Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO

Stand: 21.09.2026

zwischen

Name und Anschrift des Vertragspartners

– **Verantwortlicher** –

und der

MISSION OM GmbH
Champignystraße 1
70563 Stuttgart
Deutschland

– **Auftragsverarbeiter** –

Präambel
Der Verantwortliche beauftragt den Auftragsverarbeiter mit der Erbringung der in § 1 Abs. 1 bezeichneten Leistungen, in deren Rahmen der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen ausschließlich in dessen Auftrag und nach dessen Weisung verarbeitet. Zugleich entscheidet der Verantwortliche über Zwecke und Mittel der Datenverarbeitung. Hierzu schließen die Parteien im Sinne des Art. 28 Abs. 3 und Abs. 4 DSGVO nachfolgende Vereinbarung, welche das zwischen den Parteien bestehende Hauptvertragsverhältnis im Hinblick auf die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen konkretisiert:

§ 1 Gegenstand, Zweck, Dauer und Art der Verarbeitung

(1) Vertragsgegenstand

1.1 Der Auftragsverarbeiter erbringt für den Verantwortlichen folgende Leistungen:
Die Bereitstellung und den Betrieb der Plattform RocketFeed zur Verwaltung, zum Import, zur Normalisierung, zum Mapping, zur Optimierung, zur Speicherung und zur Ausspielung von Produktfeeds sowie zur Anbindung von Google-Diensten, zur Auswertung aggregierter KPI- und Performance-Daten, zur Planverwaltung und Abrechnung, zum Support sowie zu Logging, Monitoring und Fehleranalyse. Optional können von Seiten des Verantwortlichen ausgelöste KI-Optimierungen von Produktdaten als Vorschläge über Mistral AI verarbeitet werden.

1.2 Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem zwischen den Parteien geschlossenen Hauptvertrag in Zusammenhang stehen und bei der der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in

Berührung kommen, die von dem Verantwortlichen stammen oder für denselben erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.

1.3 Nicht Gegenstand dieses Vertrags sind Verarbeitungen, bei denen der Auftragsverarbeiter Zwecke und wesentliche Mittel der Verarbeitung selbst festlegt und deshalb als eigener Verantwortlicher handelt. Dies gilt insbesondere für die Anbahnung, Begründung, Durchführung und Abrechnung der eigenen Vertragsbeziehung, die Erfüllung handels- und steuerrechtlicher Pflichten, die eigene Forderungsverwaltung, eigene Marketingmaßnahmen sowie die allgemeine Verwaltung und Absicherung der eigenen IT- und Geschäftssysteme, soweit diese Verarbeitungen nicht im Auftrag des Verantwortlichen erfolgen. Soweit der Auftragsverarbeiter bei solchen eigenen Verarbeitungen Zwecke und wesentliche Mittel der Verarbeitung selbst festlegt, trägt er hierfür die alleinige datenschutzrechtliche Verantwortung und handelt nicht als Auftragsverarbeiter im Sinne dieses Vertrages. Über solche Verarbeitungen informiert der Auftragsverarbeiter zudem nach Maßgabe der Art. 13 und Art. 14 DSGVO.

(2) Zweck der Verarbeitung

2.1 Die Verarbeitung personenbezogener Daten erfolgt ausschließlich zur Bereitstellung, zum Betrieb, zur technischen Administration, zur Wartung, Fehlerbehebung und zur vertragsbezogenen technischen Verbesserung der Plattform RocketFeed sowie zur Erbringung der im Hauptvertrag vereinbarten Leistungen. Hierzu gehören insbesondere die Registrierung und Authentifizierung der Nutzerinnen und Nutzer, die Verwaltung von Nutzerkonten und Firmenzugehörigkeiten. Ferner umfasst der Verarbeitungszweck die technische Gewährleistung der Sicherheit und Funktionsfähigkeit der Plattform. Eine Verarbeitung zu eigenen, von der Leistungserbringung unabhängigen Zwecken des Auftragsverarbeiters, insbesondere zur eigenständigen Profilbildung, zu eigenen Marketingzwecken oder zum Training von KI-Modellen mit den übermittelten Daten, ist nicht umfasst. Etwaige KI-gestützte Optimierungen von Produktdaten erfolgen ausschließlich im Auftrag und nach Weisung des Verantwortlichen.

2.2 Im Übrigen ergeben sich Umfang und Zweck der Verarbeitung aus dem zwischen den Parteien geschlossenen Hauptvertrag.

(3) Art der Verarbeitung

3.1 Die Verarbeitung erfolgt insbesondere durch die Registrierung und Authentifizierung des Verantwortlichen. Derselbe kann sich entweder mittels E-Mail und Passwort oder über Google Login (OAuth 2.0) registrieren. Bei einem Google Login erfolgt die Authentifizierung über Google. Der Auftragsverarbeiter erhält sodann die Google-Account-Kennung und E-Mail-Adresse von Google zurück. Diese Accountdaten werden auf der Hetzner-Infrastruktur in Deutschland gespeichert. Weitere Nutzer können durch den Verantwortlichen per E-Mail-Einladung mit einmaligem Token hinzugefügt werden. Ferner erfolgt eine Abfrage und Verarbeitung des Planstatus über Stripe. Hierbei werden die Account-ID und der Planstatus mit Stripe ausgetauscht. Zahlungs- und Zahlungsmitteldaten werden innerhalb der Stripe-Systeme verarbeitet und gespeichert. Außerdem werden die Produktfeeds der Verantwortlichen aus dem Shop oder PIM der Verantwortlichen importiert. Der Import und die Speicherung finden vollständig auf der Hetzner-Infrastruktur statt. Eine Übermittlung von Produktdaten an einen KI-Dienst erfolgt ausschließlich, wenn der Verantwortliche die betreffende KI-Funktion aktiviert oder im Einzelfall auslöst. Übermittelt werden nur die für die angeforderte Optimierung erforderlichen Produkt- und Prompt-Daten sowie eine technisch erzeugte Anfragekennung.

Der Auftragsverarbeiter übermittelt keine Account-, Vertrags-, Abrechnungs- oder Authentifizierungsdaten, soweit diese nicht aus technischen Gründen zwingend erforderlich sind. Der Verantwortliche hat sicherzustellen, dass von ihm eingegebene Produktdaten und Custom Prompts keine für die Optimierung nicht erforderlichen personenbezogenen Daten oder besonderen Kategorien personenbezogener Daten enthalten. Sofern Produktdaten per KI optimiert werden, übermittelt der Auftragsverarbeiter die betroffenen Daten und einen internen Prompt an Mistral AI und erhält die Optimierungsvorschläge zurück. Optional können auf ausdrückliche Veranlassung des Verantwortlichen ausgewählte, für die Optimierung erforderliche Produktdaten, ein interner Prompt, ein optionaler Custom Prompt und eine technisch erzeugte Anfragekennung an Mistral AI SAS in der Region Europa übermittelt und dort ausschließlich zur Erstellung von Optimierungsvorschlägen im Auftrag und nach Weisung des Verantwortlichen verarbeitet werden. Direkte Kundenkennungen werden vor der Übermittlung entfernt, soweit sie für die angeforderte Verarbeitung nicht erforderlich sind.

3.2 Die Verarbeitung erfasst das Erheben, Erfassen, Speichern, Ordnen, Auslesen, Abfragen, Verwenden, Übermitteln, Abgleichen, Einschränken, Löschen oder Vernichten personenbezogener Daten, soweit dies zur Erbringung der unter § 1 Abs. 1 genannten, zwischen den Parteien gemäß des Hauptvertrages vereinbarten Leistung erforderlich ist.

(4) Dauer der Verarbeitung

4.1 Dieser Vertrag beginnt mit der Unterzeichnung des Hauptvertrages, der zwischen den Parteien geschlossen wurde, oder sobald der Verantwortliche den Bestimmungen des Hauptvertrages im Rahmen der Registrierung, der Einrichtung eines Kontos oder eines sonstigen dokumentierten elektronischen Vertragsschlussverfahrens zustimmt.

4.2 Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages und damit nach der Dauer der auftragsbezogenen Verarbeitung. Sie endet erst, wenn sämtliche Daten des Verantwortlichen nach Maßgabe des § 9 zurückgegeben oder gelöscht sind, soweit keine gesetzliche Speicherungspflicht besteht.

§ 2 Art der verarbeiteten Daten und Kreis der betroffenen Personen

(1) Art der verarbeiteten Daten

Der Auftragsverarbeiter kann für die in § 1 Abs. 1 beschriebene Leistung, welche sich nach dem zugrundeliegenden Hauptvertrag richtet, insbesondere folgende Kategorien personenbezogener Daten verarbeiten:

- Personenstammdaten und Kommunikationsdaten; insbesondere Vorname, Nachname, E-Mail-Adresse, Firmenname, Google-Account-ID sowie Nutzer- und Firmenzugehörigkeit
- Vertrags-, Plan- und Abrechnungsdaten; insbesondere Account-ID, Plan-Informationen und Planstatus sowie, soweit innerhalb von Stripe verarbeitet, Vorname, Nachname, Firmenname, Anschrift, E-Mail-Adresse, Umsatzsteuer-Identifikationsnummer und Zahlungsdaten
- Nutzungs-, Log- und Fehlerdaten; insbesondere Funktions- und Fehlermeldungen, Synchronisationsvorgänge, Login-Zeitpunkte, Nutzer-ID sowie technische Daten aus Cookies und Local Storage, darunter Session-ID, CSRF-Token, Präferenzen und der zuletzt ausgewählte Arbeitskontext
- Inhaltsdaten, soweit diese im Rahmen der Leistung bereitgestellt oder verarbeitet werden; insbesondere Produktdaten, Preise, Bestände, Produktbeschreibungen, Bild- und Produkt-URLs, Kategorien u.v.m.

Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO sowie personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO ist nicht Vertragsgegenstand. Der Verantwortliche darf solche Daten nur nach vorheriger ausdrücklicher Vereinbarung und Festlegung zusätzlicher Schutzmaßnahmen bereitstellen.

(2) Kreis der betroffenen Personen

Betroffene Personen sind insbesondere:

- Kundinnen und Kunden, Interessentinnen und Interessenten, Nutzerinnen und Nutzer der Plattform, Website-Besucherinnen und Website-Besucher sowie Ansprechpartnerinnen und Ansprechpartner der Kunden,
- Beschäftigte, freie Mitarbeitende und sonstige autorisierte Nutzerinnen und Nutzer oder Ansprechpartnerinnen und Ansprechpartner des Verantwortlichen,
- sonstige natürliche Personen,

soweit deren Daten im Rahmen der Feed-Verarbeitung, der Supportkommunikation, der Abrechnung oder der Nutzung der Website verarbeitet werden.

§ 3 Weisungsbindung des Auftragsverarbeiters

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich in Bezug auf Übermittlungen personenbezogener Daten an ein Drittland oder eine internationale Organisation, soweit er nicht durch Unionsrecht oder deutsches Recht zu einer Verarbeitung verpflichtet ist. Ist der Auftragsverarbeiter gesetzlich zu einer Verarbeitung verpflichtet, teilt er dem Verantwortlichen die betreffende rechtliche Anforderung vor der Verarbeitung mit, soweit das betreffende Recht eine solche Mitteilung nicht aus wichtigem öffentlichem Interesse untersagt. Die erstmalige Weisung ergibt sich aus diesem Vertrag, dem zugrundeliegenden Hauptvertrag und den vom Verantwortlichen innerhalb der Plattform vorgenommenen Einstellungen und Funktionsaufrufen. Weitere Weisungen können schriftlich oder in Textform, über die vereinbarten Kontakt- oder Supportkanäle, erteilt werden. Dabei dokumentiert der Auftragsverarbeiter die ihm erteilten Weisungen. Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO, das BDSG oder eine andere anwendbare Datenschutzbestimmung verstößt, informiert er den Verantwortlichen unverzüglich. Er ist berechtigt und, soweit die Ausführung der Weisung zu einem eigenen Rechtsverstoß führen würde, verpflichtet, die Ausführung bis zur Bestätigung, Änderung oder Rücknahme der Weisung auszusetzen. Eine Bestätigung durch den Verantwortlichen verpflichtet den Auftragsverarbeiter dabei nicht zur Ausführung einer rechtswidrigen Weisung. In einem solchen Fall haben die Parteien das weitere Vorgehen unverzüglich miteinander abzustimmen.

§ 4 Pflichten des Auftragsverarbeiters

(1) Verarbeitung lediglich im vereinbarten Umfang

Der Auftragsverarbeiter verarbeitet personenbezogene Daten des Verantwortlichen ausschließlich innerhalb des in diesem Vertrag und im Hauptvertrag festgelegten Auftragsumfangs. Weitergehende Weisungen sind nur verbindlich, soweit sie sich innerhalb des Vertragsgegenstands und des anwendbaren Datenschutzrechts halten. Änderungen des Gegenstands, der Art oder der Zwecke der Verarbeitung bedürfen einer dokumentierten Anpassung dieses Vertrags oder seiner Anlagen.

(2) Vertraulichkeit und Sicherheit der personenbezogenen Daten

Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung dieses Vertrags sowie des zwischen den Parteien bestehenden Hauptvertrages unbedingt erforderlich ist. Dabei gewährleistet der Auftragsverarbeiter, dass sämtliche zur Verarbeitung befugten Personen bereits vor Beginn ihrer Tätigkeit zur Vertraulichkeit verpflichtet werden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung gilt auch nach Beendigung ihrer Tätigkeit fort. Zugriffsberechtigungen sind auf das für die jeweilige Aufgabe erforderliche Maß zu beschränken und regelmäßig zu überprüfen.

(3) Technische und organisatorische Maßnahmen (TOM)

Der Auftragsverarbeiter trifft mindestens die in Anhang I aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten gemäß Art. 32 DSGVO zu gewährleisten. Dabei darf der Auftragsverarbeiter die Maßnahmen an die technische Entwicklung anpassen, sofern das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen, die sich nachteilig auf die Sicherheit der Daten des Verantwortlichen auswirken können, teilt er dem Verantwortlichen vor ihrer Umsetzung mit.

§ 5 Unterstützung des Verantwortlichen

(1) Betroffenenrechte und weitere gesetzliche Unterstützungspflichten

1.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung von Betroffenenrechten nach Kapitel III der DSGVO, insbesondere bei Auskunftsansprüchen, bei der Berichtigung, Löschung oder Einschränkung der Verarbeitung, bei der Datenübertragbarkeit und bei dem Widerspruchsrecht gemäß Art. 21 DSGVO, soweit die Erfüllung dieser Rechte die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter betrifft. Hierzu wird der Auftragsverarbeiter auf dokumentierte Weisung des Verantwortlichen unverzüglich die vom Verantwortlichen angeordneten Berechtigungen, Löschungen, Einschränkungen oder Datenübertragungen umsetzen und sicherstellen, dass entsprechende Anordnungen ebenfalls gegenüber eingesetzten Unterauftragsverarbeitern umgesetzt werden.

1.2 Außerdem stellt der Auftragsverarbeiter dem Verantwortlichen auf berechtigte Anfrage die zur Erfüllung der nach Art. 28 DSGVO erforderlichen Informationen zur Verfügung. Dies kann insbesondere durch geeignete Dokumentationen, Selbstauskünfte, Zertifizierungen, Sicherheitskonzepte oder Auditberichte erfolgen.

1.3 Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter und betrifft die Anfrage Daten des Verantwortlichen, wird der Auftragsverarbeiter die Anfrage unverzüglich an den Verantwortlichen weiterleiten, sofern keine gesetzliche Pflicht zur unmittelbaren Bearbeitung besteht. Dabei unterstützt der Auftragsverarbeiter den Verantwortlichen und befolgt dessen Weisungen.

1.4 Der Auftragsverarbeiter unterstützt den Verantwortlichen ferner bei

- der Durchführung einer Datenschutz-Folgenabschätzung, sofern eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen birgt;
- einer Konsultation der zuständigen Aufsichtsbehörde(n), sofern sich aus der Datenschutz-Folgenabschätzung ergibt, dass die Verarbeitung ein hohes Risiko zur Folge hätte und soweit der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

- der Pflicht des Verantwortlichen zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, sobald derselbe feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
- der Einhaltung dessen Pflichten gemäß Art. 32 DSGVO sowie Art. 36 DSGVO, soweit sich diese Pflichten auf die seitens des Auftragsverarbeiters durchgeführte Verarbeitung beziehen und der Verantwortliche die Unterstützung nicht selbst leisten kann.

(2) Mitteilung bei Datenschutzverletzungen

2.1 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die personenbezogene Daten des Verantwortlichen betrifft.

2.2 Die Mitteilung enthält mindestens folgende Informationen, soweit dem Auftragsverarbeiter bekannt und ohne unverhältnismäßigen Aufwand ermittelbar:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten,
- soweit möglich, die Kategorien und die ungefähre Zahl der betroffenen Personen sowie die Kategorien und die ungefähre Zahl betroffener personenbezogener Datensätze,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten sowie
- eine Beschreibung der vom Auftragsverarbeiter bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Nicht unverzüglich bereitstellbare Informationen werden ohne unangemessene Verzögerung nachgereicht.

2.3 Eigene Meldungen gegenüber Aufsichtsbehörden oder betroffenen Personen nimmt der Auftragsverarbeiter nur auf dokumentierte Weisung des Verantwortlichen vor, soweit er nicht selbst gesetzlich zu einer Meldung oder Mitwirkung verpflichtet ist. Gesetzliche Melde-, Offenlegungs- und Kooperationspflichten bleiben unberührt.

§ 6 Unterauftragsverarbeiter

(1) Allgemeine Genehmigung

1.1 Der Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine Genehmigung, nachfolgende Unterauftragsverarbeiter und Dienste im jeweils beschriebenen Umfang einzusetzen:

- **Hetzner Online GmbH** - für Hosting, Speicherung und Backups der Plattform
- **Mistral AI SAS** - für KI-gestützte Optimierungsvorschläge für Produktdaten
- **Google Ireland Ltd.** - für OAuth Login, Google Ads API und die geplante Merchant Center API
- **Stripe Payments Europe, Limited** - für Zahlungsabwicklung und Planverwaltung
- **Calendly LLC** - für Terminbuchungen
- **Atlassian Pty Ltd (Jira)** - für Supporttickets

- **PXCH Holding I, LLC (Encharge)** - für den Newsletter-Versand.

Die Kontaktdaten dieser Unterauftragsverarbeiter sowie eine konkrete Beschreibung der Verarbeitung stellt der Auftragsverarbeiter in einer als Anhang II ausgewiesenen Liste gesondert bereit.

1.2 Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich so, dass diesen Datenschutzpflichten auferlegt werden, die den in diesem Vertrag vereinbarten Pflichten entsprechen und insbesondere die Einhaltung geeigneter technischer und organisatorischer Maßnahmen im Sinne des Art. 32 DSGVO sowie die Beachtung der Weisungen des Verantwortlichen sicherstellen.

1.3 Der Auftragsverarbeiter informiert den Verantwortlichen mindestens vier Wochen im Voraus ausdrücklich über alle beabsichtigten Änderungen und Erweiterungen der Liste des Anhangs II. Der Verantwortliche kann innerhalb von 14 Kalendertagen aus nachweisbarem datenschutzrechtlichem Grund widersprechen. Die Parteien bemühen sich um eine angemessene Lösung, insbesondere durch zusätzliche Schutzmaßnahmen, Nutzung eines gleichwertigen alternativen Dienstes oder Beschränkung der betroffenen Funktion. Ist innerhalb angemessener Frist keine zumutbare Lösung möglich, kann der Verantwortliche die von der Änderung betroffene Leistung außerordentlich kündigen. Aus zwingenden Gründen der Sicherheit oder der Betriebsstabilität darf eine Änderung ausnahmsweise kurzfristiger erfolgen. Der Auftragsverarbeiter informiert den Verantwortlichen in diesem Fall unverzüglich und begründet die Verkürzung.

(2) Widerspruchsrecht

2.1 Der Verantwortliche kann der Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichem Grund innerhalb von 14 Kalendertagen nach Zugang der Information widersprechen.

2.2 Erfolgt kein fristgerechter Widerspruch, gilt die Änderung als genehmigt.

(3) Verpflichtung der Unterauftragsverarbeiter

3.1 Der Auftragsverarbeiter verpflichtet Unterauftragsverarbeiter vertraglich so, dass die Datenschutzpflichten im Wesentlichen denen dieses Vertrags entsprechen.

3.2 Der Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Einhaltung der Pflichten durch eingesetzte Unterauftragsverarbeiter verantwortlich.

(4) Keine Unterauftragsverarbeitung

Keine Unterauftragsverarbeitung im Sinne dieses Vertrags sind Nebenleistungen ohne unmittelbaren Bezug zur Hauptverarbeitung, insbesondere Telekommunikations-, Post-, Transport-, Wartungs-, Zahlungs-, Versicherungs-, Rechtsberatungs- oder Steuerberatungsleistungen, sofern diese nicht gezielt mit der Verarbeitung personenbezogener Daten des Verantwortlichen beauftragt sind.

§ 7 Datenverarbeitungen in Drittländern, außerhalb des EWR/ der EU

Der Auftragsverarbeiter verarbeitet Daten des Verantwortlichen grundsätzlich innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums. Eine Übermittlung an ein Drittland oder ein Zugriff aus einem Drittland ist nur auf dokumentierte Weisung des Verantwortlichen oder im Rahmen eines nach diesem Vertrag genehmigten Unterauftragsverarbeiters zulässig und setzt die Einhaltung der Art. 44 - Art. 49 DSGVO voraus. Soweit kein Angemessenheitsbeschluss gemäß Art. 45 DSGVO besteht, stellt der Auftragsverarbeiter durch geeignete Garantien nach Art. 46 DSGVO, insbesondere durch die anwendbaren Standardvertragsklauseln der Europäischen Kommission, ein angemessenes Schutzniveau sicher. Dabei prüft derselbe, ob unter Berücksichtigung der Umstände der Übermittlung ergänzende technische, organisatorische oder vertragliche Maßnahmen erforderlich sind, und setzt diese erforderlichenfalls um. Außerdem informiert der Auftragsverarbeiter den Verantwortlichen über das für den jeweiligen Empfänger eingesetzte Transferinstrument. Fällt dessen Wirksamkeit weg oder kann es nicht mehr eingehalten werden, setzt der Auftragsverarbeiter den Verantwortlichen unverzüglich in Kenntnis und setzt die betroffene Übermittlung aus, sofern nicht unverzüglich ein anderes wirksames Instrument bereitgestellt wird. Diese Verpflichtungen gelten dabei auch für weitere Auftragsverarbeiter und deren Unterauftragsverarbeiter.

§ 8 Kontroll- und Informationsrechte des Verantwortlichen

(1) Allgemeine Berechtigung zur Verlangung eines Nachweises

1.1 Der Verantwortliche ist berechtigt, die Einhaltung dieses Vertrages und der gesetzlichen Vorgaben im erforderlichen Umfang zu überprüfen.

1.2 Zur Vermeidung unnötigen administrativen Aufwands erfolgen die Prüfungen dabei vorrangig durch:

- Auskünfte des Auftragsverarbeiters,
- Vorlage geeigneter Dokumentationen,
- Sicherheits- oder Datenschutzkonzepte,
- Zertifikate,
- Prüfberichte oder
- standardisierte Selbstauskünfte

jeweils auf entsprechendes Verlangen des Verantwortlichen.

(2) Vor-Ort-Prüfungen

2.1 Sofern geeignete Nachweise nach § 8 Abs. 1 Ziffer 1.2 nicht ausreichen oder wenn ein begründeter Anlass besteht, insbesondere nach einer Datenschutzverletzung oder bei konkreten Anhaltspunkten für einen Vertragsverstoß, ist eine Vor-Ort-Prüfung zulässig.

2.2 Dabei sind derartige Vor-Ort-Prüfungen mit angemessener Frist anzukündigen, während üblicher Geschäftszeiten durchzuführen und auf den erforderlichen Umfang zu beschränken. Unangekündigte Prüfungen durch zuständige Aufsichtsbehörden und dringende Prüfungen aus wichtigem Grund bleiben unberührt.

2.3 Der Auftragsverarbeiter wirkt an der Vor-Ort-Prüfung mit und behebt festgestellte Verstöße ohne unangemessene Verzögerung.

§ 9 Löschung und Rückgabe nach Vertragsende

Nach Beendigung der Verarbeitung personenbezogener Daten oder nach Ende dieses Vertrags löscht der Auftragsverarbeiter sämtliche personenbezogene Daten des Verantwortlichen, die im Rahmen dieses Auftragsverarbeitungsverhältnisses verarbeitet wurden, oder er gibt sie dem Verantwortlichen nach dessen Wahl zurück, soweit keine gesetzliche Aufbewahrungspflicht für eine längere Speicherung besteht. Die Löschung umfasst insbesondere produktiv gespeicherte Daten des Verantwortlichen, einschließlich Nutzerkonten, Original- und optimierte Feeds, Prompts und KI-Outputs, Regeln und Konfigurationen, API-Keys und Tokens sowie Log- und Fehlerdaten. Der Auftragsverarbeiter hat die Durchführung der Löschung oder Rückgabe schriftlich oder in Textform zu dokumentieren und dem Verantwortlichen nachzuweisen.

§ 10 Haftungsregelungen

Der Auftragsverarbeiter haftet dem Verantwortlichen für Schäden, die dieser durch eine nicht vertragsgemäße oder nicht weisungskonforme Verarbeitung personenbezogener Daten erleidet, nach Maßgabe der gesetzlichen Bestimmungen und der im Hauptvertrag vereinbarten Haftungsregelungen. Soweit der Auftragsverarbeiter nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist, entfällt seine Haftung. Der Verantwortliche und der Auftragsverarbeiter verpflichten sich, einander im Innenverhältnis insoweit freizustellen, als einer von ihnen allein oder überwiegend für einen Verstoß gegen datenschutzrechtliche Bestimmungen oder gegen die Regelungen dieses Vertrages verantwortlich ist.

§ 11 Schlussbestimmungen

Sollten einzelne Bestimmungen dieses Vertrags unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame oder undurchführbare Bestimmung durch eine wirksame Regelung ersetzen, die dem wirtschaftlichen und rechtlichen Zweck der ursprünglichen Regelung möglichst nahekommt.

Verantwortlicher	**Auftragsverarbeiter**
Ort, Datum	Ort, Datum
Unterschrift	Unterschrift
Name in Druckbuchstaben	Name in Druckbuchstaben
Funktion	Funktion

ANHANG I

Technische und Organisatorische Maßnahmen (TOM), einschließlich zur Gewährleistung der Sicherheit der Daten

Stand: 21.09.2026

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen im Sinne des Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die in diesem Anhang beschriebenen Maßnahmen konkretisieren die im Auftragsverarbeitungsvertrag vereinbarten Anforderungen an die Sicherheit der Verarbeitung.

Diese Maßnahmen umfassen insbesondere:

1. Zugriffsbeschränkungen und Passwortschutz

Der Zugriff auf Systeme und personenbezogene Daten ist auf berechtigte Nutzer im Verantwortungsbereich des Auftragsverarbeiters beschränkt und erfolgt über individuelle Benutzerkonten. Passwörter müssen angemessene Mindestanforderungen erfüllen, insbesondere hinsichtlich Länge und Komplexität, und dürfen nicht gemeinsam genutzt oder ungesichert gespeichert werden.

2. Authentifizierungs- und Berechtigungskonzepte

Berechtigungen werden nach dem Rollen- und Need-to-know-Prinzip vergeben, regelmäßig überprüft und bei Wegfall der Erforderlichkeit unverzüglich angepasst oder entzogen. Für besonders schutzbedürftige Zugriffe, insbesondere auf administrative Konten und produktive personenbezogene Daten, wird, soweit angemessen, eine Mehrfaktor-Authentifizierung eingesetzt.

3. Verschlüsselung der Daten bei Übertragung oder Speicherung

Personenbezogene Daten werden bei der Übertragung über öffentliche Netze mittels aktueller Transportverschlüsselung, insbesondere TLS/HTTPS, geschützt. Bei erhöhtem Schutzbedarf wird zusätzlich eine Verschlüsselung gespeicherter Daten oder geeigneter Datenträger eingesetzt; kryptografische Verfahren und Schlüssellängen entsprechen dem Stand der Technik und werden regelmäßig überprüft.

4. Pseudonymisierung und Verschlüsselung personenbezogener Daten

Soweit es für den jeweiligen Verarbeitungszweck möglich und angemessen ist, werden personenbezogene Daten pseudonymisiert oder verschlüsselt verarbeitet. Zuordnungsinformationen und kryptografische Schlüssel werden organisatorisch und technisch getrennt von den pseudonymisierten oder verschlüsselten Daten und gegen unbefugten Zugriff geschützt aufbewahrt.

5. Sicherung der Verfügbarkeit und Belastbarkeit der Systeme

Systeme und Dienste werden durch geeignete technische und organisatorische Vorkehrungen gegen Ausfall, Überlastung, unbefugte Veränderungen und Verlust geschützt. Sicherheitsrelevante Aktualisierungen sowie Maßnahmen zur Erkennung und Behandlung von Störungen werden angemessen umgesetzt.

6. Gewährleistung einer Systemkonfiguration, einschließlich der Standardkonfiguration

Systeme werden nach einem dokumentierten und sicherheitsorientierten Konfigurationsverfahren eingerichtet und betrieben. Dabei werden nicht erforderliche Funktionen, Dienste und Zugänge deaktiviert oder beschränkt. Standardzugangsdaten sind vor dem produktiven Einsatz zu ändern, wobei sicherheitsrelevante Konfigurationsänderungen kontrolliert umgesetzt werden.

7. Backup- und Wiederherstellungsverfahren

Für personenbezogene Daten werden regelmäßige Sicherungskopien nach einem dokumentierten Backup-Konzept erstellt und gegen Verlust sowie unbefugten Zugriff geschützt. Wiederherstellungsverfahren werden in angemessenen Abständen getestet, um die Verfügbarkeit der Daten nach einem physischen oder technischen Zwischenfall zeitnah wiederherstellen zu können.

8. Protokollierung sicherheitsrelevanter Vorgänge

8.1 Sicherheitsrelevante Ereignisse, insbesondere Änderungen von Berechtigungen, administrative Zugriffe und erkennbare Sicherheitsvorfälle, werden soweit technisch möglich protokolliert. Die Protokolle sind gegen unbefugte Veränderung und Einsichtnahme geschützt und werden nur für festgelegte Zwecke sowie innerhalb angemessener Fristen aufbewahrt.

8.2 Sicherheitsrelevante Auffälligkeiten werden durch das bestehende Logging und Monitoring erkannt, bewertet und dokumentiert. Mitarbeitende melden vermutete oder festgestellte Sicherheitsvorfälle unverzüglich an die für Informationssicherheit und Datenschutz zuständige interne Stelle. Der Auftragsverarbeiter bewertet den Vorfall, begrenzt dessen Auswirkungen, sichert relevante Informationen und dokumentiert die ergriffenen Maßnahmen. Betrifft der Vorfall personenbezogene Daten des Verantwortlichen, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich und unterstützt ihn mit den verfügbaren Angaben bei der Prüfung und Erfüllung gesetzlicher Melde- und Benachrichtigungspflichten. Eigene Meldungen gegenüber Aufsichtsbehörden oder betroffenen Personen nimmt der Auftragsverarbeiter nur aufgrund einer Weisung des Verantwortlichen oder aufgrund einer gesetzlichen Verpflichtung vor.

9. Verfahren zur regelmäßigen Überprüfung und Anpassung der Maßnahmen

Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird regelmäßig sowie anlassbezogen, insbesondere bei wesentlichen System-, Prozess- oder Risikoveränderungen, überprüft. Festgestellte Schwachstellen und erforderliche Anpassungen werden dokumentiert und risiko-orientiert umgesetzt; der Verantwortliche wird über wesentliche Änderungen informiert, soweit sie seine Datenverarbeitung betreffen.

10. Dokumentiertes Lösch- und Rückgabeverfahren

10.1 Lösch- und Rückgabevorgänge werden auf Grundlage dokumentierter Weisungen des Verantwortlichen durchgeführt. Die Weisung enthält dabei zumindest Angaben zum betroffenen Datenbestand, zum Umfang der Löschung oder Rückgabe, zum gewünschten Zeitpunkt sowie zu etwaigen gesetzlichen Aufbewahrungspflichten. Soweit der Auftragsverarbeiter gesetzlich zur weiteren Aufbewahrung einzelner Daten verpflichtet ist, informiert er den Verantwortlichen darüber.

10.2 Der dokumentierte Löschprozess umfasst die Zuordnung der jeweiligen Datenkategorie zu einer festgelegten Speicher- und Löschfrist, die Auslösung der Löschung bei Wegfall des Verarbeitungszwecks oder nach Vertragsende, die Prüfung der Löschung sowie deren Protokollierung. Gelöschte Daten dürfen nicht erneut in Backups übernommen werden. Backups werden nach 14 Tagen überschrieben; Supportdaten werden nach zwei Tagen aus den Backups entfernt beziehungsweise nicht weiter vorgehalten. Soweit eine selektive Löschung einzelner Datensätze aus einem Backup technisch nicht möglich ist, wird dies dokumentiert und durch die begrenzte Backup-Retention kompensiert; nach Ablauf der jeweiligen Retentionsfrist sind die Daten nicht mehr rekonstruierbar.

ANHANG II

Liste der Unterauftragsverarbeiter

Stand: 21.09.2026

Der Verantwortliche hat die Inanspruchnahme folgender, im Auftragsverarbeitungsvertrag gemäß § 6 Abs. 1 Ziffer 1.1 genannten Unterauftragsverarbeiter genehmigt:

1.	
Name:	
Hetzner Online GmbH	
Anschrift:	
Industriestr. 25, 91710 Gunzenhausen, Deutschland	
Kontaktperson	
Name:	Funktion:
Datenschutzbeauftragter Hetzner Online GmbH	Datenschutzbeauftragter
Kontaktdaten:	
datenschutz@hetzner.com	
Beschreibung der Verarbeitung:	
Hosting, Betrieb und Speicherung der Plattform RocketFeed, einschließlich Datenbanken, Server-Infrastruktur, Backups und technischer Betriebsprotokolle auf Rechenzentren innerhalb Deutschlands bzw. des EWR.	

2.	
Name:	
Mistral AI SAS	
Anschrift:	
15 Rue Des Halles, 75001 Paris, Frankreich	
Kontaktperson	
Name:	Funktion:
Datenschutzkontakt Mistral AI	Datenschutz / Privacy
Kontaktdaten:	
contact@mistral.ai	
Beschreibung der Verarbeitung:	
Nutzung der von RocketFeed übermittelten Produktdaten sowie interner und ggf. kundenspezifischer Prompts zur Erstellung KI-gestützter Optimierungsvorschläge für Produktdaten ausschließlich im Auftrag und nach Weisung des Verantwortlichen; keine Nutzung zu eigenen Zwecken des Unterauftragsverarbeiters.	

3.	
Name:	
Google Ireland Limited	
Anschrift:	
Gordon House, Barrow Street, Dublin 4, Irland	
Kontaktperson	
Name:	Funktion:
Datenschutzbeauftragter Google Ireland Limited	Data Protection Office, Google Ireland Limited
Kontaktdaten:	
Datenschutz-Kontaktformular unter support.google.com/policies; postalisch an die o. g. Anschrift, Attn: Data Protection Office	
Beschreibung der Verarbeitung:	
Authentifizierung von Nutzerkonten per Google Login (OAuth 2.0) unter Verarbeitung der Google-Account-Kennung und E-Mail-Adresse; Abruf von KPI- und Performance-Daten über die Google Ads API sowie Übermittlung von Produktdaten und der Merchant-Center-Konto-ID über die Google Merchant Center API – jeweils ausschließlich im Auftrag und nach Weisung des Verantwortlichen.	

4.	
Name:	
Stripe Payments Europe, Limited	
Anschrift:	
3 Dublin Landings, North Wall Quay, Dublin 1, D01 C4E0, Irland	
Kontaktperson	
Name:	Funktion:
Privacy Team Stripe	Datenschutzkontakt
Kontaktdaten:	
privacy@stripe.com	
Beschreibung der Verarbeitung:	
Zahlungsabwicklung und Planverwaltung für die Plattform RocketFeed; Austausch von Account-ID und Plan-Status sowie Erhebung und Speicherung von Firmen-, Kontakt-, Rechnungs- und Zahlungsdaten innerhalb der Stripe-Systeme zur Abwicklung der Vergütung.	

5.	
Name:	
Calendly LLC	
Anschrift:	
271 17th St NW, 10th Floor, Atlanta, GA 30363, USA	
Kontaktperson	
Name:	Funktion:
Privacy Team Calendly	Datenschutzkontakt
Kontaktdaten:	
Kontaktformular gemäß Calendly Privacy Notice (calendly.com/legal/privacy-notice, Abschnitt „Contact"); postalisch an die o. g. Anschrift, Attn: Privacy	
Beschreibung der Verarbeitung:	
Terminbuchungen im Rahmen des Supports; Verarbeitung von Vor- und Nachname, E-Mail-Adresse sowie freiwilligen Angaben im Buchungstext ausschließlich zur Organisation und Durchführung von Support-Terminen.	

6.	
Name:	
Atlassian Pty Ltd	
Anschrift:	
Level 6, 341 George Street, Sydney NSW 2000, Australien	
Kontaktperson	
Name:	Funktion:
Privacy Team Atlassian	Datenschutzkontakt
Kontaktdaten:	
privacy@atlassian.com	
Beschreibung der Verarbeitung:	
Betrieb des Ticketsystems Jira zur Bearbeitung von Supportanfragen; Verarbeitung von Vor- und Nachname, E-Mail-Adresse sowie der Angaben im Ticket-Fließtext ausschließlich zur Bearbeitung des jeweiligen Support-Anliegens.	

7.	
Name:	
PXCH Holding I, LLC	
Anschrift:	
2423 SW 147th Ave #2262, Miami, FL 33185, USA	
Kontaktperson	
Name:	Funktion:
Slavcho Ivanov (Data Protection Representative Encharge)	Datenschutzkontakt
Kontaktdaten:	
slav@encharge.io	
Beschreibung der Verarbeitung:	
Versand des Newsletters; Verarbeitung von E-Mail-Adresse, Name, Anmeldezeitpunkt und Einwilligungsnachweis sowie – nach gesonderter Einwilligung – von Öffnungs- und Klickdaten. Datenhosting nach Anbieterangabe innerhalb der EU (AWS Frankfurt).	