

Vereinbarung zur Auftragsverarbeitung von KAIPS MARKETING® 1.0

1. Präambel

1.1 Die Vereinbarung zur Auftragsverarbeitung von KAIPS MARKETING ist Bestandteil der Allgemeinen Geschäftsbedingungen (AGB).
1.2 Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem im Hauptvertrag zur Leistungserbringung in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag zur Leistungserbringung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer beauftragte personenbezogene Daten («Daten») des Auftraggebers verarbeiten.

2. Gegenstand, Dauer und Spezifizierung der u

2.1 Aus dem Hauptvertrag zur Leistungserbringung ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

2.2 Art der Daten:

- ✓ Personenstammdaten
- ✓ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ✓ Vertragsstammdaten
- ✓ Kundenhistorie
- ✓ Abrechnungs- und Zahlungsdaten
- ✓ Planungs- und Steuerungsdaten
- ✓ Steuerdaten

2.3 Art und Zweck der Datenverarbeitung

- ✓ Bereitstellung von IT-Infrastruktur im Rahmen der KAIPS MARKETING-Cloud (sofern vom Auftraggeber genutzt)
 - ✓ Wartung und Support von KAIPS MARKETING
 - ✓ Umsetzung der vertraglichen Maßnahmen (z.B. Web Development, Marketingmaßnahmen)
- 2.4 Kategorien betroffener Personen (folglich „Nutzer“ genannt)
- ✓ Kunden
 - ✓ Interessenten
 - ✓ Beschäftigte
 - ✓ Lieferanten
 - ✓ Ansprechpartner

2.5 Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages zur Leistungserbringung, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

3. Anwendungsbereich und Verantwortlichkeit

3.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag zur Leistungserbringung und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich («Verantwortlicher» im Sinne des Art. 4 Nr. 7 DS-GVO).

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

4. Datenanforderungskatalog (DAK)

4.1 Alle Daten resultieren aus der Eingabe des Nutzers in der Kundenanmeldungsfläche, Kontaktformularen und dem DAK. Die Eingabe erfolgt jeweils ausschließlich durch den Nutzer.

4.2 Beim Zustandekommen eines Vertragsverhältnisses, wird der DAK automatisiert an die eingegebene E-Mail-Adresse des Nutzers versendet. Dieser ist umgehend und ohne Zeitverzug auszufüllen und KAIPS MARKETING zu übermitteln.

4.3 Der DAK bildet über die Gesamtvertragslaufzeit die ausschließliche Informationsquelle.

4.4 Ggf. anfallende Datensätze wie Passwörter zu Mitgliedskonten werden separat in einer verschlüsselten Datenbank gespeichert und werden dem Nutzer nur schriftlich per Einschreiben gegen Kostenübernahme mitgeteilt. Andernfalls (z.B. per E-Mail, Telefongespräche) entbindet der Nutzer KAIPS MARKETING und dessen Erfüllungsgehilfen von jeglichen Haftungsansprüchen.

4.5 Bei Schäden resultierend aus Ziffer 4.4 haftet

der Nutzer in vollem Umfang. Ferner ist KAIPS MARKETING eventuellen Schadensersatz geltend zu machen. Dieser richtet sich, sofern nur zeitlicher Aufwand, nach AGB Ziffer 4.1.

5. Pflichten des Auftragnehmers

5.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

5.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer 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. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

5.3 Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

5.4 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

5.5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer 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.

5.6 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Hauptvertrages zur Leistungserbringung anfallende Datenschutzfragen, sofern nicht gesondert gekennzeichnet gilt die Geschäftsführung als verantwortlich.

5.7 Der Auftragnehmer 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.

5.8 Der Auftragnehmer 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 der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Hauptvertrag zur Leistungserbringung bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Hauptvertrag zur Leistungserbringung bereits vereinbart.

5.9 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von

Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

5.10 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen.

6. Pflichten des Auftraggebers

6.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

6.2 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

6.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Hauptvertrages zur Leistungserbringung anfallende Datenschutzfragen.

6.4 Der Auftraggeber bestätigt, dass alle von ihm angegebene Daten vollständig und korrekt sind. Ferner liegt eine Erlaubniserklärung der jeweiligen Personen (z.B. Ansprechpartner) und/oder Unternehmen vor, dessen Daten weiterzugeben und durch KAIPS MARKETING und dessen Erfüllungsgehilfen verwendet zu werden.

7. Anfragen betroffener Personen

7.1 Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8. Nachweismöglichkeiten

8.1 Der Auftragnehmer bestätigt dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten

8.2 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 (als angemessen gilt generell mindestens zwei Wochen) durchgeführt. Der Auftragnehmer 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 dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Hauptvertrag zur Leistungserbringung vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

8.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 3 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.

9. Subunternehmer (weitere Auftragsverarbeiter)

9.1 Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

9.2 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Hauptvertrag zur Leistungserbringung vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und

Informationssicherheitsmaßnahmen zu gewährleisten.

9.3 Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden ggfs. unter Einschaltung folgender Subunternehmer durchgeführt:

-

Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.

9.4 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftraggeber, seine datenschutzrechtlichen Pflichten aus dieser Vereinbarung dem Subunternehmer zu übertragen.

10. Informationspflichten, Schriftformklausel, Rechtswahl

10.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer 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.

10.2 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

10.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages zur Leistungserbringung vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

10.4 Es gilt deutsches Recht.

11. Leistungserfüllung und Ermächtigung

11.1 Mit Akzeptanz dieser VZA ermächtigt der Nutzer KAIPS MARKETING ausdrücklich, alle von ihm angegebenen Daten zur Leistungserfüllung zu verwenden und nach Bedarf an Erfüllungsgehilfen unter Berücksichtigung der DSGVO weiterzugeben. Die Nutzung, Einsicht und Verarbeitung aller am Prozessvorgang beteiligten Personen werden von dem Auftraggeber akzeptiert.

11.2 Es erfolgt für alle Maßnahmen gemäß den vereinbarten Leistungen eine zeitlich unbefristete Einverständniserklärung zur Datennutzung, sowie für die Einleitung und den Abschluss neuer Aufträge und Maßnahmen gemäß dem Leistungsinhalt.

11.3 Der Nutzer ist zur Kontrolle der verwendeten Software, Hardware, Plug-Ins und Ähnliches verantwortlich und entbindet KAIPS MARKETING von dieser Verpflichtung.

11.4 Ebenso ist rechtmäßige Nutzung verwendeter Software, insbesondere Plug-Ins und Drittanbieter auf Webseiten, durch den Nutzer zu kontrollieren. Eine mögliche Auswertung von Nutzerdaten wie beispielsweise IP-Adressen, o.Ä. sind möglich. Der Nutzer kann jederzeit eine Übersicht der die aktuelle Verwendung von Plug-Ins, Software, o.Ä. anfragen (gemäß allgemeiner Geschäftszeiten mit angemessener Fristsetzung zur Auslieferung).

11.5 Der Nutzer hat bei Feststellung von unsachgemäßem und/oder rechtswidrigem Gebrauch umgehend den Auftragnehmer zu informieren.

11.6 Der Nutzer stellt den Auftragnehmer von der Dokumentationspflicht gemäß DSGVO zur erleichtern des Arbeitsaltages frei. Falls nicht, steht es dem Auftragnehmer frei, eine Entschädigung gemäß AGB Ziffer 4.1 zu erheben.

12. Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

13. Pseudonymisierung und Verschlüsselung personenbezogener Daten

13.1 HTTPS-Verschlüsselung in der Webkommunikation (Data-at-Transport),
13.2 Verschlüsselung/Nutzung aller

gespeicherten Datensätze,
13.3 Pseudonymisierung vor zulässiger interner statistischer Auswertung.

14. Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen

14.1 Zugang zu Systemen nur mit individuellen Benutzernamen und Kennwörtern,
14.2 Berechtigte können nur auf für sie berechtigte Daten zugreifen,
14.3 personenbezogene gespeicherte Daten können nur im Rahmen des Berechtigungskonzepts gelesen, kopiert, verändert oder entfernt werden,
14.4 Verwendung fortlaufend aktualisierter Virenschutzsoftware,
14.5 Schutz des E-Mail-Verkehrs vor Viren und Spam,
14.6 Firewallsysteme,
14.7 Sicherstellung einer hohen Widerstandsfähigkeit der DVSysteme bei starkem Zugriff bzw. starker Belastung, etwa durch Angriffe von außen,
14.8 Verwendung ausgetesteter Software,
14.9 Verpflichtung der Mitarbeiter auf das Datengeheimnis,
14.10 Hohe Passwortsicherheit,
14.11 Kein Zugang für Unbefugte zu den Datenverarbeitungsanlagen des Rechenzentrums,
14.12 Während der Geschäftszeiten Zutritt zu Geschäftsräumen durch Mitarbeiter kontrolliert;
14.13 Besucher der Rechenzentren, werden begleitet,
14.14 Festlegung der berechtigten Personen in Listen für die sensiblen Bereiche des CRM und Datentresores,
14.15 Einbruchschutzmaßnahmen, Alarmanlage,
14.16 definierter Kreis von Zugangsberechtigten,
14.17 Anzahl der Admins aufs Notwendigste begrenzt,
14.18 Sichere Löschung von Datenträgern,
14.19 Empfang besetzt während Geschäftszeiten,
14.20 Videoüberwachung des Hauptdatenträgerbackups hinter Sicherheitstüren und Triple-Key-Anwendung,
14.21 Festdefinierte Nutzung alltäglicher Software, Anbietern und Hardware.

15. Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

15.1 Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung (z. B. Datensicherung und Spiegelung von Hardwarekomponenten);
15.2 Datensicherungskonzept,
15.3 personenbezogene Daten sind ständig verfügbar und geschützt gegen zufällige Zerstörung oder Verlust durch regelmäßiges Backup,
15.4 Sicherheitskopien,
15.5 besonders geschützte Rechenzentrumsabschnitte,
15.6 geschützte Stromversorgung.

16. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Verarbeitung

16.1 Regelmäßige Prüfung, ob/in welchem Umfang Zugangsrechte noch erforderlich sind,
16.2 Regelmäßige Prüfung, ob/in welchem Umfang Zugriffsrechte noch erforderlich sind,
16.3 Auftragskontrolle bei Auftragsverarbeitung,
16.4 Durchführung von notwendigen Anpassungsmaßnahmen.

17. Unternehmensauflistung verwendeter Software zur Leistungserbringung und/oder Datenspeicherung, -Verarbeitung

17.1 Nord-Ostsee Sparkasse, Anstalt des öffentlichen Rechts, Holm 22-28, 24937 Flensburg
17.2 SEMRUSH CY LTD, Griva Digeni and Kolonakiou, Grosvenor Tower, 2nd and 3rd floors, Neapoli, 3107, Limassol, Cyprus
17.3 Google Dienste, Google LLC („Google“), Amphitheatre Parkway, Mountain View, CA 94043, USA
17.4 Debitoor GmbH, Choriner Straße 34, 10435 Berlin, Deutschland
17.5 domainfactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning
17.6 Hootsuite Inc.
17.7 Bitrix Inc. US Headquarters, 901 N. Pitt St, Suite 325, Alexandria VA 22314 USA
17.8 Aut O'Mattic Ltd. (Irland)
17.9 Dropbox International Unlimited Company,

One Park Place, Floor 5, Upper Hatch Street, Dublin 2, Irland
17.10 GMX, 1&1 Mail & Media GmbH, Zweigniederlassung Karlsruhe, Brauerstr. 48, 76135 Karlsruhe, Deutschland
17.11 Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA
17.12 Adobe Systems Software Ireland Limited, 4-6 Riverwalk, Citywest Business Campus, Dublin 24, Republic of Ireland