Auftragsverarbeitungsvertrag
Marketing Machine GmbH

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Präambel

Dieser AVV ist gemäß § 8 der Allgemeinen Geschäftsbedingungen der Marketing Machine GmbH (Stand: 01. März 2026) Bestandteil aller Verträge, in deren Rahmen der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet. Er wird nicht gesondert unterzeichnet. Mit Unterzeichnung des jeweiligen Hauptvertrages akzeptiert der Auftraggeber gleichzeitig die Geltung dieser AVV.

Der Auftraggeber beauftragt den Auftragnehmer mit Marketingberatungs- und CRM-Dienstleistungen gemäß dem zwischen den Parteien geschlossenen Hauptvertrag. Im Rahmen dieser Tätigkeit verarbeitet der Auftragnehmer personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers. Dieser AVV regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien im Einklang mit Art. 28 DSGVO.

Der Auftragnehmer ist als Auftragsverarbeiter tätig. Er übernimmt keine eigenständige Verantwortung für die Verarbeitungszwecke oder -mittel und verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers.

§ 1 – Gegenstand und Dauer

Gegenstand der Auftragsverarbeitung ist die Unterstützung des Auftraggebers bei Marketingberatung und CRM-Dienstleistungen gemäß dem zugrundeliegenden Hauptvertrag. Der Auftragnehmer verarbeitet hierzu personenbezogene Daten des Auftraggebers ausschließlich auf dessen dokumentierte Weisung.

Die Laufzeit dieses AVV entspricht der Laufzeit des Hauptvertrages. Eine Kündigung des Hauptvertrages beendet auch diesen AVV, unbeschadet weitergehender Pflichten gemäß § 7 (Löschung und Rückgabe).

§ 2 – Art und Zweck der Verarbeitung

Art der Verarbeitung: Erheben, Speichern, Lesen, Analysieren, Strukturieren, Verändern, Abfragen im Rahmen von CRM- und Marketingprojekten des Auftraggebers.

Zweck der Verarbeitung: Unterstützung des Auftraggebers bei der Konzeption, Implementierung und Optimierung von CRM-Strategien, Marketing-Automation und datengetriebenem Marketing.

Die Verarbeitung erfolgt ausschließlich in den Systemen des Auftraggebers (CRM, Marketing-Automation-Plattformen). Der Auftragnehmer betreibt keine eigene CRM-Infrastruktur für Kundendaten. Drittlandtransfers durch den Systembetreiber liegen in der Verantwortung des Auftraggebers.

§ 3 – Art der personenbezogenen Daten und Kategorien betroffener Personen

3.1 Kategorien personenbezogener Daten

- Kontaktdaten: Name, E-Mail-Adresse, Telefonnummer
- CRM-Daten: Kaufhistorie, Kundensegmente, Scores, Lebenszyklusstatus
- E-Mail-Marketing-Daten: Öffnungsraten, Klickverhalten, Abmeldestatus
- Websitedaten / Tracking: Cookie-IDs, Session-IDs, Interaktionsdaten

3.2 Kategorien betroffener Personen

- Kunden und Interessenten des Auftraggebers
- Abonnenten von Newslettern und Marketingkommunikation des Auftraggebers
- Websitebesucher des Auftraggebers

§ 4 – Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch Rechtsvorschriften der Union oder der Mitgliedstaaten zu einer anderweitigen Verarbeitung verpflichtet. In diesem Fall teilt der Auftragnehmer dem Auftraggeber die entsprechenden rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragnehmer stellt sicher, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit

verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Auftragnehmer unterstützt den Auftraggeber soweit möglich durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung seiner Pflichten gemäß Art. 32–36 DSGVO (Sicherheit der Verarbeitung, Meldepflichten, Datenschutz-Folgenabschätzung, vorherige Konsultation).

Der Auftragnehmer unterstützt den Auftraggeber bei der Beantwortung von Anfragen betroffener Personen zur Ausübung ihrer Rechte gemäß Kapitel III DSGVO (insb. Auskunft, Berichtigung, Löschung). Eingehende Anfragen betroffener Personen leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Ansicht ist, dass eine Weisung des Auftraggebers gegen die DSGVO oder andere Datenschutzvorschriften verstößt. Der Auftragnehmer ist berechtigt, die Ausführung einer rechtswidrigen Weisung bis zur Klärung auszusetzen.

Bei Datenschutzvorfällen, die personenbezogene Daten des Auftraggebers betreffen, informiert der Auftragnehmer den Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Bekanntwerden. Die Meldung enthält alle gemäß Art. 33 Abs. 3 DSGVO erforderlichen Informationen, soweit diese verfügbar sind.

§ 5 – Pflichten des Auftraggebers

Der Auftraggeber ist allein Verantwortlicher für die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten und die Wahrung der Rechte der betroffenen Personen.

Der Auftraggeber erteilt Weisungen zur Datenverarbeitung ausschließlich in dokumentierter Form (einschließlich E-Mail). Mündliche Weisungen werden vom Auftraggeber unverzüglich schriftlich bestätigt.

Der Auftraggeber ist verantwortlich für die datenschutzkonforme Einrichtung der eingesetzten Systeme (CRM, Marketing-Automation-Plattformen) sowie für die Beauftragung und AVV-Gestaltung mit den jeweiligen Systemanbietern. Der Auftragnehmer übernimmt keine Verantwortung für die Datenschutzkonformität der Systeme des Auftraggebers.

Der Auftraggeber stellt dem Auftragnehmer alle zur Erfüllung seiner Pflichten aus diesem AVV erforderlichen Informationen zur Verfügung.

§ 6 – Unterauftragsverhältnisse

Der Auftragnehmer ist berechtigt, Unterauftragsverarbeiter einzusetzen, sofern diese schriftlich auf die Einhaltung der in diesem AVV geregelten Datenschutzanforderungen verpflichtet werden. Der Auftragnehmer haftet gegenüber dem Auftraggeber für die ordnungsgemäße Datenverarbeitung durch Unterauftragsverarbeiter wie für eigenes Handeln.

Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern. Der Auftragnehmer informiert den Auftraggeber über geplante Änderungen hinsichtlich der Hinzuziehung oder des Austauschs von Unterauftragsverarbeitern und gibt dem Auftraggeber damit die Möglichkeit, Einspruch zu erheben.

§ 7 – Löschung und Rückgabe

Nach Abschluss der Auftragsverarbeitung oder auf Verlangen des Auftraggebers löscht oder gibt der Auftragnehmer alle personenbezogenen Daten zurück, die er im Rahmen des Auftrags lokal gespeichert hat, sofern keine gesetzliche Pflicht zur weiteren Speicherung besteht. Kundendaten in den Systemen des Auftraggebers verbleiben dort und werden durch den Auftraggeber selbst verwaltet.

Die erfolgte Löschung wird dem Auftraggeber auf Anfrage schriftlich bestätigt.

Gesetzliche Aufbewahrungspflichten (insb. § 257 HGB, § 147 AO) bleiben unberührt. Entsprechende Daten werden für die Dauer der gesetzlichen Aufbewahrungsfrist gesperrt und nur im gesetzlich erforderlichen Umfang verarbeitet.

§ 8 – Technische und organisatorische Maßnahmen

Der Auftragnehmer hat die in Anlage 2 (TOM) dieses Vertrages beschriebenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Der Auftragnehmer ist berechtigt, die TOMs weiterzuentwickeln und anzupassen, solange das Schutzniveau nicht unterschritten wird. Ü wesentliche Änderungen informiert der Auftragnehmer den Auftraggeber vorab.

§ 9 – Kontrollrechte

Der Auftraggeber ist berechtigt, die Einhaltung der datenschutzrechtlichen Bestimmungen und der Regelungen dieses AVV beim Auftragnehmer zu kontrollieren. Kontrollen werden mit einer Vorlaufzeit von mindestens 14 Tagen schriftlich angekündigt und sind auf das erforderliche Maß zu beschränken.

Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle zur Nachweisführung erforderlichen

Informationen zur Verfügung, insbesondere diesen AVV, die TOMs (Anlage 2) sowie Nachweise über bestehende AV-Verträge mit Unterauftragsverarbeitern.

Der Auftragnehmer ist berechtigt, einem Auditor Einsicht zu gewähren, der zur Vertraulichkeit verpflichtet ist und nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

§ 10 – Haftung und Haftungsfreistellung

Die Haftung der Parteien untereinander richtet sich nach den Regelungen des Hauptvertrages sowie den gesetzlichen Vorschriften der DSGVO.

Der Auftraggeber stellt den Auftragnehmer von Ansprüchen betroffener Personen oder Behörden frei, die darauf beruhen, dass der Auftraggeber den Auftragnehmer zu einer datenschutzrechtswidrigen Verarbeitung angewiesen hat oder die Rechtswidrigkeit auf der Verantwortungssphäre des Auftraggebers (insb. Systemkonfiguration, Rechtsgrundlage der Verarbeitung) liegt.

§ 11 – Schlussbestimmungen

Dieser AVV unterliegt deutschem Recht. Gerichtsstand ist der Geschäftssitz des Auftragnehmers.

Änderungen dieses AVV bedürfen der Schriftform. Sollte eine Bestimmung dieses AVV unwirksam sein, bleibt die Wirksamkeit des übrigen Vertrages unberührt.

Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag hat dieser AVV in datenschutzrechtlichen Fragen Vorrang.

Marketing Machine GmbH | Stand: 01. März 2026

Anlage 1 – Verarbeitungsbeschreibung

gemäß Art. 28 Abs. 3 DSGVO

Gegenstand	Marketingberatung und CRM-Dienstleistungen gemäß Hauptvertrag
Zweck	Konzeption, Implementierung und Optimierung von CRM-Strategien, Marketing-Automation und datengetriebenem Marketing für den Auftraggeber
Dauer	Entspricht der Laufzeit des Hauptvertrages
Art der Verarbeitung	Erheben, Speichern, Lesen, Analysieren, Strukturieren, Verändern, Abfragen
Verarbeitungsort	In den Systemen des Auftraggebers (CRM, Marketing-Automation). Intern: Microsoft 365, EU-Rechenzentren
Kategorien betroffener Personen	Kunden und Interessenten des Auftraggebers, Newsletter-Abonnenten, Websitebesucher
Kategorien personenbezogener Daten	Kontaktdaten (Name, E-Mail, Telefon), CRM-Daten (Kaufhistorie, Segmente, Scores), E-Mail-Marketing-Daten (Öffnungen, Klicks), Websitedaten (Cookie-IDs, Session-IDs)
Besondere Kategorien (Art. 9 DSGVO)	Keine (nicht Gegenstand dieses Auftrags)

Anlage 2 – Technisch-Organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO i.V.m. § 64 BDSG | Marketing Machine GmbH | Version 1.1 | Gültig ab 01.03.2026

1. Zutrittskontrolle

Maßnahme	Beschreibung	Umsetzung
Home Office	Alle Mitarbeitenden arbeiten ausschließlich remote. Keine gemeinsamen Büroräume mit Publikumsverkehr.	Keine physischen Serverräume; Datenverarbeitung ausschließlich in der Microsoft 365 Cloud. Jeder Mitarbeitende ist für die Sicherheit seines Arbeitsbereichs verantwortlich.
Gerätesicherheit	Dienstliche Tätigkeiten werden grundsätzlich auf firmeneigenen Geräten durchgeführt. Freelancer und geringfügig Beschäftigte können beruflich genutzte Privatgeräte einsetzen, sofern diese die Mindestanforderungen dieser TOM erfüllen und dies vertraglich vereinbart ist.	Firmeneigene Endgeräte: Keine private Nutzung zulässig. Freelancer / geringfügig Beschäftigte: Festplattenverschlüsselung, aktuelles Betriebssystem, Antivirenschutz und aktivierte Bildschirmsperre (max. 5 Min.) sind Pflichtvoraussetzung für beruflich genutzte Privatgeräte. Nachweis auf Anfrage.

2. Zugangskontrolle

Maßnahme	Beschreibung	Umsetzung
Festplattenverschlüsselung	Alle firmeneigenen Endgeräte sind vollständig verschlüsselt.	MacBooks: FileVault 2 (AES-256). iPhones: Hardware-Verschlüsselung ab iOS.
Starke Authentifizierung	Zugänge zu allen Systemen sind durch sichere Passwörter und 2FA geschützt.	Passwortmanager im Einsatz. 2FA für Microsoft 365, CRM- und Marketing-Automation-Systeme (insb. HubSpot) aktiviert.
Bildschirmsperre	Bildschirme werden bei Inaktivität automatisch gesperrt.	Automatische Sperre nach max. 5 Minuten.
VPN	Bei Zugriff auf Kundensysteme wird ein VPN genutzt.	VPN-Verbindung ist verpflichtend beim Zugriff auf Produktionssysteme von Kunden.

3. Zugriffskontrolle

Maßnahme	Beschreibung	Umsetzung
Berechtigungskonzept	Zugriff auf personenbezogene Daten nur nach dem Need-to-know-Prinzip.	Mitarbeitende erhalten nur Zugriff auf Systeme und Daten, die für ihre

		Aufgabe erforderlich sind. Zugänge werden nach Auftragsende entzogen.
Microsoft 365	Zentrale Plattform für Dateiablage, Kommunikation und Zusammenarbeit.	Berechtigungen werden zentral verwaltet. Jeder Nutzer hat einen eigenen Account. Geteilte Zugänge sind nicht zulässig.
CRM / Marketing Automation	Zugriff auf Kundendaten im CRM und Marketing-Automation-Systemen.	Zugriff ausschließlich im Rahmen des Kundenmandats. Nutzung individueller Nutzeraccounts; kein Zugriff auf nicht auftragsbezogene Datenbereiche.

4. Trennungskontrolle

Maßnahme	Beschreibung	Umsetzung
Mandantentrennung	Daten verschiedener Auftraggeber werden getrennt verarbeitet und gespeichert.	Separate Ordnerstrukturen in Microsoft 365 pro Auftraggeber. Zugänge sind mandantenbezogen beschränkt. Kundendaten werden nicht zwischen Projekten vermischt.

5. Weitergabe- und Übertragungskontrolle

Maßnahme	Beschreibung	Umsetzung
Verschlüsselung der Übertragung	Daten werden ausschließlich verschlüsselt übertragen.	Alle Dienste in Microsoft 365 nutzen TLS-Verschlüsselung (HTTPS). E-Mails werden über Outlook/Exchange mit TLS übertragen. VPN beim Zugriff auf Kundensysteme.
Keine unsicheren Kanäle	Personenbezogene Daten werden nicht über unsichere Kanäle weitergegeben.	Kommunikation ausschließlich über Microsoft Teams und Outlook. Keine Übermittlung per privaten Messengern oder SMS.
Cloud-Speicherung	Kundendaten werden ausschließlich in Microsoft 365 gespeichert.	Microsoft 365 bietet DSGVO-konformen Datenspeicher in der EU. AV-Vertrag mit Microsoft über Standardvertragsklauseln abgedeckt.

6. Verfügbarkeitskontrolle

Maßnahme	Beschreibung	Umsetzung

Regelmäßige Backups	Alle relevanten Daten werden täglich gesichert.	Redundanz und Datensicherung in der Microsoft 365 Cloud.
Antivirenschutz	Alle Endgeräte sind durch Antivirensoftware geschützt.	macOS: integrierter Systemschutz.
Software-Updates	Betriebssysteme und Software werden zeitnah aktualisiert.	Automatische Updates für macOS, iOS und Microsoft 365. Sicherheitsupdates werden innerhalb von 48 Stunden eingespielt.

7. Belastbarkeit und Wiederherstellung

Maßnahme	Beschreibung	Umsetzung
Cloud-Resilienz	Kerninfrastruktur basiert auf hochverfügbaren Cloud-Diensten.	Microsoft 365 bietet SLA-garantierte Verfügbarkeit (99,9 % Uptime). Bei Ausfall einzelner Endgeräte kann auf einem Ersatzgerät weitergearbeitet werden.
Wiederherstellbarkeit	Daten können nach einem Vorfall wiederhergestellt werden.	Microsoft 365 bietet Versionshistorie (30–90 Tage).

8. Organisatorische Maßnahmen

Maßnahme	Beschreibung	Umsetzung
Vertraulichkeitsverpflichtung	Alle Mitarbeitenden sind zur Vertraulichkeit verpflichtet.	Mitarbeitende unterzeichnen vor Aufnahme der Tätigkeit eine Vertraulichkeitsvereinbarung und werden über datenschutzrechtliche Pflichten belehrt.
Datenschutzschulung	Sensibilisierung aller Mitarbeitenden für den Datenschutz.	Einmalige Einweisung bei Arbeitsbeginn; bei wesentlichen Änderungen erneute Schulung.
Meldepflicht bei Vorfällen	Datenschutzvorfälle werden unverzüglich gemeldet und dokumentiert.	Mitarbeitende melden Vorfälle sofort an den Geschäftsführer. Dieser informiert ggf. den Auftraggeber sowie die zuständige Aufsichtsbehörde gem. Art. 33/34 DSGVO innerhalb von 24 Stunden.
Unterauftragsverarbeitung	Drittanbieter werden nur mit AV-Vertrag eingesetzt.	Mit allen Sub-Auftragsverarbeitern (insb. Microsoft) bestehen AV-Verträge. Aktuelle Liste auf Anfrage verfügbar.

Aufbewahrung und Löschung	Kundendaten werden nach Auftragsende gelöscht.	Löschung nach Ende des Auftragsverhältnisses oder auf Verlangen. Schriftliche Bestätigung auf Anfrage.

Diese Maßnahmen sind verbindlich für alle Mitarbeitenden der Marketing Machine GmbH.

Marketing Machine GmbH | Stand: 01. März 2026