AUFTRAGSVERARBEITUNGSVERTRAG

gemäß Art. 28 DSGVO

Stand: März 2026 · Version 2.0

ENTWURF — Keine Rechtsberatung. Anwaltliche Prüfung empfohlen.

Zwischen

dem Kunden der PrimeBalance-Plattform (nachfolgend „**Verantwortlicher**")

und

PrimeBalance UG (haftungsbeschränkt), Resi-Huber-Platz 1, 81371 München (nachfolgend „**Auftragsverarbeiter**")

---

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen im Rahmen der Nutzung der KI-gestützten SaaS-Plattform PrimeBalance gemäß den Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters.

(2) Art, Zweck und Umfang der Datenverarbeitung ergeben sich aus **Anlage 1** dieses Vertrags.

(3) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags (SaaS-Nutzungsvertrag).

---

§ 2 Weisungsrecht

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach dem Recht der Europäischen Union oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtliche Anforderung vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Verantwortlichen werden in diesem Vertrag festgelegt und können durch individuelle Einzelweisungen ergänzt werden. Einzelweisungen bedürfen der Textform.

(3) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt.

---

§ 3 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter gewährleistet, dass die mit der Verarbeitung betrauten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Der Auftragsverarbeiter trifft die erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO. Die konkreten Maßnahmen sind in **Anlage 2** beschrieben.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung der Pflichten nach Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldepflichten bei Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Beantwortung von Anträgen betroffener Personen nach Kapitel III der DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch).

(5) Der Auftragsverarbeiter löscht oder gibt nach Wahl des Verantwortlichen nach Abschluss der Verarbeitung alle personenbezogenen Daten zurück und löscht bestehende Kopien, es sei denn, nach dem Recht der Union oder der Mitgliedstaaten besteht eine Pflicht zur Speicherung.

(6) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen (Audits), die vom Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden. Der Auftragsverarbeiter trägt die Kosten der Mitwirkung bei Audits; die Kosten des Prüfers trägt der Verantwortliche.

---

§ 4 KI-gestützte Datenverarbeitung

(1) Im Rahmen der Erbringung der vertraglich vereinbarten Leistungen setzt der Auftragsverarbeiter **Künstliche Intelligenz (KI)** ein. Die KI-Agenten der Plattform nutzen Sprachmodelle (Large Language Models) von Drittanbietern zur Verarbeitung von Kundendaten. Die eingesetzten KI-Anbieter sind in **Anlage 3** als Unterauftragsverarbeiter aufgeführt.

(2) Die Übermittlung von Kundendaten an KI-Modell-Anbieter erfolgt ausschließlich zum Zweck der Erbringung der vertraglich vereinbarten Leistungen (insbesondere automatisierte Kategorisierung, Buchungsvorschläge, Steuerberechnungen, Lohnabrechnungen und Berichterstellung).

(3) **Kundendaten werden von den KI-Modell-Anbietern nicht zum Training, zur Verbesserung oder zur Evaluierung von KI-Modellen verwendet.** Der Auftragsverarbeiter hat mit allen KI-Modell-Anbietern vertragliche Vereinbarungen geschlossen, die ein solches Training ausdrücklich ausschließen.

(4) Die KI-Verarbeitung erfolgt über **EU-basierte Endpunkte**:

a) **Anthropic Claude**: Verarbeitung über Google Vertex AI mit Datenverarbeitung in EU-Rechenzentren (Frankfurt/Niederlande);

b) **Mistral AI**: Verarbeitung über EU-Endpunkte in Frankreich.

(5) Der Auftragsverarbeiter wendet, soweit technisch möglich und wirtschaftlich verhältnismäßig, **Pseudonymisierungsmaßnahmen** vor der Übermittlung an KI-Modelle an. Insbesondere werden direkte Personenidentifikatoren (Namen, Adressen, Steuernummern) durch Platzhalter oder Referenz-IDs ersetzt,

soweit dies die Funktionalität der KI-Verarbeitung nicht wesentlich beeinträchtigt.

(6) Der Auftragsverarbeiter dokumentiert für jede KI-Verarbeitung den eingesetzten Modellanbieter, den Verarbeitungszweck, die Art der verarbeiteten Daten und den Verarbeitungsort. Diese Dokumentation wird dem Verantwortlichen auf Anfrage bereitgestellt.

---

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen. Die aktuellen Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mindestens **30 Tage im Voraus** per E-Mail. Der Verantwortliche hat das Recht, gegen solche Änderungen innerhalb von 14 Tagen nach Mitteilung Einspruch einzulegen.

(3) Erhebt der Verantwortliche Einspruch und kann keine einvernehmliche Lösung gefunden werden, hat der Verantwortliche das Recht, den Hauptvertrag mit einer Frist von 30 Tagen zu kündigen.

(4) Der Auftragsverarbeiter legt jedem Unterauftragsverarbeiter im Wege eines Vertrags die gleichen Datenschutzpflichten auf, wie sie in diesem Vertrag festgelegt sind. Der Auftragsverarbeiter haftet dem Verantwortlichen gegenüber für die Einhaltung der Datenschutzpflichten durch den Unterauftragsverarbeiter.

---

§ 6 Übermittlung in Drittländer

(1) Der Auftragsverarbeiter verarbeitet alle Daten grundsätzlich in Rechenzentren innerhalb der Europäischen Union.

(2) Soweit Unterauftragsverarbeiter mit Sitz außerhalb des EWR eingesetzt werden (vgl. Anlage 3), erfolgt die Datenübermittlung ausschließlich auf Grundlage von:

a) einem Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO; oder

b) EU-Standardvertragsklauseln (Standard Contractual Clauses, SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO in der jeweils aktuellen Fassung (derzeit: Durchführungsbeschluss (EU) 2021/914).

(3) Der Auftragsverarbeiter stellt sicher, dass für jeden Drittlandtransfer eine dokumentierte Transferfolgenabschätzung (Transfer Impact Assessment, TIA) vorliegt und dem Verantwortlichen auf Anfrage zur Verfügung gestellt wird.

(4) Die aktuellen Drittlandtransfers sind in Anlage 3 gesondert gekennzeichnet.

---

§ 7 Meldung von Datenschutzverletzungen

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, **spätestens jedoch innerhalb von 24 Stunden** nach Bekanntwerden. Diese vertragliche Frist ist strenger als die gesetzliche 72-Stunden-Frist des Art. 33 DSGVO und soll dem Verantwortlichen ausreichend Zeit für seine eigene Meldepflicht gegenüber der Aufsichtsbehörde geben.

(2) Die Meldung enthält mindestens:

a) eine Beschreibung der Art der Verletzung;

b) die Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze;

c) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Anlaufstelle;

d) eine Beschreibung der wahrscheinlichen Folgen;

e) eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen.

(3) Die Meldekette verläuft wie folgt:

a) Auftragsverarbeiter → Verantwortlicher: **innerhalb von 24 Stunden** nach Bekanntwerden;

b) Verantwortlicher → Aufsichtsbehörde: innerhalb von 72 Stunden nach Bekanntwerden (Art. 33 Abs. 1 DSGVO), soweit die Verletzung voraussichtlich zu einem Risiko führt;

c) Verantwortlicher → Betroffene Personen: unverzüglich, soweit ein hohes Risiko besteht (Art. 34 DSGVO).

---

§ 8 Datenschutzbeauftragter

Der Datenschutzbeauftragte des Auftragsverarbeiters ist erreichbar unter: **privacy@prime-balance.de**

---

§ 9 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Im Übrigen gelten die Haftungsregelungen des Hauptvertrags (AGB).

---

§ 10 Schlussbestimmungen

(1) Dieser Vertrag unterliegt deutschem Recht.

(2) Änderungen bedürfen der Textform.

(3) Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Verantwortlicher (Kunde) · Datum, Unterschrift

PrimeBalance UG (haftungsbeschränkt) · Datum, Unterschrift

ANLAGE 1: ART UND ZWECK DER DATENVERARBEITUNG

Kategorie	Beschreibung
Zweck der Verarbeitung	Bereitstellung der KI-gestützten SaaS-Plattform PrimeBalance zur Workflow-Automation im Finanz- und Rechnungswesen. Verarbeitung von Finanzdaten, Buchhaltungsdaten, Lohndaten, Steuerdaten, Belegdaten und Mandantendaten im Auftrag des Kunden. KI-gestützte Kategorisierung, Buchungsvorschläge, Steuerberechnungen, Lohnabrechnungen, Berichterstellung und ELSTER-Übermittlung.
Art der Verarbeitung	Erhebung, Speicherung, Ordnung, Strukturierung, Abfrage, Verwendung, Übermittlung (an DATEV-Schnittstelle, ELSTER-Schnittstelle, KI-Modell-Anbieter zur Verarbeitung), Einschränkung, Löschung von Daten im Rahmen der Plattformnutzung.
Kategorien betroffener Personen	Mandanten des Kunden (natürliche Personen), Mitarbeiter des Kunden und seiner Mandanten (insb. im Rahmen der Lohnabrechnung), Geschäftspartner, Lieferanten und Kunden des Kunden bzw. seiner Mandanten, Ansprechpartner und Kontaktpersonen.
Kategorien personenbezogener Daten	Name, Adresse, Kontaktdaten (E-Mail, Telefon), Geburtsdatum, Steuernummer, Steuer-Identifikationsnummer, Sozialversicherungsnummer, Bankverbindungen (IBAN, BIC), Rechnungsdaten, Gehaltsdaten (Brutto, Netto, Abzüge, SV-Beiträge, Steuerabzüge), Steuerklasse, Kirchensteuermerkmal, Buchungsdaten, Finanzdaten, Transaktionsdaten, Kryptowährungs-Wallet-Adressen (soweit zuordenbar).

Besondere Datenkategorien (Art. 9 DSGVO)	Werden grundsätzlich nicht verarbeitet. Sollten besondere Kategorien in Belegen enthalten sein (z.B. Gesundheitsdaten in Arztrechnungen, Gewerkschaftszugehörigkeit in Lohndaten, Religionszugehörigkeit im Kirchensteuermerkmal), liegt die Verantwortung für die Rechtmäßigkeit der Verarbeitung beim Verantwortlichen. Der Verantwortliche stellt sicher, dass eine geeignete Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO vorliegt.

ANLAGE 2: TECHNISCHE UND ORGANISATORISCHE MA■NAHMEN (TOMs)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahme	Umsetzung
Zutrittskontrolle	Rechenzentren von Google Cloud Platform (GCP) mit physischer Zugangskontrolle, Biometrie, 24/7-Überwachung, Sicherheitspersonal. ISO 27001 und SOC 2 Type II zertifiziert.
Zugangskontrolle	Authentifizierung per E-Mail/Passwort mit Mindestanforderungen (min. 12 Zeichen). Optional: Multi-Faktor-Authentifizierung (MFA). Session-Timeout nach Inaktivität (30 Minuten). Brute-Force-Schutz (Rate Limiting).
Zugriffskontrolle	Rollenbasiertes Berechtigungskonzept (RBAC) auf zwei Ebenen: Organisationsebene (Owner, Admin, Member) und Mandatsebene (Manager, Editor, Viewer). Mandantentrennung auf Datenbankebene (Row-Level Security). Mitarbeiter des Anbieters haben keinen Zugriff auf Kundendaten im Regelbetrieb.
Trennungskontrolle	Logische Trennung der Mandantendaten über organisationsspezifische IDs. Keine gemeinsame Datenhaltung verschiedener Kunden. Separate Datenbank-Schemata pro Organisation.

Pseudonymisierung	Vor der Übermittlung von Kundendaten an KI-Modell-Anbieter werden, soweit technisch möglich, direkte Personenidentifikatoren durch Referenz-IDs ersetzt. Die Zuordnungstabelle verbleibt ausschließlich im System des Auftragsverarbeiters.
Field-Level-Encryption	Besonders sensible Datenfelder (Steuernummern, Steuer-IDs, Sozialversicherungsnummern, Bankverbindungen, Gehaltsdaten) werden mittels **Google Cloud KMS** auf Feldebene verschlüsselt. Die Entschlüsselung erfolgt nur bei berechtigtem Zugriff im Anwendungskontext.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahme	Umsetzung
Weitergabekontrolle	Verschlüsselung aller Datenübertragungen mit TLS 1.3. Verschlüsselung ruhender Daten mit AES-256. Field-Level-Encryption für sensible Felder (s.o.). Keine unverschlüsselte Datenübertragung.
Eingabekontrolle	Event-sourced Architektur: Jede Datenänderung wird als unveränderliches Event protokolliert. Vollständiger Audit-Trail mit Zeitstempel, Benutzer-ID, IP-Adresse und Aktion. SHA-256 Content Hashing und Chain Hashing für Integritätssicherung.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, c DSGVO)

Maßnahme	Umsetzung
Verfügbarkeitskontrolle	Hosting auf GCP Cloud Run mit automatischer Skalierung. GCP Cloud SQL mit automatischen Backups (täglich, Aufbewahrung 30 Tage). Georedundante Speicherung innerhalb der EU (mindestens zwei Rechenzentren).
Wiederherstellbarkeit	Point-in-Time-Recovery der Datenbank. Recovery Time Objective (RTO): 4 Stunden. Recovery Point Objective (RPO): 24 Stunden.
Belastbarkeit	Automatische Skalierung bei Lastspitzen (GCP Cloud Run Auto-Scaling). DDoS-Schutz durch GCP Cloud Armor.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Maßnahme	Umsetzung
Datenschutz-Management	Internes Verzeichnis der Verarbeitungstätigkeiten. Regelmäßige Überprüfung und Aktualisierung der TOMs (mindestens jährlich). Schulung der Mitarbeiter zum Datenschutz.
Incident Response	Dokumentierter Prozess für die Behandlung von Datenschutzverletzungen. Meldung an Verantwortlichen innerhalb von 24 Stunden. Eskalationskette: Support → CTO → Geschäftsführung → Datenschutzbeauftragter.
Auftragskontrolle	Sorgfältige Auswahl von Unterauftragsverarbeitern. Vertragliche Bindung aller Unterauftragsverarbeiter an die gleichen Datenschutzstandards. Jährliche Überprüfung der Unterauftragsverarbeiter.
KI-Verarbeitungskontrolle	Dokumentation aller KI-Verarbeitungsvorgänge (Modellanbieter, Verarbeitungszweck, Datenarten, Verarbeitungsort). Regelmäßige Überprüfung der vertraglichen Zusagen der KI-Anbieter bzgl. Nicht-Training.

ANLAGE 3: GENEHMIGTE UNTERAUFTRAGSVERARBEITER

Nr.	Unterauftragsvera	Zweck	Standort	Drittlandtransfer	Garantien
1	**Google Cloud Platform** (Google Ireland Ltd.)	Hosting, Datenbank (Cloud SQL), Infrastruktur (Cloud Run), Key Management (Cloud KMS), KI-Verarbeitung (Vertex AI)	EU (Frankfurt, Niederlande)	Nein	ISO 27001, SOC 2 Type II, EU-SCCs

2	**Stripe Payments Europe Ltd.**	Zahlungsabwicklung, Rechnungsstellung, SEPA-Lastschrift	EU (Irland)	Nein	PCI DSS Level 1, SOC 2, ISO 27001
3	**Anthropic PBC**	KI-Modelle (Claude) für Textverarbeitung, Kategorisierung, Buchungsvorschläge, Berichterstellung — Zugriff ausschließlich über Google Vertex AI (EU-Endpunkte)	Datenverarbeitung in EU (über GCP Vertex AI)	Nein (EU-Verarbeitung über GCP)	SOC 2, vertraglicher Ausschluss von Training auf Kundendaten, Zero Data Retention
4	**Mistral AI** (Mistral AI SAS)	KI-Modelle für spezifische Verarbeitungsaufgaben (Validierung, Kategorisierung)	EU (Frankreich)	Nein	EU-basiert, vertraglicher Ausschluss von Training auf Kundendaten
5	**Resend Inc.**	E-Mail-Versand (Transaktionsmails: Registrierungsbestätigung, Passwort-Reset, Benachrichtigungen)	USA	**Ja**	EU-Standardvertragsklauseln (SCCs), TIA dokumentiert. Verarbeitete Daten: E-Mail-Adresse, Name des Empfängers, E-Mail-Inhalt.
6	**HubSpot Inc.** (HubSpot Germany GmbH)	CRM & Marketing-Automation (Kontaktverwaltung, E-Mail-Marketing, Support-Tickets)	USA/EU (Datenverarbeitung in EU über HubSpot EU-Rechenzentrum)	**Ja** (begrenzt)	EU-Standardvertragsklauseln (SCCs), SOC 2, ISO 27001, EU-Rechenzentrum verfügbar. Verarbeitete Daten: Kontaktdaten, Kommunikationshistorie.

7	**Google Analytics** (Google Ireland Ltd.)	Website-Analyse (prime-balance.de) — keine Verarbeitung von Plattform-Kundendaten	EU	Nein	ISO 27001, EU-SCCs. Hinweis: Betrifft nur Website-Besucher, keine Plattform-Nutzer im eingeloggten Bereich.

Hinweis zu Drittlandtransfers: Für Resend Inc. (USA) und HubSpot Inc. (USA) wurden EU-Standardvertragsklauseln (SCCs) nach dem Durchführungsbeschluss (EU) 2021/914 abgeschlossen. Transfer Impact Assessments (TIAs) liegen vor und werden dem Verantwortlichen auf Anfrage bereitgestellt. Über den Resend-Dienst werden ausschließlich transaktionale E-Mails versendet; keine Finanz-, Steuer- oder Mandantendaten werden an Resend übermittelt.

PrimeBalance UG (haftungsbeschränkt) · Resi-Huber-Platz 1, 81371 München · AVV gemäß Art. 28 DSGVO · Stand März 2026

Änderungshistorie

Version	Datum	Änderung
1.0	März 2026	Erstfassung
2.0	März 2026	Komplette Überarbeitung — Neuer § 4 (KI-gestützte Datenverarbeitung), erweiterte Anlage 1 (Lohndaten, Steuerdaten, Krypto-Wallet-Adressen), aktualisierte Anlage 2 (Field-Level-Encryption, KMS, erweiterte RBAC), komplett neue Anlage 3 (+ Anthropic, Mistral, Resend, HubSpot, Google Analytics), Drittlandtransfer-Dokumentation mit SCCs/TIA, Meldeketten-Klarstellung (24h/72h).