Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO – Digitaler Abschluss

Kraft Fabrik Media Ltd.
Geschäftsführende Gesellschafter: Natalia Dziadus-Hammerschmied, Alexander Hammerschmied
Kountourioti 6, Coral Elite Residences Building 1
8560 Peyia, Cyprus
(nachfolgend „Auftragnehmer“ genannt)

Dieser Vertrag regelt die Auftragsverarbeitung personenbezogener Daten im Rahmen der von hartmut.io angebotenen Hosting-Dienste für Managed-Mautic und WooCommerce. Der Vertrag kommt automatisch zustande, sobald der Kunde die Allgemeinen Geschäftsbedingungen (AGB) inklusive dieses Auftragsverarbeitungsvertrages digital (z. B. per Checkbox beim Checkout) bestätigt. Eine separate Unterschrift oder individuelle Kundeneingaben in diesem Dokument sind nicht erforderlich.

1. Gegenstand, Grundsätzliches und Dauer der Vereinbarung

1. Der Auftragnehmer erbringt seine Hosting- und Managed-Dienstleistungen im Rahmen des Hauptvertrages, den der Kunde über die hartmut.io-Plattform abschließt. Soweit dabei personenbezogene Daten im Auftrag des Kunden verarbeitet werden, erfolgt dies „auf Weisung“ des Kunden – ohne eigene Zwecke des Auftragnehmers.
2. Die konkreten Auftragsverarbeitungsleistungen ergeben sich aus den vom Kunden gewählten Tarif- bzw. Produktparametern – sowohl für Managed-Mautic als auch für WooCommerce – sowie aus den jeweils gültigen Leistungsbeschreibungen. Diese werden in Anlage 1 („Individuelle Vertragsbestandteile“) näher konkretisiert.
3. Dieser Vertrag tritt mit der erstmaligen Bestätigung der AGB (inklusive dieses Vertrages) in Kraft und gilt für die Dauer der vertraglich vereinbarten Leistungen. Eine separate Kündigung des Auftragsverarbeitungsvertrages ist möglich, wenn ein schwerwiegender Verstoß gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Der Kunde bestimmt allein Art, Umfang und Zweck der Verarbeitung personenbezogener Daten auf der von hartmut.io bereitgestellten technischen Plattform. Dies gilt sowohl für die Managed-Mautic- als auch für die WooCommerce-Hosting-Dienste. Die konkreten Verarbeitungszwecke, Datenarten und betroffenen Personenkategorien ergeben sich aus Anlage 1.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Kunden

1. Für die Zulässigkeit der Datenverarbeitung sowie die Wahrung der Rechte der betroffenen Personen ist ausschließlich der Kunde verantwortlich.
2. Der Kunde erteilt sämtliche Weisungen zur Verarbeitung personenbezogener Daten in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich zu bestätigen.
3. Der Auftragnehmer verpflichtet sich, alle Weisungen des Kunden strikt zu befolgen, soweit nicht zwingende gesetzliche Vorgaben entgegenstehen.

4. Weisungsberechtigte des Kunden

Die weisungsberechtigten Vertreter des Kunden werden in Anlage 1 aufgeführt. Änderungen in den Ansprechpartnern sind dem Auftragnehmer unverzüglich schriftlich oder elektronisch mitzuteilen.

5. Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet die ihm vom Kunden überlassenen personenbezogenen Daten ausschließlich nach dessen Weisung und für keine eigenen Zwecke.
2. Es werden keine Kopien oder Duplikate der Daten erstellt, die nicht zur vertragsgemäßen Leistungserbringung erforderlich sind.
3. Der Auftragnehmer gewährleistet die getrennte Verarbeitung der Kundendaten von anderen Datenbeständen und ergreift alle zumutbaren technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO.
4. Die Mitarbeiter des Auftragnehmers werden vor Aufnahme ihrer Tätigkeit in Bezug auf den Datenschutz geschult und zur Verschwiegenheit verpflichtet.

6. Mitteilungspflichten bei Störungen und Datenschutzverletzungen

Der Auftragnehmer informiert den Kunden unverzüglich, sofern es zu einer Verletzung des Schutzes personenbezogener Daten kommt, und unterstützt den Kunden bei der Erfüllung seiner Meldepflichten nach Art. 33 und 34 DSGVO.

7. Unterauftragsverhältnisse

1. Der Einsatz von Subunternehmern erfolgt ausschließlich auf Grundlage der in Anlage 1 genannten Dienstleister. Eine Übermittlung von Daten in Drittländer erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. mittels Standarddatenschutzklauseln).
2. Der Auftragnehmer haftet für die Einhaltung der datenschutzrechtlichen Vorgaben auch bei Einsatz von Subunternehmern.

8. Technische und organisatorische Maßnahmen

1. Die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen bilden das Datenschutzkonzept des Auftragnehmers und gewährleisten ein dem Risiko angemessenes Schutzniveau. Diese Maßnahmen werden regelmäßig überprüft und an den Stand der Technik angepasst.
2. Sollte der Kunde ergänzende oder abweichende Anforderungen haben, informiert der Auftragnehmer den Kunden umgehend.
3. Der Kunde ist selbst verantwortlich für zusätzliche Maßnahmen, die im Rahmen seiner Datenverarbeitung erforderlich sind (z. B. SSL-Verschlüsselung auf eigenen Webseiten).

9. Verpflichtungen nach Beendigung des Auftrags

Nach Abschluss der vertraglichen Leistungen werden alle im Rahmen der Auftragsverarbeitung erstellten Daten, Unterlagen und Verarbeitungsergebnisse – sofern nicht gesetzlich anderweitig vorgeschrieben – durch den Auftragnehmer datenschutzgerecht gelöscht oder vernichtet.

10. Vergütung

Die Vergütung der Auftragsverarbeitungsleistungen ist in den jeweiligen Tarif- bzw. Produktbeschreibungen geregelt. Bei speziellen Weisungen, die zu einem Mehraufwand führen, wird eine gesonderte Vergütung vereinbart.

11. Haftung

Für Ansprüche aus der Verarbeitung personenbezogener Daten gilt Art. 82 DSGVO. Weitergehende Haftungsregelungen ergeben sich aus dem Hauptvertrag sowie den anwendbaren gesetzlichen Bestimmungen.

12. Sonstiges

1. Änderungen dieses Vertrages erfolgen durch Mitteilung in einem dokumentierten elektronischen Format.
2. Sollte eine Bestimmung dieses Vertrages unwirksam sein, so bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
3. Dieser Vertrag unterliegt zypriotischem Recht.
4. Mit der erstmaligen Bestätigung der AGB erklärt der Kunde ausdrücklich, dass er auch diesen Auftragsverarbeitungsvertrag in der jeweils aktuellen Fassung akzeptiert.
5. Die aktuelle Version dieses Vertrages ist jederzeit auf der Website von hartmut.io abrufbar.

Hinweis zum digitalen Abschluss: Durch die Aktivierung der Checkbox im Checkout bzw. die Bestätigung der AGB erklärt der Kunde, dass er diesen Auftragsverarbeitungsvertrag zur Kenntnis genommen und akzeptiert hat. Eine separate Unterschrift oder Eingabe individueller Kundendaten ist nicht erforderlich.

Anlagen

Die folgenden Anlagen sind integraler Bestandteil dieses Vertrages.

Anlage 1 – Individuelle Vertragsbestandteile

Individuelle Vertragsbestandteile zum Auftragsverarbeitungsvertrag:

1. Vereinbarte Auftragsverarbeitungsleistungen:
    - Der Gegenstand der Auftragsverarbeitung ergibt sich aus den Tarifinhalten des vom Kunden gewählten Managed-Mautic- und WooCommerce-Tarifs (Hauptvertrag) sowie aus den zugrunde liegenden Allgemeinen Geschäftsbedingungen.
    - Neben der regelmäßigen Prüfung und Wartung der Speichermedien erfolgen Zugriffe des Auftragnehmers auf (ggf. personenbezogene) Daten des Kunden im Rahmen von technischen Hilfestellungen (Supportleistungen), insbesondere bei Weisungen zur Löschung oder Sicherung von Daten.
    - Der Auftragnehmer stellt dem Kunden die technische Umgebung (Mautic-Instanz und WooCommerce-Umgebung) zur Verfügung.
    - Der Kunde ist als Verarbeiter der ihm überlassenen Daten selbst verantwortlich für die konkrete Datenverarbeitung und muss hierfür geeignete technische und organisatorische Maßnahmen (z. B. Double-Opt-In, SSL-Zertifikate) treffen.
2. Art der Verarbeitung:
    - Die Art der Verarbeitung personenbezogener Daten wird durch den Kunden bestimmt.
    - Abhängig von der Nutzung der Mautic-Instanz bzw. WooCommerce-Umgebung können u. a. folgende Verarbeitungsarten auftreten:
        - Speicherung und Löschung von Daten
        - Anbindung der Daten an das Internet
        - Sendung von Massen-E-Mails bzw. shopbezogene Kommunikationsprozesse
3. Zweck der Verarbeitung:
    - Der Zweck der Verarbeitung personenbezogener Daten wird vom Kunden festgelegt.
    - Dieser umfasst u. a.:
        - Veröffentlichung von Webseiten und Online-Shops
        - Datenhaltung in Datenbanken
        - Nutzung von E-Mail-Funktionalitäten und Shop-Kommunikation
4. Art der verarbeiteten personenbezogenen Daten:
    - Der Kunde bestimmt, welche Daten verarbeitet werden.
    - Typische Datenarten sind:
        - Protokolldateien (Server-Logfiles)
        - Online-Kennungen, E-Mail-Adressen
        - Bestands-, Nutzungs-, Rechnungs- und Inhaltsdaten von Webseiten- bzw. Shop-Besuchern und Datenbanknutzern
5. Kategorien betroffener Personen:

    - Der Kunde legt fest, welche Personengruppen von der Datenverarbeitung betroffen sind, z. B.:
        - Webseiten- bzw. Shopbesucher
        - Datenbanknutzer
        - E-Mail-Empfänger
6. Weisungsberechtigte:
    - Die weisungsberechtigten Vertreter des Kunden werden in internen Prozessen bestimmt.
    - Änderungen der Ansprechpartner sind dem Auftragnehmer unverzüglich mitzuteilen.

Anlage 2 – Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO:

1. Allgemeines: Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie des Risikos für die Rechte und Freiheiten betroffener Personen alle erforderlichen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
2. Zutrittskontrolle:
    - Physischer Schutz der Rechenzentren (in Deutschland, z. B. Nürnberg und Falkenstein)
    - Elektronische Zutrittskontrollsysteme, Überwachung und Begleitung von Besuchern
    - Einsatz von Videokameras und Anwesenheitslisten
3. Zugangskontrolle:
    - Zugang zu Datenverarbeitungssystemen nur per Authentifizierung (Benutzername/Passwort)
    - Berechtigungskonzepte mit abgestuften Zugriffsrechten
4. Datenträgerkontrolle:
    - Zugriffe auf Datenträger erfolgen ausschließlich durch autorisiertes Personal
    - Trennung von Test- und Produktionsumgebungen
    - Verschlüsselung von Daten auf Festplatten, sofern erforderlich
5. Speicherkontrolle:
    - Der Zugang zum Kundenspeicher erfolgt über gesicherte, externe Zugänge (z. B. via Internet mit Anmeldung)
    - Der Kunde trägt die Verantwortung für die Verhinderung unbefugter Eingaben in seinen Datenbereich
6. Benutzerkontrolle:
    - Einsatz von Verschlüsselungsverfahren bei Datenübertragungen
    - Schulung der Mitarbeiter im Umgang mit personenbezogenen Daten
    - Der Kunde ist für die Kontrolle von Zugriffsrechten in seinem Speicher verantwortlich
7. Übertragungskontrolle:
    - Dokumentation aller Übermittlungen personenbezogener Daten auf Weisung des Kunden

    - Schutz der Datenübertragung (z. B. mittels SSL/TLS)
8. Zugriffskontrolle (erneut):
    - Sicherstellung, dass nur berechtigte Personen Zugang zu den Daten haben
    - Der Kunde ist für die Vergabe von Zugriffsrechten auf seinen Daten verantwortlich
9. Eingabekontrolle:
    - Protokollierung von Eingaben und Änderungen (zeitliche Dokumentation, ggf. Mitarbeiterkennung)
    - Maßnahmen zur Protokollierung im Rahmen der Weisungsbearbeitung
10. Transportkontrolle:
    - Sicherstellung der Vertraulichkeit bei Datenübermittlungen (z. B. durch SSL/TLS)
    - Einsatz von zertifizierten Entsorgungsdienstleistern bei der Datenträgerentsorgung
11. Pseudonymisierung:
    - Der Kunde ist, soweit gesetzlich erforderlich, selbst für die Pseudonymisierung der Daten verantwortlich
12. Klassifikationsschema für Daten:
    - Einstufung der Daten nach Schutzbedarf (z. B. geheim, vertraulich, intern, öffentlich)
13. Datenintegrität:
    - Regelmäßige Anfertigung von Sicherheitskopien (Backups)
    - Einsatz von Reparaturstrategien, Prüfsummen, elektronischen Siegeln und Monitoring zur Überprüfung der Systemintegrität
14. Verfügbarkeitskontrolle:
    - Redundante Stromversorgung (USV, Dieselaggregate) in den Rechenzentren
    - Überwachung von Temperatur, Feuchtigkeit sowie Brand- und Frühwarnsystemen
15. Wiederherstellbarkeit:
    - Regelmäßige Datensicherungen und dokumentierte Wiederherstellungsverfahren
    - Der Kunde ist zudem angehalten, eigene Backup-Maßnahmen zu ergreifen
16. Trennbarkeit:
    - Getrennte Verarbeitung und Lagerung von Daten unterschiedlicher Verarbeitungszwecke
    - Einrichtung abgestufter Zugriffsrechte
17. Zuverlässigkeit:
    - 24/7-Monitoring der IT-Systeme zur Früherkennung von Fehlfunktionen
    - Meldung von Systemausfällen an zuständiges Personal
18. Auftragskontrolle:
    - Kennzeichnung des Auftragsverarbeitungs-Status in der Kundenmaske
    - Standardisierte Prozesse zur Gewährleistung der Einhaltung von Weisungen
19. Prüfung, Bewertung und Evaluierung:
    - Regelmäßige interne und externe Überprüfungen der technischen und organisatorischen Maßnahmen
    - Fortlaufende Schulungen der Mitarbeiter im Datenschutz

Zusätzliche Maßnahmen für die Dienste „Managed Mautic“ und „WooCommerce“:

- Anmeldesicherheit: Einrichtung von SAML SSO Regeln (für Mautic) sowie vergleichbaren Sicherheitsvorkehrungen für WooCommerce.
- Datensicherungen und Backups: Tägliche automatische Datensicherung, separater Aufbewahrungsort (z. B. Amazon S3)
- Passwortkomplexität: Empfehlung zur Verwendung starker Passwörter (mindestens 12 Zeichen, Groß-/Kleinbuchstaben, Sonderzeichen)
- 2-Faktor Authentifizierung: Aktivierung für alle Benutzer
- Automatischer Logout: Abmeldung nach definierten Inaktivitätszeiten
- Disaster Recovery: Vorhandener und regelmäßig getesteter Notfallplan
- Zugriffsversuche: Protokollierung aller Zugriffe und Versuche auf die IT-Systeme