CATMEDIA eBusiness · Auf die Ziegelhütte 11 · 66763 Dillingen/Saar
06831 7640781 · helpdesk@cat.media · catmedia.de

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

Name / Firma des Auftraggebers

Straße, PLZ, Ort

– nachfolgend „Auftraggeber“ oder „Verantwortlicher“ –

und

CATMEDIA eBusiness, Anita Becker
Auf die Ziegelhütte 11, 66763 Dillingen
– nachfolgend „Auftragnehmer“ oder „Auftragsverarbeiter“ –

gemeinsam „Parteien“ genannt.

1. Gegenstand und Zweck der Vereinbarung

Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO).

Der Auftragnehmer erbringt für den Auftraggeber Leistungen in den Bereichen IT, E-Business, Webhosting, Managed Hosting, Onlineshops, JTL-Shop, JTL-Wawi, Softwarebetreuung, Wartung, technische Administration, Support, Beratung, Datensicherung, Systempflege und damit zusammenhängende Dienstleistungen.

Soweit der Auftragnehmer im Rahmen dieser Leistungen Zugriff auf personenbezogene Daten erhält oder diese im Auftrag des Auftraggebers verarbeitet, erfolgt die Verarbeitung ausschließlich auf Grundlage dieser Vereinbarung und der dokumentierten Weisungen des Auftraggebers.

2. Art und Zweck der Verarbeitung

Die Verarbeitung erfolgt insbesondere zur Bereitstellung, Wartung, Pflege, Sicherung und Betreuung von IT-Systemen, Webservern, Onlineshops, Datenbanken, Warenwirtschaftssystemen, Kommunikationssystemen und sonstigen digitalen Anwendungen des Auftraggebers.

Hierzu können insbesondere folgende Tätigkeiten gehören:

- technisches Hosting und Serverbetrieb
- Einrichtung, Wartung und Administration von Webservern, Shopsystemen und Datenbanken
- Betreuung von JTL-Shop, JTL-Wawi und angeschlossenen Systemen
- Fehleranalyse, Support und Fernwartung
- Installation von Updates, Sicherheitskorrekturen und Erweiterungen
- Einrichtung und Betreuung von Schnittstellen
- Datensicherung und Wiederherstellung
- technische Protokollierung und Sicherheitsüberwachung
- Migration, Import, Export oder Konvertierung von Daten
- Unterstützung bei technischen oder organisatorischen Problemen

3. Dauer der Verarbeitung

Die Verarbeitung beginnt mit Beauftragung des Auftragnehmers und dauert so lange an, wie der Auftragnehmer Leistungen für den Auftraggeber erbringt oder Zugriff auf personenbezogene Daten des Auftraggebers hat.

Diese Vereinbarung gilt für die Dauer des Hauptvertrages oder der jeweiligen Einzelbeauftragung. Gesetzliche Aufbewahrungspflichten und Nachweispflichten bleiben unberührt.

4. Art der personenbezogenen Daten

Je nach beauftragter Leistung können insbesondere folgende Kategorien personenbezogener Daten verarbeitet werden:

- Stammdaten, z. B. Name, Anschrift, Kundennummer
- Kontaktdaten, z. B. E-Mail-Adresse, Telefonnummer
- Vertrags- und Bestelldaten
- Rechnungs- und Zahlungsdaten
- Liefer- und Versanddaten
- Zugangsdaten, soweit technisch erforderlich
- Kommunikationsdaten, z. B. E-Mails, Supportanfragen, Tickets
- Nutzungs-, Log- und Protokolldaten
- IP-Adressen und technische Identifikatoren
- Daten aus Shopsystemen, Warenwirtschaft, CRM, CMS oder Datenbanken
- sonstige vom Auftraggeber bereitgestellte oder in dessen Systemen gespeicherte Daten

Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO werden nur verarbeitet, wenn dies ausdrücklich beauftragt wurde oder sich aus den vom Auftraggeber bereitgestellten Systemen ergibt.

5. Kategorien betroffener Personen

Die Verarbeitung kann Daten folgender Personengruppen betreffen:

- Kunden und Interessenten des Auftraggebers
- Lieferanten und Geschäftspartner des Auftraggebers
- Beschäftigte, Ansprechpartner und Dienstleister des Auftraggebers
- Nutzer von Webseiten, Onlineshops oder Portalen
- Empfänger von E-Mails, Newslettern oder Systemnachrichten
- sonstige Personen, deren Daten in den Systemen des Auftraggebers verarbeitet werden

6. Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern keine gesetzliche Verpflichtung zur Verarbeitung besteht.

Weisungen können sich aus dem Hauptvertrag, Einzelaufträgen, Supportanfragen, Tickets, schriftlichen Mitteilungen oder sonstigen dokumentierten Freigaben ergeben.

Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, weist er den Auftraggeber darauf hin. Die Ausführung der betreffenden Weisung kann bis zur Bestätigung oder Änderung der Weisung ausgesetzt werden.

7. Vertraulichkeit

Der Auftragnehmer verpflichtet alle Personen, die Zugriff auf personenbezogene Daten des Auftraggebers erhalten können, zur Vertraulichkeit, soweit diese nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Zugriff auf personenbezogene Daten wird nur solchen Personen ermöglicht, die diesen Zugriff zur Erfüllung der beauftragten Leistungen benötigen.

8. Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Dazu gehören insbesondere Maßnahmen zur:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungskontrolle
- Sicherung, Wiederherstellung und Protokollierung
- regelmäßigen Prüfung und Bewertung der Wirksamkeit der Maßnahmen

Die konkreten Maßnahmen ergeben sich aus Anlage 2 dieser Vereinbarung. Der Auftragnehmer darf die Maßnahmen technisch weiterentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

9. Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren bei der Erfüllung datenschutzrechtlicher Pflichten, soweit dies die beauftragte Verarbeitung betrifft.

Dies betrifft insbesondere:

- Auskunfts-, Berichtigungs-, Löschungs- und Einschränkungsersuchen betroffener Personen
- Datenübertragbarkeit, soweit technisch möglich
- Nachweis- und Dokumentationspflichten
- Datenschutz-Folgenabschätzungen, soweit erforderlich
- Meldungen von Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn ihm im Zusammenhang mit der Verarbeitung eine Verletzung des Schutzes personenbezogener Daten bekannt wird.

10. Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, die Einhaltung dieser Vereinbarung und der technischen und organisatorischen Maßnahmen zu prüfen oder prüfen zu lassen.

Kontrollen sind mit angemessener Frist anzukündigen und so durchzuführen, dass Betriebsabläufe, Sicherheitsinteressen und Rechte Dritter nicht unangemessen beeinträchtigt werden.

Der Auftragnehmer kann geeignete Nachweise, Dokumentationen, Zertifikate oder Selbstauskünfte bereitstellen. Vor-Ort-Prüfungen erfolgen nur, soweit diese erforderlich und angemessen sind.

11. Unterauftragsverarbeiter

Der Auftragnehmer darf Unterauftragsverarbeiter einsetzen, soweit diese zur Leistungserbringung erforderlich sind und ein angemessenes Datenschutzniveau gewährleistet ist.

Mit Unterauftragsverarbeitern werden Vereinbarungen geschlossen, die im Wesentlichen denselben Datenschutzpflichten entsprechen, die für den Auftragnehmer gegenüber dem Auftraggeber gelten.

Der Auftragnehmer informiert den Auftraggeber über eingesetzte Unterauftragsverarbeiter gemäß Anlage 3. Änderungen bei Unterauftragsverarbeitern werden dem Auftraggeber in geeigneter Weise mitgeteilt. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.

12. Drittlandübermittlungen

Eine Übermittlung personenbezogener Daten in ein Drittland außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen der DSGVO erfüllt sind.

Soweit Dienste oder Unterauftragsverarbeiter mit Drittlandbezug eingesetzt werden, stellt der Auftragnehmer sicher, dass geeignete Garantien bestehen, z. B. Angemessenheitsbeschluss, EU-Standardvertragsklauseln oder andere zulässige Mechanismen.

13. Löschung und Rückgabe von Daten

Nach Abschluss der beauftragten Leistungen löscht oder gibt der Auftragnehmer personenbezogene Daten nach Wahl des Auftraggebers zurück, sofern keine gesetzliche Pflicht zur weiteren Speicherung besteht.

Datensicherungen können technisch bedingt für einen begrenzten Zeitraum weiterbestehen. Sie werden nicht produktiv genutzt und nach Ablauf der jeweiligen Sicherungszyklen gelöscht oder überschrieben.

14. Berichtigung, Sperrung und Löschung

Soweit der Auftraggeber die Berichtigung, Sperrung, Einschränkung oder Löschung personenbezogener Daten verlangt, unterstützt der Auftragnehmer dies im Rahmen der technischen Möglichkeiten und der beauftragten Leistungen.

Eigenständige Änderungen an personenbezogenen Daten nimmt der Auftragnehmer nur auf Weisung des Auftraggebers vor, soweit keine gesetzliche Verpflichtung besteht.

15. Pflichten des Auftraggebers

Der Auftraggeber bleibt Verantwortlicher im Sinne der DSGVO. Er ist insbesondere verantwortlich für:

- die Rechtmäßigkeit der Verarbeitung
- die Rechtsgrundlagen der Datenerhebung und Datenverarbeitung
- die Information betroffener Personen
- die Wahrung der Betroffenenrechte
- die Zulässigkeit der an den Auftragnehmer übermittelten Daten
- die Erteilung rechtmäßiger Weisungen

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

16. Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich insbesondere:

- personenbezogene Daten nur im Rahmen dokumentierter Weisungen zu verarbeiten

- die Vertraulichkeit zu wahren
- geeignete technische und organisatorische Maßnahmen umzusetzen
- den Auftraggeber bei datenschutzrechtlichen Pflichten zu unterstützen
- festgestellte Datenschutzvorfälle unverzüglich mitzuteilen
- Unterauftragsverarbeiter nur unter Beachtung dieser Vereinbarung einzusetzen
- Kontroll- und Nachweispflichten angemessen zu unterstützen
- Daten nach Ende der Verarbeitung zurückzugeben oder zu löschen

17. Haftung

Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften sowie den Regelungen des Hauptvertrages, soweit diese mit den Vorgaben der DSGVO vereinbar sind.

Diese Vereinbarung begründet keine weitergehende Haftung, soweit nicht ausdrücklich etwas anderes vereinbart wurde.

18. Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform, soweit keine strengere Form gesetzlich vorgeschrieben ist.

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Es gilt deutsches Recht, soweit keine zwingenden datenschutzrechtlichen Vorschriften entgegenstehen.

Anlage 1 – Beschreibung der Verarbeitung

Gegenstand der Verarbeitung: Technische Betreuung, Wartung, Administration, Hosting, Support und Weiterentwicklung von IT-Systemen, Webservern, Onlineshops, Warenwirtschaftssystemen, Datenbanken und verbundenen Anwendungen des Auftraggebers.

Zweck der Verarbeitung: Erbringung der beauftragten IT-, Hosting-, Support-, Wartungs-, Beratungs- und Entwicklungsleistungen.

Art der Verarbeitung: Erheben, Erfassen, Ordnen, Speichern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Abgleichen, Einschränken, Löschen, Vernichten sowie sonstige technische Verarbeitungsvorgänge, soweit zur Leistungserbringung erforderlich.

Dauer: Für die Dauer des Hauptvertrages oder der Einzelbeauftragung sowie im Rahmen gesetzlicher Aufbewahrungs- und Nachweispflichten.

Anlage 2 – Technische und organisatorische Maßnahmen

1. Zutrittskontrolle

Maßnahmen zum Schutz der Betriebsräume, Serverräume und technischen Einrichtungen vor unbefugtem Zutritt.

2. Zugangskontrolle

Verwendung individueller Benutzerkennungen, sicherer Passwörter, rollenbasierter Zugriffe und, soweit möglich, zusätzlicher Authentifizierungsverfahren.

3. Zugriffskontrolle

Beschränkung des Zugriffs auf personenbezogene Daten auf berechtigte Personen und erforderliche Zwecke.

4. Weitergabekontrolle

Schutz personenbezogener Daten bei Übertragung, Transport und Kommunikation, insbesondere durch Verschlüsselung, sichere Verbindungen und geregelte Kommunikationswege.

5. Eingabekontrolle

Nachvollziehbarkeit relevanter administrativer Tätigkeiten durch Protokollierung, soweit technisch möglich und angemessen.

6. Auftragskontrolle

Verarbeitung personenbezogener Daten ausschließlich nach Weisung des Auftraggebers und auf Grundlage dieser Vereinbarung.

7. Verfügbarkeitskontrolle

Maßnahmen zur Sicherung der Verfügbarkeit, insbesondere Datensicherung, Systemüberwachung, Schutz vor Schadsoftware, Sicherheitsupdates und Wiederherstellungsmöglichkeiten.

8. Trennungskontrolle

Trennung von Daten unterschiedlicher Auftraggeber, Systeme und Zwecke durch technische und organisatorische Maßnahmen.

Anlage 3 – Unterauftragsverarbeiter

Der Auftragnehmer kann je nach beauftragter Leistung insbesondere folgende Kategorien von Unterauftragsverarbeitern einsetzen:

- Rechenzentrums- und Hostinganbieter
- Domain- und DNS-Dienstleister
- E-Mail- und Kommunikationsdienstleister
- Software- und Wartungsdienstleister
- Backup- und Sicherheitsdienstleister
- Zahlungs-, Versand- oder Schnittstellendienstleister, soweit vom Auftraggeber beauftragt oder freigegeben

Ort, Datum	Ort, Datum
Auftraggeber (Unterschrift, Name in Druckschrift)	Auftragnehmer – CATMEDIA eBusiness