ErdiKnows

Data Processing Agreement

Stand: 4 November 2026 · 2.1

Between the customer, as recorded in the Erdi account – the controller –
and ErdiKnows – owner Steffen Giebler (sole proprietorship), Schwedter Str. 25, 10119 Berlin, Germany – the processor. Legal contact: legal@erdiknows.com (mailto:legal@erdiknows.com)

Why this exists

When you use Erdi, you bring personal data about other people into the service – above all by connecting mailboxes, calendars and business accounts. This agreement sets out our obligations as your processor under Art. 28 GDPR. It becomes part of the Terms of Service when you connect your first mailbox, calendar or business account, and runs for as long as they do.

You remain responsible for the lawfulness of the processing. You decide the purposes and means, except where they follow from how Erdi works.

1. Subject, nature, purpose

1.1 Subject: fetching, storing, analysing, displaying and sending personal data within the Erdi functions you use.

1.2 Nature: collecting, recording, organising, storing, reading, querying, analysing with AI models, summarising, using, transmitting (including sending messages through your mail server on your instruction), restricting and erasing personal data, and retrieving it from services you connect.

1.3 Purpose: we process the data solely to provide Erdi to you under the Terms of Service. We do not use it for our own purposes, do not sell it and do not use it to train general AI models.

1.4 Location: within the EU or EEA, except as set out in section 8.

2. Duration

This agreement starts when you connect your first mailbox, calendar or business account and ends when the contract ends, at the latest when deletion under section 11 is complete.

3. Categories of data subjects

• Senders and recipients of emails in your connected mailboxes, and people named in them
• Participants in your appointments
• Your customers, subscribers and buyers whose data appears in connected business accounts
• Your staff and collaborators, where they appear in emails, appointments or notes

4. Categories of personal data

• Communication data: sender and recipients, subject, date and text of emails (without attachments), reply and follow-up drafts, messages sent on your instruction
• AI results: summaries, importance ratings, tasks, deadlines and explanations derived from the above
• Calendar data: title, time, place and participants of appointments, where a calendar is connected
• Business data: mostly aggregated figures; in addition pseudonymous customer records (provider customer ID, subscription or order status, product, country, price, currency) and, where a connected source provides them, names or email addresses of your customers
• Content you enter: commands, notes, memory entries and learned writing-style rules
• Credentials for connected services: stored encrypted only

Excluded: Erdi is not designed for special categories of data under Art. 9 GDPR, data under Art. 10 GDPR or data under professional secrecy (§ 203 German Criminal Code) as a purpose of processing. Where such

data is contained in emails you receive, we process it only as part of the service and with the same protection as all other data.

5. Instructions

5.1 We process personal data only on your documented instructions. The Terms of Service, this agreement and the settings you make in Erdi (in particular how independently Erdi works per area) are your instructions.

5.2 Further instructions go in writing to legal@erdiknows.com (mailto:legal@erdiknows.com).

5.3 If we consider an instruction unlawful, we tell you without delay and may suspend it until it is clarified.

5.4 Where EU or member state law obliges us to process data, we tell you beforehand unless that law prohibits it on important grounds of public interest.

6. Confidentiality

6.1 Everyone authorised to process the data is committed to confidentiality, unless already under a statutory duty. The commitment continues after their involvement ends.

6.2 Access to production data is limited to what operation, fault fixing and support require. We do not read your emails unless you ask us to for support (and then only the messages concerned), it is necessary for security, or the law requires it.

7. Technical and organisational measures

We take the measures required by Art. 32 GDPR, described in Annex 1. We may adapt them, but not below the level of protection described there.

8. Subprocessors

8.1 You give general authorisation for us to use subprocessors. The current list – provider, purpose, location and transfer mechanism – is published at erdiknows.com/legal/subprocessors and forms part of this agreement.

8.2 We inform you at least 30 days before we engage a further subprocessor or replace one, by email to the address of your account.

8.3 You may object within 14 days for an important reason relating to data protection. If you do, either side may terminate the contract as of the planned change.

8.4 We bind each subprocessor by contract to substantially the same obligations.

8.5 Transfers outside the EU/EEA take place only on the basis of an adequacy decision or EU Standard Contractual Clauses, as stated in the list.

8.6 Services you connect yourself – for example your mail provider, Stripe, RevenueCat, Apple, Meta or Google – are not subprocessors under this agreement. You have your own contract with them; we retrieve data from them only on your instruction using the credentials you provide. Paddle, which sells our paid plans, acts as an independent controller and is not a subprocessor.

9. Support

9.1 We help you meet data subjects' rights under Chapter III GDPR. Erdi offers export, editing and deletion functions for this purpose; where they are not enough, we help on request to a reasonable extent.

9.2 If a data subject contacts us directly, we forward the request to you without delay and do not answer it on the merits ourselves.

9.3 We support you with Art. 32 to 36 GDPR, including data protection impact assessments, as far as the necessary information is available to us.

10. Personal data breaches

10.1 We notify you of any personal data breach without undue delay, as a rule within 24 hours of becoming aware of it, by email.

10.2 The notification contains, as far as known: the nature of the breach, categories and approximate number of data subjects and records, likely consequences, measures taken or proposed, and a contact point.

10.3 Notifying the supervisory authority (Art. 33 GDPR) and data subjects (Art. 34 GDPR) is your responsibility; we support you.

11. Return and deletion

11.1 Data from a mailbox or connected account is deleted when you remove that connection. All your data is deleted when you delete your account, unless a statutory retention duty applies.

11.2 You can export your data at any time while your account exists. We owe no separate handover in another format.

11.3 Backups are overwritten in the regular cycle.

11.4 On request to legal@erdiknows.com (mailto:legal@erdiknows.com) we confirm deletion in writing.

12. Evidence and audits

12.1 We provide all information needed to demonstrate compliance with Art. 28 GDPR, primarily in writing, together with Annex 1 and the certifications of our subprocessors.

12.2 Where this is not enough in an individual case, we allow an audit after at least 30 days' notice, during normal business hours, at most once a year, protecting our trade secrets and the rights of other customers. You bear the costs unless the audit finds a material breach of this agreement.

13. Liability

The liability provisions of the Terms of Service apply. Art. 82 GDPR remains unaffected.

14. Final provisions

Where this agreement and the Terms of Service conflict on data protection matters, this agreement prevails. German law applies. If a provision is invalid, the rest remains valid. This agreement is written in English; translations are provided for convenience, and the English version prevails.

Annex 1 – Technical and organisational measures

Physical access. We operate no servers of our own. Physical protection is provided by our subprocessors' certified data centres.

System access. Sign-in only with a one-time 6-digit code sent to a verified email address; no passwords. Sessions expire and are renewed automatically. Administrative functions are restricted to named administrators and checked on the server.

Data access. Each customer's data is separated at database level by row-level security; access across accounts is not possible. Credentials for mailboxes and connected services cannot be read from browsers or apps at all, only by our server.

Separation. Logical separation by account. Separate environments for development and production.

Encryption. TLS for all connections to browsers, apps, mail servers and providers. Passwords and API keys for connected services are encrypted with AES-256-GCM; the key is stored outside the database. Encryption at rest by the database provider.

Transfer control. Outgoing connections only over TLS. Incoming webhooks are verified by the provider's signature.

Input control. Every action Erdi takes or proposes, and every action you take on it, is recorded in an activity log that cannot be changed or deleted. Sign-ins, scheduled runs and errors are logged.

Control of automated actions. Critical actions (sending, actions towards new recipients, anything public, payments, contracts, deletions) need your confirmation or are excluded entirely, depending on the area and mode you choose. Messages are held in an undo window before they are sent.

Availability. Providers with redundant infrastructure. Automatic backups by the database provider. Automatic error tracking with alerts. Failed scheduled runs are retried with increasing intervals.

Data minimisation. Email attachments are not stored. Error tracking without personal data by default, no session recording, visit counting without cookies or IP addresses.

Review. Measures are reviewed when the service changes materially, at least once a year.

Diese Übersetzung dient nur der Information. Maßgeblich ist die englische Fassung.

Zwischen dem Kunden, wie im Erdi-Konto hinterlegt – dem Verantwortlichen –
und ErdiKnows – Inhaber Steffen Giebler (Einzelunternehmen), Schwedter Str. 25, 10119 Berlin, Deutschland – dem Auftragsverarbeiter. Rechtlicher Kontakt: legal@erdiknows.com (mailto:legal@erdiknows.com)

Warum es diesen Vertrag gibt

Wenn du Erdi nutzt, bringst du personenbezogene Daten anderer Personen in den Dienst ein – vor allem, indem du Postfächer, Kalender und Business-Konten verbindest. Dieser Vertrag legt unsere Pflichten als dein Auftragsverarbeiter nach Art. 28 DSGVO fest. Er wird Bestandteil der Allgemeinen Geschäftsbedingungen, wenn du dein erstes Postfach, deinen ersten Kalender oder dein erstes Business-Konto verbindest, und läuft so lange wie diese.

Du bleibst für die Rechtmäßigkeit der Verarbeitung verantwortlich. Du entscheidest über Zwecke und Mittel, außer soweit sie sich aus der Funktionsweise von Erdi ergeben.

1. Gegenstand, Art, Zweck

1.1 Gegenstand: Abrufen, Speichern, Analysieren, Anzeigen und Senden personenbezogener Daten im Rahmen der Erdi-Funktionen, die du nutzt.

1.2 Art: Erheben, Erfassen, Ordnen, Speichern, Auslesen, Abfragen, Analysieren mit KI-Modellen, Zusammenfassen, Verwenden, Übermitteln (einschließlich des Sendens von Nachrichten über deinen Mailserver auf deine Weisung), Einschränken und Löschen personenbezogener Daten sowie deren Abruf aus Diensten, die du verbindest.

1.3 Zweck: Wir verarbeiten die Daten ausschließlich, um dir Erdi nach den Allgemeinen Geschäftsbedingungen bereitzustellen. Wir verwenden sie nicht für eigene Zwecke, verkaufen sie nicht und verwenden sie nicht zum Training allgemeiner KI-Modelle.

1.4 Ort: innerhalb der EU oder des EWR, außer wie in Abschnitt 8 dargelegt.

2. Dauer

Dieser Vertrag beginnt, wenn du dein erstes Postfach, deinen ersten Kalender oder dein erstes Business-Konto verbindest, und endet mit dem Ende des Vertrags, spätestens wenn die Löschung nach Abschnitt 11 abgeschlossen ist.

3. Kategorien betroffener Personen

• Absender und Empfänger von E-Mails in deinen verbundenen Postfächern sowie darin genannte Personen
• Teilnehmer deiner Termine
• Deine Kunden, Abonnenten und Käufer, deren Daten in verbundenen Business-Konten erscheinen
• Deine Mitarbeiter und Mitwirkenden, soweit sie in E-Mails, Terminen oder Notizen erscheinen

4. Kategorien personenbezogener Daten

• Kommunikationsdaten: Absender und Empfänger, Betreff, Datum und Text von E-Mails (ohne Anhänge), Entwürfe für Antworten und Nachfassaktionen, auf deine Weisung gesendete Nachrichten
• KI-Ergebnisse: Zusammenfassungen, Wichtigkeitsbewertungen, Aufgaben, Fristen und Erklärungen, die aus dem Vorstehenden abgeleitet werden
• Kalenderdaten: Titel, Zeit, Ort und Teilnehmer von Terminen, soweit ein Kalender verbunden ist
• Business-Daten: überwiegend aggregierte Zahlen; zusätzlich pseudonyme Kundendatensätze (Kunden-ID beim Anbieter, Abonnement- oder Bestellstatus, Produkt, Land, Preis, Währung) und, soweit eine verbundene Quelle sie liefert, Namen oder E-Mail-Adressen deiner Kunden
• Von dir eingegebene Inhalte: Befehle, Notizen, Gedächtniseinträge und gelernte Regeln zum Schreibstil
• Zugangsdaten für verbundene Dienste: ausschließlich verschlüsselt gespeichert

Ausgenommen: Erdi ist nicht dafür ausgelegt, besondere Kategorien personenbezogener Daten nach Art. 9

DSGVO, Daten nach Art. 10 DSGVO oder Daten, die einem Berufsgeheimnis unterliegen (§ 203 StGB), als Zweck der Verarbeitung zu verarbeiten. Soweit solche Daten in E-Mails enthalten sind, die du erhältst, verarbeiten wir sie nur als Teil des Dienstes und mit demselben Schutz wie alle anderen Daten.

5. Weisungen

5.1 Wir verarbeiten personenbezogene Daten nur auf deine dokumentierte Weisung. Die Allgemeinen Geschäftsbedingungen, dieser Vertrag und die Einstellungen, die du in Erdi vornimmst (insbesondere, wie selbstständig Erdi je Bereich arbeitet), sind deine Weisungen.

5.2 Weitere Weisungen sind schriftlich an legal@erdiknows.com (mailto:legal@erdiknows.com) zu richten.

5.3 Halten wir eine Weisung für rechtswidrig, teilen wir dir das unverzüglich mit und können ihre Ausführung bis zur Klärung aussetzen.

5.4 Soweit uns das Recht der EU oder eines Mitgliedstaats zur Verarbeitung von Daten verpflichtet, teilen wir dir das vorher mit, sofern dieses Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

6. Vertraulichkeit

6.1 Alle zur Verarbeitung der Daten befugten Personen sind zur Vertraulichkeit verpflichtet, sofern sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung gilt nach dem Ende ihrer Tätigkeit fort.

6.2 Der Zugriff auf Produktivdaten ist auf das beschränkt, was Betrieb, Fehlerbehebung und Support erfordern. Wir lesen deine E-Mails nicht, es sei denn, du bittest uns im Rahmen des Supports darum (und dann nur die betreffenden Nachrichten), es ist aus Sicherheitsgründen erforderlich oder das Gesetz verlangt es.

7. Technische und organisatorische Maßnahmen

Wir treffen die nach Art. 32 DSGVO erforderlichen Maßnahmen, die in Anlage 1 beschrieben sind. Wir dürfen sie anpassen, jedoch nicht unter das dort beschriebene Schutzniveau.

8. Unterauftragsverarbeiter

8.1 Du erteilst uns eine allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern. Die aktuelle Liste – Anbieter, Zweck, Ort und Übermittlungsgrundlage – ist unter erdiknows.com/legal/subprocessors veröffentlicht und Bestandteil dieses Vertrags.

8.2 Wir informieren dich mindestens 30 Tage, bevor wir einen weiteren Unterauftragsverarbeiter beauftragen oder einen ersetzen, per E-Mail an die Adresse deines Kontos.

8.3 Du kannst innerhalb von 14 Tagen aus einem wichtigen datenschutzrechtlichen Grund widersprechen. In diesem Fall kann jede Seite den Vertrag zum Zeitpunkt der geplanten Änderung kündigen.

8.4 Wir verpflichten jeden Unterauftragsverarbeiter vertraglich zu im Wesentlichen denselben Pflichten.

8.5 Übermittlungen außerhalb der EU/des EWR erfolgen nur auf Grundlage eines Angemessenheitsbeschlusses oder der EU-Standardvertragsklauseln, wie in der Liste angegeben.

8.6 Dienste, die du selbst verbindest – zum Beispiel dein E-Mail-Anbieter, Stripe, RevenueCat, Apple, Meta oder Google –, sind keine Unterauftragsverarbeiter im Sinne dieses Vertrags. Du hast mit ihnen einen eigenen Vertrag; wir rufen Daten von ihnen nur auf deine Weisung mit den von dir bereitgestellten Zugangsdaten ab. Paddle, das unsere kostenpflichtigen Tarife verkauft, handelt als eigenständiger Verantwortlicher und ist kein Unterauftragsverarbeiter.

9. Unterstützung

9.1 Wir helfen dir, die Rechte betroffener Personen nach Kapitel III DSGVO zu erfüllen. Erdi bietet dafür Export-, Bearbeitungs- und Löschfunktionen; wo diese nicht ausreichen, helfen wir auf Anfrage in

angemessenem Umfang.

9.2 Wendet sich eine betroffene Person direkt an uns, leiten wir die Anfrage unverzüglich an dich weiter und beantworten sie nicht selbst in der Sache.

9.3 Wir unterstützen dich bei Art. 32 bis 36 DSGVO, einschließlich Datenschutz-Folgenabschätzungen, soweit uns die erforderlichen Informationen vorliegen.

10. Verletzungen des Schutzes personenbezogener Daten

10.1 Wir melden dir jede Verletzung des Schutzes personenbezogener Daten unverzüglich, in der Regel innerhalb von 24 Stunden, nachdem wir davon Kenntnis erlangt haben, per E-Mail.

10.2 Die Meldung enthält, soweit bekannt: die Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen, die ergriffenen oder vorgeschlagenen Maßnahmen und eine Anlaufstelle.

10.3 Die Meldung an die Aufsichtsbehörde (Art. 33 DSGVO) und die Benachrichtigung der betroffenen Personen (Art. 34 DSGVO) liegen in deiner Verantwortung; wir unterstützen dich dabei.

11. Rückgabe und Löschung

11.1 Daten aus einem Postfach oder verbundenen Konto werden gelöscht, wenn du diese Verbindung entfernst. Alle deine Daten werden gelöscht, wenn du dein Konto löschst, sofern keine gesetzliche Aufbewahrungspflicht besteht.

11.2 Du kannst deine Daten jederzeit exportieren, solange dein Konto besteht. Eine gesonderte Herausgabe in einem anderen Format schulden wir nicht.

11.3 Datensicherungen werden im regulären Zyklus überschrieben.

11.4 Auf Anfrage an legal@erdiknows.com (mailto:legal@erdiknows.com) bestätigen wir die Löschung schriftlich.

12. Nachweise und Prüfungen

12.1 Wir stellen alle Informationen bereit, die zum Nachweis der Einhaltung von Art. 28 DSGVO erforderlich sind, vorrangig in schriftlicher Form, zusammen mit Anlage 1 und den Zertifizierungen unserer Unterauftragsverarbeiter.

12.2 Reicht dies im Einzelfall nicht aus, ermöglichen wir eine Prüfung nach einer Ankündigung von mindestens 30 Tagen, während der üblichen Geschäftszeiten, höchstens einmal im Jahr und unter Wahrung unserer Geschäftsgeheimnisse und der Rechte anderer Kunden. Du trägst die Kosten, es sei denn, die Prüfung ergibt einen wesentlichen Verstoß gegen diesen Vertrag.

13. Haftung

Es gelten die Haftungsbestimmungen der Allgemeinen Geschäftsbedingungen. Art. 82 DSGVO bleibt unberührt.

14. Schlussbestimmungen

Widersprechen sich dieser Vertrag und die Allgemeinen Geschäftsbedingungen in Fragen des Datenschutzes, hat dieser Vertrag Vorrang. Es gilt deutsches Recht. Ist eine Bestimmung unwirksam, bleibt der Rest wirksam. Dieser Vertrag ist in englischer Sprache verfasst; Übersetzungen werden zur Erleichterung bereitgestellt, und die englische Fassung geht vor.

Anlage 1 – Technische und organisatorische Maßnahmen

Zutrittskontrolle. Wir betreiben keine eigenen Server. Der physische Schutz erfolgt durch die zertifizierten

Rechenzentren unserer Unterauftragsverarbeiter.

Zugangskontrolle. Anmeldung nur mit einem einmaligen 6-stelligen Code, der an eine verifizierte E-Mail-Adresse gesendet wird; keine Passwörter. Sitzungen laufen ab und werden automatisch erneuert. Administrative Funktionen sind auf namentlich benannte Administratoren beschränkt und werden auf dem Server geprüft.

Zugriffskontrolle. Die Daten jedes Kunden sind auf Datenbankebene durch Row-Level-Security getrennt; kontoübergreifender Zugriff ist nicht möglich. Zugangsdaten für Postfächer und verbundene Dienste können von Browsern oder Apps überhaupt nicht ausgelesen werden, sondern nur von unserem Server.

Trennung. Logische Trennung nach Konto. Getrennte Umgebungen für Entwicklung und Produktion.

Verschlüsselung. TLS für alle Verbindungen zu Browsern, Apps, Mailservern und Anbietern. Passwörter und API-Schlüssel für verbundene Dienste werden mit AES-256-GCM verschlüsselt; der Schlüssel wird außerhalb der Datenbank gespeichert. Verschlüsselung ruhender Daten durch den Datenbankanbieter.

Weitergabekontrolle. Ausgehende Verbindungen nur über TLS. Eingehende Webhooks werden anhand der Signatur des Anbieters überprüft.

Eingabekontrolle. Jede Aktion, die Erdi ausführt oder vorschlägt, und jede Aktion, die du daraufhin vornimmst, wird in einem Aktivitätsprotokoll erfasst, das nicht geändert oder gelöscht werden kann. Anmeldungen, geplante Ausführungen und Fehler werden protokolliert.

Kontrolle automatisierter Aktionen. Kritische Aktionen (Senden, Aktionen gegenüber neuen Empfängern, alles Öffentliche, Zahlungen, Verträge, Löschungen) benötigen deine Bestätigung oder sind vollständig ausgeschlossen, je nach dem von dir gewählten Bereich und Modus. Nachrichten werden vor dem Senden in einem Rückgängig-Zeitfenster zurückgehalten.

Verfügbarkeit. Anbieter mit redundanter Infrastruktur. Automatische Datensicherungen durch den Datenbankanbieter. Automatische Fehlererfassung mit Benachrichtigungen. Fehlgeschlagene geplante Ausführungen werden mit zunehmenden Abständen wiederholt.

Datenminimierung. E-Mail-Anhänge werden nicht gespeichert. Fehlererfassung standardmäßig ohne personenbezogene Daten, keine Sitzungsaufzeichnung, Besuchszählung ohne Cookies oder IP-Adressen.

Überprüfung. Die Maßnahmen werden überprüft, wenn sich der Dienst wesentlich ändert, mindestens einmal im Jahr.