

Vertrag zur Auftragsdatenverarbeitung (MUSTER)

Stand: 26.03.2018

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV

Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftraggeber] - [Bezeichnung Auftragnehmer]

VERTRAG ZUR AUFTRAGSDATENVERARBEITUNG (GEMÄß ART 28 DSGVO¹)

Zwischen dem

[Auftraggeber]

[Straße/Hausnummer, PLZ/Ort]

vertreten durch

[Funktion/Vorname/Nachname]

(Auftraggeber)

und

[Auftragnehmer]

[Straße/Hausnummer, PLZ/Ort]

vertreten durch

[Funktion/Vorname/Nachname]

(Auftragnehmer)

¹ DSGVO = EU-Datenschutzgrundverordnung

Vertrag zur Auftragsdatenverarbeitung (MUSTER)

Stand: 26.03.2018

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV

Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftraggeber] - [Bezeichnung Auftragnehmer]

AUFTRAGSDATENVERARBEITUNG GEMÄß ART. 28 DSGVO

Präambel

Die Parteien haben einen Vertrag [Bezeichnung Vertragstyp] über [Bezeichnung Vertragsgegenstand und Software-Anwendung] (Im folgenden „Hauptvertrag“) geschlossen. In diesem Zusammenhang ist der Auftragnehmer verpflichtet, die Anforderungen der Art. 25 DSGVO (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) und Art. 32 DSGVO (Sicherheit der Verarbeitung) zu erfüllen.

Im Rahmen der Bereitstellung der im Hauptvertrag beschriebenen Software-Anwendungen und personenbezogenen Daten hat der Auftragnehmer Zugriff auf die in der **Anlage A** des vorliegenden Vertrages dargelegten **personenbezogenen Attribute**.

Dieser vorliegende Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitungstätigkeiten ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Diese Vereinbarung tritt durch Unterzeichnung des Hauptvertrags in Kraft und gilt für die Laufzeit des Hauptvertrages.

1. Definitionen

1.1 Personenbezogene Daten

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

1.2 Datenverarbeitung im Auftrag

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

1.3 Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Sie können durch Einzelweisungen ergänzt werden.

Vertrag zur Auftragsdatenverarbeitung (MUSTER)

Stand: 26.03.2018

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV

Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftraggeber] - [Bezeichnung Auftragnehmer]

2. Anwendungsbereich und Verantwortlichkeit

- 2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO). Dabei unterstützt der Auftragnehmer den Auftraggeber bei der Wahrnehmung seiner Verantwortlichkeit.
- 2.2 Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch nach der Laufzeit des Vertrages und nach Beendigung des Vertrages die Herausgabe oder Löschung der Daten verlangen.
- 2.3 Die Inhalte dieser Vertragsanlage gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

3. Pflichten des Auftragnehmers

- 3.1 Der Auftragnehmer darf Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.
- 3.2 Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen entsprechend Art. 25 DSGVO zu. Insbesondere wird der Auftragnehmer seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen der DSGVO entsprechen. Dies beinhaltet insbesondere:
 - Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),
 - zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

Vertrag zur Auftragsdatenverarbeitung (MUSTER)

Stand: 26.03.2018

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV

Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftraggeber] - [Bezeichnung Auftragnehmer]

- 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),
 - dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
 - 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),
 - dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
 - dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
 - dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).
- 3.3 Der Auftragnehmer stellt dem Auftraggeber ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept (Security-Policy bzw. Auflistung der beim Auftragnehmer eingeführten **technischen und organisatorischen Maßnahmen** zur Realisierung eines hinreichenden Datensicherheitsniveaus) zur Verfügung. Dieses Datensicherheitskonzept liegt dem vorliegenden Vertrag als **Anlage B** bei.
- 3.4 Der Auftragnehmer stellt dem Auftraggeber die für das **Verzeichnis von Verarbeitungstätigkeiten** nach Art. 30 DSGVO notwendigen Angaben als **Anlage C** zur Verfügung.
- 3.5 Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß Art. 28 Abs. 3 Buchst. b) DSGVO zur Vertraulichkeit (Datengeheimnis) verpflichtet und in die Schutzbestimmungen der DSGVO eingewiesen worden sind.
- 3.6 Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit.

Vertrag zur Auftragsdatenverarbeitung (MUSTER)

Stand: 26.03.2018

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV

Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftraggeber] - [Bezeichnung Auftragnehmer]

- 3.7 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.
- 3.8 Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.
- 3.9 Der Auftragnehmer sichert zu, dass die im Zusammenhang mit der Vertragserfüllung gespeicherten Daten nur im Gültigkeitsbereich der DSGVO gespeichert, verarbeitet und genutzt werden.
- 3.10 Der Auftragnehmer versichert, dass die personenbezogenen Daten nicht für eigene Zwecke genutzt werden und eine Datenübermittlung nur auf Grundlage dieser Vertragsanlage erfolgt.
- 3.11 Der Auftragnehmer unterstützt den verantwortlichen Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.
- 3.12 Änderungen sind dem Auftraggeber unverzüglich anzuzeigen.

4. Pflichten des Auftraggebers

- 4.1 Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.
- 4.2 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
- 4.3 Die Pflicht zur Führung des Verzeichnisses der Verarbeitungstätigkeiten liegt beim Auftraggeber. Der Auftragnehmer unterstützt ihn dabei gemäß Art. 30 Abs. 2 DSGVO.
- 4.4 Über die Herausgabe oder Löschung der Daten nach Vertragsende (Ziffer 2.2) muss der Auftraggeber innerhalb einer von dem Auftragnehmer gesetzten Frist entscheiden.
- 4.5 Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten (Ziffer 2.2), so trägt diese der Auftraggeber.

Vertrag zur Auftragsdatenverarbeitung (MUSTER)

Stand: 26.03.2018

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV

Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftraggeber] - [Bezeichnung Auftragnehmer]

5. Anfragen Betroffener an den Auftraggeber

Ist der Auftraggeber aufgrund Kapitel III DSGVO gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber gemäß Art 28 Abs. 3 Buchst. e) DSGVO dabei unterstützen, diese Informationen bereit zu stellen.

6. Kontrollrecht

Der Auftraggeber kann sich gemäß Art 28 Abs. 3 Buchst. h) DSGVO nach rechtzeitiger Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse überzeugen.

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

7. Subunternehmer

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

Eine Auflistung der derzeit auf Seiten des Auftragnehmers eingeschalteten **Subunternehmer** mit den jeweils übertragenen Aufgabenfeldern findet sich in der **Anlage D** des vorliegenden Vertrages.

7.2 Sollen weitere/andere Dienstleister unterbeauftragt werden, so ist dies nur nach einer schriftlichen Zustimmung des Auftraggebers zulässig. In diesem Fall ist die **Anlage D** des vorliegenden Vertrages anzupassen.

7.3 Über die Unterbeauftragung von verbundenen Unternehmen gemäß Art. 28 Abs. 2 DSGVO ist der Auftraggeber stets rechtzeitig vorab zu informieren.

7.4 Werden Subunternehmer durch den Auftragnehmer eingeschaltet, so werden die vertraglichen Vereinbarungen so gestaltet, dass sie den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages entsprechen. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend Art 28 Abs. 3 Buchst. h) DSGVO einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung des Auftragnehmers Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

Vertrag zur Auftragsdatenverarbeitung (MUSTER)

Stand: 26.03.2018

Professor Dr. Rolf Lauser / Datenschutzbeauftragter / BLSV

Dr.-Gerhard-Hanke-Weg 31, 85221 Dachau, Tel.: 08131/511750, Fax: 08131/511619, rolf@lauser-nhk.de

[Bezeichnung Auftraggeber] - [Bezeichnung Auftragnehmer]

8. Sonstiges, Allgemeines

- 8.1 Sollten die Daten des Auftraggebers bei dem Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.
- 8.2 Änderungen und Ergänzungen dieser Vereinbarung/Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- 8.3 Es gilt deutsches Recht. Gerichtsstand ist [Ort].

(Ort, Datum, Firmenstempel)

(Ort, Datum, Firmenstempel)

[Vorname/Nachname]

[Vorname/Nachname]

[Funktion]

[Funktion]

[Vorname/Nachname]

[Funktion]