[+] AUFTRAGSVERARBEITUNG

Vertrag zur Auftragsverarbeitung

nach Art. 28 der Datenschutz-Grundverordnung (DSGVO) und Art. 9 des Schweizer Datenschutzgesetzes (DSG)

zwischen

Firma / Name

Ansprechperson

Strasse, Nr.

PLZ, Ort, Land

E-Mail

rocketbatch-Konto (E-Mail oder Konto-ID)

– nachstehend **Verantwortlicher** –

und

rocketbatch, Einzelunternehmen, Inhaber Timo Reichen, Güterbahnhofstrasse 7, 9000 St. Gallen, Schweiz, info@rocketbatch.com

– nachstehend **Auftragsverarbeiter** –

1. Gegenstand und Dauer

Der Auftragsverarbeiter stellt dem Verantwortlichen die Software rocketbatch zur Verfügung: eine Desktop-App für macOS und Windows mit zugehörigen Server-Diensten für Mail, Aufgaben, Notizen, Projekte, Kontakte, Termine, Kampagnen, Workflows und KI-Funktionen (der **Hauptvertrag**, d. h. die Nutzungs- und Servicebedingungen von rocketbatch). Dabei bearbeitet er personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag regelt die Rechte und Pflichten der Parteien dazu.

Der Vertrag gilt, solange der Auftragsverarbeiter im Rahmen des Hauptvertrags personenbezogene Daten für den Verantwortlichen bearbeitet. Er endet mit dem Hauptvertrag, ohne dass es einer Kündigung bedarf. Bei Widersprüchen geht dieser Vertrag dem Hauptvertrag in Fragen des Datenschutzes vor.

2. Art, Zweck und Umfang der Bearbeitung

Die Bearbeitung umfasst das Speichern, Synchronisieren, Übermitteln an die vom Verantwortlichen berechtigten Nutzer, Anzeigen, Durchsuchen, Auswerten und Löschen von Daten, soweit es für die Funktionen von rocketbatch nötig ist. Zweck ist allein die Erbringung der Leistungen nach dem Hauptvertrag.

rocketbatch arbeitet hybrid. Daraus ergibt sich der Umfang der Daten auf den Servern des Auftragsverarbeiters:

- **Private Mails** bleiben auf dem Gerät des Nutzers. Auf die Server gelangen nur Kopfzeilen (Absender, Empfänger, Betreff, Datum) und eine kurze Vorschau.
- **Geteilte Inhalte** – Mails, Notizen, Aufgaben, Kontakte und weitere Einträge, die ein Nutzer öffentlich macht oder mit anderen teilt – werden vollständig auf den Servern gespeichert, damit berechtigte Nutzer darauf zugreifen können.
- **Kampagnen**: Empfängerlisten, Versanddaten, Öffnungen und Klicks (Öffnungs-Pixel, Klick-Tracking), Besuche auf Landingpages über persönliche Kampagnenlinks, Formulareingaben auf Landingpages sowie daraus berechnete Lead- und Beziehungs-Scores.
- **KI-Funktionen** laufen mit einem vom Verantwortlichen gewählten Modell: lokal, auf einem von ihm angegebenen Server oder bei einem von ihm verbundenen KI-Anbieter. Im letzten Fall übermittelt die App Inhalte auf Weisung des Verantwortlichen an diesen Anbieter; der Anbieter ist nicht Unterauftragsverarbeiter

des Auftragsverarbeiters.

Art der Daten

- Kontakt- und Stammdaten (Name, E-Mail-Adresse, Telefonnummer, Firma, Funktion, Adresse);
- Kommunikationsdaten (Mail-Kopfzeilen und -Vorschauen; Inhalte geteilter Mails, Kommentare und Chats);
- Inhalte von Notizen, Aufgaben, Projekten, Terminen und Dateien, soweit geteilt;
- Kampagnen- und Nutzungsdaten (Öffnungen, Klicks, Besuche, Verweildauer, Scores, Formulareingaben);
- Nutzer- und Protokolldaten der Konten des Verantwortlichen (Login, Rollen, Zeitstempel, IP-Adressen).

Kategorien betroffener Personen

- Mitarbeitende und weitere Nutzer des Verantwortlichen;
- Kunden, Interessenten, Lieferanten, Partner und sonstige Kontakte des Verantwortlichen;
- Empfänger von Kampagnen und Besucher von Landingpages des Verantwortlichen;
- Mitglieder und Kontakte von Vereinen und Organisationen, soweit der Verantwortliche rocketbatch dafür nutzt.

Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO, Art. 5 lit. c DSG) sind nicht Gegenstand der Bearbeitung. Bearbeitet der Verantwortliche solche Daten dennoch mit rocketbatch, verantwortet er die Zulässigkeit und prüft, ob die Massnahmen in Anlage 1 dafür genügen.

3. Weisungen

Der Auftragsverarbeiter bearbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch bei Übermittlungen in Drittländer, ausser er ist gesetzlich zu einer Bearbeitung verpflichtet; in diesem Fall teilt er dem Verantwortlichen die rechtlichen Anforderungen vor der Bearbeitung mit, sofern das Gesetz dies nicht verbietet. Weisungen sind dieser Vertrag, der Hauptvertrag, die Einstellungen und Aktionen in rocketbatch sowie Weisungen in Textform (z. B. E-Mail). Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, teilt er dies dem Verantwortlichen unverzüglich mit und darf ihre Ausführung bis zur Klärung aussetzen.

4. Pflichten des Auftragsverarbeiters

- **Vertraulichkeit**: Personen, die Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet oder unterliegen einer gesetzlichen Schweigepflicht. Zugriff erhalten nur Personen, die ihn für die Erbringung der Leistungen brauchen.
- **Sicherheit**: Er trifft die technischen und organisatorischen Massnahmen nach Art. 32 DSGVO und Art. 8 DSG, wie in Anlage 1 beschrieben. Er darf sie weiterentwickeln, solange das Schutzniveau nicht sinkt.
- **Betroffenenrechte**: Er unterstützt den Verantwortlichen mit geeigneten Massnahmen dabei, Anfragen betroffener Personen zu beantworten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenherausgabe, Widerspruch). Erreicht eine solche Anfrage den Auftragsverarbeiter, leitet er sie unverzüglich an den Verantwortlichen weiter.
- **Weitere Unterstützung**: Er unterstützt den Verantwortlichen bei der Datensicherheit, bei Meldungen von Datenschutzverletzungen, bei Datenschutz-Folgenabschätzungen und bei Konsultationen der Aufsichtsbehörde (Art. 32 bis 36 DSGVO, Art. 22 ff. DSG), soweit ihm Informationen dafür vorliegen.
- **Verletzungen**: Er meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 48 Stunden nach Kenntnis, mit den ihm bekannten Angaben nach Art. 33 Abs. 3 DSGVO.
- **Verzeichnis**: Er führt ein Verzeichnis der Bearbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und Art. 12 DSG.
- **Ort der Bearbeitung**: Die Daten werden in der AWS-Region Europa (Irland) gespeichert, also in der EU.

5. Pflichten des Verantwortlichen

– Er ist für die Zulässigkeit der Bearbeitung verantwortlich, insbesondere für Rechtsgrundlagen und Einwilligungen, und informiert die betroffenen Personen in seiner eigenen Datenschutzerklärung.
– Versendet er Kampagnen mit Öffnungs- und Klick-Tracking oder persönlichen Kampagnenlinks, holt er die dafür nötige Einwilligung der Empfänger ein und beachtet Widersprüche.
– Er verwaltet die Zugänge seiner Nutzer, hält Zugangsdaten geheim und schützt die Geräte, auf denen private Mails liegen.
– Er informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmässigkeiten bei der Bearbeitung feststellt.

6. Unterauftragsverarbeiter

Der Verantwortliche erteilt die allgemeine Genehmigung, Unterauftragsverarbeiter beizuziehen. Die bei Vertragsschluss eingesetzten sind in Anlage 2 aufgeführt. Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage im Voraus per E-Mail über einen neuen oder ersetzten Unterauftragsverarbeiter. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen; finden die Parteien keine Lösung, kann er den Hauptvertrag auf den Zeitpunkt der Änderung kündigen.

Der Auftragsverarbeiter überträgt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten wie in diesem Vertrag und haftet gegenüber dem Verantwortlichen für deren Einhaltung. Nicht als Unterauftrag gelten Nebenleistungen wie Telekommunikation, Post oder Wartung von Hardware ohne Zugriff auf die Daten.

7. Übermittlung in Drittländer

Eine Bearbeitung ausserhalb der Schweiz und der EU/des EWR durch den Auftragsverarbeiter oder seine Unterauftragsverarbeiter findet nur statt, wenn der Verantwortliche zugestimmt hat und die Voraussetzungen von Art. 44 ff. DSGVO und Art. 16 f. DSG erfüllt sind, etwa durch einen Angemessenheitsbeschluss oder Standardvertragsklauseln. Mit Abschluss dieses Vertrags stimmt der Verantwortliche dem Einsatz von Amazon Web Services nach Anlage 2 zu, einschliesslich der dort beschriebenen Garantien für einen möglichen Zugriff aus den USA. Übermittlungen an einen KI-Anbieter, den der Verantwortliche selbst verbindet (Ziffer 2), erfolgen auf seine Weisung und in seiner Verantwortung.

8. Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags nötig sind. Der Verantwortliche kann Kontrollen selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen, nach Anmeldung mit angemessener Frist, in der Regel mindestens 30 Tagen, während der Geschäftszeiten und ohne den Betrieb unverhältnismässig zu stören. Vorrangig erfolgt der Nachweis durch schriftliche Auskünfte und Unterlagen. Für Kontrollen vor Ort kann der Auftragsverarbeiter eine angemessene Vergütung seines Aufwands verlangen.

9. Löschung und Rückgabe

Nach Ende des Hauptvertrags kann der Verantwortliche seine Daten während 30 Tagen über die Funktionen von rocketbatch exportieren. Danach löscht der Auftragsverarbeiter die Daten auf seinen Systemen, einschliesslich Kopien, ausser ein Gesetz verpflichtet ihn zur Aufbewahrung. Daten in Sicherungskopien werden im Rahmen der üblichen Rotation überschrieben. Auf Anfrage bestätigt der Auftragsverarbeiter die Löschung in Textform. Daten auf den Geräten der Nutzer, etwa lokal gespeicherte private Mails, liegen in der Verantwortung des Verantwortlichen.

10. Haftung

Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien gelten die Haftungsregeln des Hauptvertrags, soweit zwingendes Recht nicht entgegensteht.

11. Schlussbestimmungen

Änderungen und Ergänzungen bedürfen der Textform. Ist eine Bestimmung unwirksam, bleibt der übrige Vertrag gültig; die Parteien ersetzen sie durch eine Regelung, die dem Zweck am nächsten kommt. Es gilt Schweizer Recht; zwingende Bestimmungen der DSGVO bleiben vorbehalten. Gerichtsstand ist St. Gallen, soweit nicht zwingend ein anderer vorgeschrieben ist.

Unterschriften

Verantwortlicher	**Auftragsverarbeiter**
Ort, Datum	
_____	St. Gallen, Datum der Gegenzeichnung
Name, Funktion	
_____	Timo Reichen, Inhaber, rocketbatch
Unterschrift	
_____	_____

Unterzeichnet zurück an info@rocketbatch.com. Sie erhalten den Vertrag gegengezeichnet zurück.

[+] ANLAGE 1

Technische und organisatorische Massnahmen

nach Art. 32 DSGVO und Art. 8 DSG

Vertraulichkeit

- **Zutritt**: Die Server laufen in Rechenzentren von Amazon Web Services in Irland. Zutrittskontrolle, Videoüberwachung und Besucherregelung liegen beim Betreiber, der unter anderem nach ISO/IEC 27001 zertifiziert ist.
- **Zugang**: Administrativer Zugang zu den Servern nur über verschlüsselte Verbindungen mit Schlüssel-Authentifizierung; Passwörter der Nutzer werden nur gesalzen und gehasht gespeichert.
- **Zugriff**: Rollen und Berechtigungen in rocketbatch; geteilte Inhalte sind nur für die vom Nutzer berechtigten Personen sichtbar. Zugriff des Auftragsverarbeiters auf Inhalte nur, soweit für Betrieb oder Support nötig.
- **Datensparsamkeit**: Private Mails bleiben auf dem Gerät; auf den Servern liegen nur Kopfzeilen und Vorschau.
- **Trennung**: Daten verschiedener Kunden sind logisch getrennt; Test- und Produktivsysteme sind getrennt.

Integrität

- **Übertragung**: Alle Verbindungen zwischen App, Website und Servern sind mit TLS verschlüsselt.
- **Eingabe**: Änderungen an Einträgen werden mit Zeitstempel und Nutzer protokolliert, soweit die Funktion dies vorsieht.
- **IP-Adressen** in der Website-Statistik werden nur als Hashwert gespeichert.

Verfügbarkeit und Belastbarkeit

- Regelmässige Sicherungskopien der Server-Daten; Wiederherstellung wird geprüft.
- Überwachung der Systeme; Sicherheitsupdates werden zeitnah eingespielt.
- Schutz vor Angriffen auf Netzwerkebene durch Proxy und Firewall.

Verfahren zur regelmässigen Überprüfung

- Die Massnahmen werden mindestens jährlich und bei wesentlichen Änderungen überprüft und angepasst.
- Vorfälle werden dokumentiert, ausgewertet und dem Verantwortlichen nach Ziffer 4 gemeldet.
- Unterauftragsverarbeiter werden vor dem Einsatz und danach regelmässig auf geeignete Massnahmen geprüft.

[+] ANLAGE 2

Unterauftragsverarbeiter

Anbieter	Leistung	Standort der Daten
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxemburg	Server (Amazon EC2) und Dateispeicher (Amazon S3)	AWS-Region Europa (Irland), EU

AWS gehört zum US-Konzern Amazon.com, Inc. Ein Zugriff aus den USA, etwa für Support oder auf behördliche Anordnung, ist nicht vollständig auszuschliessen. Abgesichert ist er durch die Zertifizierung von Amazon nach dem EU-U.S. und dem Swiss-U.S. Data Privacy Framework sowie durch die Standardvertragsklauseln im AWS Data Processing Addendum (Ziffer 7). Änderungen an dieser Liste kündigen wir nach Ziffer 6 an.