Datenschutzerklärung

Diese Datenschutzerklärung beschreibt, wie ZORYVO Technologies personenbezogene Daten verarbeitet. Sie gilt für die Anwendung ZORYVO und für unsere öffentlichen Seiten (Startseite, Preisseite, Registrierung, Kontaktformular, Anmeldung, Passwort vergessen, Einladung, Rechtsseiten). Sie richtet sich an die Nutzer unserer Kunden (Owner-Nutzer und Mitarbeiter), an Personen, die ein Unternehmen bei uns registrieren, an Besucher dieser Seiten und, in Abschnitt 10, an Besucher der Buchungsseiten unserer Kunden.

1. Verantwortlicher und Kontakt

Verantwortlicher für die in dieser Erklärung beschriebene Verarbeitung ist, soweit Abschnitt 2 nichts anderes sagt:

- ZORYVO Technologies {{Rechtsform}}
- {{Straße und Hausnummer}}, {{PLZ Ort}}
- vertreten durch {{vertretungsberechtigte Person}}
- E-Mail: {{E-Mail-Adresse}}, Telefon: {{Telefonnummer}}
- Register: {{Registergericht und Registernummer}} (entfällt ohne Registereintragung)
- USt-IdNr.: {{USt-IdNr.}} (entfällt ohne Umsatzsteuer-Identifikationsnummer)

Für Fragen zum Datenschutz und für die Ausübung Ihrer Rechte erreichen Sie uns unter {{Datenschutz-Kontakt}}.

Unser Datenschutzbeauftragter ist {{Name und Kontakt des Datenschutzbeauftragten}}. ***[bitte klären: Benennungspflicht nach Art. 37 DSGVO und § 38 BDSG prüfen. Besteht keine Pflicht und ist niemand benannt, diesen Satz ersetzen durch: „Wir sind nicht verpflichtet, einen Datenschutzbeauftragten zu benennen, und haben keinen benannt.“]***

2. Zwei Rollen: wofür wir verantwortlich sind und wofür unsere Kunden

ZORYVO ist eine Software für Unternehmen. Unsere Vertragspartner nennen wir Kunden; in der Anwendung heißt das Kundenkonto Owner. Nutzer mit der Rolle Owner nennen wir Owner-Nutzer, die zweite Rolle heißt Mitarbeiter. Im Auftragsverarbeitungsvertrag heißt der Kunde Verantwortlicher. Ein Kunde verbindet seine Postfächer, Kalender und Dateiablagen mit ZORYVO, lädt seine Mitarbeiter ein und legt fest, was ZORYVO tun darf.

Wir sind Verantwortlicher für die Nutzerkonten und die Anmeldung (Abschnitt 4), für Registrierung, Vertragsschluss, Testphase und Abrechnung (Abschnitte 4.9 bis 4.12), für die technische Sicherheit und Fehlerüberwachung (Abschnitte 3 und 7), für System-Mails (Abschnitt 6), für unsere öffentlichen Seiten (Abschnitt 3) und für Anfragen über unser Kontaktformular (Abschnitt 11).

Für die Inhalte, die ein Kunde in ZORYVO verarbeitet, ist der Kunde Verantwortlicher. Dazu gehören seine Postfächer, Kontakte, Termine, Dateien, Rechnungen und Notizen sowie die Ergebnisse der KI-Analyse. Wir verarbeiten diese Daten als Auftragsverarbeiter nach Art. 28 DSGVO auf Grundlage eines Auftragsverarbeitungsvertrags. Dieser Vertrag ist Bestandteil unseres Vertrags mit dem Kunden; der Kunde erhält ihn mit dem Vertrag. Abschnitt 8 beschreibt, was wir dabei tun.

Sind Sie Kunde, Lieferant, Interessent oder sonstiger Korrespondenzpartner eines unserer Kunden, wenden Sie sich mit Fragen und Anträgen an diesen Kunden. Wir unterstützen ihn bei der Beantwortung. ZORYVO stellt ihm dafür je Kontakt eine Auskunft, eine Sperrung und ein endgültiges Löschen bereit (Abschnitt 8.7).

[bitte klären: Einordnung des Betreibers als Verantwortlicher für die Nutzerkonten der Mitarbeiter unserer Kunden (eigene Verantwortlichkeit oder Auftragsverarbeitung für den Kunden). Die folgenden Abschnitte gehen von eigener Verantwortlichkeit aus. Der Auftragsverarbeitungsvertrag (§ 7 Abs. 1 und 4, § 8 Abs. 4, Anlage 1) und die Mitarbeiterinformation sind gleichlautend zu fassen.]

3. Hosting und Zugriffsdaten

ZORYVO läuft bei Vercel. Die Serverfunktionen werden in der Region Frankfurt (fra1) ausgeführt. Datenbank, Anmeldedienst und Dateispeicher betreibt Supabase in der Region eu-central-1 (Frankfurt). Dort liegen alle Inhalte und Kontodaten.

Wenn Sie eine Seite aufrufen, übermittelt Ihr Browser technisch bedingt Ihre IP-Adresse, die aufgerufene Adresse, den Zeitpunkt und Angaben zu Browser und Betriebssystem. Vercel verarbeitet diese Daten, um die Seite auszuliefern.

Unsere eigenen Server-Protokolle enthalten je Eintrag unter anderem: Dienstname, Umgebung, Schweregrad, Zeitpunkt, Nachricht, Verarbeitungsschritt, Status, Dauer und die Ablaufkennung (trace_id). Wo bekannt, kommen die Kennung des Kunden und Kennungen betroffener Objekte hinzu, zum Beispiel einer Mail oder eines Kontakts. Bei Fehlern enthalten sie zusätzlich Fehlernummer, Fehlerklasse, Fehlercode und Routenmuster. Sie enthalten keine IP-Adresse, keine E-Mail-Adresse, keinen konkreten Anfragepfad und keine Inhalte. Felder wie Passwort, Token, Cookie, E-Mail, Betreff oder Text werden vor dem Schreiben geschwärzt. Bei Fehlern wird nur das Routenmuster festgehalten, nicht der konkrete Pfad, weil Pfade Einmal-Tokens enthalten können. Diese Protokolle laufen in die Laufzeit-Protokolle von Vercel.

Ihre IP-Adresse verwenden wir selbst nur für Rate-Limits (Abschnitt 4.5). Dabei speichern wir sie nicht im Klartext, sondern nur als SHA-256-Hash.

[bitte klären: ob Vercels eigene Anfrage-Protokolle die IP-Adresse der Besucher enthalten und wie lange Vercel sie im gebuchten Tarif aufbewahrt. Die Angabe ist nachzutragen.]

Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse ist der sichere und stabile Betrieb der Anwendung und der öffentlichen Seiten. Für Owner-Nutzer dient die Verarbeitung zugleich der Erfüllung des Vertrags mit dem Kunden (Art. 6 Abs. 1 lit. b DSGVO); für Mitarbeiter gilt Abschnitt 4.8.
[bitte klären: Rechtsgrundlage juristisch bestätigen; Vorschlag ohne Rechtsprüfung.]

Alle Seiten tragen Sicherheits-Header (Content-Security-Policy ohne fremde Skripte, Strict-Transport-Security, Referrer-Policy, Permissions-Policy). Eingebettet werden darf nur das Buchungs-Widget (Abschnitt 10), und nur auf den Domains, die der Kunde hinterlegt hat. Alle anderen Seiten sind gegen Einbettung in fremde Seiten gesperrt (X-Frame-Options, frame-ancestors). Es werden keine Skripte Dritter, keine Schriften von Dritten und keine Analysedienste geladen.

4. Nutzerkonto und Anmeldung

4.1 Wie ein Konto entsteht

Ein Konto entsteht auf einem von zwei Wegen. Erstens registrieren sich Unternehmen mit Sitz in Deutschland selbst unter /registrieren und testen ZORYVO 30 Tage kostenlos (Abschnitt 4.9); die registrierende Person wird Owner-Nutzer des neuen Kundenkontos, und das Konto entsteht erst, nachdem sie ihre E-Mail-Adresse über einen Link bestätigt hat. Ihre Daten erhalten wir in diesem Fall von Ihnen. Zweitens entstehen Konten über Einladungen: Weitere Personen lädt der Kunde ein und weist ihnen eine Rolle zu (Owner oder Mitarbeiter). Bei Kundenkonten, die wir als Betreiber auf Grundlage einer Pilotvereinbarung anlegen, laden wir den ersten Owner-Nutzer ein; die E-Mail-Adresse dafür nennt uns der Kunde. Ihre E-Mail-Adresse erhalten wir bei einer Einladung vom Kunden, nicht von Ihnen (Art. 14

DSGVO). Zur Einladung speichern wir: E-Mail-Adresse, Rolle, Status, einladende und annehmende Person, Ablaufzeitpunkt, Zeitpunkt des Mailversands oder des Fehlschlags und den SHA-256-Hash des Einladungstokens. Der Token selbst steht nur im Link und ist 7 Tage gültig.

Beim ersten Annehmen einer Einladung wählen Sie einen Anzeigenamen (1 bis 80 Zeichen) und ein Passwort (12 bis 128 Zeichen); bei der Registrierung geben Sie beides im Registrierungsformular an. Haben Sie schon ein Konto, melden Sie sich damit an und werden Mitglied des weiteren Kunden; Name und Passwort bleiben dann unverändert. Das Passwort speichert ausschließlich unser Anmeldedienst Supabase Auth; ZORYVO selbst speichert es nicht. Die E-Mail-Adresse gilt durch den Einladungslink oder den Bestätigungslink der Registrierung als bestätigt.

4.2 Welche Kontodaten wir speichern

Zu Ihrem Konto speichern wir: eine Kennung, E-Mail-Adresse, Anzeigename, Anlage- und Änderungszeitpunkt sowie das Merkmal, ob Sie Plattform-Admin sind. Felder für Sprache und Profilbild sind vorhanden, werden aber nicht genutzt: Die Anwendung ist fest auf Deutsch eingestellt, ein Profilbild lässt sich nicht hochladen. Je Kunde, bei dem Sie Mitglied sind, speichern wir Rolle, Rechte, anlegende Person und ein Enddatum der Mitgliedschaft. Neue Mitarbeiter erhalten automatisch die Rechte „Kundendatenbank ansehen“ und „Kundendatenbank bearbeiten“; Owner-Nutzer haben alle Rechte.

Sie können Anzeigename und E-Mail-Adresse in ZORYVO derzeit nicht selbst ändern. Für eine Berichtigung wenden Sie sich an {{Datenschutz-Kontakt}}. Die Seite „Konto“ zeigt Ihre E-Mail-Adresse, den Weg zum Passwortwechsel, den Stand der Zwei-Faktor-Anmeldung und „Auf allen Geräten abmelden“.

Kolleginnen und Kollegen im selben Kundenkonto sehen von Ihnen nur den Anzeigenamen. Wer Mitarbeiter verwalten darf (Owner-Nutzer und Personen, denen der Kunde dieses Recht gegeben hat), sieht Ihre E-Mail-Adresse in Ihrer Einladung. Der Plattform-Admin sieht E-Mail-Adresse, Anzeigename, Anlagedatum, Rolle, Sperrstatus und offene Einladungen.

4.3 Zwei-Faktor-Anmeldung und Wiederherstellungscodes

Die Zwei-Faktor-Anmeldung läuft über zeitbasierte Einmalcodes (TOTP). Sie ist Pflicht für Owner-Nutzer und für den Plattform-Admin. Für Mitarbeiter legt der Kunde fest, ob sie Pflicht ist. Ein einmal eingerichteter Faktor wird immer abgefragt. Der Faktor liegt bei Supabase Auth.

Bei der Einrichtung erhalten Sie 10 Wiederherstellungscodes mit je 12 Zeichen. Wir speichern nur deren SHA-256-Hash; jeder Code gilt einmal. Wer einen Code einlöst, entfernt damit alle Faktoren, beendet alle Sitzungen und muss die Zwei-Faktor-Anmeldung neu einrichten.

4.4 Sitzungen und Abmeldung

Die Sitzung wird in Cookies gehalten, die nur der Server liest (Abschnitt 5). Bei jeder Anfrage prüft der Server, ob die Sitzung noch gültig ist, ob das Konto gesperrt wurde und ob das Profil noch besteht. Ist das nicht der Fall, werden Sie abgemeldet. Plattform-Admins werden spätestens 8 Stunden nach der Anmeldung abgemeldet.

Sie können sich lokal abmelden oder mit „Auf allen Geräten abmelden“ alle eigenen Sitzungen beenden. Eine Liste Ihrer Sitzungen oder das Beenden einzelner Sitzungen gibt es derzeit nicht. Jeder Owner-Nutzer des Kunden kann Sie mit dem Notschalter „Sofort aussperren“ sofort aus dem Kundenkonto entfernen; dabei enden Ihre Sitzungen, wenn Sie bei keinem weiteren Kunden Mitglied sind. Der Plattform-Admin kann Ihr Konto sperren und entsperren; eine Sperre beendet Ihren Zugang sofort. Jeder dieser Eingriffe verlangt die Angabe eines Grundes und wird protokolliert.

Nach jeder erfolgreichen Anmeldung setzt ZORYVO das Cookie zoryvo_device mit einem zufälligen Wert. In der Datenbank liegt dazu nur ein SHA-256-Hash aus Ihrer E-Mail-Adresse und diesem Wert. Ein Gerät,

das sich bei diesem Konto erfolgreich angemeldet hat, bleibt dadurch 90 Tage ab dieser Anmeldung von der kontoweiten Anmeldesperre ausgenommen. Spätere Anmeldungen in diesen 90 Tagen verlängern die Frist nicht. Danach gilt die Ausnahme erst wieder ab der nächsten erfolgreichen Anmeldung.

ZORYVO sendet derzeit keine Hinweis-Mail bei Passwortänderung, neuer Anmeldung oder neuem Gerät.

4.5 Anmeldesperre und Rate-Limits

Zum Schutz vor dem Ausprobieren von Passwörtern zählt ZORYVO Anmeldeversuche: 50 je 15 Minuten je IP-Adresse, 10 je 15 Minuten je Konto und IP-Adresse, dazu 100 Fehlversuche je Stunde je Konto aus allen Adressen (bekannte Geräte ausgenommen). Eine erfolgreiche Anmeldung löscht die Konto-Zähler. Für das Zurücksetzen des Passworts, das Öffnen von E-Mail-Links, das Annehmen und Versenden von Einladungen und die Eingabe von 2FA-Codes gelten weitere Grenzen. Erreicht ein Konto die Grenze von 100 Fehlversuchen, wird das dem Plattform-Admin ohne Nennung der Adresse gemeldet.

Die Zähler liegen in unserer Datenbank. Der Schlüssel besteht aus dem Zweck und dem SHA-256-Hash des Identifikators (E-Mail-Adresse, IP-Adresse oder beides). E-Mail-Adresse und IP-Adresse stehen nie im Klartext in der Datenbank.

4.6 Sicherheitsprotokoll

Sicherheitsereignisse zu Ihrem Konto halten wir in einem Audit-Protokoll fest: Einrichtung der Zwei-Faktor-Anmeldung, Erzeugen und Einlösen von Wiederherstellungscodes, Anlegen des Kontos, Entfernen von Faktoren, Sperren und Entsperren, Beenden von Sitzungen, Änderungen an Mitgliedschaften und Einladungen. Je Ereignis speichern wir: Zeitpunkt, handelnde Person oder System, Kanal, Ereignisname, betroffenes Objekt, Metadaten (Kennungen, Zähler, Feldnamen, Grund) und die Ablaufkennung. Inhalte gehören nicht hinein. ZORYVO wertet keine Leistung von Personen aus: Es gibt keine Ranglisten, keine Antwortzeiten je Mitarbeiter und keinen Filter nach Person im Protokoll.

4.7 Was Supabase Auth selbst speichert

Supabase Auth speichert zu Ihrem Konto die E-Mail-Adresse, den Anzeigenamen (als Nutzer-Metadatum), das Passwort (nur als kryptografischer Hash ***[bitte klären: Hashverfahren laut Supabase-Dokumentation]***), den Sperrstatus, die Sitzungen und die Faktoren der Zwei-Faktor-Anmeldung. ***[bitte klären: ob Supabase Auth je Sitzung IP-Adresse, Browser-Kennung oder den Zeitpunkt der letzten Anmeldung aufzeichnet; im Projekt prüfen und hier ergänzen.]***

4.8 Rechtsgrundlagen

Für Owner-Nutzer ist die Rechtsgrundlage Art. 6 Abs. 1 lit. b DSGVO: Das Konto ist nötig, um den Vertrag mit dem Kunden zu erfüllen. Für Mitarbeiter-Konten ist die Rechtsgrundlage Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse und das des Kunden ist es, die vom Kunden beauftragte Software seinen Mitarbeitern bereitzustellen. ***[bitte klären: Rechtsgrundlage für Mitarbeiter-Konten; der Vertrag besteht mit dem Kunden, nicht mit dem Mitarbeiter. Alternativ Auftragsverarbeitung für den Kunden, siehe Abschnitt 2.]*** Für Zwei-Faktor-Anmeldung, Sitzungsprüfung, Rate-Limits und Sicherheitsprotokoll ist die Rechtsgrundlage Art. 6 Abs. 1 lit. f DSGVO in Verbindung mit Art. 32 DSGVO. Unser berechtigtes Interesse ist der Schutz der Konten und der Daten unserer Kunden. Für die Registrierung, die Testphase, die Zustimmungen, den Schutz vor wiederholten Testphasen und die Zahlungsabwicklung nennen die Abschnitte 4.9 bis 4.12 die Rechtsgrundlagen.

4.9 Registrierung und Testphase

Unternehmen mit Sitz in Deutschland können sich unter /registrieren selbst registrieren. Das geschieht in zwei Schritten.

Im ersten Schritt geben Sie nur Ihre E-Mail-Adresse ein und lösen die Bot-Prüfung aus (Captcha nach

dem ALTCHA-Protokoll, Abschnitt 10). Wir speichern die E-Mail-Adresse, den SHA-256-Hash eines Bestätigungstokens, den Ablaufzeitpunkt (24 Stunden), den Stand der Anfrage und den Zeitpunkt des Mailversands. Die Antwort ist immer dieselbe, auch wenn die Adresse schon ein Konto hat; dann erhalten Sie die Mail „Sie haben bereits ein Konto“. Das Rate-Limit beträgt 5 Anfragen je Stunde je IP-Adresse und 3 Anfragen je Tag je E-Mail-Adresse; beide Kennungen speichern wir nur als SHA-256-Hash (Abschnitt 4.5). Ein für Menschen unsichtbares Feld erkennt Programme; solche Anfragen speichern wir nicht. Die Anfrage löschen wir 7 Tage nach Ablauf oder Abschluss.

Im zweiten Schritt, hinter dem Link in der Mail, geben Sie an: den rechtlichen Namen Ihres Unternehmens mit Rechtsform, die Anschrift (Straße, Postleitzahl, Ort; das Land ist Deutschland), freiwillig die USt-IdNr. und den Handelsregistereintrag (Gericht und Nummer), Ihren Namen und ein Passwort. Mit Häkchen erklären Sie, dass Sie für ein Unternehmen mit Sitz in Deutschland handeln, das Unternehmer ist, und es vertreten dürfen, und dass Sie die AGB und den AVV in der angezeigten Fassung annehmen. Die Datenschutzerklärung nehmen Sie zur Kenntnis; ein Häkchen dafür gibt es nicht. Beim Absenden legen wir Ihr Konto, das Kundenkonto Ihres Unternehmens (Tarif „Testphase“), Ihre Mitgliedschaft als Owner-Nutzer, das Zustimmungsprotokoll (Abschnitt 4.10) und die Merkmale gegen wiederholte Testphasen (Abschnitt 4.11) an. Danach richten Sie die Zwei-Faktor-Anmeldung ein (Abschnitt 4.3). Wir prüfen die USt-IdNr. auf Format und Prüfziffer und, wenn Sie eine angegeben haben, nach der Registrierung bei der EU-Kommission (VIES, Abschnitt 4.14). Die Firmendaten können Sie später in den Einstellungen ändern; Änderungen stehen im Änderungsprotokoll.

Die Testphase dauert 30 Tage und kostet nichts; Zahlungsdaten brauchen wir dafür nicht. Wir erinnern Sie 7 Tage und 1 Tag vor dem Ende per E-Mail. Nach dem Ende können Sie die Daten nur noch lesen und exportieren, bis Sie einen Tarif buchen. Buchen Sie nicht innerhalb von 30 Tagen nach dem Ende, wird die Löschung des Kundenkontos und der Kundendaten fällig; wir erinnern Sie 14 Tage und 3 Tage vorher per E-Mail. Die Löschung führen wir in der Regel von Hand durch, nachts automatisch nur, wenn wir diese Funktion eingeschaltet haben (Abschnitt 14). ***[bitte klären: ob eine automatische Löschung nach einer Testphase ohne Buchung zulässig ist; Standard ist die Löschung von Hand.]***

Zwecke und Rechtsgrundlagen: Wir verarbeiten diese Daten, um den Vertrag mit Ihrem Unternehmen zu schließen und zu erfüllen, das Kundenkonto und Ihr Konto anzulegen und die Testphase durchzuführen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO; sind Sie Vertreter oder Beschäftigter einer juristischen Person, Art. 6 Abs. 1 lit. f DSGVO (unser berechtigtes Interesse ist der Abschluss und die Durchführung des Vertrags mit dem Unternehmen). Bot-Prüfung und Rate-Limits dienen dem Schutz vor Missbrauch (Art. 6 Abs. 1 lit. f DSGVO). Die Angaben sind für den Vertrag nötig (Abschnitt 16.1)***[bitte klären: Rechtsgrundlage für Vertreter und Beschäftigte juristischer Personen (lit. b oder lit. f); ob die Registrierung ohne weitere Prüfung der Vertretungsbefugnis zulässig ist; Vorschlag ohne Rechtsprüfung.]***

4.10 Vertragsbestätigung und Zustimmungsprotokoll

Mit dem Absenden der Registrierung und bei jeder späteren Zustimmung zu einer geänderten Fassung der AGB halten wir im Zustimmungsprotokoll fest: den Zeitpunkt, Ihren Namen und Ihre E-Mail-Adresse und die Firmendaten des Kunden (jeweils als Abschrift zum Zeitpunkt der Erklärung), Ihre Erklärungen (Unternehmer, Vertretungsbefugnis), die Fassungen von AGB und AVV, denen Sie zugestimmt haben (Nummer, Stand, Prüfsumme), die Fassung der Datenschutzerklärung, die Sie zur Kenntnis genommen haben, und den Versand der Vertragsbestätigung (Zeitpunkt, Zahl der Versuche, Prüfsumme der PDF-Datei). Wir speichern keine IP-Adresse. Nachweis sind Ihre bestätigte E-Mail-Adresse, der Zeitpunkt und die Fassungen.

Nach der Registrierung senden wir Ihnen die Vertragsbestätigung per E-Mail über Brevo (Abschnitt 6), mit AGB, AVV (mit den Angaben Ihres Unternehmens) und Datenschutzerklärung als PDF-Anhang. Das PDF erzeugen wir aus den gespeicherten Fassungen; wir speichern von ihm nur die Prüfsumme und können es jederzeit neu erzeugen. Sie finden es in den Einstellungen unter „Vertrag“. Alle Fassungen der Texte

bleiben unter /rechtliches abrufbar.

Zweck ist der Nachweis des Vertragsschlusses und der Zustimmungen, die Erfüllung der Pflichten bei Verträgen im elektronischen Geschäftsverkehr (§ 312i BGB) und die Verteidigung gegen Ansprüche. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO (Vertrag), lit. c (gesetzliche Pflichten) und lit. f (Nachweis und Verteidigung von Rechtsansprüchen). Wir bewahren das Zustimmungsprotokoll für die Laufzeit des Vertrags und danach 6 Jahre auf (Abschnitt 14); es bleibt auch nach der Löschung des Kundenkontos als Vertragsnachweis bestehen. ***[bitte klären: Aufbewahrungsdauer (6 oder 10 Jahre), Rechtsgrundlage und ob das Protokoll nach der Löschung des Kundenkontos weiter Name und E-Mail-Adresse tragen darf.]***

4.11 Schutz vor wiederholten Testphasen

Die Testphase ist einmal je Unternehmen vorgesehen (AGB § 2a). Um wiederholte Testphasen zu erkennen, vergleichen wir bei der Registrierung und später beim Verbinden eines Postfachs diese Merkmale mit denen früherer Testphasen: die USt-IdNr., den Handelsregistereintrag (Gericht und Nummer), die Domain Ihrer Firmen-E-Mail-Adresse (nicht bei allgemeinen E-Mail-Anbietern und Wegwerf-Adressen) und beim Verbinden eines Postfachs die Kennung des Microsoft-Tenants (nicht bei privaten Microsoft-Konten) oder die Domain Ihres Google Workspace. Wir speichern diese Merkmale nicht im Klartext, sondern nur als HMAC-SHA-256-Hash mit einem Geheimnis, das nur der Server kennt. Der Hash lässt sich nicht zurückrechnen, aber wer einen Wert kennt, kann ihn erraten und vergleichen; die Daten sind deshalb pseudonym, nicht anonym. Wir verwenden kein Geräte-Fingerprinting und speichern dafür keine IP-Adresse, keine Browserdaten und keine Cookies.

Ein Treffer löst keine automatische Sperre aus. Er erscheint als Hinweis in einer Liste für den Plattform-Admin, mit der Art des Merkmals und der Kennung des anderen Kundenkontos, nie mit dem Wert. Ein Mensch prüft den Fall und entscheidet; es gibt keine automatisierte Entscheidung im Sinne von Art. 22 DSGVO (Abschnitt 16.2). Dieselbe Liste zeigt, ob die USt-IdNr. wohlgeformt ist und ob die Domain eine Firmen-Domain, ein allgemeiner E-Mail-Anbieter oder eine Wegwerf-Adresse ist.

Zweck ist der Schutz der kostenlosen Testphase vor Missbrauch und vor den Kosten, die sie verursacht. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der Verhinderung von Missbrauch); Sie können nach Art. 21 DSGVO widersprechen (Abschnitt 15). Wir speichern die Merkmale 24 Monate ab Beginn der Testphase, auch wenn das Kundenkonto vorher gelöscht wird; danach löscht der nächtliche Lauf sie. ***[bitte klären: Interessenabwägung und Speicherdauer von 24 Monaten; ob Hashes von USt-IdNr. und Domain als personenbezogene Daten gelten; ob die Merkmale aus dem Konto eines Anbieters (Microsoft-Tenant, Google-Workspace-Domain) mit der Google API Services User Data Policy (Limited Use, Abschnitt 9.2) und den Microsoft-Bedingungen vereinbar sind; Hinweis in der Oberfläche der Registrierung.]***

4.12 Zahlungsabwicklung (Stripe)

Tarife buchen und bezahlen Sie über unseren Zahlungsdienstleister Stripe Payments Europe, Ltd., Irland (Stripe). Die Buchungsseite (Checkout) und das Kundenportal, in dem Sie Zahlungsmittel, Rechnungen, Tarif und Kündigung verwalten, sind Seiten von Stripe; Ihr Browser verbindet sich dafür mit Stripe. Ihre Zahlungsdaten (Kartendaten, IBAN) geben Sie nur dort ein; wir erhalten sie nie. Für die Testphase brauchen Sie keine Zahlungsdaten, und wir legen erst bei der Buchung einen Kunden bei Stripe an.

An Stripe übermitteln wir bei der Buchung: den rechtlichen Namen Ihres Unternehmens, die Anschrift, die Rechnungs-E-Mail-Adresse, die USt-IdNr. (falls angegeben), den gewählten Tarif und Abrechnungszeitraum und eine interne Kennung Ihres Kundenkontos. Stripe sendet uns Ereignisse zum Abonnement (Buchung, Zahlung, Zahlungsausfall, Kündigung). Wir speichern davon nur die Kennungen bei Stripe, den Stand des Abonnements, den Tarif, den Abrechnungszeitraum, ob und wann es endet und den Zeitpunkt der letzten fehlgeschlagenen Zahlung, dazu ein Ereignisprotokoll (Kennung, Art, Zeitpunkt, Ergebnis; ohne Inhalt) für 90 Tage zum Schutz vor doppelten Ereignissen. Wir speichern keine IBAN,

keine Kartendaten und keine Rechnungen. Rechnungen, Belege und SEPA-Vorabankündigungen versendet Stripe.

Zweck ist die Abwicklung der Zahlung, die Rechnungsstellung, die Erfüllung steuerrechtlicher Pflichten und die Steuerung des Zugangs nach dem Stand der Zahlung (Pausieren bei Zahlungsausfall). Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO (Vertrag) und lit. c (steuer- und handelsrechtliche Aufbewahrung der Rechnungen). Stripe verarbeitet Zahlungsdaten teils als eigener Verantwortlicher nach seinen Datenschutzhinweisen (Abschnitt 12). Stripe Payments Europe, Ltd. gehört zur Stripe-Gruppe mit Muttergesellschaft in den USA; Übermittlungen dorthin stützen sich auf das EU-US Data Privacy Framework und Standardvertragsklauseln (Abschnitt 13). ***[bitte klären: Rolle von Stripe (eigener Verantwortlicher oder Auftragsverarbeiter) und Vertrag; Übermittlungsgrundlage; Aufbewahrungsfristen der Rechnungen (8 Jahre); Stand des Stripe-Kontos (derzeit nicht für echte Zahlungen eingerichtet); Beleg des Auftragsverarbeitungsvertrags in docs/SUBPROCESSORS.md.]***

4.13 Empfehlungsprogramm

Wenn wir das Empfehlungsprogramm „Kunden werben Kunden“ anbieten (die Seite „Empfehlen“ im Kundenkonto zeigt, ob es läuft), gilt zusätzlich Folgendes. Wir setzen dafür keine Cookies und keine Tracking-Technik ein; der Code wird nicht im Browser gespeichert.

Wenn Sie als Kunde empfehlen: Wir erzeugen für Ihr Kundenkonto einen Empfehlungscode und speichern ihn mit der Kennung Ihres Kundenkontos. Registriert sich ein Unternehmen mit Ihrem Code oder Ihrem Link, speichern wir die Verbindung zwischen Ihrem Kundenkonto und dem neuen Kundenkonto (wer wen empfohlen hat), den Zeitpunkt der Registrierung, den Stand der Empfehlung (angemeldet, wartet auf Prüfung, belohnt, abgelehnt, abgelaufen), den Zeitpunkt der ersten bezahlten Rechnung, die Höhe und die Kennung der Gutschrift bei Stripe und, wenn bei uns eine Person über die Empfehlung entscheidet, deren Entscheidung mit Notiz. Wir zeigen Ihnen nicht, wer empfohlen wurde. Sie sehen nur Zahlen (angemeldet, zahlend, gutgeschrieben, offen) und die gutgeschriebene Summe. Wir schicken keine Nachrichten in Ihrem Namen an Dritte.

Wenn Sie sich mit einem Empfehlungscode registrieren: Sie können den Code in das freiwillige Feld im ersten Schritt der Registrierung eintragen oder über einen Link, der ihn enthält, vorausfüllen lassen. Wir prüfen den Code auf unserem Server und begrenzen die Zahl der Prüfungen je Anschluss (Zähler mit gehashter Adresse, wie in Abschnitt 4.5), damit sich Codes nicht durchprobieren lassen; die Antwort lautet nur „gültig“ oder „nicht gültig“. Wir speichern den Code mit Ihrer Registrierungsanfrage und, nach der Registrierung, die Verbindung zum werbenden Kundenkonto. Um Empfehlungen an sich selbst zu erkennen, vergleichen wir die Merkmale Ihrer Registrierung (USt-IdNr., Handelsregistereintrag, Domain der Firmen-E-Mail-Adresse) mit denen des werbenden Kundenkontos, nur als Hashwerte wie in Abschnitt 4.11. Dazu lesen wir beim Anlegen Ihres Kundenkontos die Angaben, die das werbende Kundenkonto heute bei uns hinterlegt hat (USt-IdNr., Handelsregistereintrag und die Domain der Rechnungs-E-Mail-Adresse), bilden daraus im Arbeitsspeicher dieselben Hashwerte und vergleichen sie mit Ihren; wir speichern, zeigen und protokollieren diese Angaben des werbenden Kunden dabei nicht, und es bleibt nur, ob und welche Art von Merkmal übereinstimmt (nie der Wert). Ein Treffer lehnt nichts automatisch ab: Eine Person bei uns entscheidet. ***[bitte klären: ob das Lesen der aktuellen Angaben des werbenden Kunden für diesen Vergleich (statt nur der gespeicherten Hashes aus Abschnitt 4.11, die nach 24 Monaten gelöscht werden) von der Rechtsgrundlage lit. f gedeckt ist und ob der Hinweis an den werbenden Kunden (Art. 14 DSGVO) darauf erweitert werden muss.]*** Das werbende Unternehmen erfährt nicht, wer Sie sind; es sieht nur, dass die Zahl seiner Empfehlungen gestiegen ist.

Zweck und Rechtsgrundlage: Zweck ist die Durchführung des Empfehlungsprogramms (Prüfung der Voraussetzungen, Gutschrift der Prämie) und der Schutz vor Missbrauch. Die Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO (Teilnahmebedingungen, AGB § 8a) und, für die Missbrauchserkennung, lit. f (berechtigtes Interesse). ***[bitte klären: Rechtsgrundlage für die Verarbeitung der Daten des***

geworbenen Unternehmens und seiner Ansprechperson, die der Werbende nicht kennt (Art. 6 Abs. 1 lit. b oder f DSGVO); Interessenabwägung; ob dem Werbenden im Rahmen der Information nach Art. 14 DSGVO etwas mitzuteilen ist; Hinweis auf das Widerspruchsrecht nach Art. 21 DSGVO.]

Empfänger: Für die Gutschrift schreiben wir den Betrag auf das Kundenguthaben bei Stripe (Abschnitt 4.12). An den werbenden Kunden geben wir weder Namen noch E-Mail-Adressen oder Firmen der Geworbenen weiter.

Speicherdauer: Die Zeilen einer Empfehlung bleiben, solange das Kundenkonto des werbenden Kunden besteht. Löschen wir das werbende Kundenkonto, löschen wir seine Empfehlungen und seinen Code mit. Löschen wir das geworbene Kundenkonto, löschen wir die Empfehlung, außer sie wurde schon belohnt: Dann bleibt sie ohne Verweis auf das geworbene Kundenkonto als Nachweis der Gutschrift des werbenden Kunden: Wir löschen dabei die Rechnungskennung, die Verdachtsmerkmale und die Notiz; es bleiben der Code, die Höhe der Prämie, Zeitpunkte und die Kennung der Gutschrift. ***[bitte klären: Aufbewahrung des Nachweises einer Gutschrift (Buchführung, Aufbewahrungsfristen) und deren Dauer.]***

4.14 Prüfung der USt-IdNr. bei VIES

Haben Sie bei der Registrierung eine USt-IdNr. angegeben, fragen wir nach dem Anlegen Ihres Kundenkontos bei VIES nach, dem Dienst der EU-Kommission zur Bestätigung von Umsatzsteuer-Identifikationsnummern (VAT Information Exchange System). Wir senden dabei nur das Länderkennzeichen und die Nummer, keinen Firmennamen, keine Anschrift, keine E-Mail-Adresse und keine Kennung Ihres Kontos. VIES antwortet auch mit dem Namen und der Anschrift, die zu der Nummer hinterlegt sind; diese Angaben lesen wir nicht, speichern wir nicht und protokollieren wir nicht. Wir halten nur das Ergebnis fest: „bestätigt“, „VIES kennt die Nummer nicht“ oder „nicht geprüft“, mit dem Zeitpunkt der Antwort, dazu die Zahl und den Zeitpunkt der Versuche. Das Ergebnis erscheint wie die anderen Merkmale der Registrierung (Abschnitt 4.11) in der Liste für den Plattform-Admin; es sperrt nichts und ändert nichts an Ihrer Registrierung.

Die Registrierung hängt nicht von VIES ab. Antwortet VIES nicht (oder nicht rechtzeitig, wir warten höchstens 5 Sekunden), läuft die Registrierung unverändert weiter, und wir fragen in den folgenden Nächten bis zu viermal erneut; danach bleibt die Nummer „nicht geprüft“. Bei Kundenkonten, die vor dieser Funktion angelegt wurden, fragen wir nicht nachträglich nach.

Zweck ist die Plausibilisierung der Angaben bei der Registrierung und der Schutz vor Missbrauch der kostenlosen Testphase; das Ergebnis ist ein Hinweis für eine Person bei uns und keine automatisierte Entscheidung (Abschnitt 16.2). Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an richtigen Angaben zum Vertragspartner und an der Verhinderung von Missbrauch). Die EU-Kommission betreibt VIES als eigene Verantwortliche; die Anfrage bleibt innerhalb der EU. Die Aufbewahrung folgt den Firmendaten (Abschnitt 14). ***[bitte klären: Rechtsgrundlage und Interessenabwägung der Abfrage bei VIES; ob die Nummer eines Einzelunternehmers oder Freiberuflers als personenbezogen gilt und der Hinweis in der Registrierung ergänzt werden muss; Nutzungsbedingungen von VIES für die automatisierte Abfrage; ob wir für den Nachweis der Prüfung eine qualifizierte Bestätigung (mit eigener USt-IdNr. des Betreibers als Anfragender) brauchen, die wir derzeit nicht anfordern; Stand: Die Abfrage ist nur eingeschaltet, wenn die Umgebung VIES_TRANSPORT=http setzt.]***

5. Cookies und lokale Speicherung

ZORYVO setzt nur Cookies, die für den Betrieb nötig sind. Es gibt keine Analyse-, Tracking- oder Werbe-Cookies und keine Skripte Dritter.

Name	Zweck	Laufzeit	Art

sb-…-auth-token (bei langen Werten in Teile .0, .1 aufgeteilt)	Sitzungscookie von Supabase Auth; weist Sie als angemeldet aus; wird nur vom Server gelesen	400 Tage, wird bei jeder Erneuerung der Sitzung neu gesetzt; wie lange die Sitzung selbst gilt, steht in Abschnitt 14	technisch notwendig; HttpOnly, Secure, SameSite=Lax, Pfad /
sb-…-auth-token-code-verifier	Prüfwert (PKCE) während eines E-Mail-Link-Ablaufs, zum Beispiel beim Zurücksetzen des Passworts	bis zu 400 Tage; wird beim Abschluss des Ablaufs gelöscht	technisch notwendig; HttpOnly, Secure, SameSite=Lax, Pfad /
zoryvo_device	erkennt ein Gerät wieder, das sich bei diesem Konto schon angemeldet hat, und nimmt es von der kontoweiten Anmeldesperre aus (Abschnitt 4.4)	90 Tage, wird bei jeder Anmeldung erneuert	technisch notwendig; HttpOnly, Secure, SameSite=Lax, Pfad /
zoryvo_book	Sitzung eines Besuchers der Buchungsseite (Abschnitt 10); nur auf der Buchungsadresse, Pfad /book	höchstens 2 Stunden, bei Bestätigungslinks 30 Minuten	technisch notwendig; HttpOnly, Secure, SameSite=Lax, Pfad /book

Der genaue Name der Supabase-Cookies enthält die Kennung unseres Supabase-Projekts; daher steht hier „…“.

Hell-Dunkel-Darstellung: Die Anwendung übernimmt die Einstellung Ihres Systems. Wenn Sie die Darstellung umschalten, merkt sich Ihr Browser die Wahl im lokalen Speicher (localStorage) unter dem Schlüssel „theme“. Dieser Wert verlässt Ihren Browser nicht. Auf Buchungsseiten ist die Darstellung fest hell; dort wird nichts gespeichert.

Nach unserer Einschätzung sind alle genannten Cookies und der lokale Speicher für den von Ihnen gewünschten Dienst unbedingt erforderlich (§ 25 Abs. 2 Nr. 2 TDDDG). Eine Einwilligung und ein Cookie-Banner sind daher nicht vorgesehen. Die Verarbeitung der mit diesen Cookies verbundenen Daten (Sitzungsprüfung, Geräte-Hash) beruht auf Art. 6 Abs. 1 lit. f DSGVO in Verbindung mit Art. 32 DSGVO (Abschnitt 4.8); für die Buchungssitzung gilt Abschnitt 10. ***[bitte klären: diese Einschätzung und die Rechtsgrundlage juristisch prüfen, insbesondere für das 90-Tage-Cookie zoryvo_device und die Speicherung der Darstellung.]***

6. System-Mails und Benachrichtigungen

[bitte klären: Brevo ist noch nicht eingerichtet (kein Konto, keine Absenderdomain, kein SMTP-Block für Supabase Auth; docs/GO-LIVE-CHECKLIST.md Aufgabe 15). Dieser Abschnitt beschreibt den geplanten Produktionsbetrieb und darf erst nach Einrichtung und Beleg veröffentlicht werden; bis dahin versendet Supabase Auth die Passwort-Mails selbst.]

System-Mails versenden wir über den Dienstleister Brevo (Frankreich, Server in der EU). Sie gehen nie über ein Postfach eines Kunden.

Mails zum Zurücksetzen des Passworts versendet unser Anmeldedienst Supabase Auth über Brevo. Sie enthalten nur den Link mit einem einmal verwendbaren, kurz gültigen Token. Das Öffnen solcher Links ist je IP-Adresse begrenzt. Ungültige oder abgelaufene Links führen mit einem Hinweis zur Anmeldeseite und werden nicht als technischer Fehler gemeldet. Die Antwort auf eine Anfrage zum Zurücksetzen ist für bekannte und unbekannte Adressen gleich.

Unsere eigenen Mails versendet ZORYVO über die Brevo-Schnittstelle:

- Einladung: Anrede ohne Namen, Name des Kundenkontos, Rolle, Link mit Einmal-Token, Ablaufdatum.

- Benachrichtigungen: Zahl und Art der Meldungen, gegebenenfalls Name des Postfachs, Name des Kundenkontos und ein Link in die Anwendung. Nie Betreffe, Namen, Titel oder Beträge.
- Support-Hinweis: Mitteilung an die Owner-Nutzer, wenn der Plattform-Admin unter einer Support-Freigabe Debug-Inhalte angesehen hat (Abschnitt 8.6).
- Hinweis „Neuer Termin gebucht“ an den Gastgeber eines Termins, ohne den Namen des Buchenden (Abschnitt 10).

Zu Registrierung, Testphase, Zahlung und Vertrag gehören weitere Mails, die für den Vertrag nötig sind und sich nicht abschalten lassen:

- Registrierung: Bestätigungslink (24 Stunden gültig), die Mail „Sie haben bereits ein Konto“, die Vertragsbestätigung mit PDF-Anhängen und die Willkommensmail mit den ersten Schritten (Abschnitte 4.9 und 4.10).
- Testphase und Vertrag: Erinnerung vor dem Ende der Testphase, Hinweis auf das Ende und auf die Löschung, Erinnerungen vor der Löschung, Bestätigung einer Kündigung, Hinweis auf das Ende des Vertrags (Abschnitte 4.9 und 4.12).
- Zahlung: Hinweis bei fehlgeschlagener Zahlung mit Link ins Kundenportal, Hinweis bei Pause und Wiederaufnahme des Kundenkontos (Abschnitt 4.12).
- Änderung der AGB: Ankündigung einer neuen Fassung mit Link und gegebenenfalls Bitte um Zustimmung (Abschnitt 4.10).

An Brevo übermitteln wir je Mail: Absendername „ZORYVO“, Absender- und Antwortadresse, Ihre E-Mail-Adresse, Betreff, HTML- und Textfassung, ein Schlagwort (Tag) für die Mail-Art, zum Beispiel „invitation“ oder „notification“, und gegebenenfalls Anhänge (bei der Vertragsbestätigung die PDF-Dateien mit AGB, AVV und Datenschutzerklärung). Unsere Vorlagen enthalten keine Bilder, keine Schriften aus dem Netz und keine Zählpixel. ***[bitte klären: ob die Öffnungs- und Klickverfolgung im Brevo-Konto abgeschaltet ist und wie lange Brevo Versandprotokolle (Empfängeradresse, Betreff) aufbewahrt. Ohne Abschaltung müsste die Verfolgung hier genannt werden.]***

Benachrichtigungen in der Anwendung und per E-Mail richten Sie selbst ein: Arten, Kanäle, Ruhezeiten und Tagesbündel. Benachrichtigungs-Mails gehen nur an aktuelle Mitglieder eines Kunden, höchstens 10 je Stunde; dringende Meldungen sofort, andere gebündelt in der Zeitzone des Kunden. Ihre Benachrichtigungen, Einstellungen und Zustellungen sind Ihre persönlichen Daten: Weder der Kunde noch der Plattform-Admin können sie lesen, auch nicht mit Support-Freigabe. Benachrichtigungen und Zustellungen werden nach 90 Tagen gelöscht. Ihre Einstellungen bleiben bestehen, bis Sie sie ändern; automatisch gelöscht werden sie nicht.

Telegram-Bot für Nutzer (freiwillig). Ein Nutzer kann in den Einstellungen seinen privaten Telegram-Chat mit dem ZORYVO-Bot („KI-Assistent“) verbinden, um Fragen zu stellen. Die Verbindung entsteht nur über einen einmaligen Code aus der Anwendung (zehn Minuten gültig, einmal verwendbar, bei uns nur als Hash gespeichert) und ist jederzeit in der Anwendung oder mit /stop im Chat trennbar; ohne die Verbindung erhält Telegram nichts von ZORYVO. Wir speichern die Telegram-Nutzer-Kennung und die Chat-Kennung des Nutzers, den Zeitpunkt der Verbindung und der letzten Nutzung und, wenn der Nutzer sie festlegt, einen Hash seiner PIN (Argon2id, nie die PIN selbst; nach fünf Fehlversuchen sind Aktionen mit PIN gesperrt, bis der Nutzer in der Anwendung mit Zwei-Faktor-Anmeldung eine neue PIN festlegt). Der Bot handelt nur mit den Rechten des verbundenen Nutzers und kennt keine Rechte, die dieser in der Anwendung nicht hat. Seine Antworten enthalten nur Zahlen je Art (zum Beispiel „2 Kontakte, 1 Mail“) und Links in die Anwendung, keine Namen, Betreffe, Beträge oder Mailinhalte von Kontakten oder Kunden. Ist ein Nutzer mehreren Kundenkonten zugeordnet, nennt der Kopf der Antwort den Namen des gewählten Kundenkontos. Was der Nutzer selbst in den Chat schreibt (seine Frage, seine PIN-Eingabe), liegt bei Telegram; die PIN-Nachricht löscht der Bot sofort, speichert und protokolliert sie nie. Der Bot beantwortet derzeit Fragen und löst auf Wunsch mit PIN die Notbremse des eigenen Kundenkontos aus;

Freigaben und Dateien über Telegram bietet er nicht an.**Benachrichtigungen über Telegram (Kanal, freiwillig, Vorgabe aus):**Hat ein Nutzer den Bot verbunden, kann er in den Einstellungen unter Benachrichtigungen je Art einzeln einschalten, dass ZORYVO ihm eine Nachricht an seinen verbundenen Chat schickt; ohne diese Wahl sendet ZORYVO nichts. Die Nachricht enthält nur Zahlen je Art (zum Beispiel „3 neue Freigaben“) und einen Link in die Anwendung, nie Namen, Betreffe, Beträge, Postfachnamen oder Auszüge, auch nicht den Namen des Kundenkontos; sie geht nur in den Chat des Kundenkontos, das der Nutzer im Bot gewählt hat. Ruhezeiten, Bündelung (sofort, stündlich, täglich) und das Stundenlimit gelten wie bei E-Mails; dringende Meldungen gehen auch in den Ruhezeiten. Wir speichern dafür die Wahl je Art und den Versandstatus der Nachricht (Zeitpunkt, Fehlercode, nie den Text) wie bei E-Mail-Benachrichtigungen (Abschnitt 7). Telegram sitzt außerhalb der EU, schließt keinen Auftragsverarbeitungsvertrag und ist eigener Verantwortlicher (Abschnitt 12). Rechtsgrundlage ist die Einwilligung des Nutzers durch die aktive Verbindung (Art. 6 Abs. 1 lit. a DSGVO), die er jederzeit widerrufen kann. ***[bitte klären: ob für die Übermittlung an Telegram außerhalb der EU die Einwilligung des Nutzers genügt (Art. 49 Abs. 1 lit. a DSGVO), ob der Kunde als Arbeitgeber die Nutzung durch seine Mitarbeiter erlauben oder untersagen muss, ob der Name des Kundenkontos im Kopf der Antwort bei mehreren Kundenkonten zulässig ist, ob Telegram eine Auftragsverarbeitung anbietet, ob die Einwilligung des Nutzers durch das ausdrückliche Einschalten je Art der Benachrichtigung über Telegram (Art. 6 Abs. 1 lit. a DSGVO) die Übermittlung der Zahlen und Links an Telegram außerhalb der EU trägt und wie lange der Telegram-Verlauf des Nutzers bei Telegram bleibt.]***

Rechtsgrundlage für Einladung und Passwort-Reset ist bei Owner-Nutzern Art. 6 Abs. 1 lit. b DSGVO und bei Mitarbeitern Art. 6 Abs. 1 lit. f DSGVO (Bereitstellung und Schutz des Kontos). Rechtsgrundlage für die Mails zu Registrierung, Testphase, Zahlung und Änderung der AGB ist Art. 6 Abs. 1 lit. b DSGVO (Durchführung des Vertrags). Rechtsgrundlage für Benachrichtigungen ist Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse und das des Kunden ist es, Sie über Vorgänge in den Postfächern und Bereichen zu informieren, die Sie betreuen; Arten und Kanäle (In-App, E-Mail und, wenn Sie den Telegram-Bot verbunden haben, Telegram, Abschnitt 6) legen Sie selbst fest***[bitte klären: Rechtsgrundlage juristisch bestätigen; Vorschlag ohne Rechtsprüfung.]***

7. Fehlerberichte, Überwachung, Alarme

7.1 Fehlerberichte (Sentry)

Technische Fehler melden wir an Sentry in dessen EU-Datenregion ***[bitte klären: Standort der EU-Region laut Sentry-Dokumentation nachtragen]***; die Anwendung startet nicht, wenn eine andere Region eingestellt ist. Ein Fehlerbericht enthält: Ablaufkennung, Fehlernummer, Verarbeitungsschritt, gegebenenfalls Kennung des Kunden, Fehlerklasse und Fehlertext. Vor dem Senden bereinigen wir den Bericht: Die Anfrage wird auf Methode und Adresse ohne Parameter gekürzt, das Nutzerobjekt auf die Kennung reduziert, Zusatzdaten werden gelöscht. Fehlertexte kürzen wir auf 2.000 Zeichen; Darin ersetzen wir E-Mail-Adressen durch „[email]“, entfernen Parameter aus Adressen und maskieren Einmal-Tokens in Pfaden. Fehlertexte technischer Bibliotheken können dennoch vereinzelt Inhalte wie Namen enthalten. Sentry erhält keine Aufzeichnung Ihrer Sitzung (kein Session Replay). Die Stichprobe für Leistungsdaten liegt in Produktion bei 10 %.

Im Browser ist Sentry auf den Seiten der Anwendung aktiv, einschließlich Startseite, Kontaktformular, Anmelde- und Rechtsseiten, nicht auf Buchungsseiten. Browser-Berichte gehen über unseren eigenen Server an Sentry; Ihr Browser verbindet sich nicht mit Sentry.

Konto- und Organisationsdaten unseres Sentry-Kontos liegen in den USA; das betrifft nur Beschäftigte von ZORYVO Technologies, nicht Sie.***[bitte klären: Aufbewahrungsdauer der Sentry-Ereignisse in der EU-Region; Standard laut Anbieter 90 Tage, nicht belegt.]***

7.2 Eigene Protokolle und Fehlerliste

Jeder technische Ablauf erhält eine Ablaufkennung. Daraus leiten wir eine sechsstellige Fehlernummer ab, die Sie bei technischen Fehlern sehen und die der Plattform-Admin suchen kann. Je Verarbeitungsschritt speichern wir Kennungen, Schrittname, Status, Dauer, Anbieter, HTTP-Status, Fehlercode, Versuchsnummer und KI-Modell, nie Inhalte. Gruppierte Fehler stehen in einer Fehlerliste mit Fehlerart, Stufe, Zeiten, Zählern und Bestätigung.

Fehlerdetails (Name, Meldung, Stack) und bei fehlgeschlagenen Schritten Anfrage und Antwort speichern wir nur verschlüsselt (AES-GCM mit eigenem Schlüsselring), nach Entfernen von Geheimnissen, mit einem Ablaufdatum von 14 Tagen. Nach Ablauf sind sie nicht mehr lesbar. Ein Löschlauf, der sie physisch entfernt, läuft derzeit nicht. Der Plattform-Admin sieht diese Debug-Inhalte eines Kunden nur mit gültiger Support-Freigabe (Abschnitt 8.6).

7.3 Verfügbarkeitsprüfung (healthchecks.io)

Ein Prüfjob ruft alle 5 Minuten die Statusseite der Anwendung auf und meldet den Erfolg an healthchecks.io (Betreiber in Lettland, Server in Deutschland). Übertragen wird nur der Zeitpunkt des Aufrufs: kein Inhalt, keine Kennungen, keine Daten von Nutzern. Bleiben die Meldungen aus, alarmiert healthchecks.io den Betreiber. ***[bitte klären: healthchecks.io ist noch nicht eingerichtet (kein Konto, keine Ping-Adressen; docs/GO-LIVE-CHECKLIST.md Aufgabe 13); vor Veröffentlichung belegen oder Abschnitt streichen.]***

7.4 Alarme an den Betreiber (Telegram und E-Mail)

Schwere Fehler melden wir an die Plattform-Admins per E-Mail (über Brevo) und per Telegram-Bot. ***[bitte klären: Der E-Mail-Kanal setzt Brevo voraus und fehlt bis zu dessen Einrichtung; bis dahin laufen Alarme nur über Telegram.]*** Ein Alarm enthält: Stufe, festen Fehlertitel, den betroffenen Kunden, Automation, Fehlerart, Zeiten, Zähler, Fehlernummer und einen Link in den Admin-Bereich. Den Kunden nennt die E-Mail mit Firmenname und gekürzter Kennung; per Telegram steht nur die gekürzte Kennung (die letzten 8 Zeichen der internen Kennung des Kundenkontos, ein zufällig erzeugter Teil, den Telegram ohne Zugang zu ZORYVO keinem Kunden zuordnen kann), kein Firmenname, auch nicht in der Rückfrage zur Notbremse. Nie enthalten sind Fehlermeldungen, Betreffe, Absender, Kontaktnamen oder Namen und Adressen von Nutzern. Eine neue Anfrage aus dem Kontaktformular (Abschnitt 11) meldet ZORYVO per Telegram nur mit dem Text „Neue Kontaktanfrage“, der Uhrzeit und einem Link, ohne Angaben aus dem Formular, höchstens einmal je 15 Minuten. Eine neue Registrierung (Abschnitt 4.9) meldet ZORYVO ebenso nur mit dem Text „Neue Registrierung“, der Uhrzeit und einem Link, ohne Angaben aus der Registrierung (kein Firmenname, keine Anschrift, keine E-Mail-Adresse), höchstens einmal je 15 Minuten. Telegram sitzt außerhalb der EU und schließt keinen Auftragsverarbeitungsvertrag. Drückt ein Plattform-Admin einen Knopf im Alarm, wird seine Telegram-Nutzer-Kennung im Audit-Protokoll festgehalten; das Ereignis, das den Knopfdruck verarbeitet, trägt im Job-Dienst Inngest zusätzlich die Chat-Kennung. Das betrifft nur Beschäftigte von ZORYVO Technologies ***[bitte klären: ob der Firmenname eines Kunden (zum Beispiel bei Einzelunternehmern) als personenbezogenes Datum gilt (seit 2026-10-10 steht er nur noch in der Alarm-Mail über Brevo) und wie Telegram ohne Auftragsverarbeitungsvertrag zu bewerten ist, auch für die gekürzte Kennung; ob Beschäftigte des Betreibers hier oder gesondert informiert werden.]***

Rechtsgrundlage für Abschnitt 7 ist Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse ist es, Fehler zu erkennen, zu beheben und die Sicherheit der Anwendung zu gewährleisten (Art. 32 DSGVO). ***[bitte klären: Rechtsgrundlage juristisch bestätigen; Vorschlag ohne Rechtsprüfung.]***

8. Verarbeitung im Auftrag unserer Kunden

In diesem Abschnitt ist der jeweilige Kunde Verantwortlicher. Wir handeln nach seinen Weisungen. Weisungen sind der Vertrag und die Einstellungen, die der Kunde in ZORYVO trifft.

8.1 Postfächer

Verbindet der Kunde ein Postfach (Google Workspace oder Microsoft 365), ruft ZORYVO Mails ab und speichert je Mail die Metadaten (Absender, Empfänger, Kopie, Antwortadresse, Betreff, Zeitpunkte, Labels oder Kategorien) und den Text. Das HTML der Mail wird in Text umgewandelt und nicht gespeichert; versteckter Text wird entfernt; Texte werden bei 100.000 Zeichen abgeschnitten. Anhänge werden zunächst nur als Dateiname, Typ und Größe erfasst und nur geladen, wenn eine Funktion sie braucht (Rechnungen erfassen, Anhänge ablegen). Bei Gmail werden alle Mails außer Entwürfen, Spam, Papierkorb und Chat übernommen; bei Microsoft nur Posteingang und Gesendete Elemente. Der Kunde wählt beim Verbinden, wie viele Tage alte Mails importiert werden (0, 30, 90 oder 365 Tage). Ohne KI bestimmt ZORYVO aus den Kopfzeilen, ob der Absender vom Mailserver bestätigt ist und ob es sich um eine automatische Mail oder einen Newsletter handelt.

Ein persönliches Postfach eines Mitarbeiters verbindet nur dieser Mitarbeiter selbst. Es ist zunächst nur für ihn sichtbar, und nur er kann es für andere freigeben. Geteilte Postfächer verbindet der Kunde. Welche Personen ein geteiltes Postfach lesen, Entwürfe daraus freigeben, senden oder verwalten dürfen, legt der Kunde fest.

8.2 Kalender, Dateien, Kundendatenbank

Im Kalender liest ZORYVO freie und belegte Zeiten und legt Termine an, ändert oder sagt sie ab. Geändert oder abgesagt werden nur Termine, die ZORYVO selbst angelegt hat. In Google Drive sieht und schreibt ZORYVO nur Ordner und Dateien, die es selbst angelegt hat. Bei Microsoft umfasst die erteilte Berechtigung das ganze OneDrive des verbundenen Kontos. Hochgeladene Dateien liegen in einem privaten Dateispeicher bei Supabase.

Für den Virenscan ist ein von uns betriebener Server mit ClamAV vorgesehen. Jede hochgeladene Datei und jeder geladene Anhang wird ohne Dateinamen dorthin übertragen und dort nicht gespeichert. Nur Dateien mit gespeichertem Urteil „sauber“ legt ZORYVO in Google Drive oder OneDrive ab. Derzeit ist der Scanner nicht eingerichtet: Es findet kein Virenscan statt, und ZORYVO legt keine Dateien in Google Drive oder OneDrive ab. ***[bitte klären: Server, Vertrag mit Hetzner und Standort (Deutschland oder Finnland) vor Veröffentlichung einrichten und belegen; danach den Satz „Derzeit …“ streichen.]***

Die Kundendatenbank enthält Kontakte, Firmen, Leads, Notizen, Aufgaben, Vorgänge, Termine, Rechnungsdaten (auch IBAN) und ein geschäftliches Gedächtnis je Kontakt mit Quellenangabe.

8.3 KI-Analyse

Die KI ist je Kunde standardmäßig ausgeschaltet. Der Kunde kann sie nur einschalten, wenn er zuvor in ZORYVO die Rechtsgrundlage dokumentiert (Vertrag, berechtigtes Interesse oder Einwilligung, mit Begründung, Zeitpunkt und dokumentierender Person).

[bitte klären: Die KI-Anbieter sind noch nicht eingerichtet (kein Vertex-Projekt, kein Mistral-Konto, keine Umgebungswerte; docs/GO-LIVE-CHECKLIST.md Aufgaben 16 und 17). Ohne eingerichteten Anbieter wird keine Mail analysiert. Die folgenden Angaben beschreiben das im Code festgelegte Verhalten und sind vor Veröffentlichung gegen die tatsächliche Einrichtung zu prüfen (Region, Modell, Verträge).]

Primärer Anbieter ist Google Vertex AI (Gemini) mit einem festen Endpunkt in einer EU-Region; die Anwendung lässt nur EU-Standorte zu. Ausweichanbieter ist Mistral über den EU-Server api.eu.mistral.ai. Der Kunde kann den Ausweichanbieter ausschließen. Der Ausweichanbieter wird nur genutzt, wenn der

primäre Anbieter ausfällt, und darf nie mehr automatisch ausführen als der primäre.

An die Analyse gehen je Mail: Richtung, Adresse des Postfachs, Datum, Kategorienliste des Kunden, Absenderkategorien, Absender, Empfänger, Betreff, Dateinamen und Typen der Anhänge (nicht deren Inhalt) und der Mailtext bis 20.000 Zeichen. Für Antwortentwürfe gehen zusätzlich bis zu 5 frühere Nachrichten des Verlaufs, der Kundenkontext (Anrede, Titel, Name, Firma, Position, Status, Kundennummer, Gedächtnis, vom Kunden freigegebene Felder, Zusammenfassungen oder ersatzweise Betreffe von höchstens 10 Mails), Firmenwissen und Antwort-Bausteine. Telefonnummer, Adresse und Einwilligungen bleiben verborgen. Für Dokumente und Rechnungen gehen die Dateien selbst (PDF, JPEG, PNG, bei Vertex AI auch HEIC) an den Anbieter.

Für das Firmenwissen (Texte und Dateien, die der Kunde unter „Firmenwissen“ einfügt oder hochlädt) erzeugt Google Vertex AI Einbettungen: Zahlenreihen, die den Inhalt eines Abschnitts beschreiben und die Suche nach passenden Abschnitten möglich machen. Dafür gehen die Abschnitte an den Anbieter, bei einem Antwortentwurf zusätzlich eine Suchanfrage aus dem Betreff und den ersten rund 500 Zeichen der Mail. Die Einbettungen entstehen nur in einer regionalen EU-Region, nur bei eingeschalteter KI des Kunden und werden nicht an den Ausweichanbieter gegeben; ohne sie sucht ZORYVO nur im Volltext. Die Einbettungen entstehen für jedes Dokument des Firmenwissens, auch für eines, das nur der Owner-Nutzer sieht oder das nicht „für Antworten verwenden“ eingestellt ist; ein solches Dokument wird nie in einen Antwortentwurf übernommen, aber für die Suche vorbereitet und bei der Widerspruchsprüfung gelesen (Entscheidung des Nutzers vom 2026-10-24: Aufnahme in diese Erklärung statt Ausnahme von der KI). Die gefundenen Abschnitte (höchstens acht) gehen mit dem Entwurf an die KI. ***[bitte klären: Einbettungen als zusätzliche Verarbeitung durch Google Vertex AI in Verzeichnis, Auftragsverarbeitungsvertrag und diese Erklärung gleichlautend aufnehmen; Region und Modell (gemini-embedding-001) sowie den Ausschluss vom Training dafür belegen; ob die Suchanfrage aus dem Mailanfang eine eigene Rechtsgrundlage-Aussage braucht.]*** Auf Wunsch des Kunden liest die KI die Abschnitte außerdem, um Kernaussagen vorzuschlagen (Preise, Zeiten, Ansprechpartner, Fristen) und um Widersprüche zwischen zwei Quellen zu finden; dafür gehen Abschnitte (je Aufruf rund 18.000 Zeichen oder zwei Abschnitte) an das Textmodell. Der Kunde bestätigt die Aussagen und entscheidet über Widersprüche; die KI entscheidet nichts allein. ***[bitte klären: ob die Aussage „Auswertung von Dokumenten des Kunden durch das Textmodell“ im Verzeichnis, im Auftragsverarbeitungsvertrag und hier gleichlautend steht.]*** Die Seite „ZORYVO fragen“ sucht nur in den Daten, die die fragende Person lesen darf, und zeigt Links. Bei Mails sucht sie auch im Mailtext der Mails, die die Person lesen darf (Postfächer und Kategorien wie im Posteingang); das ist eine Volltextsuche in der Datenbank von ZORYVO mit einem Index über den Mailtext, ohne KI und ohne weiteren Empfänger. Zu einer Mail, die über ihren Text gefunden wurde, zeigt die Seite der fragenden Person einen kurzen Auszug (höchstens rund 240 Zeichen); er wird nicht gespeichert und geht nicht an die KI. Nur wenn die Person „Kurzantwort mit KI“ wählt und die KI des Kunden eingeschaltet ist, gehen die Fundstellen dieser einen Suche (Titel, bei Kontakten und Leads Firma und E-Mail-Adresse, bei Mails Betreff, Absender und Datum, bei Rechnungen Aussteller, Rechnungsnummer, Status und Datum, bei abgelegten Dateien Dateiname und Ordnerpfad, bei Terminen Terminart, Name der Kundschaft und Uhrzeit, bei Aufgaben der Termin, bei Firmenwissen die gefundenen Abschnitte, jeweils höchstens 800 Zeichen, höchstens acht Quellen) zusammen mit der Frage an das Textmodell; die Antwort wird nicht gespeichert und zählt zu den KI-Aufrufen des Kunden. ***[bitte klären: ob die Fundstellen aus Kontakten, Leads, Rechnungen, abgelegten Dateien und Terminen (Namen, E-Mail-Adressen, Aussteller, Dateinamen, Ordnerpfade) in Verzeichnis und Auftragsverarbeitungsvertrag als Verarbeitung durch das Textmodell aufzunehmen sind.][bitte klären: ob Auszüge aus dem Mailtext in die „Kurzantwort mit KI“ aufgenommen werden dürfen. Der Mailtext enthält oft Daten Dritter, die Analyse der Mails ist beschrieben, die Frage einer Person an den Assistenten ist ein anderer Zweck. Bis zur Klärung gehen bei Mails weiter nur Betreff, Absender und Datum an die KI, der Auszug nicht; ob der Index über den Mailtext im Verzeichnis der Verarbeitungstätigkeiten genannt werden muss.]***

Kein Verlauf des Assistenten: ZORYVO speichert die Fragen an „ZORYVO fragen“ und die Antworten der

„Kurzantwort mit KI“ nicht. Es gibt keinen Verlauf der Fragen und keine Auswertung oder Liste „Fragen je Mitarbeiter“.

Nicht automatisch analysiert werden: Mails, die der Kunde per Regel ausschließt (zum Beispiel ein Postfach oder ein Label); eingehende automatische Mails und Newsletter, sofern keine Regel des Kunden sie zulässt (Mails aus vom Kunden hinterlegten Webformularen werden analysiert); Mails von Absendern der Kategorien Privat und Personal/Bewerber nach einer Schutz-Vorgabe, die als Regel nur ein Owner-Nutzer mit ausdrücklicher Bestätigung lockern kann.

Eine Person mit dem Recht „Freigeben“ oder „Verwalten“ für das Postfach kann eine solche Mail einzeln mit „Analysieren“ dennoch analysieren lassen. Das gilt auch für die Kategorien Privat und Personal/Bewerber. Die Anforderung wird mit Person und Zeitpunkt im Protokoll festgehalten. Ist die KI ausgeschaltet, findet auch dann keine Analyse statt. Mails gesperrter Kontakte (Einschränkung der Verarbeitung) werden nie analysiert, auch nicht auf Anforderung.

Importierte alte Mails lösen nie Aktionen aus; für sie gibt es höchstens Vorschläge. Die KI ist angewiesen, Anweisungen aus Mails nie zu befolgen und besondere Kategorien personenbezogener Daten (Gesundheit, Religion, politische Meinung, Gewerkschaft, sexuelle Orientierung, ethnische Herkunft, Vorstrafen) sowie Privates nicht in das Gedächtnis zu schreiben. Das ist eine Anweisung an das Modell, kein deterministischer Filter.

Gespeichert werden zur Analyse Anbieter, Modell, Versuche, Token-Zahlen, Dauer, Kategorie, Zusammenfassung, strukturierte Ausgabe und die Rohantwort. Ob die KI-Anbieter übermittelte Daten zum Training ihrer Modelle verwenden, hängt von Vertragseinstellungen ab, die wir vor dem ersten Einsatz treffen. ***[bitte klären: Beleg für Training-Ausschluss, Datenresidenz und Caching bei Vertex AI sowie Training-Opt-out und Zero-Data-Retention bei Mistral (Standard dort: Training an, Aufbewahrung 30 Tage). Ohne Beleg keine Zusage „kein Training“.]***

8.4 Keine automatisierten Entscheidungen mit Rechtswirkung

ZORYVO trifft keine Entscheidungen, die gegenüber einer Person rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (Art. 22 DSGVO). Die KI sortiert, fasst zusammen, erkennt Aufgaben und entwirft. Antwortentwürfe werden von einer Person freigegeben; der automatische Versand von KI-Antworten ist im Code gesperrt. Von der KI aus Rechnungsdateien (PDF, Bilder) gelesene Werte werden nie ohne Prüfung durch eine Person abgelegt; ZORYVO bezahlt keine Rechnungen.

Vor jeder Aktion nach außen prüfen feste Tore Sicherheitsregeln. Vor dem Versand sind das unter anderem Notbremse, importierte Mail, unbestätigter Absender, automatische Mail, Zahlungsthemen und „bereits beantwortet“. Vor der Ablage von Rechnungen und Anhängen sind das unter anderem Notbremse, importierte Mail und die Warnung bei geänderter Bankverbindung. Nach den Schutz-Vorgaben erhalten Behörden, Gerichte, Sozialversicherung, Banken, Versicherungen und Berater keine automatische Antwort; ein Owner-Nutzer kann eine Schutz-Vorgabe nur mit ausdrücklicher Bestätigung lockern, was protokolliert wird. Keine Automation überschreibt, was eine Person von Hand gesetzt hat.

Jede fachliche Änderung wird mit altem und neuem Wert, handelnder Person oder Automation und Begründung protokolliert. Änderungen an Kontakten und Firmen lassen sich je Feld rückgängig machen, Übernahmen aus Dateien je Datei. Ein allgemeines Rückgängig für alle Änderungen gibt es derzeit nicht.

8.5 Kennzeichnung gesendeter Mails

Jede Mail mit KI-Text trägt die Kopfzeilen X-ZORYVO-AI-Generated mit dem Wert „assisted“ und X-ZORYVO-AI-Model (Anbieter und Modell). KI-Antworten gehen derzeit nur nach Freigabe durch eine Person hinaus (Abschnitt 8.4). Am Ende der Mail steht ein sichtbarer Hinweis, in der Vorgabe: „Diese Nachricht wurde mit Unterstützung eines KI-Systems erstellt.“ Der Hinweis ist vorgegeben und nur von der Rolle Owner abschaltbar. Automatisch versendete Vorlagen-Mails ohne KI-Text, zum Beispiel Erinnerungen, tragen keine KI-Kopfzeilen, aber die Kopfzeile Auto-Submitted: auto-replied. Gesendete

Mails gehen über das Postfach des Kunden und enthalten keine Bilder und keine Zählelemente.

8.6 Zugriff des Betreibers auf Inhalte

Der Plattform-Admin ist in der Datenbank ein normaler Nutzer. Ohne Freigabe sieht er nur Metadaten: Kunde, Automation, Aufgabentyp, Status, Fehlerart, Fehlernummer, Zeitpunkte, Nutzungs- und Kostenzahlen, Verbindungsstatus, Tarif, Stand der Testphase und des Abonnements sowie Firmendaten und Zustimmungsprotokoll des Kunden, dazu E-Mail-Adresse, Anzeigename, Rolle und Sperrstatus der Nutzer und offene Einladungen (Abschnitt 4.2) sowie Audit-Einträge mit Kennungen, ohne Inhalte. Betreff, Absenderadresse, Kontaktnamen, Beträge, Dateinamen und Entwürfe gelten als Inhalt und sind gesperrt.

Inhalte sieht er nur mit einer Support-Freigabe, die ein Owner-Nutzer des Kunden erteilt: mit Umfang (Debug-Inhalte, ein bestimmtes Objekt oder alle Inhalte), Grund und Dauer (Vorgabe 48 Stunden, höchstens 7 Tage), jederzeit widerrufbar. Persönliche Postfächer von Mitarbeitern kann ein Owner-Nutzer so nicht öffnen. Protokolliert werden Erteilung, Änderung und Widerruf jeder Freigabe sowie jedes Ansehen von Debug-Inhalten. Das Lesen einzelner Mails oder Kontakte unter einer Freigabe wird derzeit nicht je Zugriff protokolliert. Beim ersten Ansehen von Debug-Inhalten je Freigabe erhalten die Owner-Nutzer eine Mail, danach höchstens eine Tageszusammenfassung.

8.7 Rechte der Betroffenen gegenüber dem Kunden

Der Kunde kann je Kontakt eine Auskunft (JSON) erstellen, einen Kontakt sperren und einen Kontakt endgültig löschen. Die Sperrung setzt die Einschränkung der Verarbeitung nach Art. 18 DSGVO um: Mails der Person werden nicht mehr analysiert, der Kontakt fällt aus Automationen, Antwortkontext und Export heraus und ist nur noch für die Rolle Owner sichtbar.

Das endgültige Löschen entfernt den Kontakt, die von ihm gesendeten Mails und die Mails, deren einzige Empfänger seine Adressen sind, samt Analysen, Gedächtnis, Aufgaben, Freigaben, Buchungen, Dateien und Debug-Inhalten. In übrigen Texten, in Mails mit weiteren Beteiligten und in Protokollen schwärzt es E-Mail-Adresse, Name und Telefonnummer in der Schreibweise, die im Kontakt gespeichert ist, jeweils nur als Ganzes (eine längere Adresse oder Nummer, die sie enthält, bleibt unverändert); Nennungen nur mit Vor- oder Nachname oder in anderer Schreibweise werden nicht gefunden, und eine Telefonnummer, die auch ein anderer Kontakt oder eine Firma hat (etwa eine Zentrale), bleibt stehen. Rechnungen und die Dateien, aus denen eine Rechnung erfasst wurde, bleiben bestehen und werden nicht geschwärzt; die Vorschau weist darauf hin. Ob eigene Aufbewahrungspflichten das Behalten rechtfertigen, beurteilt der Kunde als Verantwortlicher. Kopien, die ZORYVO in Google Drive oder OneDrive des Kunden abgelegt hat, werden nicht gelöscht, sondern dem Kunden in der Vorschau aufgelistet, damit er sie selbst löscht. Termine im Kalender des Kunden und die Originale im Postfach des Kunden bleiben unberührt; ZORYVO zeigt diese Termine in der Vorschau nicht an und löscht sie nicht.

9. Nutzung von Google-Nutzerdaten

Dieser Abschnitt beschreibt, wie ZORYVO Daten aus Google-Konten verwendet, die ein Kunde verbindet. Er gilt zusätzlich zu Abschnitt 8.

9.1 Welche Daten und Berechtigungen

ZORYVO fragt nur die Berechtigungen an, die zu den vom Kunden gewählten Fähigkeiten gehören:

Fähigkeit	Google-Berechtigungen (Scopes)	Verwendung
Identität (immer)	openid, userinfo.email, userinfo.profile	verbundenes Konto erkennen und anzeigen

Postfach	gmail.modify	Mails lesen (alle Mails außer Entwürfen, Spam, Papierkorb und Chat, einschließlich der Labels), Entwürfe anlegen und eigene, nicht mehr benötigte Entwürfe wieder entfernen, nach Freigabe senden, Labels setzen; keine endgültige Löschung von Mails. Nur wenn der Kunde „Signatur aus dem Postfach verwenden“ einschaltet (Vorgabe aus), zusätzlich die Signatur der Hauptadresse lesen
Kalender	calendar.events, calendar.freebusy, calendar.calendarlist.readonly	Termine anlegen und ändern, Frei/Belegt lesen, Kalenderliste lesen
Dateien	drive.file	nur Ordner und Dateien, die ZORYVO selbst angelegt hat

Wählt der Nutzer im Google-Dialog Berechtigungen ab, erkennt ZORYVO das und schaltet die Fähigkeit nicht ein. Die Oberfläche zeigt je Verbindung die erteilten Berechtigungen.

Für Gmail-Änderungsmeldungen ist Google Cloud Pub/Sub im Google-Cloud-Projekt des Betreibers vorgesehen. Die Meldung enthält nur die Postfachadresse und eine Änderungsnummer, keine Inhalte. Unabhängig davon fragt ZORYVO alle 30 Minuten selbst nach Änderungen. ***[bitte klären: Region des Pub/Sub-Themas; Pub/Sub ist noch nicht eingerichtet, bis dahin holt ZORYVO Änderungen nur über diese regelmäßige Abfrage.]***

9.2 Wofür wir Google-Nutzerdaten verwenden

Wir verwenden Google-Nutzerdaten ausschließlich, um die Funktionen bereitzustellen, die der Kunde eingeschaltet hat: Mails speichern und analysieren, Antworten entwerfen, nach Freigabe senden, Rechnungen erfassen, Anhänge ablegen, Termine verwalten. Wir verwenden sie nicht für Werbung und verkaufen sie nicht. Eine Ausnahme beschreibt Abschnitt 4.11: Beim Verbinden eines Postfachs lesen wir aus dem Google-Konto die Domain des Google Workspace und prüfen mit ihrem Hash, ob dieses Unternehmen schon eine Testphase hatte. ***[bitte klären: Vereinbarkeit mit der Google API Services User Data Policy (Limited Use); andernfalls das Merkmal nicht erheben.]*** Wir geben sie an Dritte nur weiter, soweit es zur Bereitstellung dieser Funktionen nötig ist, zur Abwehr eines Sicherheitsvorfalls oder weil ein Gesetz es verlangt.

Zur Bereitstellung nötig sind nur diese Auftragsverarbeiter: Vercel (Ausführung der Anwendung in Frankfurt), Supabase (Speicherung in Frankfurt), Google Cloud Pub/Sub (Postfachadresse und Änderungsnummer), Google Vertex AI und ausweichend Mistral (KI-Analyse, nur wenn der Kunde die KI eingeschaltet hat), der von uns betriebene Virenscanner bei Hetzner (Anhänge) sowie Inngest (nur Kennungen und Status) und Sentry (Fehlerberichte mit gekürzten und maskierten Fehlertexten, Abschnitt 7.1). Pub/Sub, die KI-Anbieter und der Virenscanner sind derzeit nicht eingerichtet (Abschnitte 8.2, 8.3 und 9.1).

Menschen bei ZORYVO Technologies lesen Google-Nutzerdaten nur mit einer Support-Freigabe des Kunden (Abschnitt 8.6), wenn es zur Abwehr eines Sicherheitsvorfalls nötig ist oder wenn das Gesetz es verlangt. Wir verwenden Google-Nutzerdaten nicht, um allgemeine KI-Modelle zu trainieren. ***[bitte klären: Beleg Vertex/Mistral zum Training-Ausschluss, siehe Abschnitt 8.3; ohne Beleg Satz anpassen.]***

Die Verwendung der aus Google-APIs erhaltenen Daten durch ZORYVO und ihre Weitergabe an andere Anwendungen richten sich nach der Google API Services User Data Policy einschließlich der Anforderungen zur eingeschränkten Nutzung (Limited Use). ***[bitte klären: Wortlaut vor der Google-Verifizierung gegen die aktuelle Policy prüfen; Link auf die Policy einfügen, sobald die Adresse in docs/SUBPROCESSORS.md (Quellen) steht.]***

9.3 Speicherung und Trennung

Zugriffs- und Erneuerungstoken speichern wir mit AES-256-GCM verschlüsselt, gebunden an Kunde und Verbindung. Die Tabelle mit den Tokens kann nur die Systemrolle unserer Anwendung (Server und

Hintergrundverarbeitung) lesen, kein Nutzerkonto. Der Job-Dienst Inngest erhält keine Tokens, nur Kennungen. Trennt der Kunde die Verbindung, beendet ZORYVO die Änderungsmeldungen, widerruft das Token bei Google und löscht alle Tokens. Bereits in ZORYVO gespeicherte Mails und Dateien bleiben, bis der Kunde sie löscht oder der Vertrag endet (Abschnitt 14).

9.4 Microsoft-Daten

Für Microsoft 365 fragt ZORYVO an: openid, profile, email, offline_access, User.Read (Identität); Mail.ReadWrite, Mail.Send (Postfach); Calendars.ReadWrite (Kalender); Files.ReadWrite (OneDrive, umfasst das ganze OneDrive des Kontos); für geteilte Postfächer zusätzlich Mail.ReadWrite.Shared, Mail.Send.Shared, Calendars.ReadWrite.Shared. Synchronisiert werden nur Posteingang und Gesendete Elemente. Verwendung, Weitergabe und Zugriff gelten wie in Abschnitt 9.2. Beim Trennen löscht ZORYVO die Tokens; einen Widerruf der Berechtigung bei Microsoft kann ZORYVO nicht auslösen. Der Kunde oder sein Microsoft-Administrator entfernt ZORYVO selbst in den Einstellungen seines Microsoft-Kontos.

10. Öffentliche Buchungsseiten und Widget

Kunden können eine öffentliche Buchungsseite und ein einbettbares Widget nutzen. Die Buchungsseiten liegen auf einer eigenen Buchungsadresse unter dem Pfad /book, getrennt von der Adresse der Anwendung. Verantwortlicher für die Daten, die Sie dort eingeben, ist der Kunde, dessen Termin Sie buchen. Sein Impressum und seine Datenschutzerklärung sind im Fuß jeder Buchungsseite verlinkt; ohne diese Links lässt sich keine Buchungsseite aktivieren. Wir verarbeiten die Daten technisch in seinem Auftrag.

Das Formular erhebt: Name und E-Mail-Adresse (Pflicht), Telefonnummer und Anmerkung (freiwillig), bis zu drei Antworten auf Fragen des Kunden (freiwillig, sofern der Kunde sie nicht als Pflicht kennzeichnet), eine Adresse nur bei Terminen vor Ort (dann Pflicht), Ihre Sprache und Zeitzone, die gewählte Zeit und die Lösung der Bot-Prüfung. Nach dem Absenden wird der Termin 30 Minuten reserviert, und Sie erhalten eine Mail mit einem Bestätigungslink. Erst der Klick auf „Termin bestätigen“ bucht den Termin. Unbestätigte Anfragen werden nach 24 Stunden mit allen Angaben gelöscht. Mit der Bestätigung entstehen in der Kundendatenbank des Kunden ein Kontakt und ein Lead (Interessent). Ist Ihre Adresse dort schon als Kontakt erfasst, bleibt dieser unverändert. Sind Sie dort bereits als Kunde oder als Ansprechpartner einer Kundenfirma geführt, entsteht kein Lead. Besteht schon ein offener Lead, entsteht kein zweiter. Im Kalender des Kunden wird ein Termin mit Ihrem Namen, Ihrer E-Mail-Adresse und Ihren Angaben angelegt; die Kalendereinladung sendet der Kalenderanbieter des Kunden. Sie erhalten eine Terminbestätigung mit Kalenderdatei (.ics) sowie Mails bei Verschiebung und Absage. Hat der Kunde es für die Terminart eingestellt, erhalten Sie außerdem eine Erinnerung 24 Stunden vor dem Termin (Vorgabe an) und 1 Stunde vor dem Termin (Vorgabe aus).

Diese Mails gehen über das Postfach, das der Kunde für seine Buchungsseiten gewählt hat, oder bei einer Buchung aus einer Mail-Unterhaltung über das Postfach dieser Unterhaltung. Ist kein solches Postfach festgelegt oder ist es nicht nutzbar (zum Beispiel getrennt oder abgelaufen), versendet Brevo sie mit dem Firmennamen des Kunden als Absender; Brevo erhält dann Ihren Namen, Ihre E-Mail-Adresse und die Termindaten. Brevo ist derzeit nicht eingerichtet (Abschnitt 6). Der Gastgeber erhält einen Hinweis „Neuer Termin gebucht“ ohne Ihren Namen.

Die Bot-Prüfung (Captcha nach dem ALTCHA-Protokoll) läuft vollständig auf unseren Servern und in Ihrem Browser, ohne Drittanbieter und ohne fremdes Skript; sie verarbeitet keine Daten über Sie. Ihre IP-Adresse dient nur Rate-Limits (60 Seitenaufrufe je Minute, 10 Formular-Absendungen je Stunde) und wird nur als SHA-256-Hash gespeichert. Das Cookie zoryvo_book (Abschnitt 5) hält Ihre Buchungssitzung; es gilt nur auf der Buchungsadresse. Die Buchungsseiten setzen kein weiteres Cookie, laden keine fremden Skripte oder Schriften, sind für Suchmaschinen gesperrt (noindex) und senden keinen Referrer. Im Browser läuft dort kein Fehlerberichtsdienst. Das Widget-Skript setzt kein Cookie und

sendet nichts über Sie; es erstellt nur einen Rahmen und übernimmt dessen Höhe. Die Buchungsseite zeigt nur freie Zeitfenster, nie andere Termine des Kunden.

Für diese technischen Schutzmaßnahmen und für die Zugriffsdaten des Hostings (Abschnitt 3) sind wir Verantwortlicher. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse ist der sichere Betrieb der Buchungsseiten und der Schutz vor Missbrauch. ***[bitte klären: Rollenverteilung für die Zugriffsdaten der Buchungsseiten (eigene Verantwortlichkeit oder Auftragsverarbeitung für den Kunden) und Rechtsgrundlage juristisch bestätigen; Vorschlag ohne Rechtsprüfung.]***

Trägt Ihre Adresse beim Kunden das Kennzeichen „Nicht anschreiben“, wird keine Bestätigungsmail gesendet; die Seite zeigt das nicht an. Bei pausiertem Kunden oder ausgelöster Notbremse ist die Online-Buchung nicht möglich.

11. Kontaktformular „Zugang anfragen“

Wenn Sie sich nicht selbst registrieren möchten oder können (zum Beispiel, weil Ihr Unternehmen nicht in Deutschland sitzt) oder Fragen vor der Registrierung haben, können Sie über das Formular unter /kontakt einen Zugang anfragen. Die Selbst-Registrierung beschreibt Abschnitt 4.9. Verantwortlicher ist ZORYVO Technologies (Abschnitt 1).

Das Formular erhebt: Name, Firma, E-Mail-Adresse und Nachricht (Pflicht), Telefonnummer und den Anbieter Ihres Postfachs (Google Workspace, Microsoft 365, anderer Anbieter, weiß nicht; freiwillig) sowie die Lösung der Bot-Prüfung. Wir verwenden die Angaben nur, um Ihre Anfrage zu beantworten. Wir antworten persönlich per E-Mail oder Telefon; ZORYVO sendet keine automatische Bestätigung.

Die Anfrage liegt in unserer Datenbank bei Supabase in Frankfurt (Abschnitt 3). Lesen kann sie nur der Plattform-Admin von ZORYVO Technologies. Eine neue Anfrage meldet ZORYVO dem Betreiber per Telegram nur mit dem Text „Neue Kontaktanfrage“, der Uhrzeit und einem Link in den Admin-Bereich, ohne Ihre Angaben (Abschnitt 7.4). Die Bot-Prüfung (Captcha nach dem ALTCHA-Protokoll) läuft wie auf den Buchungsseiten nur auf unseren Servern und in Ihrem Browser (Abschnitt 10). Ihre IP-Adresse dient nur einem Rate-Limit (5 Absendungen je Stunde) und wird nur als SHA-256-Hash gespeichert (Abschnitt 4.5). Ein für Menschen unsichtbares Feld erkennt Programme, die jedes Feld ausfüllen; solche Absendungen speichern wir nicht.

Wir löschen die Anfrage 180 Tage nach Eingang automatisch. Anfragen können wir auch früher von Hand löschen, etwa wenn sie erledigt sind oder Sie die Löschung verlangen. Wird aus der Anfrage ein Vertrag, übernehmen wir die nötigen Angaben in die Vertragsunterlagen. ***[bitte klären: Speicherdauer von 180 Tagen bestätigen; ob Anfragen, aus denen ein Vertrag wird, länger aufzubewahren sind (Handels- und Steuerrecht) und ob das hier zu nennen ist.]***

Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO (Anbahnung eines Vertrags auf Ihre Anfrage); fragen Sie für ein Unternehmen an, dessen Vertreter oder Beschäftigter Sie sind, Art. 6 Abs. 1 lit. f DSGVO, unser berechtigtes Interesse ist die Beantwortung Ihrer Anfrage. Für Bot-Prüfung und Rate-Limit gilt Art. 6 Abs. 1 lit. f DSGVO (Schutz vor Missbrauch). ***[bitte klären: Rechtsgrundlage juristisch bestätigen (lit. b oder lit. f bei Anfragen für ein Unternehmen); Vorschlag ohne Rechtsprüfung.]***

12. Empfänger und Unterauftragsverarbeiter

Die folgenden Dienste erhalten Daten von uns. Supabase, Vercel, Inngest, Google Vertex AI, Mistral, Brevo, Hetzner, Sentry und Google Cloud Pub/Sub sind für Kundendaten (Abschnitt 8) unsere Unterauftragsverarbeiter nach Art. 28 Abs. 2 DSGVO und in Anlage 3 des Auftragsverarbeitungsvertrags aufgeführt. healthchecks.io und Telegram erhalten keine Inhalte unserer Kunden und, außer beim freiwillig verbundenen Bot (Abschnitt 6), keine Daten der Nutzer unserer Kunden; sie handeln als eigene Verantwortliche ohne Auftragsverarbeitungsvertrag. Die folgenden Dienste erhalten Daten von uns.

Supabase, Vercel, Inngest, Google Vertex AI, Mistral, Brevo, Hetzner, Sentry und Google Cloud Pub/Sub sind für Kundendaten (Abschnitt 8) unsere Unterauftragsverarbeiter nach Art. 28 Abs. 2 DSGVO und in Anlage 3 des Auftragsverarbeitungsvertrags aufgeführt. healthchecks.io, Telegram und VIES erhalten keine Inhalte unserer Kunden und keine Daten der Nutzer unserer Kunden; sie handeln als eigene Verantwortliche ohne Auftragsverarbeitungsvertrag.

Google Vertex AI, Mistral, Brevo, Hetzner, healthchecks.io und Google Cloud Pub/Sub sind derzeit nicht eingerichtet und erhalten heute keine Daten (Abschnitte 6 bis 9).

Dienst	Zweck	Daten	Standort	Datenschutzhinweise
Supabase	Datenbank, Anmeldedienst, Dateispeicher	alle Inhalte und Kontodaten	eu-central-1 Frankfurt	https://supabase.com/legal/dpa
Vercel	Hosting der Anwendung	Rechenleistung, Anfrage-Protokolle, Umgebungswerte	Funktionen in Frankfurt (fra1); Verarbeitungsstandorte des Anbieters in den USA	https://vercel.com/legal/dpa
Inngest	Hintergrundjobs	nur Kennungen und Status (Kunde, Objekt, Ablauf, Fehler); bei Alarm-Knöpfen Telegram-Kennungen des Admins; keine Inhalte	AWS, Region vom Anbieter nicht angegeben	https://www.inngest.com/privacy
Google Vertex AI	KI-Analyse (primär), Einbettungen für die Suche im Firmenwissen	Mailinhalte, Dokumente, Bilder, Kundenkontext, Abschnitte des Firmenwissens, Suchanfragen aus Betreff und Mailanfang; nur bei eingeschalteter KI	EU-Region oder EU-Multiregion; Einbettungen in einer regionalen EU-Region	Google Cloud Data Processing Addendum
Mistral	KI-Analyse (Ausweich)	wie Vertex AI; vom Kunden ausschließbar	EU-Server	https://legal.mistral.ai/terms/data-processing-addendum/
Brevo	System-Mails; Buchungsmails, wenn kein nutzbares Absender-Postfach des Kunden festgelegt ist	Empfängeradresse, Betreff, Mailtext; bei Buchungsmails Name und Termin; bei der Vertragsbestätigung PDF-Anhänge	EU (Frankreich, Deutschland, Belgien)	https://help.brevo.com/hc/en-us/articles/360001005510-Data-storage-location
Stripe	Zahlungsabwicklung für die Tarife (Checkout, Kundenportal, Rechnungen)	rechtlicher Name der Firma, Anschrift, Rechnungs-E-Mail-Adresse, USt-IdNr. (falls angegeben), Tarif, Kennung des Kundenkontos; Zahlungsdaten gibt der Kunde direkt bei Stripe ein; keine Inhalte	Stripe Payments Europe, Ltd., Irland; Verarbeitung auch durch die Muttergesellschaft in den USA	https://stripe.com/de/privacy
VIES	Bestätigung der	nur Länderkennzeichen	EU-Kommission,	https://ec.europa.eu/taxation_custom

(EU-Kommission)	USt-IdNr. nach der Registrierung (Abschnitt 4.14)	und Nummer der USt-IdNr.; keine Firmennamen, keine Anschrift, keine Kennung; VIES antwortet auch mit Name und Anschrift zur Nummer, die wir nicht lesen und nicht speichern; eigener Verantwortlicher, kein Auftragsverarbeitungsvertrag	Brüssel; bei der Anfrage keine Übermittlung außerhalb der EU	s/vies/
Hetzner (ClamAV-Server)	Virenscan	Dateiinhalte ohne Dateinamen, nicht gespeichert	Deutschland oder Finnland, noch nicht festgelegt	von uns betriebener Server
Sentry	Fehlerberichte	Fehlerberichte; Fehlertexte gekürzt, E-Mail-Adressen und Tokens maskiert	Ereignisse: EU-Datenregion; Kontodaten des Betreibers: USA	https://sentry.io/legal/dpa/
Google Cloud Pub/Sub	Änderungsmeldungen für verbundene Google-Postfächer	Postfachadresse und Änderungsnummer, keine Inhalte	Region wählbar ***[bitte klären: Region des Pub/Sub-Themas]***	Google Cloud Data Processing Addendum
healthchecks.io	Verfügbarkeitsprüfung	nur Zeitstempel; eigener Verantwortlicher, kein Auftragsverarbeitungsvertrag	Lettland, Server in Deutschland	https://healthchecks.io/privacy/
Telegram	Alarme an den Betreiber; auf Wunsch eines Nutzers Fragen an den Bot (Abschnitt 6)	Alarm-Metadaten (Abschnitt 7.4) und der Hinweis „Neue Kontaktanfrage“ ohne Angaben (Abschnitt 11); beim Bot die Telegram-Kennungen des Nutzers, was er selbst schreibt, und Antworten und auf Wunsch Benachrichtigungen nur mit Zahlen und Links; eigener Verantwortlicher, kein Auftragsverarbeitungsvertrag	außerhalb der EU	https://telegram.org/privacy

Stripe erhält keine Inhalte und keine Kundendaten im Sinne von Abschnitt 8, sondern nur die Abrechnungsdaten des Kunden (Abschnitt 4.12); es ist deshalb nicht in Anlage 3 des Auftragsverarbeitungsvertrags als Unterauftragsverarbeiter aufgeführt. ***[bitte klären: Einordnung von Stripe, siehe Abschnitt 4.12.]***

Google (Gmail, Kalender, Drive) und Microsoft (Postfach, Kalender, OneDrive) sind keine Empfänger von uns. Sie sind Dienste des Kunden, die ZORYVO in dessen Auftrag anspricht.

[bitte klären: Vertragsbelege je Dienst (Supabase-DPA, Vercel-DPA ab Tarif Pro, Brevo-DPA, Sentry-DPA, Stripe-DPA, Hetzner-AVV, Inngest-AVV) liegen beim Betreiber vor? Der AVV mit Inngest

ist Bedingung vor dem ersten Kunden. Die Adresse des Google Cloud Data Processing Addendum (Vertex AI, Pub/Sub) eintragen, sobald sie in docs/SUBPROCESSORS.md (Quellen) steht.]

13. Übermittlung in Drittländer

Inhalte und personenbezogene Daten unserer Kunden und ihrer Kontakte speichern wir nur in der EU. Dienste, die Daten außerhalb der EU verarbeiten, erhalten höchstens Metadaten. Vercel, Google und Sentry haben ihren Sitz in den USA, verarbeiten Inhalte aber in EU-Regionen. Stripe erhält keine Inhalte, nur die Abrechnungsdaten des Kunden (Abschnitt 4.12). Einzelheiten und Übermittlungsgrundlagen:

- Vercel (USA): Die Serverfunktionen laufen in Frankfurt. Anfrage-Protokolle und Sicherungen des Anbieters können in den USA verarbeitet werden. Grundlage sind die Standardvertragsklauseln der EU-Kommission (2021) im Auftragsverarbeitungsvertrag von Vercel. ***[bitte klären: Der Vercel-Vertrag zur Auftragsverarbeitung gilt erst ab Tarif Pro; Buchung und Annahme belegen; Übermittlungsgrundlage juristisch formulieren.]***
- Sentry (USA): Fehlerberichte bleiben in der EU-Region. Konto- und Organisationsdaten unseres Sentry-Kontos liegen in den USA; sie betreffen nur Beschäftigte von ZORYVO Technologies. Grundlage: EU-US Data Privacy Framework, ersatzweise Standardvertragsklauseln.
- Stripe (Irland, Muttergesellschaft in den USA): erhält die Abrechnungsdaten des Kunden (Abschnitt 4.12), keine Inhalte. Grundlage für Übermittlungen in die USA sind nach den Angaben von Stripe das EU-US Data Privacy Framework und Standardvertragsklauseln. ***[bitte klären: Übermittlungsgrundlage und Vertrag mit Stripe belegen, siehe Abschnitt 4.12.]***
- VIES (EU-Kommission): erhält nur das Länderkennzeichen und die Nummer der USt-IdNr. (Abschnitt 4.14); die Anfrage bleibt innerhalb der EU, eine Übermittlung in ein Drittland findet nicht statt.
- Inngest (AWS, Region nicht angegeben): erhält nur Kennungen und Status, keine Inhalte und keine Adressen. ***[bitte klären: Auftragsverarbeitungsvertrag mit Inngest und Region; ohne Vertrag Wechsel auf selbst betriebenes Inngest in der EU.]***
- Google Vertex AI: Verarbeitung an EU-Endpunkten. Google ist ein US-Unternehmen; es gilt das Google Cloud Data Processing Addendum mit Standardvertragsklauseln und Data Privacy Framework. ***[bitte klären: Datenresidenz je Modell und Region belegen.]***
- Google Cloud Pub/Sub: erhält nur Postfachadresse und Änderungsnummer. Grundlage wie bei Vertex AI: Google Cloud Data Processing Addendum mit Standardvertragsklauseln und Data Privacy Framework. ***[bitte klären: Region des Pub/Sub-Themas.]***
- Telegram (außerhalb der EU): erhält Alarme an den Betreiber und den Hinweis auf neue Kontaktanfragen, ohne personenbezogene Daten von Nutzern, Kontakten oder Anfragenden und ohne Firmennamen von Kunden (nur die gekürzte Kennung, Abschnitt 7.4); dazu, nur wenn ein Nutzer den Bot freiwillig verbindet, dessen Telegram-Kennungen, seine Nachrichten an den Bot und die Antworten und Benachrichtigungen (nur wenn er sie je Art einschaltet) mit Zahlen und Links, ohne Namen und Inhalte von Kontakten (Abschnitt 6); Telegram ist eigener Verantwortlicher ohne Auftragsverarbeitungsvertrag. ***[bitte klären: Bewertung, siehe Abschnitt 7.4.]***
- healthchecks.io: EU-Unternehmen, Server in Deutschland; Sicherungen des Anbieters liegen verschlüsselt bei AWS S3 ohne Regionsangabe. Es werden nur Zeitstempel übertragen.

14. Speicherdauer

Wie lange wir Daten heute speichern, zeigt die folgende Übersicht. Wo derzeit keine automatische Löschung läuft, steht das dabei.

Daten	Speicherdauer

Nutzerkonto (Profil, Anmeldekonto bei Supabase Auth)	solange eine Mitgliedschaft bei einem Kunden besteht. Entfernt der Kunde Sie, endet die Mitgliedschaft; Profil und Anmeldekonto bleiben derzeit bestehen, bis wir sie auf Anfrage über {{Datenschutz-Kontakt}} oder beim Vertragsende des Kunden von Hand löschen. Eine Selbstlöschung gibt es nicht
Einladungen	7 Tage gültig; Einladungsdatensätze werden derzeit nicht automatisch gelöscht
Sitzungen	bis zur Abmeldung, zum Beenden durch Kunde oder Admin oder bis zum Ablauf nach {{Sitzungsbegrenzung laut Supabase-Projekteinstellungen}}; bei Plattform-Admins höchstens 8 Stunden ***[bitte klären: ob im Produktionsprojekt eine Sitzungsbegrenzung (Zeitfenster oder Inaktivität) gesetzt ist; ohne Einstellung laufen Sitzungen nicht von selbst ab.]***
Cookie zoryvo_device	Cookie 90 Tage; der Hash in der Datenbank wird 91 Tage nach Beginn seines Fensters nachts automatisch gelöscht (er wirkt nur 90 Tage ab Beginn seines Fensters)
Rate-Limit-Zähler (nur Hashes)	2 Tage nach dem Ende ihres Zeitfensters nachts automatisch gelöscht; ein neues Zeitfenster überschreibt nur den Zählerstand; nach erfolgreicher Anmeldung werden die Konto-Zähler gelöscht
Audit-Protokoll, Aktivitätsprotokoll, Änderungshistorie, Fehlerliste	Aktivitätsprotokoll 180 Tage; Änderungshistorie und Audit-Protokoll 365 Tage; danach nachts automatisch gelöscht, **nur bei eingeschalteter Funktion** (derzeit aus). Einträge zu Löschungen und zum Lebenslauf eines Kundenkontos bleiben im Audit-Protokoll ohne Frist stehen. Die Fehlerliste wird derzeit nicht automatisch gelöscht. Ob und wie die Protokolle bei Vertragsende eines Kunden gelöscht werden, ist noch nicht festgelegt (siehe unten). Beim endgültigen Löschen eines Kontakts werden die Werte zu diesem Kontakt darin geschwärzt ***[bitte klären: Frist und Verfahren festlegen.]***
Verschlüsselte Debug-Inhalte	14 Tage lesbar, danach gesperrt und weitere 16 Tage später (30 Tage nach dem Entstehen) nachts automatisch gelöscht
Benachrichtigungen und Zustellungen	90 Tage
Verbindung zum Telegram-Bot (Kennungen, PIN-Hash, Fehlversuche)	bis der Nutzer sie trennt (in der Anwendung oder mit /stop), er aus dem Kundenkonto entfernt oder gesperrt wird oder das Kundenkonto gelöscht wird; mit der Trennung ist auch der PIN-Hash gelöscht
Einmal-Codes zum Verbinden des Telegram-Bots (nur Hashes)	10 Minuten gültig, einmal verwendbar; abgelaufene oder benutzte Einträge werden einen Tag danach beim nächsten Erzeugen eines Codes gelöscht
Papierkorb der Kundendatenbank	30 Tage nach dem Löschen, dann endgültig
Unbestätigte Buchungsanfragen	24 Stunden
Kontaktanfragen (Formular „Zugang anfragen“)	180 Tage nach Eingang, dann automatisch gelöscht; früher von Hand, etwa wenn sie erledigt sind oder Sie die Löschung verlangen
Registrierungsanfragen (E-Mail-Adresse, Hash des Tokens)	24 Stunden gültig; 7 Tage nach Ablauf oder Abschluss automatisch gelöscht
Firmendaten und Registrierungsangaben	für die Laufzeit des Vertrags; bei einer Testphase ohne Buchung 30 Tage nach dem Ende der Testphase gelöscht, mit dem Kundenkonto
Daten einer Testphase ohne Buchung	nur Lesen und Export bis 30 Tage nach dem Ende der Testphase, danach Löschung des Kundenkontos und der Kundendaten, in der Regel von Hand, nachts automatisch nur bei eingeschalteter Funktion; Erinnerungen 14 und 3 Tage vor dem Termin***[bitte klären: Frist von 30 Tagen und Ablauf der Löschung, siehe AGB § 2a.]***

Zustimmungsprotokoll (Vertragsnachweis)	für die Laufzeit des Vertrags und danach 6 Jahre; es bleibt auch nach der Löschung des Kundenkontos bestehen ***[bitte klären: Aufbewahrungsdauer und Personenbezug, siehe Abschnitt 4.10.]***
Merkmale gegen wiederholte Testphasen (nur Hashes)	24 Monate ab Beginn der Testphase, auch nach der Löschung des Kundenkontos; danach automatisch gelöscht
Daten zum Abonnement (Kennungen bei Stripe, Stand, Tarif, Abrechnungszeitraum)	für die Laufzeit des Vertrags
Ereignisprotokoll der Zahlungsabwicklung (ohne Inhalt)	90 Tage
Rechnungen und Zahlungsdaten	8 Jahre nach den steuer- und handelsrechtlichen Fristen, bei uns und bei Stripe ***[bitte klären: Aufbewahrungsfrist und Aufbewahrungsort der Rechnungen mit dem Steuerberater festlegen.]***
Fassungen der Rechtstexte	unbefristet; sie enthalten keine personenbezogenen Daten
Zwischenzustände beim Verbinden eines Kontos (OAuth)	10 Minuten gültig; abgelaufene Einträge werden einen Tag nach ihrem Ablauf nachts automatisch gelöscht
Mails, Analysen, Dateien, Kundendatenbank (Kundendaten)	bis der Kunde sie löscht (Papierkorb oder endgültiges Löschen je Kontakt) oder bis zum Vertragsende. Davon abweichend, nachts automatisch und nur bei eingeschalteter Funktion (derzeit aus): der Text einer E-Mail wird 12 Monate nach dem Datum der E-Mail aus ZORYVO gelöscht (Absender, Betreff, Anhangsliste und das Original im Postfach bleiben), die Rohantwort und das Ergebnis der KI-Analyse einer E-Mail 180 Tage nach der Analyse (die Zusammenfassung bleibt). Für Dateien, Rechnungen und die Kundendatenbank gibt es keine automatische Aufbewahrungsfrist
Datenbank-Sicherung	Vorgesehen ist die Point-in-Time-Recovery von Supabase mit einem Wiederherstellungsfenster von {{PITR-Wiederherstellungsfenster}}. Gelöschte Daten verschwinden aus der Sicherung mit Ablauf dieses Fensters. Dateien im Dateispeicher sind in der Sicherung nicht enthalten und werden derzeit nicht gesondert gesichert ***[bitte klären: PITR-Add-on gebucht? Fenster erst nach Buchung eintragen.]***
Protokolle und Ereignisse bei Vercel, Sentry, Brevo	nach den Fristen der Anbieter ***[bitte klären: Fristen nachtragen]***

Bei Vertragsende exportiert und löscht der Betreiber die Daten des Kunden derzeit nach Absprache von Hand, mit Nachweis in Textform; ein automatischer Ablauf existiert nicht. Ausnahme ist die Löschung nach einer Testphase ohne Buchung, die der Löschdienst der Anwendung ausführt (in der Regel auf Veranlassung eines Mitarbeiters, automatisch nur bei eingeschalteter Funktion). ***[bitte klären: Fristen für Rückgabe und Löschung bei Vertragsende festlegen.]***

15. Ihre Rechte

Sie haben gegenüber uns als Verantwortlichem folgende Rechte: Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18), Datenübertragbarkeit (Art. 20) und Widerspruch (Art. 21, siehe unten). Beruht eine Verarbeitung auf Ihrer Einwilligung, können Sie diese jederzeit mit Wirkung für die Zukunft widerrufen (Art. 7 Abs. 3).

Widerspruchsrecht: Soweit wir Daten auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO verarbeiten (Abschnitte 3, 4.8, 4.9 für Bot-Prüfung und Rate-Limits, 4.11, 5, 6, 7, 10 und 11), können Sie aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit Widerspruch einlegen (Art. 21 DSGVO). Wir verarbeiten die Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Zur Ausübung wenden Sie sich per E-Mail an {{Datenschutz-Kontakt}}. Für Ihr Nutzerkonto gibt es in ZORYVO keinen Selbstservice für Auskunft, Export oder Löschung; wir bearbeiten Ihre Anfrage von Hand. ***[bitte klären: Verfahren und Frist für Betroffenenanfragen zu Nutzerkonten (Löschung von Profil und Anmeldekonto durch den Betreiber) festlegen.]***

Betrifft Ihre Anfrage Daten, die ein Kunde in ZORYVO verarbeitet (Abschnitte 8 und 10), richten Sie sie an diesen Kunden. Er ist Verantwortlicher und kann Auskunft, Sperrung und Löschung je Kontakt in ZORYVO auslösen. Wir unterstützen ihn dabei.

Sie haben das Recht, sich bei einer Datenschutz-Aufsichtsbehörde zu beschweren (Art. 77 DSGVO), insbesondere bei {{zuständige Aufsichtsbehörde}}.

16. Weitere Angaben

16.1 Pflicht zur Bereitstellung

Für ein Nutzerkonto müssen Sie eine E-Mail-Adresse, einen Anzeigenamen, ein Passwort und, wo Pflicht, einen zweiten Faktor bereitstellen. Ohne diese Angaben können Sie ZORYVO nicht nutzen. Für die Registrierung eines Unternehmens sind außerdem der rechtliche Name, die Anschrift in Deutschland und die Erklärungen zu Unternehmereigenschaft, AGB und AVV Pflicht; USt-IdNr. und Handelsregistereintrag sind freiwillig. Ohne die Pflichtangaben können wir den Vertrag nicht schließen. Auf Buchungsseiten sind Name und E-Mail-Adresse Pflicht, bei Terminen vor Ort zusätzlich die Adresse; der Kunde kann einzelne seiner Fragen als Pflichtangabe kennzeichnen. Ohne Pflichtangaben ist keine Buchung möglich. Im Kontaktformular sind Name, Firma, E-Mail-Adresse und Nachricht Pflicht; ohne sie können wir die Anfrage nicht annehmen. Alle anderen Angaben sind freiwillig.

16.2 Keine automatisierte Entscheidungsfindung

Wir treffen keine Entscheidungen im Sinne von Art. 22 DSGVO. Rate-Limits und die Anmeldesperre begrenzen nur die Zahl der Versuche in einem Zeitfenster und heben sich von selbst auf; sie entfalten keine rechtliche Wirkung. Auch die Prüfung auf wiederholte Testphasen (Abschnitt 4.11) sperrt nichts automatisch; ein Mensch entscheidet. Das Pausieren eines Kundenkontos bei Zahlungsausfall oder nach dem Ende der Testphase folgt aus dem Vertrag und betrifft das Unternehmen (Abschnitt 4.12).***[bitte klären: ob das automatische Pausieren bei Zahlungsausfall gegenüber Einzelunternehmern eine Entscheidung nach Art. 22 DSGVO ist.]*** Zur KI-Verarbeitung im Auftrag unserer Kunden siehe Abschnitt 8.4.

16.3 Datensicherheit

Wir schützen Daten mit folgenden Maßnahmen: Mandantentrennung durch Zugriffsregeln auf jeder Tabelle der Datenbank (Row Level Security), die auch für Hintergrundjobs und den Plattform-Admin gelten; Zwei-Faktor-Anmeldung; Übertragung nur über HTTPS (Strict-Transport-Security für zwei Jahre); Verschlüsselung von Zugriffstoken und Debug-Inhalten mit AES-256-GCM und getrennten Schlüsselringen; Speicherung von Einmal-Tokens (Einladungen, Registrierungslinks, Buchungslinks), Wiederherstellungscodes und Rate-Limit-Identifikatoren nur als Hash; getrennte Umgebungen für Entwicklung, Test und Betrieb, ohne echte Daten in der Entwicklung; Protokolle ohne Inhalte und Fehlerberichte mit gekürzten und maskierten Fehlertexten (Abschnitt 7.1); Ablage von Dateien in Google Drive oder OneDrive nur nach Virenscan (derzeit ist kein Scanner eingerichtet, daher findet keine solche Ablage statt); eine Notbremse für alle Aktionen nach außen; Support-Freigaben mit Frist und Protokoll; interne Sicherheitsprüfungen des Codes. Ein externer Penetrationstest und eine Zertifizierung liegen nicht vor.

16.4 Änderungen dieser Erklärung

Wir passen diese Erklärung an, wenn sich Funktionen, Dienstleister oder die Rechtslage ändern. Die jeweils aktuelle Fassung finden Sie unter /rechtliches/datenschutz. Maßgeblich ist der unten genannte Stand.

Stand: 2026-10-17

ENTWURF