Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Leere Vorlage zur Prüfung, Fassung 2026-11-22

Verantwortlicher

Name	_____
Anschrift	_____
Ansprechpartner	_____
Benachrichtigungs-E-Mail	_____

Auftragsverarbeiter

Name	valie media GmbH
Anschrift	Brühlscher Weg 91, 47608 Geldern, Deutschland (Amtsgericht Kleve, HRB 16313)
Benachrichtigungs-E-Mail	contact@moreflow.io

Die Parteien schließen den nachstehenden Vertrag zur Verarbeitung personenbezogener Daten im Auftrag. Die deutsche Fassung ist maßgeblich.

§ 1 Gegenstand und Dauer

Der Auftragsverarbeiter verarbeitet für den Verantwortlichen personenbezogene Daten im Rahmen der Bereitstellung der Software-as-a-Service-Plattform Moreflow. Gegenstand, Art, Zweck sowie Kategorien betroffener Personen und Daten ergeben sich aus Anlage 1.

Dieser Vertrag gilt für die Dauer des Hauptvertrags über die Nutzung von Moreflow und endet mit dessen Beendigung, soweit sich aus § 10 nichts anderes ergibt.

§ 2 Weisungsgebundenheit

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, eine Verarbeitung ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zu der er verpflichtet ist erforderlich; in diesem Fall teilt er dies dem Verantwortlichen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet. Die Nutzung der Funktionen von Moreflow durch den Verantwortlichen gilt als Weisung.

§ 3 Vertraulichkeit

Der Auftragsverarbeiter stellt sicher, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 4 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Er darf diese fortentwickeln, sofern das Schutzniveau nicht unterschritten wird.

§ 5 Unterauftragsverarbeiter

Der Verantwortliche erteilt die allgemeine Genehmigung zum Einsatz der in Anlage 3 aufgeführten Unterauftragsverarbeiter. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen an dieser Liste, indem er die Änderung an die hinterlegte Benachrichtigungs-E-Mail-Adresse sendet und im Trust Center veröffentlicht. Der Verantwortliche kann innerhalb von 14 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Widerspricht der Verantwortliche fristgerecht und kann der Auftragsverarbeiter keine zumutbare Alternative ohne den neuen Unterauftragsverarbeiter bereitstellen, kann der Verantwortliche die betroffene Leistung oder den Hauptvertrag außerordentlich zum Zeitpunkt des Wirksamwerdens der Änderung kündigen.

Der Auftragsverarbeiter schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der im Wesentlichen dieselben Datenschutzpflichten enthält, und haftet für dessen Erfüllung.

§ 6 Übermittlung in Drittländer

Eine Verarbeitung außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nur unter den Voraussetzungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (z. B. EU-US Data Privacy Framework) oder von EU-Standardvertragsklauseln. Der jeweils aktuelle Stand je Unterauftragsverarbeiter ist in Anlage 3 sowie im Trust Center (app.moreflow.io/trust/subprocessors) dokumentiert.

§ 7 Unterstützung des Verantwortlichen

Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen (Art. 12 bis 23 DSGVO) sowie bei der Einhaltung der Pflichten nach Art. 32 bis 36 DSGVO, einschließlich Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) und vorheriger Konsultationen (Art. 36 DSGVO).

Verletzungen des Schutzes personenbezogener Daten meldet der Auftragsverarbeiter dem Verantwortlichen unverzüglich — mit dem Ziel einer Erstinformation innerhalb von 48 Stunden — nachdem sie ihm bekannt geworden sind, und stellt die zur Erfüllung von Art. 33 und 34 DSGVO erforderlichen Angaben bereit.

§ 8 Löschung und Rückgabe

Nach Beendigung der Verarbeitungsleistungen löscht oder gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten zurück, soweit nicht eine gesetzliche Aufbewahrungspflicht besteht. Nach Vertragsende bleibt das Konto mindestens 30 Tage im Nur-Lese-Modus zum Export zugänglich; anschließend erfolgt die Löschung. In Datensicherungen können gelöschte Daten bis zu deren turnusmäßiger Überschreibung enthalten bleiben; sie werden daraus nicht wiederhergestellt, außer zur Wiederherstellung des Gesamtsystems nach einem Ausfall, in welchem Fall sie erneut gelöscht werden.

§ 9 Nachweise und Überprüfung

Der Auftragsverarbeiter stellt dem Verantwortlichen die zum Nachweis der Einhaltung dieses Vertrags erforderlichen Informationen zur Verfügung, vorrangig über die veröffentlichten Dokumentationen im Trust Center und schriftliche Auskünfte. Soweit darüber hinaus erforderlich, ermöglicht der Auftragsverarbeiter Überprüfungen einschließlich Inspektionen durch den Verantwortlichen oder einen zur Verschwiegenheit verpflichteten Prüfer nach angemessener vorheriger Ankündigung während der üblichen Geschäftszeiten ohne Störung des Betriebsablaufs.

§ 10 Haftung und Vorrang

Die Haftung richtet sich nach Art. 82 DSGVO und den Regelungen des Hauptvertrags. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags zum Datenschutz vor.

§ 11 Abschluss

Der Vertrag kommt durch die elektronische Annahme durch eine zeichnungsberechtigte Person des Verantwortlichen zustande. Die Annahme, der Zeitpunkt, die handelnde Person, die Vertragsversion und die Prüfsumme des erzeugten Dokuments werden in diesem Dokument ausgewiesen.

Anlage 1: Gegenstand, Art und Zweck der Verarbeitung

Gegenstand	Bereitstellung der Software-as-a-Service-Plattform Moreflow für CRM, Kundenkommunikation, Verträge, Rechnungen, Dateien und Automatisierung.
Art der Verarbeitung	Erheben, Erfassen, Organisieren, Speichern, Anpassen, Abfragen, Verwenden, Übermitteln, Löschen.

Zweck	Vertragserfüllung gegenüber dem Verantwortlichen: Betrieb der Plattform, Nutzerverwaltung, Abrechnung und Support.
Betroffene Personen	Beschäftigte und Nutzer des Verantwortlichen; Kunden, Interessenten und Ansprechpartner des Verantwortlichen; sonstige Personen, deren Daten der Verantwortliche in der Plattform verarbeitet.
Datenkategorien	Kontakt- und Stammdaten, Kommunikationsinhalte, Dateien, Vertrags- und Zahlungsdaten, Nutzungs- und Protokolldaten; je nach Nutzung auch besondere Inhalte, die der Verantwortliche selbst einträgt.

Anlage 2: Technische und organisatorische Maßnahmen

Zutrittskontrolle

Die Anwendung wird bei Infrastrukturanbietern mit eigenen Zutrittskontrollen betrieben. Der Auftragsverarbeiter besitzt keine eigenen Rechenzentren.

Zugangs- und Zugriffskontrolle

Anmeldung erfolgt über einen dedizierten Identitätsdienst mit Sitzungsverwaltung; Passwörter werden nur als Hash gespeichert, und jede Person kann eine Zwei-Faktor-Authentifizierung aktivieren. Sitzungen werden beim Zurücksetzen des Passworts beendet. Berechtigungen sind rollenbasiert je Konto (Inhaber, Administrator, Vertrieb, Abrechnung); Schutzfunktionen zur Beschränkung von Anfragen sind aktiv.

Mandantentrennung

Jede Operation prüft serverseitig die Kontozugehörigkeit und Rolle des Handelnden, und der Datenzugriff ist auf das Konto beschränkt, für das die Operation ausgeführt wird. Dateien werden mit kontobezogenen Speicherpfaden abgelegt und nur über kurzlebige signierte Links ausgegeben.

Weitergabekontrolle und Verschlüsselung bei der Übertragung

Die Kommunikation zwischen Nutzer, Anwendung und Schnittstellen erfolgt über verschlüsselte Verbindungen (TLS). Ausgehende Dokumentabrufe erfolgen über kurzlebige signierte Links.

Verschlüsselung im Ruhezustand

Datenbank- und Objektspeicher werden durch die jeweiligen Infrastrukturanbieter verschlüsselt gespeichert, soweit der Anbieter dies bereitstellt. Zugangsdaten verbundener Dienste und Webhook-Geheimnisse verschlüsselt der Auftragsverarbeiter zusätzlich selbst mit AES-256-GCM; API-Tokens werden nur als schlüsselgebundener Hash (HMAC) gespeichert.

Eingabekontrolle und Protokollierung

Eingaben werden serverseitig validiert. Änderungen an Konten, Verträgen und Dokumenten werden in Aktivitäts- und Betriebsprotokollen festgehalten; Zugriffe von Mitarbeitern des Auftragsverarbeiters auf Kundenkonten und Änderungen an Integrationen werden gesondert protokolliert. Betriebsprotokolle und Fehlerberichte werden vor dem Speichern automatisch um erkennbare personenbezogene Daten wie E-Mail-Adressen, Telefonnummern, Namen und Nachrichteninhalte bereinigt.

Verfügbarkeit und Wiederherstellbarkeit

Datenbanksicherungen und Wiederherstellung werden durch den Datenbankanbieter bereitgestellt; Betrieb mit Überwachung und Statusseite.

Auftragskontrolle

Unterauftragsverarbeiter werden vertraglich verpflichtet und sind in Anlage 3 offengelegt. Änderungen werden nach § 5 mitgeteilt.

Datenminimierung und Löschung

Betriebsdaten wie Protokolle, Sitzungen und Zustellnachweise werden durch geplante Bereinigungsläufe nach festgelegten Fristen gelöscht. Vom Verantwortlichen gelöschte Kontakte werden 30 Tage in einem Papierkorb aufbewahrt; eine endgültige Löschung einzelner Kontakte erfolgt auf dokumentierte Weisung des Verantwortlichen sowie im Rahmen der regulären Aufbewahrungs- und Löschregeln der Plattform. Die Löschung eines Kontos führt der Auftragsverarbeiter nach einem vollständigen Export durch; sie umfasst gespeicherte Dateien und alle kontobezogenen Datensätze, soweit keine gesetzliche Aufbewahrungspflicht besteht. In Datenbanksicherungen verbleiben gelöschte Daten nur bis zur turnusmäßigen Überschreibung.

Anlage 3: Unterauftragsverarbeiter

Stand der Liste: 2026-10-25. Die Liste wird bei Änderungen nach § 5 mitgeteilt.

Unterauftragsverarbeiter	Zweck	Ort	Datenkategorien	Übermittlungsgrundlage
Hetzner	Hosting der Anwendung	Deutschland (EU)	Plattformdaten des Kontos	Nur EU/EWR
PlanetScale	Datenbank	Deutschland (EU)	Plattformdaten des Kontos	Noch nicht festgestellt
Cloudflare R2	Dateispeicherung	EU	Dateien und Medien	Nur EU/EWR
Cloudflare Turnstile	Schutz vor Automatisierung	Noch nicht festgestellt	Authentifizierungs- und Sicherheitsdaten	Noch nicht festgestellt
Temporal Cloud	Workflow-Steuerung	Deutschland (EU)	Workflow-Nutzdaten	Noch nicht festgestellt
Axiom	Protokollierung	Deutschland (EU)	Nutzungs- und Diagnosedaten	Noch nicht festgestellt
Sentry	Fehlerüberwachung	EU	Nutzungs- und Diagnosedaten	Noch nicht festgestellt
Amazon SES (AWS)	Transaktions-E-Mail; E-Mails an Kunden; Messung von E-Mail-Interaktionen; Empfang von E-Mail-Antworten	Deutschland (EU)	Konto- und Kontaktdaten; Kommunikationsinhalte; Nutzungs- und Diagnosedaten	Noch nicht festgestellt
Cloudflare for SaaS	Messung von E-Mail-Interaktionen	Weltweit (nächstgelegenes Rechenzentrum)	Nutzungs- und Diagnosedaten	EU-US Data Privacy Framework
Stripe	Abonnement-Abrechnung	Noch nicht festgestellt	Konto- und Kontaktdaten; Zahlungs- und Abrechnungsdaten	Noch nicht festgestellt
Twilio (SMS)	Telefonie und Nachrichten	USA	Konto- und Kontaktdaten; Kommunikationsinhalte	Noch nicht festgestellt
Twilio (Voice)	Telefonie und Nachrichten	EU	Konto- und Kontaktdaten; Kommunikationsinhalte	Noch nicht festgestellt
OpenAI	KI-Verarbeitung	USA	Ein- und Ausgaben von KI-Funktionen	Standardvertragsklauseln
Anthropic	KI-Verarbeitung	Noch nicht festgestellt	Ein- und Ausgaben von KI-Funktionen	Noch nicht festgestellt
Google	KI-Verarbeitung; Adressvervollständigung	Noch nicht festgestellt	Ein- und Ausgaben von KI-Funktionen; Adressabfragen	Noch nicht festgestellt
Tavily	Web-Recherche	Noch nicht festgestellt	Suchanfragen für Web-Recherche	Noch nicht festgestellt
DataForSEO	Web-Recherche	Noch nicht festgestellt	Suchanfragen für Web-Recherche	Noch nicht festgestellt
Bright Data	Web-Recherche	Noch nicht festgestellt	Suchanfragen für Web-Recherche	Noch nicht festgestellt
BytePlus	Medienerzeugung	Noch nicht festgestellt	Eingaben für Medienerzeugung	Noch nicht festgestellt
OpenRouter	Medienerzeugung	Noch nicht festgestellt	Eingaben für Medienerzeugung	Noch nicht festgestellt
Paywise	Forderungseinzug	Noch nicht festgestellt	Forderungs- und Schuldnerdaten	Noch nicht festgestellt
Expo (push notifications)	Push-Benachrichtigungen	Noch nicht festgestellt	Konto- und Kontaktdaten; Kommunikationsinhalte; Nutzungs- und Diagnosedaten	Noch nicht festgestellt
Apple Push Notification service	Push-Benachrichtigungen	Noch nicht festgestellt	Nutzungs- und Diagnosedaten	Noch nicht festgestellt

Hinweis zur Vorlage

Diese leere Vorlage dient der Prüfung vor Vertragsschluss. Kundinnen und Kunden schließen den AVV in moreflow unter Einstellungen > Daten & Datenschutz ab. Die ausgefertigte Fassung enthält die Angaben des Verantwortlichen, den bei Abschluss geltenden Stand der Unterauftragsverarbeiter und den Nachweis der Annahme.