Vereinbarung über eine Auftragsverarbeitung gemäß Art 28 DSGVO

abgeschlossen zwischen

dem Verantwortlichen, nachstehend „Auftraggeber“ genannt, der dieser Vereinbarung zustimmt –
und dem/der
Auftragsverarbeiterin – FirmenABC Marketing GmbH, Karl-Hammerschmidt-Straße 1, 85609 Aschheim –
nachstehend „Auftragnehmer“ genannt.

1. Gegenstand/Gültigkeit der Vereinbarung

Diese Vereinbarung ist ausschließlich in Verbindung mit einem aufrechten Vertrag mit FirmenABC während des aktiven Leistungszeitraums gültig.

(1) Gegenstand dieses Auftrages:
Austausch von Daten für die Erbringung von Leistungen, basierend auf den AGB des Auftragnehmers FirmenABC

(2) Folgende Datenkategorien werden verarbeitet:
Daten des Auftraggebers

(3) Folgende Kategorien betroffener Personen:
Auftraggeber, allenfalls Partner sowie Kunden oder Mitarbeiter des Auftraggebers

2. Dauer der Vereinbarung

Die Vereinbarung ist für den im Hauptvertrag vereinbarten Zeitraum geschlossen.

3. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er – sofern gesetzlich zulässig – den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit vertraglich und schriftlich zur Vertraulichkeit und Geheimhaltung verpflichtet hat oder diese Personen einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht. Auf Wunsch des Auftraggebers ist der Auftragnehmer verpflichtet, die Einhaltung dieser Verpflichtung nachzuweisen.

(3) Die Verpflichtungen nach Abs 1 und 2 überbindet der Auftragnehmer vertraglich auf alle Personen, die, wenn auch nur vorübergehend, Zugriff auf die Daten und Verarbeitungsergebnisse haben (insbesondere Arbeitnehmer, Gehilfen, Reinigungs-, Wartungs-, Technik- und Serviceunternehmen etc).

(4) Der Auftragnehmer erklärt, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage zu entnehmen).

(5) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen gegenüber der betroffenen Person jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Mangels abweichender Regelung sind die notwendigen Informationen unverzüglich zu überlassen.

(6) Wird ein entsprechender Antrag einer betroffenen Person direkt an den Auftragnehmer gerichtet und lässt dieser Antrag erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(7) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(8) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht auf jederzeitige Einsichtnahme und Kontrolle, sei es auch durch von ihm

(9) 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.

(10) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben ODER in dessen Auftrag zu vernichten, soweit dem nicht gesetzliche Verpflichtungen zur Aufbewahrung oder Bereithaltung entgegenstehen.

Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen, Format herauszugeben. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

(11) der Union oder der Mitgliedstaaten.

4. Ort der Durchführung der Datenverarbeitung

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

5. Sub-Auftragsverarbeiter

Der Auftragnehmer ist befugt, Sub-Auftragsverarbeiter hinzuziehen. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem jeweiligen Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

6. Sonstige Regelungen

(1) Diese Vereinbarung unterliegt österreichischem materiellem Recht und Ausschluss von Verweisungsnormen und des UN-Kaufrechts.

(2) Für Streitigkeiten aus dieser Vereinbarung ist das sachlich zuständige Gericht in Linz, Österreich, zuständig.

(3) Nebenabreden zu dieser Vereinbarung existieren nicht. Änderungen dieser Vereinbarung bedürfen der Schriftform. Das gilt auch für ein Abgehen vom Schriftlichkeitsgebot.

Anlage – Technisch-organisatorische Maßnahmen

Vertraulichkeit

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy [komplexe Kennwörter, regelmäßige Änderung,...]), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis", Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen
Berechtigungen, insb von administrativen Benutzerkonten;
Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, und gesondert aufbewahrt.
Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität

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

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
Rasche Wiederherstellbarkeit/Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen; Incident-Response-Management; Datenschutzfreundliche Voreinstellungen;
Auftragskontrolle: Keine (Sub-)Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung), Vorabüberzeugungspflicht, laufende Nachkontrollen.