorhergesehen vom vereinbarten Standard abweichen, benachrichtigt er den Auftraggeber unverzüglich.

§ 8 Vertragsdauer

(1) Der Vertrag

- beginnt am _____ und endet am _____.

- mit Auftragserledigung.

- wird auf unbestimmte Zeit geschlossen.

Er ist mit einer Frist von _____ Monaten zum Quartalsende kündbar.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen des BDSG oder dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der Aufsichtsbehörde vertragswidrig verweigert.

§ 9 Vergütung

[...]

§ 10 Haftung

(1) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber den Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

§ 11 Vertragsstrafe

Bei Verstoß gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung des Datenschutzes, wird eine Vertragsstrafe von _____ EUR vereinbart.

§ 12 Sonstiges

(1) Der Auftragnehmer übereignet dem Auftraggeber zur Sicherung die Datenträger, auf denen sich Dateien befinden, die Daten des Auftraggebers enthalten. Diese Datenträger sind besonders zu kennzeichnen und von anderen Datenbeständen getrennt zu halten.

(2) Sollten Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Hinweis:

Diese Klausel muss wegen § 11 Nr. 2 AGBG gesondert vereinbart werden.

§ 13 Wirksamkeit der Vereinbarung

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

_____

Ort, Datum, Unterschriften

Erläuterungen zu § 7 Datensicherungsmaßnahmen

In dem Vertrag müssen die technischen und organisatorischen Maßnahmen festgelegt werden, die bei der Datenverarbeitung umzusetzen sind.

Rechtsgrundlage ist § 11 Abs. 2 BDSG, in dem beschrieben ist, welche Prüfungen ein Auftraggeber vor einer Auftragsvergabe durchzuführen hat. So muss der Auftragnehmer unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Das Ergebnis der Vorabprüfung ist zu dokumentieren. Im Auftrag sind insbesondere die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Insbesondere hat der Auftraggeber zu prüfen, ob beim Auftragnehmer die nach § 9 BDSG erforderlichen Maßnahmen getroffen werden. Die Kontrollen sind regelmäßig während der Auftragserfüllung durchzuführen und zu dokumentieren.

Werden personenbezogene Daten bei der Fernwartung zur Kenntnis genommen, deren Verarbeitung für die Betroffenen keine besonderen Risiken erwarten lässt, so bietet das Grundschutzhandbuch des BSI für bestimmte technische Konstellationen einen Katalog an Sicherheitsmaßnahmen. (Das Handbuch, in dem die Maßnahmen erläutert werden, kann auf Datenträgern beim BSI bestellt werden).

Wenn der Auftragnehmer ein Datensicherheitskonzept besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. Ist das Konzept nicht ausreichend, sind ergänzende Maßnahmen zu vereinbaren. Das daraus resultierende Sicherheitskonzept sollte zum Vertragsbestandteil gemacht werden. In diesem Fall kann darauf verzichtet werden, im Sicherheitskonzept genannte Maßnahmen im Vertragstext zu wiederholen.

Wenn der Auftragnehmer kein Datensicherheitskonzept vorlegen kann, das § 9 BDSG genügt, müssen die einzelnen Maßnahmen im Vertrag gemeinsam festgelegt werden. Es handelt sich um keinen abschließenden Maßnahmenkatalog. Insbesondere bei der Verarbeitung sensibler Daten sind in der Regel zusätzliche Maßnahmen erforderlich.

Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

- Verantwortlichkeiten: Aus unklaren Aufgabenverteilungen, bspw. bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.

- Abschottung: Es müssen Maßnahmen ergriffen werden, die ein (unberechtigtes) Eindringen in zu wartende Rechner soweit wie möglich verhindern. Dabei kann die Lösung vom einfachen Ausschalten des Modems bis zu technisch hochwertigen Challenge-Response-Verfahren gehen, die auf Chipkarten die geheimen Schlüssel speichern. Fallweise kann es nötig werden zu erkennen, ob und wie unberechtigte Personen versuchen einzudringen. Technische Komponenten, die dies feststellen können, sind Firewalls oder Intrusion Detection Systeme.

- Abhören der Kommunikation: Zum Schutz gegen unberechtigtes Abhören sind die Daten, die bei der Fernwartung übertragen werden, zu verschlüsseln.

- Anmeldeprozeduren: Die Anmeldung im System oder der zu wartenden Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.

A10. EU-Standardvertragsklauseln („Auftragsverarbeiter“)

Hinweise: *Der nachfolgende Mustertext[4] sollte unter Konkretisierung an angezeigten Stellen im Vertragstext bzw. in den Anlagen seitens des Datenexporteurs unverändert übernommen werden. Abweichungen von dem EU-Standardvertrag bedürfen in der Regel der Abstimmung mit der zuständigen Aufsichtsbehörde[5].*

Der EU-Standardvertrag ist - einschließlich der Erwägungsgründe der Kommissionsentscheidung - in mehreren Sprachen im Internet abrufbar[6].

STANDARDVERTRAGSKLAUSELN (AUFTRAGSVERARBEITER)

gem. Artikel 26 Absatz 2 der Richtlinie 95/46/EG für die Übermittlung personenbezogener Daten an Auftragsverarbeiter, die in Drittländern niedergelassen sind, in denen kein angemessenes Schutzniveau gewährleistet ist

Bezeichnung der Organisation (Datenexporteur):

_____

Adresse: _____

Tel.: _____ Fax: _____ E-Mail: _____

Weitere Angaben zur Identifizierung der Organisation:

_____
(„Datenexporteur“)
und

Bezeichnung der Organisation (Datenimporteur):

_____

Adresse: _____

Tel.: _____ Fax: _____ E-Mail: _____

Weitere Angaben zur Identifizierung der Organisation:

_____
(„Datenimporteur“)

Vereinbaren die folgenden Vertragsklauseln („Klauseln“), um angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen für die Übermittlung der in Anlage 1 zu diesen Vertragsklauseln spezifizierten personenbezogenen Daten vom Datenexporteur an den Datenimporteur bereitzustellen.

Klausel 1
Begriffsbestimmungen

Im Rahmen der Vertragsklauseln gelten folgende Begriffsbestimmungen:

[4] Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (2010/87/EU).
[5] Simitis, in: Simitis, BDSG 7. Aufl., § 4c Rn. 51.
[6] http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

a) die Ausdrücke "personenbezogene Daten", "besondere Kategorien personenbezogener Daten", "Verarbeitung", "für die Verarbeitung Verantwortlicher", "Auftragsverarbeiter", "betroffene Person" und "Kontrollstelle" entsprechen den Begriffsbestimmungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[7];

b) der "Datenexporteur" ist der für die Verarbeitung Verantwortliche, der die personenbezogenen Daten übermittelt;

c) der "Datenimporteur" ist der Auftragsverarbeiter, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten entgegenzunehmen und sie nach der Übermittlung nach dessen Anweisungen und den Bestimmungen der Klauseln in dessen Auftrag zu verarbeiten und der nicht einem System eines Drittlandes unterliegt, das angemessenen Schutz im Sinne von Artikel 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet;

d) der "Unterauftragsverarbeiter" ist der Auftragsverarbeiter, der im Auftrag des Datenimporteurs oder eines anderen Unterauftragsverarbeiters des Datenimporteurs tätig ist und sich bereit erklärt, vom Datenimporteur oder von einem anderen Unterauftragsverarbeiter des Datenimporteurs personenbezogene Daten ausschließlich zu dem Zweck entgegenzunehmen, diese nach der Übermittlung im Auftrag des Datenexporteurs nach dessen Anweisungen, den Klauseln und den Bestimmungen des schriftlichen Unterauftrags zu verarbeiten;

e) der Begriff "anwendbares Datenschutzrecht" bezeichnet die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Personen, insbesondere des Rechts auf Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten, die in dem Mitgliedstaat, in dem der Datenexporteur niedergelassen ist, auf den für die Verarbeitung Verantwortlichen anzuwenden sind;

f) die "technischen und organisatorischen Sicherheitsmaßnahmen" sind die Maßnahmen, die personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung schützen sollen.

Klausel 2
Einzelheiten der Übermittlung

Die Einzelheiten der Übermittlung, insbesondere die besonderen Kategorien personenbezogener Daten, sofern vorhanden, werden in Anhang 1 erläutert, der Bestandteil dieser Klauseln ist.

Klausel 3
Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

[7] Die Parteien können die Begriffsbestimmungen der Richtlinie 95/46/EG in diese Klausel aufnehmen, wenn nach ihrem Dafürhalten der Vertrag für sich allein stehen sollte.

Klausel 4
Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:
a) die Verarbeitung der personenbezogenen Daten einschließlich der Übermittlung entsprechend den einschlägigen Bestimmungen des anwendbaren Datenschutzrechts durchgeführt wurde und auch weiterhin so durchgeführt wird (und ggf. den zuständigen Behörden des Mitgliedstaats mitgeteilt wurde, in dem der Datenexporteur niedergelassen ist) und nicht gegen die einschlägigen Vorschriften dieses Staates verstößt;
b) er den Datenimporteur angewiesen hat und während der gesamten Dauer der Datenverarbeitungsdienste anweisen wird, die übermittelten personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dem anwendbaren Datenschutzrecht und den Klauseln zu verarbeiten;
c) der Datenimporteur hinreichende Garantien bietet in Bezug auf die in Anhang 2 zu diesem Vertrag beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen;
d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligen Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;
e) er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt;
f) die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis gesetzt worden ist oder gesetzt wird, dass ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;
g) er die gem. Klausel 5 Buchstabe b sowie Klausel 8 Absatz 3 vom Datenimporteur oder von einem Unterauftragsverarbeiter erhaltene Mitteilung an die Kontrollstelle weiterleitet, wenn der Datenexporteur beschließt, die Übermittlung fortzusetzen oder die Aussetzung aufzuheben;
h) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen ggf. die Kopie des Vertrags über Datenverarbeitungsdienste zur Verfügung, der gem. den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;
i) bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter die Verarbeitung gem. Klausel 11 erfolgt und die personenbezogenen Daten und die Rechte der betroffenen Person mindestens ebenso geschützt sind, wie vom Datenimporteur nach diesen Klauseln verlangt; und
j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Klausel 5
Pflichten des Datenimporteurs*

*Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.

Der Datenimporteur erklärt sich bereit und garantiert, dass:
a) er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;
b) er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen, und eine Gesetzesänderung, die sich voraussichtlich sehr nachteilig auf die Garantien und Pflichten auswirkt, die die Klauseln bieten sollen, dem Datenexporteur mitteilen wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;
c) er vor der Verarbeitung der übermittelten personenbezogenen Daten die in Anhang 2 beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen ergriffen hat;

d) er den Datenexporteur unverzüglich informiert über
i) alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, bspw. durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;
ii) jeden zufälligen oder unberechtigten Zugang und
iii) alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;
e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt;
f) er auf Verlangen des Datenexporteurs seine für die Verarbeitung erforderlichen Datenverarbeitungseinrichtungen zur Prüfung der unter die Klauseln fallenden Verarbeitungstätigkeiten zur Verfügung stellt. Die Prüfung kann vom Datenexporteur oder einem vom Datenexporteur ggf. in Absprache mit der Kontrollstelle ausgewählten Prüfgremium durchgeführt werden, dessen Mitglieder unabhängig sind, über die erforderlichen Qualifikationen verfügen und zur Vertraulichkeit verpflichtet sind;
g) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und ggf. einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;
h) er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat;
i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;
j) er dem Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt, den er nach den Klauseln geschlossen hat.

Klausel 6
Haftung

(1) Die Parteien vereinbaren, dass jede betroffene Person, die durch eine Verletzung der in Klausel 3 oder 11 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, vom Datenexporteur Schadenersatz für den erlittenen Schaden zu erlangen.
(2) Ist die betroffene Person nicht in der Lage, gem. Absatz 1 gegenüber dem Datenexporteur wegen Verstoßes des Datenimporteurs oder seines Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 genannte Pflichten Schadenersatzansprüche geltend zu machen, weil das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist, ist der Datenimporteur damit einverstanden, dass die betroffene Person Ansprüche gegenüber ihm statt gegenüber dem Datenexporteur geltend macht, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen.
Der Datenimporteur kann sich seiner Haftung nicht entziehen, indem er sich auf die Verantwortung des Unterauftragsverarbeiters für einen Verstoß beruft.
(3) Ist die betroffene Person nicht in der Lage, gem. den Absätzen 1 und 2 gegenüber dem Datenexporteur oder dem Datenimporteur wegen Verstoßes des Unterauftragsverarbeiters gegen in den Klauseln 3 und 11 aufgeführte Pflichten Ansprüche geltend zu machen, weil sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, ist der Unterauftragsverarbeiter damit einverstanden, dass die betroffene Person im Zusammenhang mit seinen Datenverarbeitungstätigkeiten auf Grund der Klauseln gegenüber ihm statt gegenüber dem Datenexporteur oder dem Datenimporteur einen Anspruch geltend machen kann, es sei denn, ein Rechtsnachfolger hat durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen; in diesem Fall kann die betroffene Person ihre Ansprüche gegenüber dem Rechtsnachfolger geltend machen. Eine solche Haftung des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach diesen Klauseln beschränkt.

Klausel 7
Schlichtungsverfahren und Gerichtsstand

(1) Für den Fall, dass eine betroffene Person gegenüber dem Datenimporteur Rechte als Drittbegünstigte und/oder Schadenersatzansprüche auf Grund der Vertragsklauseln geltend macht, erklärt sich der Datenimporteur bereit, die Entscheidung der betroffenen Person zu akzeptieren, und zwar entweder:
a) die Angelegenheit in einem Schlichtungsverfahren durch eine unabhängige Person oder ggf. durch die Kontrollstelle beizulegen oder
b) die Gerichte des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, mit dem Streitfall zu befassen.

(2) Die Parteien vereinbaren, dass die Entscheidung der betroffenen Person nicht die materiellen Rechte oder Verfahrensrechte dieser Person, nach anderen Bestimmungen des nationalen oder internationalen Rechts Rechtsbehelfe einzulegen, berührt.

Klausel 8
Zusammenarbeit mit Kontrollstellen

(1) Der Datenexporteur erklärt sich bereit, eine Kopie dieses Vertrags bei der Kontrollstelle zu hinterlegen, wenn diese es verlangt oder das anwendbare Datenschutzrecht es so vorsieht.
(2) Die Parteien vereinbaren, dass die Kontrollstelle befugt ist, den Datenimporteur und etwaige Unterauftragsverarbeiter im gleichen Maße und unter denselben Bedingungen einer Prüfung zu unterziehen, unter denen die Kontrollstelle gem. dem anwendbaren Datenschutzrecht auch den Datenexporteur prüfen müsste.
(3) Der Datenimporteur setzt den Datenexporteur unverzüglich über Rechtsvorschriften in Kenntnis, die für ihn oder etwaige Unterauftragsverarbeiter gelten und eine Prüfung des Datenimporteurs oder von Unterauftragsverarbeitern gem. Absatz 2 verhindern. In diesem Fall ist der Datenexporteur berechtigt, die in Klausel 5 Buchstabe b vorgesehenen Maßnahmen zu ergreifen.

Klausel 9
Anwendbares Recht

Für diese Klauseln gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: …

Klausel 10
Änderung des Vertrags

Die Parteien verpflichten sich, die Klauseln nicht zu verändern. Es steht den Parteien allerdings frei, erforderlichenfalls weitere, geschäftsbezogene Klauseln aufzunehmen, sofern diese nicht im Widerspruch zu der Klausel stehen.

Klausel 11
Vergabe eines Unterauftrags

(1) Der Datenimporteur darf ohne die vorherige schriftliche Einwilligung des Datenexporteurs keinen nach den Klauseln auszuführenden Verarbeitungsauftrag dieses Datenexporteurs an einen Unterauftragnehmer vergeben. Vergibt der Datenimporteur mit Einwilligung des Datenexporteurs Unteraufträge, die den Pflichten der Klauseln unterliegen, ist dies nur im Wege einer schriftlichen Vereinbarung mit dem Unterauftragsverarbeiter möglich, die diesem die gleichen Pflichten auferlegt, die auch der Datenimporteur nach den Klauseln erfüllen muss[8]. Sollte der Unterauftragsverarbeiter seinen Datenschutzpflichten nach der schriftlichen Vereinbarung nicht nachkommen, bleibt der Datenimporteur gegenüber dem Datenexporteur für die Erfüllung der Pflichten des Unterauftragsverarbeiters nach der Vereinbarung uneingeschränkt verantwortlich.
(2) Die vorherige schriftliche Vereinbarung zwischen dem Datenimporteur und dem Unterauftragsverarbeiter muss gem. Klausel 3 auch eine Drittbegünstigtenklausel für Fälle enthalten, in denen die betroffene Person nicht in der Lage ist, einen Schadenersatzanspruch gem. Klausel 6 Absatz 1 gegenüber dem Datenexporteur oder dem Datenimporteur geltend zu machen, weil diese faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind und kein Rechtsnachfolger durch Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs oder des Datenimporteurs übernommen hat. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.
(3) Für Datenschutzbestimmungen im Zusammenhang mit der Vergabe von Unteraufträgen über die Datenverarbeitung gem. Absatz 1 gilt das Recht des Mitgliedstaats, in dem der Datenexporteur niedergelassen ist, nämlich: …
(4) Der Datenexporteur führt ein mindestens einmal jährlich zu aktualisierendes Verzeichnis der mit Unterauftragsverarbeitern nach den Klauseln geschlossenen Vereinbarungen, die vom Datenimporteur nach Klausel 5 Buchstabe j übermittelt wurden. Das Verzeichnis wird der Kontrollstelle des Datenexporteurs bereitgestellt.

Klausel 12
Pflichten nach Beendigung der Datenverarbeitungsdienste

(1) Die Parteien vereinbaren, dass der Datenimporteur und der Unterauftragsverarbeiter bei Beendigung der Datenverarbeitungsdienste je nach Wunsch des Datenexporteurs alle übermittelten personenbezogenen Daten und deren Kopien an den Datenexporteur zurückschicken oder alle personenbezogenen Daten zerstören und dem Datenexporteur bescheinigen, dass dies erfolgt ist, sofern die Gesetzgebung, der der Datenimporteur unterliegt, diesem

[8] Dies kann dadurch gewährleistet werden, dass der Unterauftragsverarbeiter den nach diesem Beschluss geschlossenen Vertrag zwischen dem Datenexporteur und dem Datenimporteur mitunterzeichnet.

die Rückübermittlung oder Zerstörung sämtlicher oder Teile der übermittelten personenbezogenen Daten nicht untersagt. In diesem Fall garantiert der Datenimporteur, dass er die Vertraulichkeit der übermittelten personenbezogenen Daten gewährleistet und diese Daten nicht mehr aktiv weiterverarbeitet.
(2) Der Datenimporteur und der Unterauftragsverarbeiter garantieren, dass sie auf Verlangen des Datenexporteurs und/oder der Kontrollstelle ihre Datenverarbeitungseinrichtungen zur Prüfung der in Absatz 1 genannten Maßnahmen zur Verfügung stellen.

Für den Datenexporteur:

Name (ausgeschrieben): _____

Stellung: _____

Adresse: _____

Ggf. weitere Angaben, die den Vertrag verbindlich machen:

_____

Unterschrift: _____

(Stempel der Organisation)

Für den Datenimporteur:

Name (ausgeschrieben): _____

Stellung: _____

Adresse: _____

Ggf. weitere Angaben, die den Vertrag verbindlich machen:

_____

Unterschrift: _____

(Stempel der Organisation)

Anhang 1 zu den Standardvertragsklauseln
Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden.
Die Mitgliedstaaten können entsprechend den nationalen Verfahren Zusatzangaben, die in diesem Anhang enthalten sein müssen, ergänzen.

Datenexporteur
Der Datenexporteur ist (bitte erläutern Sie kurz Ihre Tätigkeiten, die für die Übermittlung von Belang sind):

_____

_____

_____

Datenimporteur
Der Datenimporteur ist (bitte erläutern Sie kurz die Tätigkeiten, die für die Übermittlung von Belang sind):

_____

_____

_____

Betroffene Personen
Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen (bitte genau angeben):

_____

_____

_____

Kategorien von Daten
Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):

_____

_____

_____

Besondere Datenkategorien (falls zutreffend)
Die übermittelten personenbezogenen Daten umfassen folgende besondere Datenkategorien (bitte genau angeben):

_____

_____

_____

Verarbeitung
Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen (bitte genau angeben):

_____

_____

_____

DATENEXPORTEUR
Name: _____

Unterschrift des/der Bevollmächtigten:_____

DATENIMPORTEUR
Name: _____

Unterschrift des/der Bevollmächtigten: _____

Anhang 2 zu den Standardvertragsklauseln

Dieser Anhang ist Bestandteil der Klauseln und muss von den Parteien ausgefüllt und unterzeichnet werden.

Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gem. Klausel 4 Buchstabe d und Klausel 5 Buchstabe c eingeführt hat (oder Dokument/Rechtsvorschrift beigefügt):

_____

_____

_____

Beispiel für eine Entschädigungsklausel (Fakultativ)

Haftung

Die Parteien erklären sich damit einverstanden, dass, wenn eine Partei für einen Verstoß gegen die Klauseln haftbar gemacht wird, den die andere Partei begangen hat, die zweite Partei der ersten Partei alle Kosten, Schäden, Ausgaben und Verluste, die der ersten Partei entstanden sind, in dem Umfang ersetzt, in dem die zweite Partei haftbar ist.

Die Entschädigung ist abhängig davon, dass

a) der Datenexporteur den Datenimporteur unverzüglich von einem Schadenersatzanspruch in Kenntnis setzt und

b) der Datenimporteur die Möglichkeit hat, mit dem Datenexporteur bei der Verteidigung in der Schadenersatzsache bzw. der Einigung über die Höhe des Schadenersatzes zusammenzuarbeiten[9].

[9] Der Absatz über die Haftung ist fakultativ.