logicline.
Implementing Your Digital Business

Vereinbarung zur Auftragsdatenverarbeitung

zwischen

- nachfolgend "Auftraggeber" genannt –

und

nachfolgend „Auftragnehmer“ genannt

gemeinsam die „Parteien“ genannt

logicline GmbH · Planiestraße 10 · 71063 Sindelfingen, Germany
Tel. +49 7031 611 77 0 · www.logicline.de · info@logicline.de

Präambel

Seit dem 25.05.2018 ist die Datenschutz-Grundverordnung (DSGVO) geltendes Recht. Die DSGVO enthält u.a. auch Regelungen zur Auftragsdatenverarbeitung (Art. 28 ff. DSGVO). Der Auftraggeber erteilt dem Auftragnehmer mit der Vereinbarung vom („Hauptvertrag“) einen Auftrag zur Datenverarbeitung. Um den Hauptvertrag datenschutzrechtlich zu begleiten ist es erforderlich, eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO abzuschließen. Vor diesem Hintergrund schließen die Parteien folgende Vereinbarung als Datenschutzvereinbarung über die Auftragsdatenverarbeitung („DSV“).

1 Allgemeine Vorschriften

1.1 Gültigkeit

a. Diese DSV nach Art. 28 DSGVO tritt mit ihrer Unterzeichnung in Kraft. Sie ist eine eigenständige Vereinbarung zwischen den Parteien und steht neben dem zwischen den Parteien geschlossenen Hauptvertrag. Wenn und soweit der Hauptvertrag Regelungen enthält, die denjenigen der DSV entgegenstehen, so haben die Regelungen der DSV Vorrang, soweit in der DSV nicht etwas anderes geregelt ist. Die Laufzeit dieser DSV folgt der Laufzeit des Hauptvertrags; sie endet automatisch mit dem Hauptvertrag.

1.2 Alleinige Vereinbarung und Schriftform

a. Die Regelungen der DSV sind abschließend.
b. Jede Änderung bedarf der Schriftform. Das Schriftformerfordernis gilt nicht für die Aktualisierung der Anlagen, hier ist die Textform (auch per E-Mail) ausreichend.

2 Auftragsverarbeitung nach Art. 28 DSGVO

2.1 Grundsätze der Datenverarbeitung

a. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des für die Datenverarbeitung verantwortlichen Auftraggebers (Auftragsverarbeitung). Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten sind in Anlage 1 zu hinterlegen.
b. Die Erhebung, Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in Staaten, auch durch einen Unterauftragnehmer des Auftragnehmers, außerhalb der EU / des EWR bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen von Kapitel 5 DSGVO erfüllt sind.
c. Für die Ziffer 2 dieser Vereinbarung gelten die Definitionen der DSGVO (insbesondere Art. 4 DSGVO).

2.2 Rechte und Pflichten des Auftraggebers

a. Der Auftraggeber ist für den Schutz der Rechte und Freiheiten der betroffenen Personen verantwortlich. Er erteilt dem Auftragnehmer die für den Schutz der Rechte und Freiheiten erforderlichen Weisungen..
b. Der Auftraggeber ist für die Vereinbarkeit der von ihm an den Auftragnehmer erteilten Weisungen mit den jeweils für die Verarbeitung einschlägigen rechtlichen Anforderungen verantwortlich.

c. Der Auftraggeber weist den Auftragnehmer hiermit an, selbständig keine Zweckänderung der Datenverarbeitung durchzuführen und die personenbezogenen Daten, die ihm vom Auftraggeber zum Zwecke der Datenverarbeitung zur Verfügung gestellt werden, nicht für eigene Zwecke zu verwenden.
d. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei den Verarbeitungsergebnissen feststellt, insbesondere wenn er Grund zu der Annahme hat, dass die Art und Weise der Verarbeitung der Daten durch den Auftragnehmer gegen datenschutzrechtliche Anforderungen verstößt.
e. Der Auftraggeber erfüllt alle Pflichten zur Wahrung der Informations-, Auskunfts- und sonstigen Rechte der betroffenen Personen, die sich aus den jeweils für die Verarbeitung gültigen Rechtsgrundlagen ergeben. Der Auftragnehmer ist verpflichtet, an der Erfüllung dieser Pflichten, mitzuwirken und dem Auftraggeber alle für die Erfüllung dieser Pflichten notwendigen Informationen zur Verfügung zu stellen.

2.3 Rechte und Pflichten des Auftragnehmers

a. Der Auftragnehmer ist verpflichtet, personenbezogene Daten, die ihm im Rahmen des Auftrags vom Auftraggeber zum Zwecke der Datenverarbeitung zur Verfügung gestellt werden oder die ihm während der Durchführung, als Ergebnis der Datenverarbeitung oder auf sonstige Weise bekannt werden, nur entsprechend den Weisungen des Auftraggebers zu verarbeiten
b. Der Auftragnehmer versichert, dass ihm alle einschlägigen datenschutzrechtlichen Vorschriften, die zu einer rechtmäßigen Durchführung der Datenverarbeitung erforderlich sind, bekannt sind und gewährleistet deren Umsetzung. Er gewährleistet, dass alle von ihm mit der Durchführung des Auftrags beauftragten Personen zur Vertraulichkeit verpflichtet worden sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
c. Soweit der Auftraggeber aus technischen oder tatsächlichen Gründen nicht in der Lage ist, von der Verarbeitung betroffene personenbezogene Daten zu berichtigen, zu sperren oder zu löschen, ist der Auftragnehmer dazu verpflichtet, den Auftraggeber bei der Durchführung der jeweiligen Maßnahme zu unterstützen.
d. Nach Beendigung des Auftragsverhältnisses hat der Auftragnehmer etwaige noch nicht übergebene personenbezogene Daten zu übergeben oder zu löschen. Es sei denn, dass er aufgrund gesetzlicher Vorschriften zur Aufbewahrung der personenbezogenen Daten verpflichtet ist. Der Auftragnehmer bestätigt dem Auftraggeber schriftlich die Löschung oder Sperrung der Daten.
e. Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich und vor Eintritt dieser Maßnahmen zu verständigen, damit die Daten des Auftraggebers rechtzeitig von den DV-Systemen des Auftragnehmers genommen werden können.
f. Insbesondere hat der Auftragnehmer ein internes Meldesystem vorzuhalten, dass dem Auftraggeber die Einhaltung der Meldefrist aus Art. 33 DSGVO bei Datenpannen ermöglicht.

2.4 Technische und organisatorische Maßnahmen

a. Der Auftraggeber legt unter Berücksichtigung der Art, des Umfangs, der Umstände und Zwecke der Datenverarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen gemeinsam mit dem Auftragnehmer die für die Datenverarbeitung geeigneten und nach dem Stand der Technik erforderlichen technischen und organisatorischen Maßnahmen fest. Das Ergebnis wird in Anlage 2 dokumentiert.

b. Der Auftragnehmer ist berechtigt und verpflichtet, die technischen und organisatorischen Maßnahmen dem jeweiligen Stand der Technik anzupassen. Eine Anpassung ist erforderlich, wenn eine Änderungsforderung des Auftraggebers auf einer Weisung oder Empfehlung einer für die Datenverarbeitung zuständigen Aufsichtsbehörde beruht.
c. Der Auftragnehmer garantiert, dass die Umsetzung der technisch-organisatorischen Maßnahmen gemäß Ziffer 2.4 und Anlage 2 den Anforderungen der DSGVO entspricht.

2.5 Unterauftragnehmer

a. Der Auftragnehmer ist verpflichtet, bei jedem Unterauftragnehmer sicherzustellen, dass sämtliche Pflichten aus dieser Vereinbarung an den Unterauftragnehmer auf vertraglicher Basis weitergegeben werden und der Unterauftragnehmer insbesondere geeignete technisch-organisatorische Maßnahmen gemäß Ziffer 2.4 gewährleisten kann.

2.6 Haftung

Auftraggeber und Auftragnehmer haften im Rahmen ihrer Verantwortlichkeiten gemäß den gesetzlichen Bestimmungen des Art. 82 DSGVO gegenüber Dritten für Schäden, die durch eine nicht der DSGVO entsprechenden Datenverarbeitung entstanden sind.

3 Schlussbestimmungen

Wenn und soweit Vorgaben der Aufsichtsbehörden und/oder zusätzliche gesetzliche Vorgaben die Änderung von Bestimmungen der DSV und/oder der zugehörigen Anlagen erforderlich machen, sind die Parteien verpflichtet, an der Umsetzung der Anforderungen und der Aufnahme in die DSV mitzuwirken. Vorgaben der für die vom Auftrag umfasste Datenverarbeitung zuständigen Aufsichtsbehörde oder einer sonstigen zuständigen offiziellen Stelle sind dabei als verbindlich zu betrachten.

Auftraggeber	Auftragnehmer
Datum:	Datum:
Name:	Name:
Funktion:	Funktion:
Unterschrift:	Unterschrift:

Übersicht Anlagen

Anlage	Inhalt
Anlage 1	Gegenstand der Datenverarbeitung
Anlage 2	Technische und organisatorische Maßnahmen

Anlage 1: Gegenstand der Datenverarbeitung

Gegenstand und Dauer der Datenverarbeitung sind wie folgt geplant:

Ergänzend wird auf die Leistungsbeschreibung des Hauptvertrags verwiesen.

Art und Zweck der Datenverarbeitung wie folgt geplant:

Ergänzend wird auf die Leistungsbeschreibung des Hauptvertrags verwiesen.

Die Datenverarbeitung umfasst die folgenden Arten personenbezogener Daten:

Die Verarbeitung umfasst die folgenden Kategorien betroffener Personen:

Anlage 2: Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, elektrische Türöffner;
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN);
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);