Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen

{{Firma des Verantwortlichen}}, {{Anschrift des Verantwortlichen}}, vertreten durch {{vertretungsberechtigte Person des Verantwortlichen}}

(nachfolgend „Verantwortlicher“)

und

ZORYVO Technologies {{Rechtsform}} {{Straße und Hausnummer}}, {{PLZ Ort}}, vertreten durch {{vertretungsberechtigte Person}}, eingetragen unter {{Registergericht und Registernummer}}, E-Mail {{E-Mail-Adresse}}, Telefon {{Telefonnummer}}

(nachfolgend „Auftragsverarbeiter“; für den technischen Betrieb von ZORYVO auch „Betreiber“)

Präambel

Der Auftragsverarbeiter betreibt die Software ZORYVO. Der Verantwortliche nutzt ZORYVO auf Grundlage des Hauptvertrags ({{Bezeichnung und Datum des Hauptvertrags}}, nachfolgend „Hauptvertrag“). Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag regelt die Rechte und Pflichten der Parteien nach Art. 28 DSGVO. Er ist Bestandteil des Hauptvertrags.

In ZORYVO heißt das Kundenkonto des Verantwortlichen „Owner“. Nutzer des Verantwortlichen mit der Rolle Owner heißen in diesem Vertrag Owner-Nutzer, Nutzer mit der Rolle Mitarbeiter heißen Mitarbeiter.

§ 1 Gegenstand und Dauer

(1) Gegenstand ist der Betrieb von ZORYVO für den Verantwortlichen. ZORYVO bindet die E-Mail-Postfächer, Kalender und Dateiablagen des Verantwortlichen (Microsoft 365 oder Google Workspace) an, speichert eingehende und gesendete E-Mails, analysiert sie mit einem KI-System, erstellt Antwortentwürfe, führt Aktionen nach Freigabe oder nach den Regeln des Verantwortlichen aus (Versand, Termine, Dateiablage), erfasst Rechnungen und verwaltet eine Kundendatenbank, Aufgaben, Fristen und Termine einschließlich einer öffentlichen Buchungsseite. Einzelheiten stehen in Anlage 1.

(2) Der Vertrag beginnt mit dem Hauptvertrag und endet mit ihm. Die Pflichten aus § 9 (Rückgabe und Löschung) gelten darüber hinaus, bis sie erfüllt sind.

(3) Der Hauptvertrag betrifft ZORYVO im eingeschränkten Funktionsumfang des Pilotbetriebs, sei es als Pilotvereinbarung, als Testphase nach der Registrierung oder als gebuchter Tarif. Wo dieser Vertrag vom Testpiloten spricht, gilt das für jede dieser Formen, solange die Software im Pilotbetrieb ist. ***[bitte klären: ob die Bezeichnung „Testpilot“ für Kunden, die sich online registrieren und einen Tarif buchen, beibehalten oder durch den Stand der Software ersetzt wird (Anlage 5).]*** Funktionen, die Anlage 5 nennt, sind nicht gebaut und nicht Gegenstand dieses Vertrags. Erweitert der Auftragsverarbeiter den Funktionsumfang während des Testpiloten um neue Datenarten oder neue Kategorien betroffener Personen, kündigt er das dem Verantwortlichen vorher in Textform an und aktualisiert die betroffenen Anlagen. Dasselbe gilt, wenn er eine Leistung einrichtet, die dieser Vertrag als nicht eingerichtet bezeichnet, etwa die Datenbank-Sicherung, den Virenscanner oder den System-Mailversand. Für neue Unterauftragsverarbeiter gilt § 6 Abs. 2.

(4) Die Anbindung von Google Workspace steht im Testpiloten nur eingeschränkt zur Verfügung, solange die Verifizierung durch Google aussteht. Im Testmodus des Anbieters läuft eine Verbindung nach 7 Tagen ab, und es sind höchstens 100 Testnutzer möglich. ***[bitte klären: Stand der Google-Verifizierung zum***

Pilotstart.]

(5) Inhalte (E-Mails, Dokumente, Kontaktdaten, KI-Ergebnisse) werden in der Europäischen Union gespeichert und verarbeitet: Datenbank, Authentifizierung und Dateispeicher bei Supabase in Frankfurt (Region eu-central-1), die Anwendung auf Vercel in Frankfurt (Region fra1), die KI-Verarbeitung an EU-Endpunkten der in Anlage 3 genannten Anbieter, der Versand von System- und Buchungs-E-Mails bei Brevo in der EU. Kennungen und Metadaten ohne Inhalte erhalten auch Dienste außerhalb der EU oder Dienste, deren Serverregion nicht angegeben ist. Welche Dienste das sind, mit welchen Daten und auf welcher vertraglichen Grundlage, steht in Anlage 3.

§ 2 Art und Zweck der Verarbeitung, Datenarten, betroffene Personen

Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen sind in Anlage 1 beschrieben.

§ 3 Weisungen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 lit. a DSGVO). Das gilt auch für die Übermittlung in ein Drittland oder an eine internationale Organisation; eine solche Übermittlung findet nur im Rahmen von Anlage 3 statt. Ausgenommen ist eine Verarbeitung, zu der der Auftragsverarbeiter nach dem Recht der Union oder eines Mitgliedstaats verpflichtet ist. In diesem Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

(2) Weisungen sind dieser Vertrag und die Einstellungen, die der Verantwortliche in ZORYVO vornimmt. Dazu gehören insbesondere:

- das Einschalten der KI-Verarbeitung mit der dort dokumentierten Rechtsgrundlage sowie das Erlauben oder Ausschließen des Ausweich-Anbieters;
- die Auswahl, die Reihenfolge und der Modus der Automationen (aus, Vorschlag, Freigabe, automatisch) sowie die Regeln des Verantwortlichen;
- die Schutz-Vorgaben und ihre Lockerung durch die Rolle Owner;
- die verbundenen Postfächer, Kalender und Laufwerke, der Importzeitraum alter E-Mails und das Scharfschalten der Automationen;
- die Rechte je Postfach (lesen, freigeben, senden, verwalten) und die Sichtbarkeit von Kategorien für Mitarbeiter;
- Support-Freigaben für den Betreiber (§ 4);
- Sperren, Auskunft und endgültiges Löschen einzelner Kontakte (§ 7).

Jede dieser Einstellungen wird mit Zeitpunkt und handelnder Person im Audit-Log des Verantwortlichen festgehalten. Weitere Weisungen erteilt der Verantwortliche in Textform an {{E-Mail-Adresse}}. Mündliche Weisungen bestätigt der Auftragsverarbeiter unverzüglich in Textform.

(3) Weisungsberechtigt sind die Owner-Nutzer des Verantwortlichen. Im Umfang ihres Rechts sind außerdem die Nutzer weisungsberechtigt, denen der Verantwortliche in ZORYVO ein Recht eingeräumt hat, etwa „Firmeneinstellungen“ (KI-Verarbeitung, Rechtsgrundlage, Ausweich-Anbieter, Zwei-Faktor-Pflicht für Mitarbeiter), „Automationen verwalten“ (Modus und Regeln der Automationen), „Geteilte Postfächer verbinden“ oder das Recht „verwalten“ an einem Postfach. Jeder Nutzer verbindet sein eigenes persönliches Postfach selbst. Das Lockern von Schutz-Vorgaben, das Scharfschalten der Automationen, Support-Freigaben und die Funktionen nach § 7 Abs. 2 bleiben der Rolle Owner vorbehalten. Der Verantwortliche kann weitere Personen in Textform benennen.

(4) Hält der Auftragsverarbeiter eine Weisung für einen Verstoß gegen die DSGVO oder andere

Datenschutzvorschriften, informiert er den Verantwortlichen unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung aussetzen, bis der Verantwortliche die Weisung bestätigt oder ändert.

(5) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere gegenüber seinen Beschäftigten und Korrespondenzpartnern. Die Rechtsgrundlage der KI-Verarbeitung stellt er selbst fest und dokumentiert sie in ZORYVO (Einstellungen, Datenschutz: Auswahl zwischen Vertrag, berechtigtem Interesse und Einwilligung sowie eine Begründung). Ohne diese Dokumentation lässt ZORYVO die KI-Verarbeitung nicht einschalten. ZORYVO prüft die Angabe nicht inhaltlich.

§ 4 Vertraulichkeit

(1) Der Auftragsverarbeiter gewährt nur Personen Zugang zu personenbezogenen Daten, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.

(2) Der Auftragsverarbeiter als Betreiber der Plattform (in ZORYVO: Rolle Plattform-Admin) sieht Inhalte des Verantwortlichen (E-Mails, Betreffe, Absenderadressen, Kontakte, Namen, Beträge, Dateinamen, Dokumente, Entwürfe, Debug-Inhalte) nur mit einer Support-Freigabe, die der Verantwortliche selbst erteilt. Die Freigabe nennt Umfang (nur Debug-Inhalte fehlgeschlagener Schritte, ein einzelnes Objekt oder alle Inhalte), Grund und Dauer. Sie gilt im Regelfall 48 Stunden und höchstens 7 Tage, ist jederzeit widerrufbar und wird in der Datenbank selbst durchgesetzt, nicht nur in der Oberfläche. Erteilung, Änderung und Widerruf einer Freigabe sowie jedes Ansehen von Debug-Inhalten stehen im Audit-Log des Verantwortlichen. Das Lesen einzelner E-Mails oder Kontakte unter einer Freigabe wird derzeit nicht je Zugriff protokolliert. Beim ersten Ansehen von Debug-Inhalten je Freigabe werden die Owner-Nutzer per E-Mail benachrichtigt, danach höchstens einmal täglich mit einer Zusammenfassung; das setzt den eingerichteten System-Mailversand voraus (Anlage 3, Brevo). Eine Freigabe für alle Inhalte deckt nur Postfächer, die der erteilende Owner-Nutzer selbst lesen darf; persönliche Postfächer von Mitarbeitern kann der Verantwortliche nicht ohne diese freigeben.

(3) Ohne Freigabe sieht der Betreiber nur Metadaten und Einstellungen: Firmenname und Kennung des Verantwortlichen, Automation, Aufgabentyp, Status, Fehlerart und Fehlernummer, Zeitpunkte, Nutzungs- und Kostenzahlen, Tarif und Stand der Testphase und des Abonnements, die Firmendaten und das Zustimmungsprotokoll des Verantwortlichen, Verbindungsstatus mit Adresse und Anzeigename der verbundenen Postfächer (auch der persönlichen Postfächer von Mitarbeitern), die Einstellungen der Automationen (einschließlich Signaturen und Ton-Vorgaben der Antwortentwürfe), Terminarten, Gastgeber und Buchungseinstellungen sowie E-Mail-Adresse, Anzeigename, Rolle und Sperrstatus der Nutzer des Verantwortlichen und dessen offene Einladungen. Audit-Einträge enthalten Kennungen der handelnden Nutzer, keine Inhalte. ***[bitte klären: ob Audit-Einträge mit Nutzerkennung als Metadaten ohne Freigabe für den Betreiber sichtbar sein dürfen.] [bitte klären: ob Signaturen und Postfachadressen ohne Freigabe für den Betreiber sichtbar bleiben sollen.]***

(4) Benachrichtigungen der Nutzer und deren Einstellungen liest nur die jeweilige Person selbst, nicht der Verantwortliche und nicht der Betreiber, auch nicht mit Freigabe.

§ 5 Sicherheit der Verarbeitung

(1) Der Auftragsverarbeiter trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die Anlage 2 beschreibt (Art. 28 Abs. 3 lit. c DSGVO).

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie ändern, wenn das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen teilt er dem Verantwortlichen in Textform mit und aktualisiert Anlage 2.

(3) Anlage 2 beschreibt Maßnahmen, die in ZORYVO umgesetzt sind. Hängt eine Maßnahme von einem

Dienst ab, der zum Stand dieses Vertrags nicht eingerichtet ist, sagt Anlage 2 das bei der Maßnahme ausdrücklich; zugesagt ist sie erst ab der Einrichtung (§ 1 Abs. 3). Geplante Maßnahmen stehen in Anlage 5 und sind nicht zugesagt.

§ 6 Unterauftragsverarbeiter

(1) Der Auftragsverarbeiter hält die Bedingungen für die Inanspruchnahme von Unterauftragsverarbeitern nach Art. 28 Abs. 2 und 4 DSGVO ein (Art. 28 Abs. 3 lit. d DSGVO). Der Verantwortliche erteilt die allgemeine Genehmigung für die in Anlage 3 genannten Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO).

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens 30 Tage vor dem Wechsel in Textform. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichen Grund in Textform widersprechen. Widerspricht er, suchen die Parteien eine Lösung. Kommt keine zustande, kann der Verantwortliche den Hauptvertrag mit Wirkung zum Zeitpunkt des Wechsels kündigen. Ohne Widerspruch gilt der Wechsel als genehmigt. ***[bitte klären: Ankündigungsfrist bestätigen.]***

(3) Der Auftragsverarbeiter legt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung dieser Pflichten.

(4) Ausnahmen, die der Verantwortliche kennt und billigt: Für Telegram und healthchecks.io besteht kein Vertrag nach Art. 28 Abs. 4 DSGVO, weil beide Anbieter keinen anbieten. Telegram erhält ausschließlich Alarme an den Betreiber ohne E-Mail-Inhalte und ohne Kontaktdaten (Alarmstufe, fester Fehlertitel, gekürzte Kennung des Verantwortlichen ohne Firmenname, Automation, Fehlerart, Zeitpunkte und Anzahl des Auftretens, Fehlernummer, Link in den Admin-Bereich). healthchecks.io erhält nach seiner Einrichtung nur den Zeitpunkt eines Pings ohne Inhalt und ohne Kennungen. ***[bitte klären: datenschutzrechtliche Bewertung von Telegram, insbesondere ob die gekürzte Kennung des Verantwortlichen dort ein personenbezogenes Datum ist (den Firmennamen erhält Telegram seit 2026-10-10 nicht mehr; ob der Firmenname eines Einzelunternehmers ein personenbezogenes Datum ist, bleibt für die Alarm-Mail über Brevo offen).]***

(5) Für den Dienst Inngest (Hintergrundjobs; erhält nur Kennungen und Status) liegt zum Stand dieses Vertrags noch kein Vertrag nach Art. 28 Abs. 4 DSGVO vor. Der Auftragsverarbeiter setzt Inngest für Daten des Verantwortlichen erst ein, wenn dieser Vertrag geschlossen ist oder Inngest auf einer vom Auftragsverarbeiter selbst betriebenen Instanz in der EU läuft. Vor Beginn der Verarbeitung für den Verantwortlichen teilt er in Textform mit, welche der beiden Varianten gilt, und aktualisiert Anlage 3.

(6) Die Dienste des Verantwortlichen selbst (Google Workspace, Microsoft 365: Postfach, Kalender, Dateiablage) sind keine Unterauftragsverarbeiter des Auftragsverarbeiters. ZORYVO spricht sie im Auftrag des Verantwortlichen mit den Zugriffsrechten an, die der Verantwortliche oder seine Nutzer beim Verbinden erteilen. Für die Verarbeitung durch diese Anbieter gelten die Verträge des Verantwortlichen mit ihnen.

§ 7 Unterstützung bei den Rechten der betroffenen Personen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anfragen betroffener Personen nach Kapitel III der DSGVO zu beantworten (Art. 28 Abs. 3 lit. e DSGVO). Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst. Ausgenommen sind Anfragen von Beschäftigten des Verantwortlichen zu ihrem eigenen Nutzerkonto (Absatz 4).

(2) ZORYVO stellt dem Verantwortlichen je Kontakt seiner Kundendatenbank drei Funktionen bereit. Sie stehen nur Owner-Nutzern zu und lassen sich nicht an Mitarbeiter übertragen. Sie sind nur im laufenden Betrieb verfügbar, nicht im pausierten Konto (§ 9 Abs. 2). Anfragen betroffener Personen nach Art. 15 bis 18 DSGVO, die der Verantwortliche im pausierten Konto nicht selbst bearbeiten kann, erledigt der Auftragsverarbeiter auf Weisung in Textform von Hand innerhalb von {{Frist für Betroffenenanfragen im pausierten Kundenkonto}}; das gilt auch nach dem Vertragsende bis zur Löschung (§ 9 Abs. 2). Jede Nutzung wird im Audit-Log des Verantwortlichen festgehalten.

a) **Auskunft erstellen** (Art. 15 DSGVO): ein maschinenlesbarer Export (JSON) der zu dem Kontakt gespeicherten Daten, soweit der Owner-Nutzer sie lesen darf. Enthalten sind:

- Stammdaten, eigene Felder und Kunden-Memory;
- E-Mails des Kontakts mit Metadaten und KI-Zusammenfassung;
- Leads, Aufgaben, Vorgänge, Erwartungen, Notizen und Änderungshistorie;
- Freigaben und Antwortentwürfe;
- Buchungen mit den Angaben des Kunden sowie Terminangebote (nur Metadaten);
- hochgeladene Dateien und E-Mail-Anhänge mit ihrem Text sowie eine Liste der von ZORYVO im Laufwerk des Verantwortlichen abgelegten Kopien (Name, Ordner, Link und Status, nicht die Kopien selbst);
- Automationsläufe.

Was an E-Mails aus Postfächern hängt, die der Owner-Nutzer nicht lesen darf, wird nur gezählt. Nicht enthalten sind Rechnungen, die Dateien selbst (nur ihr Text), Kalendereinträge beim Kalenderanbieter, Datenbank-Sicherungen und Nennungen der Person ohne Zuordnung zum Kontakt. Die Listen sind auf die jeweils neuesten Einträge begrenzt: Memory 1.000; E-Mails, Notizen, Änderungen, Freigaben, Buchungen, Terminangebote, Aufgaben, Vorgänge und Erwartungen je 500; Leads, Dateien und Automationsläufe je 200. Bei E-Mails, Notizen, Änderungen, Automationsläufen, Freigaben, Buchungen, Terminangeboten und Dateien weist der Export aus, wenn die Grenze erreicht ist. Bei Memory, Leads, Aufgaben, Vorgängen und Erwartungen fehlt dieser Hinweis. Den Rest der Auskunft ergänzt der Verantwortliche aus seinen eigenen Systemen (Postfach, Kalender, Buchhaltung).

b) **Endgültig löschen** (Art. 17 DSGVO): Nach einer Vorschau mit Zählung je Bereich und ausdrücklicher Bestätigung löscht eine Datenbankfunktion in einer Transaktion:

- den Kontakt mit E-Mail-Adressen, Kategorien, Tags und eigenen Feldern;
- seine Leads, Notizen und Memory-Punkte;
- E-Mails, die er gesendet hat, und ausgehende E-Mails, deren einzige Empfänger seine Adressen sind, samt KI-Analysen;
- Aufgaben, Vorgänge und Erwartungen;
- Freigaben und Entwürfe zu diesen E-Mails oder allein an seine Adressen (Entwürfe, die auch an andere Empfänger gehen, bleiben ohne seine Adresse bestehen);
- Buchungen und Terminangebote;
- hochgeladene Dateien und E-Mail-Anhänge mit Text, Vorschlägen und dem Objekt im Dateispeicher;
- die Debug-Inhalte zu diesen Objekten.

In allen übrigen Textfeldern und in den Protokollen des Verantwortlichen werden E-Mail-Adresse (nur als ganze Adresse), Name (Vor- und Nachname zusammen, als ganze Wörter, wie im Kontakt geschrieben) und Telefonnummer (ab sechs Ziffern, wie im Kontakt geschrieben, nicht als Teil einer längeren Nummer) durch „[gelöscht am TT.MM.JJJJ auf Anfrage]“ ersetzt; eine Telefonnummer, die auch ein anderer Kontakt oder eine Firma des Verantwortlichen hat (etwa eine Zentrale), und die Telefonfelder anderer Datensätze bleiben unverändert; die Protokolleinträge selbst bleiben bestehen. Die Löschung wirkt in Datenbank und

Dateispeicher sofort. Scheitert das Entfernen eines Dateiobjekts, wird die gesamte Löschung zurückgerollt und kann wiederholt werden. Das Löschprotokoll enthält nur Zählungen und Kennungen, keine Daten der Person.

c) **Sperren** (Art. 18 DSGVO): Der Kontakt bleibt bestehen, ist nur noch für die Rolle Owner sichtbar und wird von Automationen, vom Kontext für Antwortentwürfe und vom CSV-Export der Kundendatenbank ausgenommen; die Auskunft nach Buchstabe a bleibt möglich. E-Mails der Person werden nicht mehr analysiert. Ein optionales Enddatum dient nur als Erinnerung; es löscht nichts und hebt die Sperre nicht auf.

(3) Was das endgültige Löschen nicht erreicht, ist dem Verantwortlichen bekannt: Rechnungen und die Dateien, aus denen eine Rechnung erfasst wurde, bleiben bestehen (die Datei verliert nur die Zuordnung zum Kontakt); ob er sie wegen eigener Aufbewahrungspflichten behält, entscheidet der Verantwortliche, und ZORYVO weist in der Vorschau darauf hin. Kopien, die ZORYVO im Google Drive oder OneDrive des Verantwortlichen abgelegt hat, werden in der Vorschau aufgelistet, nicht gelöscht; der Verantwortliche löscht sie selbst. Antwortentwürfe, die ZORYVO auf Wunsch des Verantwortlichen im Postfach abgelegt hat (Anlage 1 Nr. 1, Antwortentwürfe), bleiben dort; der Verantwortliche löscht sie selbst. Termine im Kalender des Verantwortlichen und die Originale im Postfach bleiben unberührt. E-Mails mit weiteren Beteiligten werden nur geschwärzt. Nennungen nur mit Vor- oder Nachname, in anderer Schreibweise oder mit Anschrift werden nicht gefunden. Die E-Mail-Adresse der Person wird nicht gesperrt; ein späterer Abruf kann neue E-Mails dieser Adresse wieder anlegen. Besteht eine Datenbank-Sicherung (Anlage 4), verschwinden Kopien darin erst mit Ablauf des Sicherungsfensters.

(4) Für die Nutzerkonten der Beschäftigten des Verantwortlichen (E-Mail-Adresse, Anzeigename, Passwort und Faktoren beim Authentifizierungsdienst, Sitzungen, Sicherheitsereignisse) ist der Auftragsverarbeiter nach seiner Datenschutzerklärung (Abschnitte 2 und 4) selbst Verantwortlicher. Anfragen dazu beantwortet er selbst unter {{Datenschutz-Kontakt}} und informiert den Verantwortlichen. ZORYVO bietet für Nutzerkonten keine Selbstbedienung für Auskunft, Berichtigung oder Löschung; der Auftragsverarbeiter erledigt sie von Hand außerhalb der Oberfläche und bestätigt sie in Textform. Der Verantwortliche kann Mitgliedschaften beenden und Zugänge sofort beenden (Anlage 2 Nr. 1, Notschalter). Ebenso ist der Auftragsverarbeiter selbst Verantwortlicher für die Registrierungs-, Vertrags- und Abrechnungsdaten des Verantwortlichen und für den Schutz vor wiederholten Testphasen (Anlage 1 Nr. 1, letzter Absatz; Datenschutzerklärung, Abschnitte 4.9 bis 4.12).***[bitte klären: Einordnung als eigene Verantwortlichkeit oder als Auftragsverarbeitung (Nutzerkonten sowie Registrierungs-, Vertrags- und Abrechnungsdaten, Stripe), gleichlautend mit der Datenschutzerklärung (Abschnitte 2 und 4.9 bis 4.12) und § 8 Abs. 4; Verfahren und Frist für Auskunft und Löschung von Nutzerkonten.]***

§ 8 Unterstützung bei Sicherheit, Meldungen und Datenschutz-Folgenabschätzung

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen (Art. 28 Abs. 3 lit. f DSGVO).

(2) Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft, unverzüglich nach Kenntnis, spätestens innerhalb von 24 Stunden. Die Frist beginnt mit der Kenntnis des Auftragsverarbeiters, auch wenn ein Unterauftragsverarbeiter die Verletzung meldet. Die Meldung erfolgt in Textform an {{Meldeadresse des Verantwortlichen}}. ZORYVO hat dafür keine Funktion in der Oberfläche.***[bitte klären: Meldefrist bestätigen.]***

(3) Die Meldung enthält, soweit bekannt: Art der Verletzung; Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze; wahrscheinliche Folgen; ergriffene und vorgeschlagene

Maßnahmen; Zeitpunkt der Kenntnis; Name und Kontaktdaten der Ansprechperson ({{Datenschutz-Kontakt}}). Fehlen Informationen, meldet der Auftragsverarbeiter zuerst, was er weiß, und liefert den Rest ohne unangemessene Verzögerung nach. Er dokumentiert jede Verletzung mit Fakten und Kennungen, ohne Inhalte.

(4) Die Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) und die Benachrichtigung der betroffenen Personen (Art. 34 DSGVO) obliegen dem Verantwortlichen. Der Auftragsverarbeiter liefert dafür Fakten, Protokollauszüge (ohne Inhalte, soweit nicht freigegeben) und Textbausteine. Soweit der Auftragsverarbeiter für Daten selbst Verantwortlicher ist (nach § 7 Abs. 4 für die Nutzerkonten), meldet er an {{zuständige Aufsichtsbehörde}}. ***[bitte klären: Abgrenzung, für welche Daten der Auftragsverarbeiter selbst Verantwortlicher ist, insbesondere Nutzerkonten, Vertrags- und Zahlungsdaten.]***

(5) Zur Eindämmung einer Verletzung darf der Auftragsverarbeiter ohne gesonderte Weisung alle externen Aktionen des Verantwortlichen anhalten (Notbremse), Zugänge einzelner Nutzer beenden, Konten sperren und Geheimnisse der Plattform tauschen. Ebenso darf er Verbindungen zu Postfächern, Kalendern und Laufwerken trennen und Support-Freigaben widerrufen; dafür hat er keine Funktion in der Oberfläche, er tut es durch einen dokumentierten Eingriff in die Datenbank. Er informiert den Verantwortlichen über jeden Eingriff unverzüglich. Daten löscht oder schwärzt er zur Aufklärung nicht, bevor der Umfang geklärt ist.

(6) Für eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und eine vorherige Konsultation (Art. 36 DSGVO) stellt der Auftragsverarbeiter die Informationen aus den Anlagen 1 bis 4 bereit und beantwortet Fragen zur Funktionsweise von ZORYVO in angemessener Frist. Die Vorlagen für die Information der Beschäftigten und des Betriebsrats, die ZORYVO zum Download anbietet, sind Entwürfe des Auftragsverarbeiters und ersetzen keine eigene Prüfung des Verantwortlichen.

§ 9 Rückgabe und Löschung nach Ende der Verarbeitung

(1) Nach Ende des Hauptvertrags gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten zurück oder löscht sie und löscht vorhandene Kopien, soweit nicht das Recht der Union oder eines Mitgliedstaats eine Speicherung verlangt (Art. 28 Abs. 3 lit. g DSGVO).

(2) Umsetzung im Testpiloten: Es gibt keine automatische Export-Phase, keinen Gesamtexport auf Knopfdruck, keine automatische Löschung des Kontos nach dem Vertragsende (ausgenommen die Löschung nach einer Testphase ohne Buchung, Buchstabe e) und keine automatisch erzeugte Löschbestätigung. Der Auftragsverarbeiter führt Rückgabe und Löschung, außer im Fall des Buchstaben e, von Hand durch und weist beides in Textform nach. Der Ablauf:

a) Der Auftragsverarbeiter kündigt dem Verantwortlichen das Pausieren des Kontos rechtzeitig in Textform an. Auskünfte je Kontakt (JSON) sowie das Sperren und endgültige Löschen einzelner Kontakte sind nur im laufenden Betrieb möglich; der Verantwortliche erstellt sie vor dem Pausieren. Spätestens zum Vertragsende versetzt der Auftragsverarbeiter das Konto in den Zustand „pausiert“. Bei einem Konto mit Abrechnung über Stripe geschieht das mit dem Ende der Laufzeit automatisch (AGB § 9 Abs. 5), bei dem Ende der Testphase gilt Buchstabe e; bei einem Konto auf Grundlage einer Pilotvereinbarung geschieht es nicht automatisch. Ist dort bereits eine Kündigung mit Enddatum eingetragen, pausiert der Auftragsverarbeiter das Konto außerhalb der Oberfläche und weist das in Textform nach, weil die Verwaltungsoberfläche nur laufende Konten pausiert.***[bitte klären: Vorgehen in der Betriebsanleitung festlegen oder das Pausieren aus dem Zustand „gekündigt“ nachbauen.]*** Im Zustand „pausiert“ stoppt der Abruf von E-Mails, Automationen laufen nicht mehr, und externe Aktionen finden nicht mehr statt. Ausgenommen ist das Entfernen abgelaufener oder nicht mehr benötigter vorläufiger Reservierungen aus dem Kalender des Gastgebers, damit dort keine verwaisten Einträge stehen bleiben (Anlage 2 Nr. 2). Die öffentliche Buchungsseite zeigt „Online-Buchung derzeit nicht möglich“. Die Nutzer des Verantwortlichen können dann nur noch lesen. Im Rahmen ihrer Rechte bleiben zusätzlich möglich: der CSV-Export der Kundendatenbank und der Rechnungsdaten, das Trennen von Verbindungen, das

Entziehen von Postfach-Freigaben, der Widerruf von Support-Freigaben und die eigenen Benachrichtigungseinstellungen.

b) Der Verantwortliche teilt dem Auftragsverarbeiter innerhalb von 30 Tagen nach dem Vertragsende in Textform mit, ob er die Rückgabe oder die sofortige Löschung wünscht. Bis dahin kann er im pausierten Konto die Kundendatenbank (Kontakte und Firmen) und die Rechnungsdaten als CSV exportieren; Auskünfte je Kontakt erstellt er vorher (Buchstabe a). Teilt er nichts mit, löscht der Auftragsverarbeiter nach Ablauf der Frist.

c) Wählt der Verantwortliche die Rückgabe, übergibt der Auftragsverarbeiter die Daten innerhalb von 30 Tagen nach der Wahl in gängigen maschinenlesbaren Formaten (JSON, CSV, Dateien im Original) über einen verschlüsselten Übertragungsweg, den die Parteien abstimmen. Umfang und Form stimmen die Parteien vorher in Textform ab.

d) Danach, oder sofort bei der Wahl „Löschung“, löscht der Auftragsverarbeiter innerhalb von 30 Tagen nach der Wahl alle Daten des Verantwortlichen in Datenbank und Dateispeicher, einschließlich der Mitgliedschaften seiner Beschäftigten, der verschlüsselten Zugriffstoken und der Protokolle. Die Nutzerkonten der Beschäftigten löscht er mit, soweit sie keinem anderen Kunden des Auftragsverarbeiters angehören. Er bestätigt die Löschung in Textform mit Datum und Umfang. Besteht eine Datenbank-Sicherung (Anlage 4), nennt er auch den Zeitpunkt, ab dem sie keine Daten des Verantwortlichen mehr enthält. ***[bitte klären: Fristen für Wahl, Rückgabe und Löschung bestätigen.]***

e) Endet die Testphase nach der Registrierung ohne Buchung eines Tarifs (AGB § 2a), pausiert der Auftragsverarbeiter das Konto mit dem Ablauf der Testphase automatisch; es gilt der Zustand „pausiert“ nach Buchstabe a. Der Verantwortliche teilt dem Auftragsverarbeiter innerhalb von 30 Tagen nach dem Ende der Testphase in Textform mit, ob er die Rückgabe oder die sofortige Löschung wünscht (Buchstabe b), und kann in dieser Zeit die CSV-Exporte nutzen. Bucht er einen Tarif, besteht der Hauptvertrag fort, und das Konto wird wieder nutzbar. Bucht er keinen Tarif und teilt er nichts mit, löscht der Auftragsverarbeiter nach Ablauf der 30 Tage alle Daten des Verantwortlichen nach Buchstabe d mit dem Löschdienst der Anwendung; er erinnert den Verantwortlichen 14 Tage und 3 Tage vorher per E-Mail. Die Löschung veranlasst in der Regel ein Mitarbeiter des Auftragsverarbeiters; nur wenn der Auftragsverarbeiter eine automatische nächtliche Löschung eingeschaltet hat, läuft sie ohne dessen Zutun, und auch dann nur für ein Konto, das sich selbst registriert und nie einen Tarif gebucht hat. ***[bitte klären: Löschfrist nach dem Ende der Testphase (30 Tage) gleichlautend mit AGB § 2a Abs. 5 festlegen; ob die Löschung automatisch laufen darf (Standard: Löschung per Admin-Aktion, die Automatik ist ausgeschaltet) oder nur nach einer Prüfung durch einen Menschen; Rückgabe der Daten aus der Testphase.]***

(3) Die Verbindungen zu Postfächern, Kalendern und Laufwerken trennt der Verantwortliche selbst in ZORYVO; das ist auch im pausierten Konto möglich. Ein persönliches Postfach trennt die Person, die es verbunden hat, oder ein Nutzer, dem sie das Recht „verwalten“ an diesem Postfach gegeben hat, einzeln oder über seine Rolle. Ohne diese Freigabe können Owner-Nutzer persönliche Postfächer anderer Nutzer nicht trennen. Beim Trennen beendet ZORYVO die Push-Abonnements, löscht die gespeicherten Zugriffstoken und widerruft bei Google den Zugriff beim Anbieter. Bei Microsoft kann ZORYVO den Zugriff nicht widerrufen; der Verantwortliche oder sein Tenant-Administrator entfernt die Anwendung ZORYVO im eigenen Microsoft-Konto. Wird eine Verbindung nicht getrennt, löscht der Auftragsverarbeiter die Zugriffstoken mit der Löschung nach Absatz 2 Buchstabe d. Ein Widerruf beim Anbieter findet dann nicht statt; der Verantwortliche entfernt ZORYVO selbst in seinen Konten bei Google und Microsoft. Dateien und Termine, die ZORYVO im Google Drive, OneDrive oder Kalender des Verantwortlichen angelegt hat, bleiben beim Verantwortlichen. Ebenso bleiben Antwortentwürfe, die ZORYVO auf Wunsch im Postfach abgelegt hat; der Verantwortliche löscht sie selbst.

(4) Daten bei Unterauftragsverarbeitern: Dauerhaft liegen Inhalte nur bei Supabase (Datenbank, Dateispeicher). Die KI-Anbieter erhalten Inhalte zur Verarbeitung; wie lange sie diese aufbewahren, richtet

sich nach Anlage 3 und ist nicht zugesagt, bis die dort genannten Einstellungen belegt sind. Der Virenscanner prüft Dateien nach seiner Einrichtung und speichert sie nicht. Brevo erhält die System- und Buchungs-E-Mails zum Versand (Anlage 3) und bewahrt Versanddaten nach seinen eigenen Fristen auf. Die übrigen Dienste (Anlage 3) erhalten nur Kennungen und Metadaten und löschen nach ihren eigenen Fristen. Stripe erhält keine Inhalte, sondern die Abrechnungsdaten des Verantwortlichen (Anlage 3, Absatz zu Stripe) und bewahrt sie nach seinen eigenen Fristen und den handelsrechtlichen Aufbewahrungspflichten auf. ***[bitte klären: Aufbewahrungsfristen von Brevo, Inngest, Sentry, Stripe, Vercel-Protokollen und healthchecks.io sowie die Aufbewahrung bei Vertex AI und Mistral nach Beleg nachtragen.]***

(5) Beim Auftragsverarbeiter verbleiben nach der Löschung nur der Hauptvertrag und dieser Vertrag mit dem Zustimmungsprotokoll (Nachweis des Vertragsschlusses), seine Rechnungen an den Verantwortlichen und die Zahlungsdaten, der Nachweis der Löschung, die Merkmale gegen wiederholte Testphasen (nur als Hash, bis zu 24 Monate nach Beginn der Testphase) und ein Protokoll mit Kennung des Verantwortlichen und Datum der Löschung. Keine Inhalte und keine Kontaktdaten betroffener Personen. Die Aufbewahrung richtet sich nach den handels- und steuerrechtlichen Fristen. ***[bitte klären: Fristen der eigenen Unterlagen mit dem Steuerberater bestätigen.]***

§ 10 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung dieses Vertrags zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO). Dazu gehören Anlage 2 und Anlage 3 in ihrer jeweils aktuellen Fassung, das Audit-Log des Verantwortlichen in ZORYVO (Einstellungen, Support-Freigaben und Ansichten von Debug-Inhalten, Datenschutz-Vorgänge), die Änderungshistorie je Objekt und auf Anfrage die Dokumentation der internen Sicherheitsprüfungen.

(2) Der Verantwortliche oder ein von ihm beauftragter, zur Vertraulichkeit verpflichteter Prüfer darf die Einhaltung dieses Vertrags überprüfen. Eine Überprüfung kündigt der Verantwortliche mindestens 14 Tage vorher in Textform an und nennt Gegenstand und Umfang; bei einem konkreten Verdacht auf eine Verletzung gilt eine angemessen kürzere Frist. Die Überprüfung findet während der üblichen Geschäftszeiten statt und ohne besonderen Anlass höchstens einmal je Kalenderjahr. Sie erfolgt zuerst durch schriftliche Auskunft. Eine Einsicht in Systeme beschränkt sich auf das, was Daten des Verantwortlichen betrifft, und berührt keine Daten anderer Kunden des Auftragsverarbeiters. ***[bitte klären: Ankündigungsfrist bestätigen.]***

(3) Soweit die Verarbeitung bei Unterauftragsverarbeitern stattfindet, erfüllt der Auftragsverarbeiter das Kontrollrecht durch Vorlage der Berichte, Zertifikate oder vertraglichen Zusagen dieser Anbieter, soweit sie ihm zugänglich sind.

(4) Jede Partei trägt die Kosten ihrer Mitwirkung an einer Überprüfung selbst. Geht eine Überprüfung ohne konkreten Anlass über die schriftliche Auskunft hinaus, kann der Auftragsverarbeiter für seinen Aufwand eine angemessene Vergütung von {{Stundensatz für Kontrollen}} je angefangener Stunde verlangen. Ergibt die Überprüfung einen erheblichen Verstoß des Auftragsverarbeiters gegen diesen Vertrag, trägt er die Kosten. ***[bitte klären: Kostenregelung mit dem Hauptvertrag abstimmen.]***

§ 11 Haftung

(1) Für die Haftung der Parteien gelten die Regelungen des Hauptvertrags.

(2) Art. 82 DSGVO bleibt unberührt. Im Innenverhältnis haften die Parteien entsprechend ihrem Anteil an der Verantwortung für den Schaden (Art. 82 Abs. 5 DSGVO).

[bitte klären: Haftungsregelung für diesen Vertrag mit dem Hauptvertrag abstimmen (Haftungsgrenzen, Freistellung bei Bußgeldern, Verhältnis zu Art. 82 Abs. 5 DSGVO).]

§ 12 Schlussbestimmungen

(1) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen für die Verarbeitung personenbezogener Daten die Regelungen dieses Vertrags vor. Im Übrigen bleibt der Hauptvertrag unberührt.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Das gilt auch für die Aufhebung dieser Klausel. Anlage 2 aktualisiert der Auftragsverarbeiter nach § 5 Abs. 2, Anlage 3 nach § 6 Abs. 2 und Abs. 5, die Anlagen 1, 4 und 5 nach § 1 Abs. 3. Jede Aktualisierung teilt er dem Verantwortlichen in Textform mit und vermerkt ihr Datum in der Stand-Angabe am Ende dieses Vertrags.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für Streitigkeiten aus diesem Vertrag ist der Sitz des Auftragsverarbeiters, soweit der Verantwortliche Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

(4) Ist eine Bestimmung dieses Vertrags unwirksam, bleibt der Vertrag im Übrigen wirksam. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die ihrem Zweck am nächsten kommt. Zwingende Vorgaben des Art. 28 DSGVO gelten in jedem Fall.

(5) Die Anlagen 1 bis 5 sind Bestandteil dieses Vertrags.

Abschluss

(1) Dieser Vertrag wird in Textform geschlossen (Art. 28 Abs. 9 DSGVO). Bei der Registrierung in ZORYVO schließt der Verantwortliche ihn durch das Häkchen zum AVV in der angezeigten Fassung (Nummer, Stand, Prüfsumme) und das Absenden der Registrierung; der Auftragsverarbeiter erklärt die Annahme mit der Vertragsbestätigung per E-Mail. Zeitpunkt, erklärende Person (Name und E-Mail-Adresse), Firma und Fassung hält ZORYVO im Zustimmungsprotokoll fest. Die Vertragsfelder (Firma, Anschrift, vertretungsberechtigte Person und Meldeadresse des Verantwortlichen, Bezeichnung und Datum des Hauptvertrags, Ort und Datum) füllt ZORYVO beim Abschluss aus den Angaben der Registrierung und dem Zeitpunkt des Abschlusses; die ausgefüllte Fassung steht als PDF in der Vertragsbestätigung und im Kundenkonto. ***[bitte klären: Abschluss in elektronischem Format nach Art. 28 Abs. 9 DSGVO durch Häkchen und Vertragsbestätigung (Form, Nachweis, Vertretungsbefugnis der erklärenden Person); aus welchen Angaben die Felder gefüllt werden, insbesondere die Meldeadresse für Datenpannen (E-Mail-Adresse der registrierenden Person oder Rechnungs-E-Mail-Adresse) und die Bezeichnung des Hauptvertrags; wo der Verantwortliche die Angaben später ändert.]***

(2) Wird der Vertrag nicht im Internet geschlossen, unterschreiben die Parteien:

Für den Verantwortlichen	Für den Auftragsverarbeiter
{{Firma des Verantwortlichen}}	ZORYVO Technologies {{Rechtsform}}
{{Ort und Datum}}	{{Ort und Datum}}
{{vertretungsberechtigte Person des Verantwortlichen}}	{{vertretungsberechtigte Person}}
Unterschrift	Unterschrift

Anlage 1: Gegenstand, Datenarten, betroffene Personen

1. Art, Gegenstand und Zweck der Verarbeitung

Art der Verarbeitung: Erheben (Abruf aus den verbundenen Postfächern und Kalendern, Uploads, Eingaben der Nutzer und Eingaben auf der Buchungsseite), Speichern, Auswerten mit einem KI-System,

Übermitteln an die in Anlage 3 genannten Anbieter, Versenden und Ablegen im Auftrag, Löschen. Gegenstand und Zweck je Bereich:

Bereich	Was ZORYVO tut
Postfächer	Abruf und Speicherung eingehender und gesendeter E-Mails aus den verbundenen Postfächern (Microsoft 365: Posteingang und Gesendete Elemente; Google: Postfach ohne Entwürfe, Spam, Papierkorb und Chat). Den Importzeitraum alter E-Mails wählt der Verantwortliche beim Verbinden (Vorgabe 90 Tage, höchstens 365 Tage). Gespeichert werden Metadaten und der aus HTML gewonnene Text (höchstens 100.000 Zeichen; das HTML selbst wird nicht gespeichert). Anhänge werden zunächst nur als Metadaten (Name, Typ, Größe) erfasst; ihr Inhalt wird nur geladen, wenn eine Automation ihn braucht (Rechnungen, Dateiablage).
KI-Analyse (A1)	Einordnung jeder E-Mail (Kategorie, Zusammenfassung, Vorschläge für Aufgaben), nur wenn der Verantwortliche die KI eingeschaltet hat. Ausgeschlossen sind E-Mails nach den Regeln des Verantwortlichen (Postfächer, Labels, Absender), automatische E-Mails und Newsletter, E-Mails gesperrter Kontakte sowie Absender der Kategorien Privat und Personal (Schutz-Vorgabe). Diese Ausschlüsse gelten für die automatische Analyse. Ein Nutzer mit dem Recht „freigeben“ oder „verwalten“ am Postfach kann eine ausgeschlossene E-Mail einzeln von Hand analysieren lassen. Dabei greifen die Regeln des Verantwortlichen, der Vorfilter für automatische E-Mails und Newsletter und die Schutz-Vorgabe Privat/Personal nicht. Es greifen weiter: die Sperre gesperrter Kontakte, der KI-Schalter, die dokumentierte Rechtsgrundlage und die Freischaltung der KI-Analyse für das Konto. Jede solche Anforderung steht im Audit-Log. An die KI gehen Richtung, Adresse des Postfachs, Datum mit Zeitzone, die Kategorienliste des Verantwortlichen, Absenderkategorien, Absender, Empfänger, Cc, Betreff, Dateinamen und Typen der Anhänge (nicht ihr Inhalt) und der Text bis 20.000 Zeichen.
Antwortentwürfe (A2)	Entwürfe zu einer E-Mail. An die KI gehen die E-Mail (Text bis 20.000 Zeichen), bis zu fünf frühere Nachrichten des Verlaufs (Zusammenfassung oder Auszug bis 1.500 Zeichen), der Kundenkontext (Anrede, Titel, Name, Firma, Position, Status, Kundennummer, Memory, für die KI freigegebene Felder, Zusammenfassungen oder ersatzweise Betreffe von höchstens zehn E-Mails; keine Telefonnummern, Adressen oder Einwilligungen; gesperrte Kontakte liefern keinen Kontext), das Firmenwissen des Verantwortlichen (Unternehmen, Leistungen, Öffnungszeiten, Kontakte, Preise, Richtlinien), Antwort-Bausteine der anderen Automationen und gegebenenfalls eine Anweisung des prüfenden Nutzers. Versand nur nach Freigabe durch einen Nutzer des Verantwortlichen über das Postfach, in dem die E-Mail einging. Ein automatischer Versand ohne Freigabe ist im Testpiloten gesperrt. Auf Wunsch des Verantwortlichen (Einstellung „Entwurf im Postfach“, Vorgabe aus) legt ZORYVO den Entwurf zusätzlich im Postfach ab und löscht ihn dort, wenn die Freigabe abgelehnt wird oder fehlschlägt. E-Mails mit KI-Text sind gekennzeichnet (Anlage 2 Nr. 2).
Firmenwissen (Wissensbasis)	Der Verantwortliche fügt unter „Firmenwissen“ Texte ein oder lädt Dateien dafür hoch (nur die Rolle Owner). ZORYVO teilt den Text in Abschnitte und speichert sie im Konto des Verantwortlichen mit einem Volltextindex und einer Einbettung (Zahlenreihe, die der KI-Anbieter erzeugt). Bei einem Antwortentwurf (A2) sucht ZORYVO die passenden Abschnitte: Dafür geht eine Suchanfrage aus dem Betreff und den ersten rund 500 Zeichen der E-Mail an den Anbieter der Einbettungen; die gefundenen Abschnitte (höchstens acht, je bis 1.000 Zeichen) gehen mit dem Entwurf an die KI (Zeile Antwortentwürfe). Genutzt werden nur Dokumente, die der Verantwortliche veröffentlicht, für Antworten freigegeben hat und die heute gelten. Einbettungen entstehen nur bei eingeschalteter KI; es gibt dafür keinen Ausweichanbieter, ohne sie läuft die Suche nur über den Volltext. Auf Wunsch des Verantwortlichen lässt ZORYVO die KI die Abschnitte lesen, um Kernaussagen vorzuschlagen (je Aufruf rund 18.000 Zeichen Text) und um zu prüfen, ob zwei Abschnitte einander widersprechen (zwei Abschnitte je Prüfung); der Verantwortliche bestätigt die Aussagen und entscheidet über Widersprüche selbst, die Aussagen werden im Konto gespeichert. Dafür gehen die Abschnitte an dasselbe Textmodell wie die E-Mail-Analyse (Zeile Google Cloud, Vertex AI; bei Ausfall an den Ausweichanbieter, wenn der Verantwortliche ihn zugelassen hat).***[bitte klären: Einbettungen als weitere Verarbeitung des KI-Anbieters in Anlage 3 und im Verzeichnis führen und mit dem Beleg zu Region, Modell und Ausschluss vom Training verbinden; die Kernaussagen und Widersprüche als Zweck „Auswertung von Dokumenten des***

	Verantwortlichen“ in der Zeile des Textmodells in Anlage 3 benennen.]
Kundendatenbank (A8, A9)	Kontakte, Firmen, Leads, Notizen, Kategorien, Tags, Kunden-Memory mit Quellenangabe; Zuordnung von Absendern zu Kontakten, Firmen und Kategorien; Dubletten-Prüfung.
Rechnungen (A3)	Erfassung von Rechnungsdaten aus E-Rechnungen (ohne KI) und aus PDF oder Bildern (mit KI) mit Fundstelle; Prüfung von Beträgen und IBAN. ZORYVO bucht und zahlt nicht.
Dateien (A4, A12)	Hochladen von PDF, Bildern (JPG, PNG, HEIC) und Textdateien (TXT, Markdown, CSV, XML) bis 25 MB und 200 Seiten; Texterkennung und Auslesen mit KI; an die KI gehen die Datei oder ihr Text, das Upload-Datum und, wenn die Datei an einem Kontakt, einer Firma oder einem Lead hochgeladen wurde, dessen Name; Vorschläge für die Kundendatenbank; Virenscan nach Einrichtung des Virenscanners (Anlage 2 Nr. 2). Ablage von Dateien im Laufwerk einer Person des Verantwortlichen per Vorgabe nur nach Freigabe. Der Verantwortliche kann den Modus automatisch wählen, soweit sein Tarif es erlaubt und keine Sicherheitsregel ihn absenkt; Anhänge unbestätigter Absender landen dann im Ordner Ungeprüft. Dateien aus Uploads und von der KI gelesene Rechnungen legt ZORYVO nie ohne Freigabe ab. Ohne Virenscan-Urteil „sauber“ legt ZORYVO keine Datei ab.
Termine und Buchungsseite (A5, A10)	Lesen freier Zeiten; Anlegen, Ändern und Absagen von Terminen, die ZORYVO selbst angelegt hat; Einladungen, Änderungen und Absagen an Dritte per Vorgabe nur nach Freigabe (Modus automatisch nach Weisung des Verantwortlichen, § 3 Abs. 2); vorläufige Reservierungen ohne Kundennamen; öffentliche Buchungsseite mit Formular (Name, E-Mail-Adresse, freiwillig Telefon, Adresse, Anmerkung, bis zu drei Antworten) und Bestätigung per E-Mail-Link.
Aufgaben, Fristen, Erwartungen (A6, A7, A11)	Aufgaben und Vorgänge aus E-Mails, täglicher Fristenlauf mit Erinnerungen an die Nutzer, Nachfassen offener Erwartungen; Erinnerungs-E-Mails an Dritte nur nach Freigabe oder nach den Regeln des Verantwortlichen; Erinnerungen zu Zahlungen gehen nie ohne Freigabe durch eine Person.
Nutzerverwaltung	Rollen, Einzelrechte, Mitgliedschaften und Einladungen der Beschäftigten des Verantwortlichen; Benachrichtigungen in der App und per E-Mail (per E-Mail nach Einrichtung des System-Mailversands, Anlage 3). Die Nutzerkonten selbst verarbeitet der Auftragsverarbeiter als eigener Verantwortlicher (§ 7 Abs. 4).
Protokolle	Audit-Log, Änderungshistorie je Objekt, Aktivitätsprotokoll je Verarbeitungsschritt; Debug-Inhalte fehlgeschlagener Schritte verschlüsselt.

Bei E-Mail-Analyse, Antwortentwürfen, Dateien und Rechnungen erhält die KI außerdem den Firmennamen des Verantwortlichen.

Nicht Gegenstand der Auftragsverarbeitung sind die Registrierungs-, Vertrags- und Abrechnungsdaten des Verantwortlichen: Firma, Anschrift, USt-IdNr., Handelsregistereintrag, Rechnungs-E-Mail-Adresse, Name und E-Mail-Adresse der registrierenden Person, das Zustimmungsprotokoll, die Merkmale gegen wiederholte Testphasen (nur als Hash) und die Daten bei Stripe. Dafür ist der Auftragsverarbeiter selbst Verantwortlicher (§ 7 Abs. 4; Datenschutzerklärung, Abschnitte 4.9 bis 4.12).***[bitte klären: Einordnung dieser Daten als eigene Verantwortlichkeit des Auftragsverarbeiters; Rolle von Stripe (eigener Verantwortlicher für Zahlungsdaten oder Auftragsverarbeiter) und Aufnahme in Anlage 3.]***

2. Arten personenbezogener Daten

Datenart	Beispiele	Herkunft
E-Mail-Daten	Absender, Empfänger, Cc, Betreff, Zeitpunkte, Labels, Text, Namen und Typen der Anhänge, Inhalte geladener Anhänge	Postfächer des Verantwortlichen
Kontakt- und Firmendaten	Name, E-Mail-Adressen, Telefonnummer, Firma, Position, Anschrift, Kundennummer, Status, Kategorien, eigene Felder, Notizen, Kunden-Memory	Kundendatenbank, Zuordnung aus E-Mails, Buchungen, Import
Termindaten	Zeitpunkte, Titel, Teilnehmer, Ort, Anmerkungen, Antworten der	Kalender des

	Buchenden, Zeitzone und Sprache	Verantwortlichen, Buchungsseite
Dokumente	hochgeladene Dateien und E-Mail-Anhänge mit erkanntem Text und daraus gelesenen Angaben	Uploads, Postfächer
Rechnungsdaten	Rechnungssteller, Nummern, Beträge, Steuerzeilen, Zahlungsdaten einschließlich IBAN	E-Rechnungen, Dokumente
KI-Ergebnisse	Kategorien, Zusammenfassungen, Entwürfe, extrahierte Felder, Rohantwort des Modells	KI-Verarbeitung
Mitgliedschaften	Rolle, Rechte, Mitgliedschaft, Einladungen (E-Mail-Adresse der eingeladenen Person)	Verantwortlicher und seine Beschäftigten
Protokolldaten	Kennungen der handelnden Nutzer, Zeitpunkte, Ereignisnamen, alte und neue Feldwerte, technische Codes	Betrieb von ZORYVO

3. Kategorien betroffener Personen

Beschäftigte und sonstige Nutzer des Verantwortlichen; Kunden, Interessenten, Lieferanten, Dienstleister, Partner, Behördenvertreter und sonstige Korrespondenzpartner des Verantwortlichen; Besucher der öffentlichen Buchungsseite des Verantwortlichen; Personen, die in E-Mails, Anhängen und Dokumenten genannt werden.

4. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO)

ZORYVO sucht besondere Kategorien nicht gezielt und wertet sie nicht aus. Sie können in E-Mails, Anhängen und Dokumenten enthalten sein, die der Verantwortliche verarbeiten lässt (etwa Krankmeldungen, Bewerbungen, Schreiben von Krankenkassen). Der Analyse-Prompt untersagt dem KI-System, Angaben zu Gesundheit, Religion, politischer Meinung, Gewerkschaftszugehörigkeit, sexueller Orientierung, ethnischer Herkunft und Vorstrafen in das Kunden-Memory zu übernehmen; das ist eine Anweisung an das Modell, keine technische Sperre. Der Verantwortliche steuert, welche Postfächer, Labels und Absender die KI-Analyse ausschließt, und belässt die Schutz-Vorgabe für die Kategorien Privat und Personal, soweit er solche Daten erwartet. Diese Ausschlüsse gelten nur für die automatische Analyse. Eine E-Mail, die ein Nutzer mit dem Recht „freigeben“ oder „verwalten“ am Postfach von Hand analysieren lässt, geht trotz dieser Ausschlüsse an die KI, sofern der Kontakt nicht gesperrt ist (Nr. 1, KI-Analyse). ***[bitte klären: Einordnung nach Art. 9 DSGVO und erforderliche Hinweise an den Verantwortlichen.]***

5. Dauer

Für die Dauer des Hauptvertrags; danach § 9.

Anlage 2: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Diese Anlage nennt Maßnahmen, die in ZORYVO umgesetzt sind. Hängt eine Maßnahme von einem Dienst ab, der zum Stand dieses Vertrags nicht eingerichtet ist, steht das bei der Maßnahme (§ 5 Abs. 3). Leistungen der Unterauftragsverarbeiter sind als solche gekennzeichnet.

1. Vertraulichkeit

Zugangskontrolle. Konten entstehen über Einladungen oder über die Registrierung eines Unternehmens mit Sitz in Deutschland. Die Registrierung legt das Konto erst an, nachdem die E-Mail-Adresse über einen Link bestätigt ist; sie ist durch ein Captcha, ein für Menschen unsichtbares Feld und Rate-Limits geschützt, und ihre Antwort sagt nie, ob eine Adresse schon ein Konto hat. Der Einladungslink trägt einen einmaligen Zufallswert, der 7 Tage gilt, der Bestätigungslink der Registrierung einen, der 24 Stunden gilt;

beide werden nur als Hash gespeichert. Passwörter haben mindestens 12 Zeichen und liegen nur beim Authentifizierungsdienst (Supabase Auth), nicht in ZORYVO. Die Zwei-Faktor-Anmeldung (TOTP) ist für den Betreiber und alle Owner-Nutzer Pflicht; für Mitarbeiter stellt der Verantwortliche sie ein; ein einmal eingerichteter Faktor wird immer abgefragt. Jeder Nutzer mit eingerichteter Zwei-Faktor-Anmeldung erhält zehn einmalige Wiederherstellungscodes, die nur als Hash gespeichert werden; das Einlösen eines Codes entfernt alle Faktoren und beendet alle Sitzungen; wo die Zwei-Faktor-Anmeldung Pflicht ist, muss danach ein neuer Faktor eingerichtet werden. Sitzungen laufen über Cookies mit den Merkmalen HttpOnly, Secure und SameSite, die nur der Server liest; jede Anfrage prüft in der Datenbank, ob die Sitzung noch gilt, der Nutzer nicht gesperrt und das Profil nicht gelöscht ist. Sitzungen des Betreibers enden nach 8 Stunden. Nutzer können sich auf allen Geräten gleichzeitig abmelden.

Schutz vor Missbrauch. Anmeldeversuche sind begrenzt (50 je 15 Minuten je IP-Adresse; 10 je 15 Minuten je Konto und IP-Adresse; 100 Fehlversuche je Stunde je Konto, danach Alarm an den Betreiber), ebenso das Zurücksetzen von Passwörtern (3 je Stunde je Konto und IP-Adresse, 1 je 90 Sekunden je Konto, 20 je Stunde je IP-Adresse), 2FA-Codes (10 je 15 Minuten), Einladungen, die Registrierung (5 Anfragen je Stunde je IP-Adresse, 3 je Tag je E-Mail-Adresse), Checkout und Kundenportal (je Nutzer), Webhooks (auch der Webhook von Stripe, der Signaturen prüft und doppelte Ereignisse verwirft) und die öffentliche Buchungsseite. Für diese Zähler werden E-Mail-Adressen und IP-Adressen nur als SHA-256-Hash gespeichert. Diese Grenzen setzt die Anwendung durch. Ruft jemand den Authentifizierungsdienst direkt auf, gelten nur dessen eigene Grenzen. ***[bitte klären: Auth-Hooks vor Pilotstart einrichten oder als Restrisiko benennen.]*** Die öffentliche Buchungsseite, das Kontaktformular und die Registrierung schützt ein selbst betriebenes Captcha (ALTCHA-Protokoll) ohne Drittanbieter.

Notschalter. Der Verantwortliche (jeder Owner-Nutzer) beendet den Zugang eines Nutzers sofort: Die Mitgliedschaft endet mit Wirkung ab der nächsten Anfrage; die Sitzungen des Nutzers werden zusätzlich beendet, wenn er keinem anderen Kunden des Auftragsverarbeiters angehört. Der Betreiber kann alle Sitzungen eines Nutzers beenden und das Konto sperren. Jeder Eingriff verlangt einen Grund und wird im Audit-Log festgehalten.

Zugriffskontrolle. Rollen Owner und Mitarbeiter mit Einzelrechten, zentral geprüft. Mitarbeiter sehen nur die Postfächer und Kategorien, die der Verantwortliche freigibt. Automationen und Regeln sehen alle Mitarbeiter lesend; ändern dürfen sie nur Nutzer mit dem Recht „Automationen verwalten“. Mitarbeiter mit Verwaltungsrecht vergeben nur Rechte, die sie selbst haben. Rechte je Postfach (lesen, freigeben, senden, verwalten) gelten überall, auch in Suche, Zeitstrahl und Export. Ein persönliches Postfach verbindet nur die Person selbst. Kolleginnen und Kollegen sehen voneinander nur den Anzeigenamen. Der Betreiber sieht Inhalte nur mit Support-Freigabe (§ 4). Die Anwendung erreicht die Datenbank nur über zwei festgelegte Zugriffspfade mit eingeschränkten Datenbankrollen, die die Zeilensicherheit nicht umgehen können. Für den Dateispeicher und für die Verwaltungsschnittstelle des Authentifizierungsdienstes nutzt sie serverseitig den Dienstschlüssel des Anbieters, der die Zeilensicherheit umgeht; jeder Dateipfad wird dabei im Code gegen den Verantwortlichen geprüft. Die Verwaltungsschnittstelle ist im Code auf vier Vorgänge beschränkt (Nutzer anlegen, Nutzer löschen, Faktoren entfernen, sperren und entsperren), jeweils mit Pflichtgrund und Audit-Eintrag; das Löschen eines Nutzers ist in der Oberfläche nicht angebunden. Der Datenbankzugang mit Vollrechten dient Migrationen, benannten Wartungsskripten und den Eingriffen von Hand nach § 8 Abs. 5, § 9 Abs. 2 und Anlage 4 Nr. 3; diese Eingriffe dokumentiert der Auftragsverarbeiter mit Grund. ***[bitte klären: Prüfliste und Freigabe für Eingriffe per SQL festlegen.]***

Trennungskontrolle. Jede Zeile der Fachtabellen trägt die Kennung genau eines Verantwortlichen; Plattformtabellen (Nutzerprofile, Rate-Limit-Zähler, plattformweite Protokollzeilen, Rechtstext-Fassungen, Registrierungsanfragen, das Zustimmungsprotokoll) enthalten keine Inhalte des Verantwortlichen. Zeilensicherheit (Row-Level-Security) gilt auf allen Tabellen, auch für Hintergrundjobs und für den Betreiber; jede Tabelle steht in einem Register, und Isolationstests prüfen je Tabelle, dass ein Verantwortlicher keine Zeilen eines anderen sieht. Dateien liegen in einem privaten Speicherbereich unter

dem Präfix des Verantwortlichen; bei Zugriffen des Servers mit dem Dienstschlüssel sichert die Prüfung des Pfads im Code diese Trennung, nicht die Zeilensicherheit. Nutzer lesen Dateien nur über den Server mit kurzlebigen signierten Adressen (höchstens 300 Sekunden). Beim Hochladen schickt der Browser die Datei über eine einmalige, vom Server ausgestellte Upload-Adresse direkt in den Dateispeicher; die Adresse gilt zwei Stunden und nur für den vorgegebenen Pfad des Verantwortlichen. Inhalte und Metadaten liegen in getrennten Tabellen. Entwicklung und Staging haben eigene Datenbanken, Schlüssel und Zugänge. ***[bitte klären: Umgebung des Testpiloten festlegen (eigene Produktionsumgebung oder Staging).]*** In Entwicklung und Tests werden nur erfundene Daten verwendet.

Pseudonymisierung und Verschlüsselung. Transport nur über TLS; die Anwendung erzwingt HTTPS für zwei Jahre einschließlich Subdomains (HSTS). Zugriffstoken für Postfächer, Kalender und Laufwerke werden mit AES-256-GCM aus einem eigenen Schlüsselring verschlüsselt, an Verantwortlichen und Verbindung gebunden und sind nur für die Job-Rolle lesbar. Debug-Inhalte fehlgeschlagener Schritte werden mit einem zweiten, getrennten Schlüsselring verschlüsselt, Geheimnisse (Passwörter, Token, Cookies) vorher entfernt; sie sind 14 Tage lesbar und danach gesperrt (ein physisches Löschen erfolgt mit der Löschung des zugehörigen Kontakts oder bei Vertragsende). Einladungs-Token, Wiederherstellungscodes, Geräte-Cookies, Buchungslinks, die Einmal-Referenzen der Bestätigungsknöpfe in Telegram-Alarmen an den Betreiber und Rate-Limit-Kennungen werden nur als Hash gespeichert. Schlüsselringe liegen nur in der Laufzeitumgebung, werden mit Kennung rotiert und beim Start geprüft; ein ungültiger Ring verhindert das Deployment. Die Verschlüsselung ruhender Daten in Datenbank, Dateispeicher und auf dem Virenscan-Server ist Leistung der Anbieter nach deren Vertragsbedingungen. ***[bitte klären: Verschlüsselung ruhender Daten bei Supabase und Hetzner mit dem jeweiligen Vertrag belegen.]***

2. Integrität

Protokollierung. Drei Protokolle: die Änderungshistorie je Objekt (feldgenau mit altem und neuem Wert, Akteur, Automation oder Regel; bei Kontakten, Firmen und Dateien je Feld rückgängig machbar), das Audit-Log (wer hat welche Einstellung oder Entscheidung getroffen) und das Aktivitätsprotokoll (technischer Schritt mit Status, Dauer, Anbieter, Fehlercode). Protokolle werden in derselben Transaktion wie die Änderung geschrieben; ein Datenbank-Trigger lehnt Änderungen an Fachtabellen ohne Protokollkontext ab. Audit-Log und Aktivitätsprotokoll enthalten Kennungen und Codes, keine Inhalte. Die Werte der Änderungshistorie gelten als Inhalt und unterliegen der Support-Freigabe (§ 4). Jeder Ablauf trägt eine Nachverfolgungs-Kennung, aus der eine kurze Fehlernummer für Nutzer abgeleitet wird. Der Anwendungs-Logger erhält keine Inhalte. Als zusätzliche Sicherung schwärzt er Felder, die nach Passwörtern, Token, Cookies, E-Mail-Adressen, Betreffen oder Texten benannt sind. Konkrete Anfragepfade werden nie geloggt. Fehlerberichte gehen nur in die EU-Region des Fehlerdienstes, ohne Inhalte, mit maskierten E-Mail-Adressen und entfernten Token, ohne Sitzungsaufzeichnung. ZORYVO wertet keine Leistung von Personen aus: keine Ranglisten, keine Zähler je Mitarbeiter, kein Filter des Protokolls nach Person.

Kontrolle externer Aktionen. Vor jeder Aktion nach außen (Versand, Termine, Dateiablage) prüft ZORYVO in fester Reihenfolge Notbremse, Status des Verantwortlichen, importierte E-Mail (löst nie eine externe Aktion aus) und bestehende Verbindung. Ausgenommen ist das Entfernen abgelaufener oder nicht mehr benötigter vorläufiger Reservierungen aus dem Kalender des Gastgebers: Es prüft nur die Notbremse, nicht den Status des Verantwortlichen, damit auch in einem pausierten Konto keine verwaisten Einträge stehen bleiben. Bei E-Mails prüft ZORYVO außerdem das Kennzeichen „Nicht anschreiben“ und gültige Empfänger, bei Erinnerungen eine neue Nachricht des Kontakts und bei Antworten eine inzwischen versandte Antwort im Verlauf; diese letzte Sperre kann eine Person nach Bestätigung übergehen. Die Dateiablage hat eine eigene Prüfung von Notbremse, Status, importierter E-Mail und Verbindung zum Laufwerk. Buchungs-E-Mails prüfen Notbremse, Status des Verantwortlichen und „Nicht anschreiben“ gesondert. Jede Aktion wird vor dem Aufruf des Anbieters reserviert und genau einmal ausgeführt; ein unklarer Ausgang wird nie automatisch wiederholt, sondern dem Betreiber

gemeldet. Sicherheitsregeln sind fest im Code und von niemandem änderbar; sie senken den Modus einer Automation nur ab (unbestätigter Absender, automatische E-Mail, eigenes Postfach, IBAN-Abweichung, Uploads). Der automatische Versand von KI-Antworten ist im Testpiloten gesperrt; jeder Entwurf wird von einer Person freigegeben. Von der KI gelesene Rechnungsdaten werden nie ohne Prüfung durch eine Person abgelegt. Automationen überschreiben nie Werte, die eine Person gesetzt hat. Regeländerungen werden versioniert; das Lockern einer Schutz-Vorgabe ist nur der Rolle Owner mit Bestätigung möglich und wird protokolliert.

Kennzeichnung von KI-Text. Gesendete E-Mails mit KI-Text tragen die maschinenlesbaren Kopfzeilen X-ZORYVO-AI-Generated und X-ZORYVO-AI-Model. Der sichtbare Hinweis („Diese Nachricht wurde mit Unterstützung eines KI-Systems erstellt.“) ist im Modus automatisch im Code erzwungen und sonst per Vorgabe eingeschaltet. Für Entwürfe, die eine Person freigibt, kann die Rolle Owner ihn abschalten (Weisung des Verantwortlichen). Da KI-Antworten im Testpiloten nur nach Freigabe versendet werden, kann der sichtbare Hinweis dann bei allen versendeten KI-Antworten fehlen. ***[bitte klären: Vereinbarkeit mit Art. 50 KI-Verordnung.]***

Schutz vor schädlichen Eingaben. Eine Datei geht nur dann in ein Laufwerk des Verantwortlichen, wenn für genau diese Bytes ein gespeichertes Virenscan-Urteil „sauber“ vorliegt. Der Virenscan ist für einen vom Auftragsverarbeiter betriebenen ClamAV-Server in der EU ausgelegt (Anlage 3, Hetzner): Übertragen werden nur die Bytes ohne Dateinamen, gespeichert wird nur das Urteil. Ein Fund sperrt die Datei; sie wird nie verarbeitet, angezeigt oder weitergegeben. Zum Stand dieses Vertrags ist der Server nicht eingerichtet. Bis zur Einrichtung findet kein Virenscan statt, und keine Datei wird in ein Laufwerk übertragen; Texterkennung und Auslesen mit KI (Anlage 1) laufen auch für ungeprüfte Dateien.***[bitte klären: Einrichtung des Servers und Vertrag mit Hetzner vor Pilotstart belegen.]*** Der Dateityp wird aus dem Inhalt bestimmt; Programme, Skripte, Makro-Dokumente und Archive werden abgelehnt, nichts wird ausgeführt oder gerendert; XML mit externen Entitäten wird abgelehnt; unsichtbare Steuerzeichen werden entfernt. E-Mail-Kopfzeilen werden bereinigt, E-Mail-HTML wird nie als HTML ausgegeben, versteckter Text wird vor der Analyse entfernt. Die KI-Prompts behandeln E-Mails und Dokumente als nicht vertrauenswürdige Daten; Anweisungen an das System werden als Verdacht markiert und führen zu keiner Aktion. Diese Erkennung erfolgt durch das Modell und ist keine Garantie. Im Browser gilt eine Content-Security-Policy mit Einmalwert je Anfrage ohne Drittskripte, dazu die Sicherheits-Header gegen Einbettung, Typ-Erkennung und Referrer-Weitergabe. Webhooks prüfen Signaturen, sind je Adresse begrenzt und verarbeiten jede Nachricht nur einmal. Verbindungen zu Postfächern nutzen OAuth mit PKCE und Zustandsprüfung, gebunden an Nutzer und Sitzung.

3. Verfügbarkeit und Belastbarkeit

Datenbank, Authentifizierung und Dateispeicher laufen bei Supabase in Frankfurt, die Anwendung auf Vercel in Frankfurt. Eine Sicherung der Datenbank ist zum Stand dieses Vertrags nicht eingerichtet (Anlage 4). Ein Prüfjob ruft alle 5 Minuten die Gesundheitsschnittstelle der Anwendung (einschließlich Datenbankprobe) auf und meldet einen Fehlschlag direkt über Telegram. Der Prüfjob ist für einen externen Totmannschalter (healthchecks.io, Anlage 3) ausgelegt, der den Betreiber von außen alarmiert, wenn die Meldungen ausbleiben. Fehler werden klassifiziert und dem Betreiber mit Eskalationsstufen gemeldet; dringende Alarme wiederholen sich bis zur Bestätigung. Die Alarme sind für zwei Kanäle ausgelegt (Telegram und E-Mail über Brevo). Zum Stand dieses Vertrags sind der Totmannschalter und der E-Mail-Kanal nicht eingerichtet; Alarme laufen nur über Telegram.***[bitte klären: Einrichtung von Totmannschalter und E-Mail-Kanal vor Pilotstart belegen.]*** Hintergrundjobs wiederholen fehlgeschlagene Schritte mit wachsenden Pausen; Aufholjobs alle 5 Minuten verarbeiten Liegengebliebenes; ein Sicherheitsnetz ruft Postfächer alle 30 Minuten auch ohne Push ab. Je KI-Anbieter hält ein Schutzschalter den Anbieter bei gehäuften Fehlern zurück; fällt die KI aus, warten E-Mails gespeichert und werden nachgeholt, nichts geht verloren. Die Notbremse hält alle externen Aktionen plattformweit oder je Verantwortlicher an; der Verantwortliche kann sie für sein Konto selbst ziehen. Deployments laufen in fester Reihenfolge (Migrationen, dann Anwendung); eine unvollständige Umgebung

bricht das Deployment ab. Die Anwendung ist auf ein vorheriges Deployment zurücksetzbar, soweit der Tarif des Hosting-Anbieters das vorsieht.***[bitte klären: Rücksetzen im gebuchten Vercel-Tarif prüfen.]***

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Bei jeder Codeänderung laufen automatisch Typprüfung, Lint, Tests, eine Prüfung der Abhängigkeiten (blockiert bei hohen und kritischen Schwachstellen) und ein Scan auf Geheimnisse über die gesamte Historie; ein Pre-Commit-Hook blockiert Commits mit Geheimnissen; Abhängigkeiten werden wöchentlich automatisch zur Aktualisierung vorgeschlagen. Statische Prüfungen erzwingen die Architekturregeln (Datenbankzugriff nur über die beiden Zugriffspfade, keine Auswertung je Person, keine übersprungenen Tests). Integrationstests gegen eine Entwicklungsdatenbank prüfen, dass jede Tabelle im Register der Zeilensicherheit steht und kein Verantwortlicher Zeilen eines anderen sieht. Interne Sicherheitsprüfungen fanden am 2026-09-26 und am 2026-09-28 statt. Die Funde sind behoben bis auf einen offenen Fund mittlerer Stufe (Weiterleitungsadressen der Staging-Umgebung, Entscheidung ausstehend), einen offenen Punkt der Prüfpipeline (Prüfläufe für automatische Abhängigkeits-Updates) und dokumentierte niedrige Merkposten. ***[bitte klären: offene Funde vor Pilotstart entscheiden oder als bekannte Restrisiken benennen.]*** Ein externer Penetrationstest und eine Zertifizierung liegen nicht vor. Die Betriebsabläufe (Deploy, Rollback, Tausch von Geheimnissen, Vorfall, Anbieterausfall, Wiederherstellung) sind in einer Betriebsanleitung dokumentiert. Geheimnisse liegen nur in den Laufzeitumgebungen; ein offengelegtes Geheimnis wird sofort getauscht.

5. Auftragskontrolle

Weisungen werden über die Einstellungen in ZORYVO erteilt und protokolliert (§ 3). Externe Dienste erhalten nur, was Anlage 3 nennt: Hintergrundjobs nur Kennungen und Status; Fehlerberichte ohne Inhalte; Alarme ohne Inhalte und ohne Kontaktdaten; der E-Mail-Versanddienst nur die System- und Buchungs-E-Mails mit den in Anlage 3 genannten Angaben; der Virenscanner nach seiner Einrichtung nur Bytes ohne Namen; die KI-Anbieter nur die in Anlage 1 genannten Eingaben über EU-Endpunkte. Der Verantwortliche kann die KI-Verarbeitung jederzeit ausschalten und den Ausweich-Anbieter ausschließen.

Anlage 3: Unterauftragsverarbeiter

Dienst	Rolle und Zweck	Daten	Standort	Vertragslage
Supabase	Datenbank, Authentifizierung, Dateispeicher; Datenbank-Sicherung (nach Buchung, Anlage 4)	alle Inhalte und Kontodaten des Verantwortlichen	EU, Frankfurt (eu-central-1); Daten werden dort gespeichert und vorrangig verarbeitet, Ausnahmen laut Vertrag nur, wenn gesetzlich oder für den Dienst nötig	Auftragsverarbeitungsvertrag als Teil der Nutzungsbedingungen; Standardvertragsklauseln als Rückfall
Vercel	Hosting der Anwendung und der Serverfunktionen	Rechenleistung; Anfrage-Protokolle der Plattform ***[bitte klären: ob sie IP-Adresse, Pfad und Browser-Kennung enthalten und wie lange der Anbieter sie aufbewahrt]***; Anwendungsprotokolle ohne Inhalte (als zusätzliche Sicherung	Funktionen in Frankfurt (fra1); Verwaltungssysteme und Sicherungen des Anbieters in den USA	Auftragsverarbeitungsvertrag im Tarif Pro; Standardvertragsklauseln 2021. ***[bitte klären: Tarif Pro und Vertrag vor Pilotstart belegen.]***

		schwärzt der Logger Felder, die nach Passwörtern, Token, Cookies, E-Mail-Adressen, Betreffen oder Texten benannt sind; die Anwendung loggt keine konkreten Anfragepfade); Build- und Umgebungswerte		
Inngest	Warteschlange und Zeitpläne für Hintergrundjobs	nur Kennungen und Status (Kennungen von Verantwortlichem, Objekten, Fehlern und Abläufen); bei Alarm-Knöpfen die Telegram-Nutzer- und Chat-Kennung des Betreibers; keine Inhalte	bei Nutzung des Anbieters: AWS, Serverregion laut öffentlicher Seite des Anbieters nicht angegeben; bei Eigenbetrieb nach § 6 Abs. 5: EU ***[bitte klären: Variante und Region vor Pilotstart belegen]***	Vertrag nach Art. 28 Abs. 4 DSGVO steht aus; Einsatz für Daten des Verantwortlichen nur nach § 6 Abs. 5
Google Cloud, Vertex AI	KI-Verarbeitung (primär): E-Mail-Analyse, Antwortentwürfe, Memory-Formulierung, Texterkennung, Dokumenten- und Rechnungsauslesen, Einbettungen für die Wissensbasis	E-Mail-Text bis 20.000 Zeichen mit Richtung, Postfachadresse, Absender, Empfänger, Cc, Betreff, Datum sowie Dateinamen und Typen der Anhänge; Kategorienlisten des Verantwortlichen; der Firmenname des Verantwortlichen; für Antwortentwürfe Verlauf, Kundenkontext, Firmenwissen und Antwort-Bausteine (Anlage 1 Nr. 1); Memory-Texte; hochgeladene Dokumente, E-Mail-Anhänge und Bilder (PDF, JPEG, PNG, HEIC), bei Uploads mit Upload-Datum und dem Namen des Kontakts, der Firma oder des Leads, an dem die Datei hochgeladen wurde; für die Einbettungen die Abschnitte der Wissensbasis (Dokumente und Textfelder „Firmenwissen“) und je Antwortentwurf eine Suchanfrage aus Betreff	EU-Regionen oder EU-Multiregion; nur EU-Standorte sind in ZORYVO zugelassen; Einbettungen in einer regionalen EU-Region	Google Cloud Data Processing Addendum; Standardvertragsklauseln, EU-US Data Privacy Framework. ***[bitte klären: Modell, Region, Zwischenspeicherung und Ausschluss vom Training belegen; ohne Beleg keine Zusage „kein Training“.]***

ENTWURF

		und den ersten rund 500 Zeichen der E-Mail		
Mistral AI	KI-Ausweichanbieter; nur, wenn der Primäranbieter gestört ist und der Verantwortliche den Ausweich erlaubt	wie Vertex AI, ohne HEIC	EU (Endpunkt api.eu.mistral.ai)	Auftragsverarbeitungsvertrag als Teil der Vereinbarung. ***[bitte klären: Ausschluss vom Training und Verzicht auf Speicherung der Anfragen (Zero Data Retention) aktivieren und belegen; Standard des Anbieters ist Training an und 30 Tage Aufbewahrung.]***
Brevo	Versand von System-E-Mails (Einladungen, Bestätigungslinks und Vertragsbestätigungen der Registrierung mit PDF-Anhängen, Passwort-Zurücksetzen, Benachrichtigungen, Hinweise zu Testphase und Zahlung) und von Buchungs-E-Mails, wenn kein Postfach des Verantwortlichen verbunden ist; zum Stand dieses Vertrags nicht eingerichtet	Empfängeradresse, Betreff und Text der System-E-Mail (ohne Inhalte der E-Mails des Verantwortlichen), bei der Vertragsbestätigung die PDF-Anhänge (AGB, AVV mit den Angaben des Verantwortlichen, Datenschutzerklärung); bei Buchungs-E-Mails Name, E-Mail-Adresse und Termindaten des Buchenden sowie Firmenname des Verantwortlichen	EU (Rechenzentren in Frankreich, Deutschland und Belgien); Cloudflare als CDN und Web-Firewall in der Infrastruktur des Anbieters, ob die Versandschnittstelle darüber läuft, ist nicht belegt	Auftragsverarbeitungsvertrag als Teil der Nutzungsbedingungen (Fassung 1. Oktober 2025). ***[bitte klären: Konto und Absenderdomain einrichten; Öffnungs- und Klickverfolgung abschalten und belegen; Aufbewahrung der Versandprotokolle nachtragen.]***
Hetzner Online	Server für den vom Auftragsverarbeiter betriebenen Virenscanner (ClamAV); zum Stand dieses Vertrags nicht eingerichtet	Bytes hochgeladener Dateien und E-Mail-Anhänge ohne Dateinamen, nur zur Prüfung; keine Speicherung	Deutschland oder Finnland	Auftragsverarbeitungsvertrag über die Verwaltungskonsole des Anbieters. ***[bitte klären: Server einrichten, Standort festlegen und Vertrag abschließen.]***
Sentry	Fehlerberichte	Fehlerberichte ohne Inhalte (E-Mail-Adressen maskiert, Token entfernt, Nutzer nur als Kennung), Kennung des Verantwortlichen, Fehlernummer	Ereignisdaten in der EU-Region (in ZORYVO erzwungen); Konto- und Organisationsdaten des Betreibers in den USA	Auftragsverarbeitungsvertrag, per Klick im Konto angenommen; EU-US Data Privacy Framework, Standardvertragsklauseln als Rückfall
Google Cloud, Pub/Sub	Benachrichtigung über Änderungen in Google-Postfächern; nur bei einer Google-Anbindung; zum Stand dieses Vertrags nicht eingerichtet	Postfachadresse und Änderungsnummer, keine Inhalte	Region wählbar	Google Cloud Data Processing Addendum. ***[bitte klären: Region festlegen, nur falls Google im Testpiloten genutzt wird.]***

Ohne Vertrag nach Art. 28 Abs. 4 DSGVO (§ 6 Abs. 4): healthchecks.io (SIA Monkey See Monkey Do, Riga; Server bei Hetzner in Deutschland, Sicherungen des Anbieters verschlüsselt bei AWS S3, Region nicht angegeben) erhält nach seiner Einrichtung Zeitstempel von Pings ohne Inhalt und ohne Kennungen; das Konto des Betreibers verarbeitet der Anbieter als eigener Verantwortlicher. Telegram (außerhalb der

EU) erhält Alarme an den Betreiber ohne Inhalte, ohne Kontaktdaten und ohne Firmennamen des Verantwortlichen (Inhalt nach § 6 Abs. 4).

Stripe Payments Europe, Ltd. (Irland; Muttergesellschaft Stripe, Inc., USA) wickelt die Zahlungen für die Tarife ab. Zum Stand dieses Vertrags läuft das nur im Testmodus. Stripe erhält keine Kundendaten im Sinne dieses Vertrags, keine Inhalte und keine Daten der Nutzer außer der Rechnungs-E-Mail-Adresse, sondern die Abrechnungsdaten des Verantwortlichen: rechtlicher Name der Firma, Anschrift, USt-IdNr. (falls angegeben), Rechnungs-E-Mail-Adresse, gebuchter Tarif und eine interne Kennung des Kundenkontos. Zahlungsmittel (IBAN, Kartendaten) gibt der Verantwortliche unmittelbar bei Stripe ein; der Auftragsverarbeiter erhält sie nie. Für diese Abrechnungsdaten ist der Auftragsverarbeiter selbst Verantwortlicher; Stripe verarbeitet die Zahlungsdaten teils als eigener Verantwortlicher, teils in seinem Auftrag. Die USt-IdNr. des Kunden wird nach der Registrierung bei der EU-Kommission (VIES) bestätigt; dabei gehen nur das Länderkennzeichen und die Nummer hinaus (Datenschutzerklärung, Abschnitt 4.14). ***[bitte klären: ob die Abfrage bei VIES in diese Tabelle gehört; die EU-Kommission ist eigener Verantwortlicher und erhält keine Kundendaten im Sinne dieses Vertrags.][bitte klären: Einordnung von Stripe (eigener Verantwortlicher oder Auftragsverarbeiter, Vertrag, Standort, Übermittlung in die USA nach Data Privacy Framework oder Standardvertragsklauseln); ob Stripe in diese Tabelle gehört, obwohl keine Kundendaten im Sinne dieses Vertrags dorthin gehen; Konto, Verifizierung und DPA belegen.]***

Keine Unterauftragsverarbeiter des Auftragsverarbeiters sind Google Workspace und Microsoft 365 (Postfach, Kalender, Dateiablage des Verantwortlichen, § 6 Abs. 6) sowie das Captcha der Buchungsseite (läuft vollständig in ZORYVO). Der Quellcode wird bei GitHub (USA) verwaltet; dort liegen keine Daten des Verantwortlichen.

Anlage 4: Sicherung, Wiederherstellung, Löschung aus Sicherungen

1. Datenbank

Die Sicherung der Datenbank ist als zeitpunktgenaue Wiederherstellung (Point-in-Time-Recovery) des Anbieters Supabase vorgesehen. Zum Stand dieses Vertrags ist diese Zusatzleistung nicht gebucht. Eine Sicherung und ein Sicherungsfenster sagt der Auftragsverarbeiter erst zu, wenn die Buchung und ein Wiederherstellungstest belegt sind; er teilt das dem Verantwortlichen nach § 1 Abs. 3 mit. Ab der Buchung beträgt das Sicherungsfenster {{gebuchtes Sicherungsfenster}}. Gelöschte Daten verschwinden aus der Sicherung mit Ablauf dieses Fensters. Der Auftragsverarbeiter hält keine weiteren Kopien der Datenbank, insbesondere keine Abzüge in Code-Verwaltung oder Build-Systemen. Kopien innerhalb der Infrastruktur des Anbieters richten sich nach dessen Vertrag (Anlage 3). Eine Wiederherstellung löst der Auftragsverarbeiter in der Verwaltungsoberfläche des Anbieters aus; der Wiederherstellungstest ist vor Beginn des Testpiloten vorgesehen, sein Ergebnis wird dokumentiert. ***[bitte klären: Point-in-Time-Recovery vor Pilotstart buchen, gebuchtes Fenster eintragen und den Wiederherstellungstest dokumentieren.]***

2. Dateien

Für Dateien im Dateispeicher (Uploads, E-Mail-Anhänge, Rechnungsoriginale, Logos) gibt es im Testpiloten keine gesonderte Sicherung. Die Datenbank-Sicherung enthält nur ihre Metadaten, nicht die Dateien. Beim endgültigen Löschen eines Kontakts entfernt ZORYVO die zugehörigen Dateiobjekte sofort aus dem Dateispeicher. ***[bitte klären: ob und wie lange der Anbieter des Dateispeichers entfernte Objekte intern vorhält.]***

3. Wiederherstellung

Eine Wiederherstellung der Datenbank auf einen früheren Zeitpunkt stellt auch Daten wieder her, die seit

diesem Zeitpunkt endgültig gelöscht wurden, und setzt das Löschprotokoll mit zurück. Der Auftragsverarbeiter liest deshalb vor jeder Wiederherstellung die Kennungen der seit dem Zeitpunkt ausgeführten Löschaufträge aus, wendet die Löschungen danach von Hand erneut an und prüft durch eine Suche nach Name, E-Mail-Adresse und Telefonnummer, dass nichts zurückgeblieben ist. Ein automatisches erneutes Anwenden und ein Löschregister außerhalb der Datenbank gibt es nicht. Während der Wiederherstellung hält der Auftragsverarbeiter alle externen Aktionen an (Notbremse) und setzt vor der Freigabe das Scharfschalten der Automationen zurück, damit erneut gelesene E-Mails keine externen Aktionen auslösen. Dateiverweise können nach einer Wiederherstellung ins Leere zeigen oder Dateien ohne Verweis zurückbleiben; eine Konsistenzprüfung gibt es nicht. Der Auftragsverarbeiter informiert den Verantwortlichen vor und nach einer Wiederherstellung in Textform.

4. Aufbewahrung im laufenden Betrieb

Automatisch gelöscht werden heute nur: Objekte im Papierkorb der Kundendatenbank 30 Tage nach dem Löschen, Benachrichtigungen der Nutzer nach 90 Tagen, unbestätigte Buchungsanfragen 24 Stunden nach Erstellung, abgelaufene Buchungssitzungen und Zwischenzustände von Verbindungsaufbauten, Registrierungsanfragen 7 Tage nach Ablauf oder Abschluss, Webhook-Protokolle von Stripe nach 90 Tagen, die Merkmale gegen wiederholte Testphasen 24 Monate nach Beginn der Testphase. Ebenso entfernt ZORYVO die Dateiobjekte abgelehnter, doppelter und abgebrochener Uploads; der Eintrag mit dem Dateinamen bleibt. Das Kundenkonto samt Kundendaten nach einer Testphase ohne Buchung (§ 9 Abs. 2 Buchstabe e) löscht der Auftragsverarbeiter nach dem Ende der Frist von 30 Tagen mit dem Löschdienst der Anwendung, in der Regel auf Veranlassung eines Mitarbeiters und nur bei eingeschalteter Funktion zusätzlich nachts automatisch; die Erinnerungen 14 Tage und 3 Tage vor dem Termin gehen automatisch per E-Mail. ***[bitte klären: gleichlautend mit AGB § 2a Abs. 5 und § 9 Abs. 2 Buchstabe e.]*** Alle übrigen Daten (E-Mails und ihre Texte, KI-Analysen, Protokolle, Dateien, Debug-Inhalte, abgelaufene Einladungen) bleiben bis zum endgültigen Löschen des zugehörigen Kontakts oder bis zur Löschung nach § 9 gespeichert. Aufbewahrungsfristen, die der Verantwortliche selbst wählt, sind nicht Teil des Testpiloten (Anlage 5).

Anlage 5: Nicht Teil des Testpiloten

Folgende Funktionen sind nicht gebaut und nicht Gegenstand dieses Vertrags. Der Auftragsverarbeiter sagt sie nicht zu:

- Assistent im Dashboard, Telegram-Bot für den Verantwortlichen oder seine Beschäftigten, Microsoft-Teams-Bot;
- Sicherung der Dateien im Dateispeicher, Konsistenzprüfung zwischen Datenbank und Dateispeicher, Wiederherstellung einzelner Dateien;
- Löschregister außerhalb der Datenbank und automatisches erneutes Anwenden von Löschaufträgen nach einer Wiederherstellung;
- automatische Aufbewahrungsfristen über die in Anlage 4 Nr. 4 genannten hinaus (insbesondere für E-Mail-Inhalte, KI-Analysen, Protokolle und Debug-Inhalte) und die Wahl einer Aufbewahrungsfrist durch den Verantwortlichen;
- vollständig automatischer Ablauf bei Vertragsende: Export-Phase, Gesamtexport aller Daten auf Knopfdruck, Löschbestätigung als Dokument, automatischer Widerruf aller Zugriffe bei den Anbietern zum Vertragsende (das Trennen einer einzelnen Verbindung widerruft bei Google, § 9 Abs. 3). Enthalten sind die Kündigung im Kundenportal, das Pausieren mit dem Ende der Laufzeit und die Löschung nach einer Testphase ohne Buchung (§ 9 Abs. 2 Buchstabe e);
- Löschung einer Person, die keinen Kontakt in der Kundendatenbank hat; Wahl zwischen Löschen und Sperren von Rechnungskopien; Löschung von Kalendereinträgen oder Laufwerkskopien durch ZORYVO;

- Selbstbedienung für Nutzerkonten (Auskunft, Export, Löschung des eigenen Kontos, Änderung von Name oder E-Mail-Adresse, Liste eigener Sitzungen);
- automatischer Versand von KI-Antworten ohne Freigabe (A2 im Modus automatisch) und automatische Ablage von Rechnungen, die die KI gelesen hat;
- Anbindungen an Zoom, DATEV, SharePoint, IMAP und andere Mailanbieter; die Eskalation von Freigaben an eine Vertretung; der Tarif Pro;
- Benachrichtigung der Nutzer bei Passwortänderung, neuer Anmeldung oder neuem Gerät.

Stand: 2026-10-17

ENTWURF