Vereinbarung

Zwischen dem Verantwortlichen/Auftraggeber:

Beispiel GmbH, Musterstr. 200, 12345 Beispielhausen

(nachstehend Auftraggeber oder Verantwortlicher genannt)

und dem Auftragsverarbeiter:

rapidmail GmbH, Wentzingerstr. 21, 79106 Freiburg i.Br., Deutschland

(nachstehend Auftragnehmer oder Auftragsverarbeiter genannt)

wird die folgende Vereinbarung zur Datenverarbeitung getroffen.

Präambel

Diese Vereinbarung wird unter Beachtung des Bundesdatenschutzgesetzes (BDSG) und der Datenschutzgrundverordnung (DSGVO) sowie aller sonstigen einschlägigen datenschutzrechtlichen Vorschriften geschlossen. Für diese Vereinbarung gelten die jeweils in Kraft stehenden Gesetzesvorschriften in ihrer jeweils aktuellen Fassung.

Diese Vereinbarung betrifft die Erhebung, Verarbeitung und Nutzung personenbezogener Daten i.S.d. BDSG und DSGVO durch den Auftragnehmer im Auftrag des Auftraggebers („Auftragsverarbeitung“). Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person („Betroffener“). Die Vereinbarung hat die Auftragsverarbeitung von personenbezogenen Daten zum Gegenstand („Auftragsdaten“).

Vor diesem Hintergrund vereinbaren die Parteien Folgendes:

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der wesentliche Gegenstand des Vertrages ist die Verarbeitung von Adressdaten des Auftraggebers zur Versendung von Newslettern per E-Mail und transaktionalen E-Mails. Die Einzelheiten der Leistungen ergeben sich aus den Allgemeinen Geschäftsbedingungen (https://www.rapidmail.de/agb), welche bei der Registrierung vom Auftraggeber akzeptiert werden. Auf diese Leistungen wird hier verwiesen (im Folgenden auch zusammenfassend „Leistungsvereinbarung“).

(2) Dauer

Die Laufzeit des vorliegenden Vertrages richtet sich nach der Leistungsvereinbarung und den dortigen Kündigungsfristen. Eventuell bestehende Verträge zur Auftragsverarbeitung werden durch den Abschluss des vorliegenden Vertrages ersetzt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Zur Erfüllung der Pflichten des Auftragnehmers aus der Leistungsbeschreibung und den Allgemeinen Geschäftsbedingungen, der Erstellung aggregierter Übersichten und Auswertungen über die Nutzung der Leistungen des Auftragnehmers sowie ggf. der Migration vorhandener Daten werden personenbezogene Daten aus dem Herrschaftsbereich des Auftraggebers durch den Auftragnehmer vollumfänglich i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet, insbesondere, soweit jeweils erforderlich erhoben, gespeichert, verändert, ausgelesen, abgefragt, verwendet, offengelegt, abgeglichen, verknüpft und gelöscht. Der Zweck der Verarbeitung hängt damit von der jeweiligen Leistungsvereinbarung ab.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung sind personenbezogene Kundendaten des Auftraggebers. Die durch die Verarbeitung ihrer personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen sind Kunden, Geschäftskontakte und Interessenten des Auftraggebers. Die verarbeiteten Arten von Daten, sowie die Kategorien betroffener Personen ergeben sich im Einzelnen aus dem folgenden Abschnitt oder durch Auswahl der Datenarten im digitalen Abschluss dieser Auftragsverarbeitung durch den Auftraggeber.

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/- Kategorien (Aufzählung/ Beschreibung der Datenkategorien):

- ☐ Stammdaten (z.B. Namen, Anschriften, Geburtsdaten),
- ☐ Kontaktdaten (z.B. E-Mail-Adressen, Telefonnummern),
- ☐ Inhaltsdaten (z.B. Texteingaben, Fotografien, Videos, Inhalte von Dokumenten/Dateien),
- ☐ Vertragsdaten (z.B. Vertragsgegenstand, Laufzeiten, Kundenkategorie),
- ☐ Nutzungsdaten (z.B. Verlauf auf unseren Web-Diensten, Nutzung bestimmter Inhalte, Zugriffszeiten),
- ☐ Verbindungsdaten (z.B. Geräte-Informationen, IP-Adressen, URL-Referrer), und
- ☐ Standortdaten (z.B. GPS-Daten, IP-Geolokalisierung, Zugriffspunkte).
- ☐ Andere

Bitte beachten Sie, dass wir Ihnen die Dateneingabe in unsere Lösungen nicht einschränken, somit können sich weitere Arten der zu verarbeitenden Daten ergeben.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Kunden, Interessenten und insbesondere Newsletter-Abonnenten des Auftraggebers
- ☐ Beschäftigte des Auftraggebers
- ☐ Lieferanten und Partner des Auftraggebers
- ☐ Andere

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c) und Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung, sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen [Einzelheiten in der Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Vor dem Hintergrund der großen Datenübermittlungen bei transaktionalen E-Mails, werden abweichend von der Löschung auf Weisung bei der Leistungserbringung zu transaktionalen E-Mails automatische Löschroutinen von 30 Tagen durch den Auftragnehmer eingestellt.

(2) Soweit gesetzlich geschuldet oder vom vertraglich vereinbarten Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

(3) Der Auftragnehmer unterstützt, soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten über den gesetzlich normierten Umfang hinaus (Art. 28, Abs. 3, lit. e) und lit. f) DSGVO; Ziff. 5 j) dieser Vereinbarung) bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO, sowie bei der Einhaltung der in Artt. 33 bis 36 DSGVO genannten Pflichten.

(4) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Artt. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DSGVO ausübt. Als externer Datenschutzbeauftragter ist beim Auftragnehmer:

Herr Nils Möllers, Keyed GmbH, n.moellers@keyed.de, +49 2505 – 63 97 97

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c), 32 DSGVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

i) Der Auftragnehmer wird nach den Weisungen des Auftraggebers angemessene Maßnahmen ergreifen, um weitere unrechtmäßige Kenntnisnahmen durch Dritte auszuschließen und/oder weitere Beeinträchtigungen von den Betroffenen abzuwenden. Bis zu etwaigen Weisungen des Auftraggebers wird der Auftragnehmer alle zur Datensicherung und Schadensminimierung erforderlichen Maßnahmen ergreifen.

j) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung seiner gesetzlichen Pflichten, insbesondere Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Informationspflichten gegenüber Betroffenen und Aufsichtsbehörden, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Dasselbe gilt auch dann, wenn der Auftraggeber einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung ausgesetzt ist. Der Auftragnehmer wird dem Auftraggeber auf Anfrage das von ihm nach Maßgabe der einschlägigen Gesetzesvorschriften zu erstellende Verzeichnis aller Verarbeitungstätigkeiten in kopierter Form zur Verfügung stellen.

k) 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.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	**Anschrift/Land**	**Leistung**
MEGASPACE Internet Service GmbH	Max-von-Laue-Str. 2b 76829 Landau / Pfalz Deutschland	Die durch MEGASPACE erbrachte Leistung ist das Hosting der Server an Standorten innerhalb der Bundesrepublik Deutschland.

c) ☒ Die Auslagerung auf Unterauftragnehmer oder / der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber mindestens 2 Wochen vorher vorab schriftlich oder in Textform anzeigt und
- Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch beispielsweise

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Die Meldung an den Verantwortlichen bei Schutzverletzungen kann über die üblichen (elektronischen, telefonischen) Kommunikationskanäle getätigt werden vor dem Hintergrund der Meldepflichten wird der schnellstmögliche Informationsaustausch gewährleistet.

9. Haftung

(1) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden. Zur Haftung gelten die Regelungen des Art. 82 DSGVO.

(2) Der Auftragnehmer, seine gesetzlichen Vertreter oder Erfüllungsgehilfen haften nicht bei leichter Fahrlässigkeit. Dieser Ausschluss für die Haftung bei leichter Fahrlässigkeit gilt jedoch dann nicht, wenn es sich um die Verletzung einer wesentlichen Vertragspflicht (Kardinalpflicht) handelt. Kardinalpflichten bzw. wesentliche Vertragspflichten sind solche Pflichten des Auftragnehmers, deren Erfüllung die ordnungsgemäße Durchführung dieses konkreten Vertrages überhaupt erst ermöglicht und auf deren

Einhaltung der Kunde regelmäßig vertrauen darf; mithin also Pflichten, deren Verletzung die Erreichung des Vertragszwecks gefährden würde.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. Dies gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

10. Weisungsbefugnis des Auftraggebers

Die Entscheidungs- bzw. Weisungsbefugnis für die Auftragsverarbeitung hat allein der Auftraggeber. Der Auftragnehmer wird allein im Auftrag und im Interesse des Auftraggebers tätig. Die Verantwortung für die Einhaltung des Datenschutzrechts und die Rechtmäßigkeit der Auftragsverarbeitung sowie für die Wahrung der Rechte der Betroffenen liegt beim Auftraggeber.

Der Auftragnehmer führt die Auftragsverarbeitung ausschließlich im Rahmen der Vereinbarung und nach schriftlichen Weisungen des Auftraggebers durch, wobei die Weisungen vorrangig gelten, oder wenn eine gesetzliche Verpflichtung zur Verarbeitung besteht. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich bestätigen. Der Auftragnehmer ist nicht berechtigt, ohne vorherige schriftliche Zustimmung durch den Auftraggeber Erklärungen gegenüber den Betroffenen abzugeben. Im Falle einer gesetzlichen Verpflichtung teilt der Auftragnehmer dem Auftraggeber diese Verpflichtung vor der Verarbeitung mit.

Der Auftragnehmer darf die Auftragsdaten nicht eigenmächtig, sondern nur nach schriftlicher Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Der Auftragnehmer wird den Auftraggeber über sämtliche Anfragen und Beanstandungen der Betroffenen unverzüglich schriftlich unterrichten sowie den Auftraggeber bei Wahrung der Rechte der Betroffenen unterstützen, wie z.B. durch Benachrichtigung, Auskunftserteilung oder Berichtigung, Sperrung und Löschung von Auftragsdaten.

Die Parteien beachten im Rahmen der Auftragsverarbeitung die einschlägigen datenschutzrechtlichen Vorschriften. Ist der Auftragnehmer der Ansicht, dass eine Vereinbarung oder Weisung gegen datenschutzrechtliche Vorschriften verstößt, wird er den Auftraggeber hierüber unverzüglich schriftlich informieren. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung, solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung, solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(4) Der Auftraggeber und der Auftragnehmer vereinbaren einen Ausschluss des zivilrechtlichen Zurückbehaltungsrechts nach § 273 BGB zum Ausschluss der Zurückhaltung von verarbeiteten personenbezogenen Daten und Datenträgern im Falle von Vertrags-/Leistungsstörungen.

12. Geheimhaltung

Der Auftragnehmer wird die im Rahmen der Auftragsverarbeitung empfangenen Informationen und Unterlagen, insbesondere die Auftragsdaten, streng geheim halten („Geschäfts- und Betriebsgeheimnisse“). Die Geheimhaltungs-/Verschwiegenheitspflichten gelten auch nach Beendigung dieser Vereinbarung unbefristet fort.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

Die Geheimhaltungspflicht gilt nicht oder entfällt, wenn die Informationen und Unterlagen bereits bei Abschluss dieser Vereinbarung der Öffentlichkeit oder dem Auftragnehmer bekannt waren oder nach Abschluss dieser Vereinbarung der Öffentlichkeit bekannt werden, ohne dass den Auftragnehmer hieran ein Verschulden trifft, oder dem Auftragnehmer durch einen Dritten bekannt werden, vorausgesetzt der Dritte verletzt bei Übergabe der Informationen keine eigene Geheimhaltungsverpflichtung. Nachweispflichtig für diese Tatbestände ist der Auftragnehmer.

13. Informationspflichten, Schriftformklausel, Rechtswahl

(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.

(2) Änderungen und Ergänzungen dieser Anlage 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.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

14. Sonstiges, Allgemeines

Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile einschließlich etwaiger Zusicherungen des Auftragnehmers bedürfen einer schriftlichen Vereinbarung 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.

Gerichtsstand ist Freiburg i.Br. (79106).

Technische und organisatorische Maßnahmen

Mit diesem Dokument informieren wir Sie über die getroffenen Maßnahmen, welche im Zusammenhang mit Verarbeitungen von personenbezogenen Daten getätigt werden.

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“ (Art. 32 (1) DSGVO).

Verantwortlicher:	rapidmail GmbH
Anschrift:	Wentzingerstraße 21, 79106 Freiburg im Breisgau
Datenschutzbeauftragter:	Nils Möllers
IT-Verantwortlicher:	Herr Sven Kummer
Datum:	03.02.2022

Grundlegende Angaben

- [x] Es liegt eine wirksame Bestellung eines Datenschutzbeauftragten vor.
- [x] Die Beschäftigten sind auf die Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) verpflichtet.
- [x] Beschäftigte werden regelmäßig zum Schutz personenbezogener Daten unterwiesen.
- [x] Es besteht ein aktuelles Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO).

Hinweis: Bitte beachten Sie, dass Sie die Angaben wahrheitsgetreu beantwortet worden sind, damit eine grundsätzliche Bewertung des Sicherheitsniveaus vollzogen werden kann. Nicht jede Frage muss mit „Ja“ beantwortet werden, da einige Fragen eventuell nicht erforderlich oder zutreffend sind. Darüber hinaus gewährleisten wir laufend die Optimierung unserer Maßnahmen in enger Absprache mit unserem Datenschutzbeauftragten. Sofern Aktualisierungen dieser technischen und

organisatorischen Maßnahmen stattfinden, ist der Auftragsverarbeiter gem. Art. 28 Abs. 2 DSGVO verpflichtet dem Verantwortlichen eine Information diesbezüglich zukommen zu lassen oder sogar eine schriftliche Genehmigung einzuholen.

1. Maßnahmen zur Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle (Räumlicher Zutrittsschutz)

- [x] Einsatz von Berechtigungsausweisen.
- [x] Einsatz von elektronischen Zutrittscodekarten/ Zutrittstransponder.
- [x] Bestehen eines Zutrittsberechtigungskonzeptes.
- [x] Einsatz einer Videoüberwachung zum Zweck der Zutrittskontrolle.
- [x] Einsatz einer Alarmanlage.
- [x] Umzäunung des Rechenzentrums.
- [x] Jeder Zutritt zum Rechenzentrum wird zeitlich protokolliert und ausgewertet.
- [x] Es besteht eine Schlüsselregelung / ein Schlüsselkonzept.
- [x] Einsatz von Besucherausweisen.
- [x] Begleitung von Besucherzutritten durch eigene Mitarbeiter oder Sicherheitspersonal.
- [x] Sicherung auch außerhalb der Arbeitszeit durch (24/7) Werkschutz.
- [x] Spezialverglasung für sensible Bereiche oder zum Schutz von Einsichtnahmen Dritter.
- [x] Gesondert gesicherter Zutritt zu Server-Umgebungen oder dem Rechenzentrum.

1.2 Zugangskontrolle (Ein unbefugter Zugang und die Nutzung Unbefugter von IT-Systemen ist zu verhindern.)

- [x] Einsatz geeigneter Verschlüsselung der Netzwerke.
- [x] Passwortsicherung von Bildschirmarbeitsplätzen.
- [x] Verwendung von individuellen Passwörtern bzw. Verhinderung von Gruppen-Passwörtern.
- [x] Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner).

- [x] Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern.
- [x] Einsatz einer Passwort-Richtlinie, welche eine sichere Passwortkomplexität fordert.
- [x] Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern.
- [x] Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern.
- [x] Prozess zum Rechteentzug bei Austritt von Mitarbeitern.

1.3 Zugriffskontrolle (Unerlaubte Tätigkeiten in IT-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.)

- [x] Einsatz eines Berechtigungskonzeptes, welches die Zugriffe aller Mitarbeiter und Dienstleister transparent steuert.
- [x] Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung nach Maßgabe des Rollen- & Berechtigungskonzeptes.
- [x] Regelmäßige Überprüfung von Berechtigungen.
- [x] Protokollierung von Zugriffen auf Kundensysteme.
- [x] Protokollierung von Löschungen auf Weisungen des Verantwortlichen (Auftraggeber).
- [x] Einsatz einer Anti-Viren-Schutz Lösung auf jedem Endgerät.
- [x] Einsatz einer Firewall inkl. Spam-Schutz.
- [x] SSL-Verschlüsselung für Import/Export von Daten aus rapidmail.

1.4 Auftragskontrolle (Es ist sicherzustellen, dass Dienstleister, welche im Auftrag Daten verarbeiten, nur gemäß der Weisung des Auftraggebers Daten verarbeiten.)

- [x] Vertragsgestaltung der Auftragsverarbeitung gem. gesetzlichen Vorgaben (Art. 28 DSGVO).
- [x] Zentrale Erfassung vorhandener Dienstleister und Auftragsverarbeiter.
- [x] Es werden Kontrollen der technischen und organisatorischen Maßnahmen vor Verarbeitungsbeginn durchgeführt.

1.5 Trennungskontrolle (Es ist sicherzustellen, dass Daten, die zu unterschiedlichen Zwecken, Personen und Unternehmen erhoben wurden, getrennt voneinander verarbeitet werden können.)

- [x] Trennung von Kunden (Mandantenfähigkeit der verwendeten Systeme).
- [x] Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern) in Datenbanken.
- [x] Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeberdaten von Daten anderer Kunden Rechnung trägt.
- [x] Trennung von Entwicklungs-, Test- und Produktivsystemen.

2. Maßnahmen zur Gewährleistung der Integrität

2.1 Weitergabekontrolle (Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: elektronische Übertragung, Datentransport, sowie deren Kontrolle.)

- [x] Es besteht eine sichere Versendungsart der Daten zwischen Auftraggeber, Auftragnehmer und Dritten.
- [x] Für den E-Mailversand sind verschlüsselte ZIP-Dateien möglich.
- [x] Einsatz von VPN-Verbindungen.
- [x] Es findet ein Datenaustausch über eine SSL (https)-Verschlüsselung statt.
- [x] Dokumentierte Verwaltung von mobilen Endgeräten und Datenträgern.
- [x] Sicherstellung der Datenträgerentsorgung / Sichere Löschung von Datenträgern.
- [x] Einsatz von Aktenvernichtern (Shredder gem. DIN 66399).

2.2 Eingabekontrolle (Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.)

- [x] Kennzeichnung erfasster Daten.
- [x] Protokollierung von Eingaben/Löschungen.

- [x] Einsatz eines Protokollauswertungssystems.
- [x] Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke (4 Wochen).

3. Maßnahmen zur Gewährleistung der Verfügbarkeit

3.1 Verfügbarkeitskontrolle (Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.)

- [x] Es bestehen Datensicherungs- und Backupkonzepte. Die Datensicherung wird in regelmäßigen Testroutinen überprüft und somit wird die Wiederherstellung gewährleistet.
- [x] Tägliche Durchführung der Datensicherungs- und Backupkonzepte für Daten und Systeme (Bare Metal Restore).
- [x] Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal.
- [x] Brandmeldeanlagen in Serverräumlichkeiten oder im Rechenzentrum.
- [x] Rauchmelder in Serverräumlichkeiten oder im Rechenzentrum.
- [x] Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten oder im Rechenzentrum.
- [x] Klimatisierte Serverräumlichkeiten.
- [x] Blitz-/ Überspannungsschutz.
- [x] Serverräumlichkeiten in separaten Brandabschnitt.
- [x] Unterbringung von verschlüsselten Backupsystemen (rijndael-256 / AES) in separaten Räumlichkeiten und Brandabschnitt.
- [x] Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben).
- [x] USV-Anlage (Unterbrechungsfreie Stromversorgung).
- [x] Einsatz eines Stromgenerators bei Stromausfällen.

4. Maßnahmen zur Gewährleistung der Belastbarkeit

4.1 Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

- [x] Es sind Ausweich-Rechenzentren / Server vorhanden.
- [x] Redundante Datenanbindung.
- [x] Datenspeicherung auf RAID-Systemen (RAID 1 und höher).
- [x] Durchführung von Penetrationstests.
- [x] Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden.
- [x] Definition von Zeiträumen, in denen die Updates implementiert werden sollen (Perioden niedrigerer Operationen, Wartungszeiten usw.).
- [x] Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen.
- [x] Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit.
- [x] Durchführung einer Risikoanalyse unter Berücksichtigung all dieser Systeme, Geräte und Vermögenswerte, die identifiziert wurden, zur Ermittlung der Bedrohungen, inklusive ihrer Wahrscheinlichkeit und ihrer Auswirkungen.
- [x] Abdeckung der Risiken, die nicht mit technischen Sicherheitsmaßnahmen ausgestattet sind, mit einer Cyber-Versicherung, welche den Umfang, die Entschädigungen und die Abdeckungsausnahmen festlegen.

5. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren

- [x] Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten.
- [x] Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert.
- [x] Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen.

- [x] Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess).

- [x] Es wird ein Datenschutz-Management-System eingesetzt.

Diese technischen und organisatorischen Maßnahmen werden fortlaufend in regelmäßigen Abständen durch die **Keyed GmbH** auditiert. rapidmail gewährleistet im Ergebnis einen sehr hohen Schutz für die Systeme, welche Bestandsteil von Verarbeitungen sind.