# Anlage Auftragsverarbeitung zu den Allgemeinen Geschäftsbedingungen

## 1 Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem zwischen den Parteien geschlossenen Vertrag (Allgemeinen Geschäftsbedingungen) ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte von customweb oder durch customweb Beauftragte personenbezogene Daten (nachfolgend „Daten“) des Vertragspartners verarbeiten. In der folgenden Anlage verstehen wir unter dem Auftraggeber den Kunden oder Vertragspartner von customweb. In den AGB teilweise auch als Kunde referenziert.

Alle Personenbezeichnungen beziehen sich auf Personen beider Geschlechter.

## 2 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Einzelheiten in Bezug auf die Dienstleistung von customweb sind in dem jeweiligen Vertrag zwischen customweb und dem Vertragspartner (nachfolgend „Vertrag“) geregelt.

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung, sofern in dieser Anlage nichts Abweichendes aufgeführt ist.

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

## 3 Anwendungsbereich und Verantwortlichkeit

customweb verarbeitet die in Anhang A genannten Daten im Auftrag des Auftraggebers zu dem dort genannten Zweck in dem genannten Umfang. Dies umfasst Tätigkeiten, die im Vertrag und in dieser Anlage konkretisiert sind.

Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmässigkeit der Datenweitergabe an customweb sowie für die Rechtmässigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO).

Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die von customweb bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform durch den Auftraggeber nachzuholen.

## 4 Zweck der Datenerhebung

customweb stellt dem Auftraggeber ein Zahlungsservice zur Verfügung, mit dem er transaktionsbezogene Daten, die er über seine E-Commerce-Seite oder anderen manuellen oder automatischen Verkaufssystemen (physischen Terminals / virtuellen Terminals) erhalten hat, empfangen, verwalten sowie an die Finanzdienstleister senden kann, die er für die Abwicklung der Zahlungen (Transaktionen) ausgewählt hat, sofern diese Auswahl verfügbar und mit dem Service des Auftragnehmers vereinbar ist.

Der Zweck der Verarbeitung von personenbezogenen Daten ist die Verarbeitung von transaktionsbezogenen Daten (wie z.B. aber nicht beschränkt auf Anfragen zur Autorisierung einer Zahlung) und allen ergänzenden oder verbundenen Aktivitäten, die für die Verarbeitung von transaktionsbezogenen Daten erforderlich sind.

Die Verarbeitung besteht darin, personenbezogene Daten mithilfe der vom Auftraggeber bestellten E-Commerce Plattform oder anderen manuellen oder automatischen Absatzssystemen (Terminals, virtual Terminals, etc) und der mit ihr über Netzwerkverbindungen und Standardprotokollen verbundenen Tools zu erfassen, zusammenzufassen, zu vergleichen, zu verschlüsseln, zu entschlüsseln, zu organisieren, zu prüfen, zu analysieren, zu kontrollieren,

zu registrieren, zu berechnen, wiederzugeben, zu erweitern, zu kopieren, zu duplizieren und sie an Subunternehmen, Finanzdienstleister oder andere (juristische oder natürliche) Personenweiterzuleiten, die an der Verarbeitung der Transaktionen beteiligt sind. Bei den personenbezogenen Daten, die Gegenstand dieser Verarbeitung sind, handelt es sich um Daten, die vom System des Auftraggebers an das System des Auftragnehmers verschlüsselt übermittelt wurden und bei der Verarbeitung der Transaktionen erfasst und verarbeitet worden sind. Zusätzlich werden im Zuge der Auftragsverarbeitung auch personenbezogene Daten von Beschäftigten des Auftraggebers verarbeitet.

## 5 Ort der Datenverarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschliesslich in einem Mitgliedsstaat der Europäischen Union oder in der Schweiz statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen des Art 44 ff. DSGVO erfüllt sind. Informationen bezüglich Ort der Datenverarbeitung bei Subunternehmer findet sich in der entsprechenden Auflistung.

## 6 Pflichten von customweb

1. customweb darf Daten von betroffenen Personen im Rahmen der genannten Zwecke verarbeiten; ausser es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. customweb informiert den Auftraggeber unverzüglich, wenn wir der der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstösst. customweb darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

2. customweb wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. customweb wird technische und organisatorische Massnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. customweb hat technische und organisatorische Massnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Massnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3. Die von customweb getroffenen Massnahmen werden in Anhang B näher beschrieben. Die technischen und organisatorischen Massnahmenunterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem customweb gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. customweb unterstützt soweit den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

5. customweb gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für customweb tätigen Personen untersagt ist, die Daten ausserhalb der Weisung zu verarbeiten. Ferner gewährleistet customweb, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

6. customweb unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. customweb trifft die erforderlichen Massnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

7. customweb nennt dem Auftraggeber den folgenden Ansprechpartner für im

Rahmen des Vertrages anfallende Datenschutzfragen: Anfragen sind zu richten an info@customweb.com

8. customweb gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmässigen Überprüfung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen. customweb berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt customweb die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber

9. customweb wird nach Beendigung des Vertrags und Erreichung der Zweckerfüllung personenbezogene Daten autoautomatisch löschen. Auf Verlangen des Auftraggebers sind personenbezogene Daten nach Vertragsende zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

10. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich customweb den Auftraggeber bei der Abwehr des Anspruches im Rahmen der vorliegenden und zumutbaren Möglichkeiten zu unterstützen.

11. Leistungen in dieser Ziffer sind customweb gemäss den aktuellen Stundensätzen bzw. externer Aufwände zu vergüten.

12. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht der Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

## 7 Pflichten des Auftraggebers

Der Auftraggeber ist für die Rechtmässigkeit seiner Anweisungen an customweb vollumfänglich verantwortlich. Insbesondere liegt es in der Verantwortung des Auftraggebers zu prüfen, ob die Integration eines Service / Dienstleistung / Produkt, welches customweb zur Verfügung stellt, keine Datenschutzbestimmungen verletzen. Zudem obliegen dem Auftraggeber folgende Pflichten:

1. Der Auftraggeber hat customweb unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmässigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt Ziffer 6 Absatz 10 entsprechend.

3. Der Auftraggeber nennt customweb den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen, sofern dieser von den durch den Auftraggeber bereits benannten Ansprechpartnern abweicht.

## 8 Anfrage betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an customweb, wird customweb die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist.

customweb leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. customweb unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart.

customweb haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht,

nicht richtig oder nicht fristgerecht beantwortet wird.

## 9 Nachweismöglichkeiten

customweb weist dem Auftraggeber die Einhaltung der in dieser Anlage niedergelegten Pflichten mit geeigneten Mitteln nach. Dies erfolgt durch einen Selbstaudit und/oder Zertifizierung gemäss PCI DSS.

Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. customweb darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Massnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu customweb stehen, hat customweb gegen diesen ein Einspruchsrecht.

Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoss nach dem Strafgesetzbuch strafbewehrt ist.

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann customweb einen Vergütungsanspruch geltend machen.

## 10 Subunternehmer

Die Beauftragung von Subunternehmern durch customweb ist zulässig, soweit diese im Umfang des Unterauftrags ihrerseits die Anforderungen der vorliegenden Anlage erfüllen. Eine Liste der aktuellen Subunternehmer ist hier abrufbar: https://wallee.com/de/subcontractor.html

Ausgenommen sind Nebenleistungen, die der customweb z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt

Der Auftraggeber stimmt zu, dass customweb Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert customweb den Auftraggeber. customweb ist verpflichtet den Auftraggeber über die Beauftragung eines Subunternehmers durch Aktualisierung der eben genannten Übersicht zu informieren. Die Übersicht ist jeweils mindestens 14 Tage vorab zu aktualisieren. Der Auftraggeber wird regelmässig die Übersicht einsehen. Der Auftraggeber kann der Änderung – innerhalb dieser 14 Tage – aus wichtigem Grund – gegenüber customweb widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird customweb ein Sonderkündigungsrecht eingeräumt.

Erteilt customweb Aufträge an Subunternehmer, so obliegt es customweb, seine datenschutzrechtlichen Pflichten aus dieser Anlage dem Subunternehmer zu übertragen. Subunternehmer, welche keinen Zugriff auf Kundendaten haben bzw. keine Bearbeitung von Kundendaten vornehmen, sind von diesem Kapitel ausgenommen und werden entsprechend nicht in der genannten Liste erscheinen.

## 11 Informationspflichten

Sollten die Daten des Auftraggebers bei customweb durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Massnahmen Dritter gefährdet werden, so hat customweb den Auftraggeber unverzüglich darüber zu informieren. customweb wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschliesslich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

## 12 Haftung

Die Haftung richtet sich nach dem Vertrag.

## 13 Sonstiges

Im Übrigen gelten die Regelungen des Vertrags. Bei etwaigen Widersprüchen zwischen Regelungen dieser Anlage und den Regelungen des Vertrages geht diese Anlage vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit des Vertrags und der Anlage im Übrigen nicht.

Die Anlagen sind wesentlicher Bestandteil dieses Vertrags.

# Anhang A zur Auftragsdatenverarbeitung

| | |
|---|---|
| Gegenstand des Auftrags | Verarbeitung von personenbezogenen Daten des Auftraggebers im Rahmen seiner Nutzung der Leistungen von customweb als Software as a Service. |
| Art und Zweck der vorgesehenen Verarbeitung von Daten | Die vom Auftraggeber verarbeiteten personenbezogenen Daten werden an customweb im Rahmen der Software as a Service Leistungen übertragen. customweb verarbeitet diese Daten ausschliesslich nach der getroffenen Vereinbarung respektive des gewählten Produktes.<br><br>Je nach ausgewählter Dienstleistung / Produkt überträgt customweb weitere Daten an diesen Dienstleister (bspw. Acquirer / Processor / etc.). Der Auftraggeber ist dafür verantwortlich, dass diese Übertragung keine Rechte seiner Kunden verletzt. |
| Art der personenbezogenen Daten | Gegenstand der Zusatzvereinbarung sind folgende Datenarten und -kategorien:<br><br>• Personenstammdaten<br>• Kommunikationsdaten (z.B. Telefon, E-Mail)<br>• Online-Kennung (IP-Adresse, Cookie)<br>• Zahlungsdaten (Details zu getätigten Bestellungen und Zahlungen)<br>• Vertragsstammdaten (Vertragsbeziehung, Bestelldaten, Produkt- bzw. Vertragsinteresse)<br>• Auskunftsangaben (z.B. Bonitätsprüfung über Zahlungsanbieter)<br>• Nutzerverhalten |
| Kategorien betroffener Personen | Der Kreis der durch diese Zusatzvereinbarung Betroffenen umfasst:<br><br>• Kunden und Interessenten des Auftraggebers<br>• Mitarbeiter und Lieferanten des Auftraggebers |
| Löschung, Sperrung und Berichtigung von Daten | Anfragen zur Löschung, Sperrung und Berichtigung sind an den Auftraggeber zu richten; im Übrigen gelten die Regelungen des Vertrages. |

# Anhang B zur Auftragsdatenverarbeitung

Technische und organisatorische Massnahmen gemäss Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO

## 1 Zutrittskontrolle

Es findet eine Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen) statt. Dies umfasst die folgenden Massnahmen:

- Schlüssel / Schlüsselvergabe
- Türsicherung (elektrische Türöffner usw.)
- Die Zugänge zu den verarbeitenden Servern und Computern werden gemäss Vorgaben von PCI DSS geschützt (Kapitel 9) vgl. auch https://aws.amazon.com/de/compliance/data-center/controls.
- Protokollierung des Zutritts

## 2 Zugangskontrolle

Es findet eine Zugangskontrolle (keine unbefugte Systembenutzung) statt. Dies umfasst die folgenden Massnahmen:

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmässiger Wechsel des Kennworts)
- Zwei-Faktor-Authentifizierung wird eingesetzt
- Automatische Sperrung (z.B. Pausenschaltung)
- Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk

## 3 Zugriffskontrolle

Es findet eine Zugriffskontrolle statt. Dies umfasst die folgenden Massnahmen:

- Erstellen eines Berechtigungskonzepts
- Umsetzen von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Protokollierung des Datenzugriffs

## 4 Transport und Weitergabekontrolle

Es findet eine Transport- und Weitergabekontrolle statt. Dies umfasst die folgenden Massnahmen:

- Sichere Datenübertragung zwischen Server und Client
- Sicherung der Übertragung im Backend
- Sicherung der Übertragung zu externen Systemen
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Härtung der Backendsysteme
- Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
- Maschine-Maschine Authentisierung
- Datenträgerverwaltung (Verfahren)

- Prozess zur Sammlung und Entsorgung
- Datenschutzgerechtes Lösch-/ Zerstörungsverfahren

## 5 Eingabekontrolle

Es findet eine Eingabekontrolle statt. Dies umfasst die folgenden Massnahmen:

- Dokumentation der Eingabeberechtigungen
- Protokollierung der Eingaben

## 6 Auftragskontrolle

- Dokumentation der Eingabeberechtigungen
- Protokollierung der Eingaben

## 7 Verfügbarkeitskontrolle:

Es findet eine Verfügbarkeitskontrolle statt. Dies umfasst die folgenden Massnahmen:

- Backup-Konzept
- Notfallplan
- Aufbewahrung der Backups
- Prüfung der Notfalleinrichtungen
- Virenschutz / Firewall

## 8 Trennungskontrolle

Es findet eine Trennungskontrolle / Verwendungszweckkontrolle (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden) statt. Dies umfasst die folgenden Massnahmen:

- Interne Mandantenfähigkeit" ist hergestellt
- Kontrolle der Zweckbindung
- Funktionstrennung: Production, Staging, Testing
- Getrennte Verarbeitung