ErdiKnows

Data Processing Agreement

Stand: 22 August 2026 · v1.0

Data Processing Agreement

Version 1.0 · 22 August 2026 · under Art. 28 GDPR

Between the user, as recorded in the account — the controller —
and 52N34S Group – Steffen Giebler, Schwedter Str. 25, 10119 Berlin, Germany — the processor.

Why this exists

We run ErdiKnows. When you use it, you may send us personal data about other people — most obviously by forwarding incoming email to an address we assign you, but also through events and metrics you submit.

This agreement sets out our obligations under Art. 28 GDPR. It becomes part of the Terms when you register and runs for as long as they do.

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

1. Subject, nature, purpose

1.1 Subject: storing, displaying and transmitting personal data within the functions of ErdiKnows you use.

1.2 Nature: collecting, recording, organising, storing, reading, querying, using, transmitting, restricting and erasing.

1.3 Purpose: providing the service under the Terms, and nothing else. We do not process the data for our own purposes.

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

2. Duration

Starts on registration, ends when the user relationship ends, at the latest once deletion under section 11 is complete.

3. Categories of data subject

• Your customers, prospects and other contacts, in particular senders of forwarded email
• Users of your apps and websites, where their data appears in events you submit
• Your staff and collaborators, where they are named in events or board cards

4. Categories of personal data

• Communication data: sender name and address, subject, body and time of forwarded email, plus your internal notes on it
• Content data: text you enter freely in events, board cards, releases and notes
• Usage and metric data: aggregated values without direct personal reference, plus technical identifiers where you submit them
• Third-party credentials: keys to services you connect, stored encrypted only

Excluded: you do not send special categories of personal data under Art. 9 GDPR, no data under Art. 10 GDPR, and nothing covered by professional secrecy under § 203 StGB. The service is not built for it. If you do so anyway, the consequences are yours alone.

5. Instructions

5.1 We process personal data only on your documented instructions. The Terms, this agreement, and the settings you make in the app are the initial instruction.

5.2 Further instructions go in writing to support@52n34s.com (mailto:support@52n34s.com).

5.3 If we consider an instruction unlawful, we say so without delay and may suspend it until the matter is settled.

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

6. Confidentiality

6.1 Everyone authorised to process is committed to confidentiality, unless already under a statutory duty. The commitment survives the end of their involvement.

6.2 Access to production data is limited to what operation, fault-fixing and support require.

7. Technical and organisational measures

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

8. Subprocessors

8.1 You give general authorisation for the following subprocessors:

Company · Service · Where
Supabase, Inc., 970 Toa Payoh North #07-04, Singapore 318992 · database, authentication · EU (Frankfurt)
Vercel, Inc., 340 S Lemon Ave #4133, Walnut, CA 91789, USA · hosting, compute · EU, partly USA
Resend (Plus Five Five, Inc.), 2093 Philadelphia Pike #1811, Claymont, DE 19703, USA · sending and receiving email · EU, partly USA
Functional Software, Inc. dba Sentry, 45 Fremont Street, San Francisco, CA 94105, USA · error tracking · EU region
Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA · domain name resolution · worldwide

8.2 We tell you at least 30 days before we engage a further subprocessor or replace an existing one, in writing to the address in your account.

8.3 You may object within 14 days for an important, data-protection-related reason. If you do, we may terminate the contract as of the planned change; there is no right to have the previous arrangement continued.

8.4 We put each subprocessor under substantially the same obligations by contract.

8.5 Where processing happens outside the EU or EEA, we ensure appropriate safeguards under Chapter V GDPR — standard contractual clauses or an adequacy decision.

9. Support

9.1 We help you meet data subject rights under Chapter III GDPR. Export, editing and deletion functions in the app are there for that. Where they don't suffice, we help on request to a reasonable extent.

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

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

9.4 For support beyond what Art. 28 GDPR requires we may charge a reasonable fee, announced in advance.

10. Reporting breaches

10.1 We report any personal data breach to you without delay and within 24 hours of becoming aware of it,

in writing.

10.2 The report includes, as far as known: nature of the breach, categories and approximate number of records, likely consequences, measures taken and proposed, and a contact point.

10.3 Reporting to the supervisory authority under Art. 33 GDPR and to data subjects under Art. 34 GDPR is yours to do.

11. Return and deletion

11.1 After the contract ends we delete all personal data within 30 days, unless a statutory retention duty applies.

11.2 Until then you can retrieve the data through the export function. We owe no separate handover in another format.

11.3 Backups are overwritten in the regular cycle, at the latest after 30 days.

11.4 We confirm deletion in writing on request.

12. Evidence and audits

12.1 We make available all information needed to demonstrate compliance with Art. 28 GDPR.

12.2 Evidence is provided primarily in writing, together with Annex 1 and the certifications of our subprocessors.

12.3 Where that does not suffice 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 other users' rights. You bear the resulting costs.

13. Liability

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

14. The rest

Where this agreement and the Terms conflict, this agreement prevails on data protection matters. German law applies. If one provision is invalid, the rest stays valid.

Annex 1 — Technical and organisational measures

Physical access. No servers of our own. Physical protection is with our subprocessors, who operate certified data centres.

System access. Sign-in only through one-time links to a verified email address. No password stored. Sessions expire after 30 days, or 14 days without use; refresh tokens rotate. Sign-in from an unknown device triggers a notification. Admin functions are protected in two stages — menu entry only for admins, route additionally checked server-side.

Data access. Tenant separation at database level through row level security. Every record belongs to a project; access across project boundaries is not possible. The ingest endpoint runs with elevated rights but determines the project solely from the token supplied and writes only there.

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

Pseudonymisation and encryption. TLS for all transport. Third-party API keys encrypted with AES-256-GCM; the key lives outside the database and the column is not readable by grant. API tokens stored only as SHA-256 hashes, never in clear text. Device recognition via hashes, without storing the IP address. Encryption at rest by the database provider.

Transfer control. Outbound connections to third-party services over TLS only. Inbound webhooks verified by provider-specific signature checks — HMAC-SHA1, HMAC-SHA256, JWT or Svix — with the secret stored encrypted per endpoint.

Input control. Logging of sign-ins, outgoing messages, scheduled runs and rejected API requests. Inbound mail addresses carry a random identifier rather than the project name, so knowing a project name does not let anyone create tickets in it.

Availability. Providers with redundant infrastructure. Automatic backups by the database provider. 1,000 API requests per hour per token. Automatic error tracking with notification. Exponential backoff on repeatedly failing scheduled runs.

Review. Measures reviewed on material changes to the service, at least annually. Data processing agreements with all subprocessors. Privacy-friendly defaults: visitor counting without cookies and without IP storage, error tracking without personal data by default, no session recording, digests off by default.

Auftragsverarbeitungsvertrag

Version 1.0 · 22. August 2026 · nach Art. 28 DSGVO

Zwischen dem Nutzer, wie im Konto hinterlegt — dem Verantwortlichen —
und 52N34S Group – Steffen Giebler, Schwedter Str. 25, 10119 Berlin, Deutschland — dem Auftragsverarbeiter.

Warum es das gibt

Wir betreiben ErdiKnows. Bei der Nutzung kannst du uns personenbezogene Daten anderer Personen übermitteln — am deutlichsten durch die Weiterleitung eingehender Mail an eine dir zugewiesene Adresse, aber auch über Events und Metriken.

Dieser Vertrag regelt unsere Pflichten nach Art. 28 DSGVO. Er wird mit der Registrierung Bestandteil der Nutzungsbedingungen und gilt für deren Laufzeit.

Du bleibst für die Rechtmäßigkeit der Verarbeitung verantwortlich. Du entscheidest über Zwecke und Mittel, soweit sie sich nicht aus der Funktionsweise des Dienstes ergeben.

1. Gegenstand, Art, Zweck

1.1 Gegenstand: Speicherung, Darstellung und Übermittlung personenbezogener Daten im Rahmen der von dir genutzten Funktionen von ErdiKnows.

1.2 Art: Erheben, Erfassen, Organisieren, Speichern, Auslesen, Abfragen, Verwenden, Übermitteln, Einschränken, Löschen.

1.3 Zweck: die Erbringung des Dienstes nach den Nutzungsbedingungen, nichts darüber hinaus. Eine Verarbeitung zu eigenen Zwecken findet nicht statt.

1.4 Ort: innerhalb der EU beziehungsweise des EWR, mit Ausnahme von Abschnitt 8.

2. Dauer

Beginnt mit der Registrierung, endet mit dem Ende des Nutzungsverhältnisses, spätestens mit Abschluss der Löschung nach Abschnitt 11.

3. Kategorien betroffener Personen

• Deine Kunden, Interessenten und sonstigen Kontakte, insbesondere Absender weitergeleiteter Mail
• Nutzer deiner Anwendungen und Websites, soweit ihre Daten in übermittelten Events enthalten sind
• Deine Beschäftigten und Mitwirkenden, soweit sie in Events oder Board-Karten genannt werden

4. Kategorien personenbezogener Daten

• Kommunikationsdaten: Absendername und -adresse, Betreff, Inhalt und Zeitpunkt weitergeleiteter Mail sowie deine internen Vermerke dazu
• Inhaltsdaten: frei eingegebene Texte in Events, Board-Karten, Releases und Notizen
• Nutzungs- und Kennzahlendaten: aggregierte Werte ohne unmittelbaren Personenbezug sowie technische Kennungen, soweit du solche übermittelst
• Zugangsdaten Dritter: Schlüssel zu von dir verbundenen Diensten, ausschließlich verschlüsselt gespeichert

Ausgeschlossen: Du übermittelst keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO, keine Daten nach Art. 10 DSGVO und nichts, was unter § 203 StGB fällt. Der Dienst ist dafür nicht gebaut. Verstößt du dagegen, trägst du die Folgen allein.

5. Weisungen

5.1 Wir verarbeiten personenbezogene Daten ausschließlich auf deine dokumentierte Weisung. Die

Nutzungsbedingungen, dieser Vertrag und die von dir in der Anwendung vorgenommenen Einstellungen sind die Erstweisung.

5.2 Weitere Weisungen erfolgen in Textform an support@52n34s.com (mailto:support@52n34s.com).

5.3 Halten wir eine Weisung für rechtswidrig, teilen wir das unverzüglich mit und dürfen die Ausführung bis zur Klärung aussetzen.

5.4 Verpflichtet uns Unions- oder mitgliedstaatliches Recht zu einer Verarbeitung, unterrichten wir dich vorher, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.

6. Vertraulichkeit

6.1 Alle zur Verarbeitung befugten Personen sind auf Vertraulichkeit verpflichtet, soweit sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung wirkt über das Ende der Tätigkeit hinaus.

6.2 Der Zugriff auf Produktivdaten ist auf das für Betrieb, Fehlerbehebung und Unterstützung erforderliche Maß beschränkt.

7. Technische und organisatorische Maßnahmen

Wir treffen die Maßnahmen nach Art. 32 DSGVO, beschrieben in Anlage 1. Wir können sie anpassen, das dort beschriebene Schutzniveau dabei aber nicht unterschreiten.

8. Unterauftragsverarbeiter

8.1 Du erteilst die allgemeine Genehmigung für folgende Unterauftragsverarbeiter:

Unternehmen · Leistung · Ort
Supabase, Inc., 970 Toa Payoh North #07-04, Singapur 318992 · Datenbank, Authentifizierung · EU (Frankfurt)
Vercel, Inc., 340 S Lemon Ave #4133, Walnut, CA 91789, USA · Hosting, Rechenleistung · EU, teils USA
Resend (Plus Five Five, Inc.), 2093 Philadelphia Pike #1811, Claymont, DE 19703, USA · Versand und Empfang von Mail · EU, teils USA
Functional Software, Inc. dba Sentry, 45 Fremont Street, San Francisco, CA 94105, USA · Fehleranalyse · EU-Region
Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA · Namensauflösung · weltweit

8.2 Wir informieren dich mindestens 30 Tage vor Beauftragung eines weiteren oder Austausch eines bestehenden Unterauftragsverarbeiters, in Textform an die im Konto hinterlegte Adresse.

8.3 Du kannst innerhalb von 14 Tagen aus wichtigem, datenschutzrechtlich begründetem Anlass widersprechen. In dem Fall können wir zum Zeitpunkt der geplanten Änderung kündigen; ein Anspruch auf Fortführung des bisherigen Zustands besteht nicht.

8.4 Wir verpflichten jeden Unterauftragsverarbeiter vertraglich im Wesentlichen gleich.

8.5 Erfolgt eine Verarbeitung außerhalb der EU beziehungsweise des EWR, stellen wir geeignete Garantien nach Kapitel V DSGVO sicher — Standardvertragsklauseln oder Angemessenheitsbeschluss.

9. Unterstützung

9.1 Wir unterstützen dich bei Betroffenenrechten nach Kapitel III DSGVO. Export-, Bearbeitungs- und Löschfunktionen in der Anwendung sind dafür da. Reichen sie nicht, unterstützen wir auf Anfrage in angemessenem Umfang.

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

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

9.4 Für Unterstützung, die über Art. 28 DSGVO hinausgeht, können wir eine angemessene Vergütung verlangen, vorher angekündigt.

10. Meldung von Verletzungen

10.1 Wir melden dir jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 24 Stunden ab Kenntnis, in Textform.

10.2 Die Meldung enthält, soweit bekannt: Art der Verletzung, betroffene Kategorien und ungefähre Zahl der Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen, Kontaktstelle.

10.3 Die Meldung an die Aufsichtsbehörde nach Art. 33 DSGVO und an betroffene Personen nach Art. 34 DSGVO obliegt dir.

11. Rückgabe und Löschung

11.1 Nach Vertragsende löschen wir alle personenbezogenen Daten innerhalb von 30 Tagen, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.

11.2 Bis dahin kannst du die Daten über die Exportfunktion abrufen. Eine gesonderte Herausgabe in anderem Format schulden wir nicht.

11.3 Sicherungskopien werden im regulären Zyklus überschrieben, spätestens nach 30 Tagen.

11.4 Auf Verlangen bestätigen wir die Löschung in Textform.

12. Nachweise und Kontrollen

12.1 Wir stellen alle Informationen bereit, die zum Nachweis der Einhaltung von Art. 28 DSGVO erforderlich sind.

12.2 Der Nachweis erfolgt vorrangig in Textform, zusammen mit Anlage 1 und den Nachweisen der Unterauftragsverarbeiter.

12.3 Reicht das im Einzelfall nicht, ermöglichen wir eine Überprüfung nach Ankündigung mit mindestens 30 Tagen Frist, während üblicher Geschäftszeiten, höchstens einmal jährlich, unter Wahrung unserer Betriebsgeheimnisse und der Rechte anderer Nutzer. Die Kosten trägst du.

13. Haftung

Es gelten die Haftungsregelungen der Nutzungsbedingungen. Art. 82 DSGVO bleibt unberührt.

14. Der Rest

Bei Widersprüchen zwischen diesem Vertrag und den Nutzungsbedingungen geht dieser Vertrag in Datenschutzfragen vor. Es gilt deutsches Recht. Ist eine Bestimmung unwirksam, bleibt der Rest wirksam.

Anlage 1 — Technische und organisatorische Maßnahmen

Zutritt. Keine eigenen Server. Der physische Schutz liegt bei den Unterauftragsverarbeitern, die zertifizierte Rechenzentren betreiben.

Zugang. Anmeldung nur über einmalige Links an eine verifizierte Mailadresse. Kein Passwort gespeichert. Sitzungen laufen nach 30 Tagen ab, bei Inaktivität nach 14 Tagen; Refresh-Token rotieren. Anmeldung von unbekanntem Gerät löst eine Benachrichtigung aus. Verwaltungsfunktionen zweistufig geschützt — Menüeintrag nur für Admins, Route zusätzlich serverseitig geprüft.

Zugriff. Mandantentrennung auf Datenbankebene über Row Level Security. Jeder Datensatz gehört zu einem Projekt; ein Zugriff über Projektgrenzen hinweg ist nicht möglich. Der Ingest-Endpoint arbeitet mit erhöhten Rechten, ermittelt das Projekt aber ausschließlich über das übergebene Token und schreibt nur dorthin.

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

Pseudonymisierung und Verschlüsselung. TLS für jede Übertragung. API-Schlüssel Dritter mit AES-256-

GCM verschlüsselt; der Schlüssel liegt außerhalb der Datenbank, die Spalte ist per Grant nicht lesbar. API-Token nur als SHA-256-Hashwert gespeichert, nie im Klartext. Geräteerkennung über Hashwerte, ohne Speicherung der IP-Adresse. Verschlüsselung im Ruhezustand durch den Datenbankanbieter.

Weitergabe. Ausgehende Verbindungen zu Diensten Dritter nur über TLS. Eingehende Webhooks über anbieterspezifische Signaturprüfung verifiziert — HMAC-SHA1, HMAC-SHA256, JWT oder Svix — das Geheimnis liegt je Endpunkt verschlüsselt.

Eingabe. Protokollierung von Anmeldungen, ausgehenden Nachrichten, geplanten Läufen und abgewiesenen API-Anfragen. Eingangsadressen für Mail tragen eine Zufallskennung statt des Projektnamens, damit die Kenntnis eines Projektnamens niemandem erlaubt, dort Tickets zu erzeugen.

Verfügbarkeit. Anbieter mit redundanter Infrastruktur. Automatische Sicherungen durch den Datenbankanbieter. 1.000 API-Anfragen pro Stunde und Token. Automatische Fehlerprotokollierung mit Benachrichtigung. Exponentiell steigende Wartezeiten bei wiederholt fehlschlagenden Läufen.

Überprüfung. Maßnahmen werden bei wesentlichen Änderungen des Dienstes überprüft, mindestens jährlich. Auftragsverarbeitungsverträge mit allen Unterauftragsverarbeitern. Datenschutzfreundliche Voreinstellungen: Besucherzählung ohne Cookies und ohne IP-Speicherung, Fehleranalyse ohne personenbezogene Daten in der Voreinstellung, keine Sitzungsaufzeichnung, Berichte standardmäßig aus.

Maßgeblich ist die deutsche Fassung. · The German version prevails.