

Verpflichtung eines Dienstleisters nach §11 BDSG(Novelle 2009)

Pflichten des Auftragnehmers **(-Name und Anschrift der Firma eintragen)**

Der Dienstleister könnte im Rahmen seiner Aufgabenerfüllung Zugang zu personenbezogenen Daten des Auftraggebers erlangen. Jede Verarbeitung dieser Art unterliegt im Allgemeinen den Vorschriften laut Art. VIII der EU Richtlinie 95/46/EU (siehe Anlage) und den folgend aufgeführten spezifischen Anordnungen.

1. Der Auftragnehmer darf Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Siehe Details **(Auftrags Nr. ----- vom -----)**
2. Der Umfang, die Art und der Zweck der Datenverarbeitung, sowie die Art der Daten und der Kreis der Betroffenen ergibt sich aus dem genannten Auftrag.
3. Der Auftragnehmer wird auf die Rechte der Betroffenen bezüglich Berichtigung, Löschung und Sperrung ihrer Daten hingewiesen. Im Falle diesbezüglicher Anfragen Betroffener übernimmt der Auftragnehmer diese Pflichten.
4. Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 Bundesdatenschutzgesetz (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind.
5. Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten seines betrieblichen Datenschutzbeauftragten mit.

Data Privacy Clause per § 11 BDSG (revision 2009)

Duties of Service Provider

(Specify Name & Address of Service provider Company):

Service Provider (processor) may have access or process personal data of contractor (controller). Any such access or processing shall be subject to the general provisions of Section VIII of the EU directive 95/46/EU, (attached) and following specific provisions:

1. Processor may access or use any data provided by Controller only for the purpose specified in the contract _____(No. , date)between the parties
2. The purpose and nature of data processing, as well as the type of data and the persons affected is specified in above contract.
3. Processor is specifically advised of the rights of data subjects concerning correction, deletion or blocking of their data. In case data subjects' requests, processor will take on these duties.
4. Processor shall employ only workers that have been instructed to keep controller's data confidential, and have signed a statement per §5 BDSG.
5. Processor shall advise contact details of his Data Privacy Officer (or similar function if outside Germany)
6. Processor shall notify controller without delay if he believes that instructions given by controller are in conflict with data privacy laws or regulations. If reasonable cause to believe that data breaches or other irregularities exists, processor must inform controller without delay.

6. Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.

7. Aufträge an Subunternehmer dürfen nur mit schriftlicher Genehmigung des Auftraggebers vergeben werden. Subunternehmer sind auf die hierin genannten Maßnahmen zu verpflichten.

8. Der Auftragnehmer räumt dem Auftraggeber das Recht ein, die Einhaltung der gesetzlichen Vorschriften des Datenschutzes beim Auftragnehmer zu kontrollieren, und ihn dabei aktiv zu unterstützen. Solche Kontrollen erfolgen nur nach vorheriger Absprache.

9. Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer. Nach Beendigung des Auftrages sind alle Datenträger und/oder gespeicherte Daten an den Auftraggeber zurückzugeben.

10. Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen entsprechend § 9

7. Processor shall employ subcontractors only if processor has agreed in writing. Subcontractors shall be bound to the same principles and provisions as stated herein.

8. Controller reserves the right to inspect the security provisions at processor's premises upon prior notice. Controller may employ third party inspectors if processor has agreed. Controller may prove compliance with the data security regulations by independent certification authorities or by declaration.

9. If necessary to perform the contractual obligations, processor may produce temporary duplicates. However it is expressly agreed that no content may be modified and that all media and copies shall be returned to controller or securely destroyed upon completion of services. The same applies to test or deleted material. Any confidential data shall be securely stored until completion. Logs or other proof of secure deletion must be provided to controller if requested. Address data that may be provided must only be used for communication with controller; under no circumstances may such data be used for marketing purposes.

10. In his area of responsibility, contractor will assure the technical and organizational measures in compliance with §9 BDSG are complied with. Specifically, contractor shall organize its internal processes in such a manner that it will comply with the special requirements of data privacy.

Bundesdatenschutzgesetz zu. Insbesondere wird der Auftragnehmer seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen des Bundesdatenschutzgesetzes entsprechen. Dies beinhaltet insbesondere

Bei jeder der folgend aufgeführten Maßnahmen (a.-i.) hat der Auftragnehmer anzugeben, wie in seinem Unternehmen diese von Gesetzgeber geforderte Maßnahme durchgeführt wird.

~~10.~~

- a. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),
- b. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- c. dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
- d. dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert,

This includes specifically:

The contractor shall specify how each of the measures (a.-i.) listed below will be implemented in his business,

- a. **Unauthorized persons will not have access to locations or facilities**
- b. **Unauthorized persons will be denied access to IT Systems**
- c. **Data is accessible only to persons authorized for the process in question, and that data cannot be read, copied or modified or deleted without authorization.**
- d. **To take precautions so that data cannot be read, modified or deleted during electronic transmission or storage on media, and that it is documented with which parties electronic transmission has been established.**
- e. **That it can be determined after the fact which person has entered or deleted personal data into systems.**
- f. **That personal data processed by others can only be processed as specified in the order.**
- g. **That personal data is protected from accidental loss or destruction.**
- h. **That data collected for different purposes can be processed separately.**
- i. **That personal or sensitive data is encrypted by state-of-the art algorithms when transmitted by electronic means.**

<p>verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),</p> <ul style="list-style-type: none">e. dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),f. dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),g. dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),h. dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).i. Bei der Übermittlung personenbezogener oder sensibler Daten ist ein dem Stand der Technik entsprechendes Verschlüsselungsverfahren einzusetzen.	