

Privacy Policy

A product of Two Roads srl

Version 1.1 · Effective 22 September 2026 · Prepared by Two Roads srl

Table of contents

Table of contents	1
1. Who we are	2
2. Two roles: controller and processor	2
3. Personal data we collect	2
3.1 Account and User data (we are the controller)	2
3.2 Connector credentials (we are the processor, acting on the business customer's instruction)	3
3.3 Customer Content (we are the processor)	3
3.4 Usage and technical data	3
4. How we use personal data, and our legal basis	4
5. Automated processing and human review	4
6. Who we share personal data with	5
6.1 The systems our business customer connects	5
6.2 Sub-processors	5
6.3 Legal and safety disclosures	5
7. International data transfers	6
8. Cookies and similar technologies	6
9. Data retention	7
10. Security measures	7
11. Your rights	8
12. Children	9
13. Changes to this Policy	9
14. Contact us	9

Two Roads srl ("Two Roads," "Alfred," "we," "us," or "our") provides Alfred, a software platform that helps small and medium-sized businesses automate repetitive work across email, chat, CRM, and ERP systems — triaging incoming messages, drafting replies, and proposing follow-up actions for a human to review and approve. This Privacy Policy explains what personal data we process, why, and what rights you have.

This Policy applies to (a) the personal data of our business customers' account administrators and employee users ("Users") who sign in to Alfred, and (b) the personal data contained in the emails, CRM records, ERP records, and related content that Alfred processes on a business customer's behalf ("Customer Content") in order to provide the service. Section 2 explains why we wear two different hats — controller and processor — depending on which of these applies.

1. Who we are

Two Roads srl is a company registered in Belgium (VAT BE644.745.142), with its registered address at 21 Champ d'Al Vau, 1380 Lasne, Belgium. We are the operator of Alfred and, depending on context, act either as a data controller or as a data processor as set out below.

2. Two roles: controller and processor

As a controller — for the account and login data of the people who use Alfred directly: business administrators who set up an Alfred account, and the employees they invite. We decide why and how this data is processed (for example, to authenticate sign-ins, manage permissions, and operate the approval workspace), so GDPR treats us as the controller for this category.

As a processor — for Customer Content: the content of emails, CRM records, ERP records, contract and invoice data, and shipment information that Alfred reads and acts on in order to triage messages, draft replies, and propose CRM/ERP updates. Our business customer decides what systems to connect and what this data is used for; we process it strictly on their documented instructions, under a separate Data Processing Agreement with that customer. If you are the end customer of one of our business customers (for example, someone who emailed a company that uses Alfred), your data is being processed under that company's own privacy policy and instructions — Two Roads srl is their processor, not the controller of your data, and you should direct data-subject requests to them in the first instance. We will assist our business customers in responding to such requests.

3. Personal data we collect

3.1 Account and User data (we are the controller)

- Name, work email address, and role/team assignment for account administrators and invited employees.

- Authentication data — password (stored hashed, never in plain text) or single sign-on identifier, and session data needed to keep you signed in.
- Permission and team settings you or your administrator configure within Alfred.
- A permanent activity log of actions taken in the app — approvals, edits, rejections, sends, and configuration changes — recording who did what and when. This log is deliberately never deleted for as long as the account exists, so it remains a trustworthy record; it is deleted, along with the rest of the account's data, if the account itself is deleted. See Section 9 on retention.

3.2 Connector credentials (we are the processor, acting on the business customer's instruction)

When a business customer connects an email provider, CRM, ERP, or invoicing tool, Alfred stores the resulting access token or API key needed to keep that connection working (currently supported: Gmail, Outlook, Odoo, HubSpot, Zoho Invoice, Billit, and Exact Online). These credentials are stored encrypted, never in plain text — see Section 10 — and are used only to operate the connection the customer set up.

3.3 Customer Content (we are the processor)

To do its job, Alfred reads and processes personal data contained in the systems a business customer connects, which may include:

- The content of inbound and outbound emails — sender and recipient addresses, subject, body, thread history, and any attached files. Where an email carries a PDF or Word attachment, Alfred extracts the text it contains so that it can be taken into account when drafting a reply; where a PDF holds only scanned images, that text is extracted by the AI model described in Section 5.
- AI-drafted reply text produced in response to that content.
- Customer records fetched from a connected CRM or ERP for context — for example, a name, contact details, contract terms and renewal/notice dates, invoice and payment history, discount terms, and shipment or order-tracking details.
- Notes Alfred writes back to a CRM/ERP record summarizing how a message was handled, and a regenerated "relationship summary" per customer capturing recurring themes.
- Reference documents a business customer chooses to upload to Alfred — for example contracts, price lists, or delivery terms — which Alfred reads and summarizes once on upload, and then draws on when an incoming message relates to them.

3.4 Usage and technical data

- Records of each AI processing call, linked to the business account: token counts and cost, used to enforce spend limits and for billing — never the content of the underlying prompt beyond what's needed for that call.
- Connector health status (working / broken / disconnected) and pipeline activity counts.
- Error and diagnostic data sent to our monitoring tool when something fails, deliberately minimized — for example, an internal reference number is logged rather than a customer's email address.
- **Sign-in and abuse-prevention counters.** To limit how often sign-in, password-reset, sign-up and similar sensitive requests can be attempted, we hold a short-lived counter against the IP address a request came from, and against the email address used in a failed sign-in. These counters live only in temporary memory, are never written to our database, and expire automatically within minutes.
- **Origin records for security events.** At a small number of specific, security-relevant moments we store a record containing the IP address the request came from, the browser user-agent string it reported, the email address used, the time, and (where known) which account and user it belonged to. Those moments are: creating an account, signing in, a failed sign-in attempt, connecting an email, CRM or ERP provider, and a sign-up form flagged as automated. We do this to detect and investigate abuse of the service, such as repeated or automated sign-up attempts, and to be able to answer a security question about a specific account after the fact. This data is kept for 90 days and then deleted automatically (see Section 9). We do not use it to build a profile of you, to track you across other websites, or for analytics or advertising.

4. How we use personal data, and our legal basis

We process personal data for the following purposes, relying on the GDPR legal bases indicated:

- **To provide the service (Art. 6(1)(b) — performance of a contract):** authenticating Users, operating the connectors a customer has chosen, triaging incoming messages, drafting proposed replies, retrieving context from connected systems, and proposing CRM/ERP actions for human approval.
- **To keep the service secure and accountable (Art. 6(1)(f) — legitimate interests):** maintaining the permanent activity log, monitoring for errors and abuse, enforcing per-account spend limits, and keeping each customer's data isolated from every other customer's data.
- **To meet legal obligations (Art. 6(1)(c)):** responding to lawful requests from regulators or courts, and retaining records needed for tax, accounting, or audit purposes.
- **With consent, where applicable (Art. 6(1)(a)):** for any processing not covered by the bases above, such as optional product communications.

5. Automated processing and human review

Alfred uses an AI model (currently an Anthropic Claude model) to classify incoming messages, draft proposed replies, and suggest CRM/ERP updates. By design, no reply is ever sent to a customer, and no CRM or ERP record is ever changed, without a human User first reviewing and individually approving that specific action — each proposed action is separately checkable, not approved as an all-or-nothing bundle. Because of this human-in-the-loop step, Alfred does not make decisions about you solely by automated means that produce legal or similarly significant effects within the meaning of Art. 22 GDPR.

6. Who we share personal data with

We do not sell personal data. We share it only as follows:

6.1 The systems our business customer connects

Alfred reads from and writes to the email provider, CRM, ERP, and invoicing systems a business customer chooses to connect (currently Gmail, Outlook, Odoo, HubSpot, Zoho Invoice, Billit, and Exact Online), strictly to provide the service to that customer. These are the customer's own systems and accounts, not ours.

6.2 Sub-processors

We use a small number of specialist providers to operate Alfred, each permitted to process personal data only as needed to provide their service to us, and each required to be engaged under a data processing agreement before any live customer data is passed to them:

- **Anthropic** — processes message and context content in order to generate the AI classification and draft replies described in Section 5.
- **A transactional email provider** — sends account, approval, and failure-alert notifications on our behalf.
- **Amazon Web Services (AWS)** — provides the encryption service (KMS) used to protect connector credentials at rest, as described in Section 10.
- **Railway** — hosts the application, database, and background-processing infrastructure that runs Alfred.
- **Sentry** — receives deliberately minimized error and diagnostic data to help us detect and fix failures.

An up-to-date list of sub-processors is available on request.

6.3 Legal and safety disclosures

We may disclose personal data if required by law, or where we believe in good faith it is necessary to protect the rights, property, or safety of Two Roads srl, our customers, or others.

7. International data transfers

Two Roads srl is based in Belgium, and our own infrastructure agreements are chosen with EU/EEA processing in mind. Some sub-processors listed in Section 6.2 may process data in, or from, countries outside the European Economic Area. Where that is the case, we rely on legally recognized transfer mechanisms, such as the European Commission's Standard Contractual Clauses or a valid adequacy framework (for example, the EU-U.S. Data Privacy Framework, where the relevant provider is certified), to ensure your data continues to receive an equivalent level of protection. You can request more detail about the safeguards in place for a specific transfer by contacting us using the details in Section 14.

8. Cookies and similar technologies

Alfred sets one cookie, and only in the one situation described immediately below. Apart from that it sets none at all: none for ordinary sign-in, none for form security, and none for analytics or marketing. When you sign in with a password, Alfred keeps you authenticated using a token stored in your browser's local storage rather than a cookie, sent with each request you make. Our public website's "Request a pilot" form does not currently use any cookie-based protection either.

Company sign-in (single sign-on). If your employer has enabled company sign-in, Alfred sets one short-lived security cookie, named `alfred_sso_binder`, at the moment you begin signing in. It holds a random value and nothing else, cannot be read by scripts running in the page, is sent only to the sign-in address it belongs to, and expires after ten minutes or as soon as sign-in completes. Its only purpose is to confirm that the sign-in coming back is the one you started, so that nobody can hijack it in mid-flow. Because it is strictly necessary for that security function, it is set without asking for your consent, as the law permits.

Cookie consent banner. Even though the only cookie we set is the strictly necessary one described above, Alfred shows a cookie banner the first time you visit any page of the public website, so the mechanism is in place and ready before any cookie — analytics, marketing, or otherwise — is ever added:

NOTE

We use a small number of cookies to improve your experience with Alfred.

Your answer ("Accept all" or "Necessary only") is saved in your own browser's local storage — not sent to or stored on our servers, and not a cookie itself, though we're disclosing it here since it's a similar kind of local storage technology. Neither answer currently changes anything about how the site behaves, since there is nothing to turn on or off yet. Your browser remembers your answer for 3 months (checked locally, by comparing the current time to when you answered — we're never informed of this check), after which the banner will ask again.

Analytics and marketing cookies. We do not currently use any analytics, advertising, or marketing cookies on our website or in the app — no visitor tracking is deployed as of the date of this Policy. If that changes, we will update this section before the change goes live. Any such cookie will be set only after you actively choose "Accept all" in the banner described above — never by default, and never inferred from inaction.

Managing or withdrawing your cookie choice. Since nothing is currently gated behind your answer, there is nothing to withdraw in practice today. Once a real cookie category exists, this section will be updated to describe how to change your choice going forward.

Do Not Track. Because we do not currently track visitors across sites, we do not respond differently to browser "Do Not Track" signals; we will revisit this if that changes.

9. Data retention

We keep personal data only as long as needed for the purposes described in this Policy:

- Account and User data is kept for as long as the business account remains active, and for a limited period afterward to meet legal and accounting obligations.
- Connector credentials are kept only while a connection remains active, and are deleted once a customer disconnects that system.
- The permanent activity log described in Section 3.1 is retained for as long as the account exists, as the authoritative record of what actions were taken on an account and by whom, and is deleted with the rest of that account's data when the account is deleted. We recognize that retaining it indefinitely during the life of an account raises its own question, distinct from other data categories, and we keep it under review.
- Usage, billing, and diagnostic records are kept for as long as needed for billing, security, and legal-compliance purposes.
- Origin records for security events (Section 3.4) are kept for 90 days from the moment they are recorded, and are then deleted automatically by a daily process. They are also deleted, along with everything else, if the account they belong to is deleted.

Where a business customer's own instructions or applicable law require a different retention period for specific Customer Content, that instruction governs, consistent with our Data Processing Agreement with that customer.

10. Security measures

We apply technical and organizational measures appropriate to the sensitivity of the data we process, including:

-
- Per-customer data isolation: data used to generate a reply for one customer's email is drawn from a database query scoped to that customer alone, and nothing about how the AI model is called is cached or reused across customers.
 - Encryption of connector credentials at rest using envelope encryption, bound to the specific account and connector so that a credential cannot be decrypted outside its intended context.
 - Enforced spend limits, checked before each AI processing call, so that a malfunction cannot silently run away with a customer's data or budget.
 - A human-in-the-loop approval step (Section 5) before any customer-facing message is sent or any CRM/ERP record is changed.
 - Deliberately minimized data sent to our error-monitoring tool, reviewed specifically for privacy risk.
 - Separate infrastructure and encryption configuration for our staging/testing environment and our live production environment, so testing activity cannot expose real customer data.

No method of transmission or storage is completely secure. If we become aware of a personal data breach affecting you, we will notify affected customers and, where legally required, the relevant supervisory authority, without undue delay.

11. Your rights

If you are based in the European Economic Area, the United Kingdom, or another jurisdiction with similar protections, you have the following rights over your personal data, subject to certain exceptions and conditions under applicable law:

- **Access** — to obtain a copy of the personal data we hold about you.
- **Rectification** — to have inaccurate or incomplete personal data corrected.
- **Erasure** — to have your personal data deleted, where applicable.
- **Restriction** — to have us limit how we use your personal data in certain circumstances.
- **Portability** — to receive personal data you provided to us in a structured, commonly used, machine-readable format.
- **Objection** — to object to processing based on our legitimate interests.
- **Withdrawal of consent** — where processing is based on consent, at any time, without affecting processing carried out before withdrawal.

To exercise any of these rights, contact us using the details in Section 14. If your data was provided to us by a business that uses Alfred (i.e., you are that business's customer, not our direct User), please also contact that business directly, since it controls how and why your data is processed — we will support them in responding to your request.

You also have the right to lodge a complaint with a supervisory authority. In Belgium, this is:

Autorité de protection des données / Gegevensbeschermingsautoriteit (APD/GBA)

Drukpersstraat 35, 1000 Brussels, Belgium

Phone: +32 2 274 48 00

Email: contact@apd-gba.be

Website: www.dataprotectionauthority.be

12. Children

Alfred is a business tool intended for use by adults acting on behalf of a company. It is not directed at, and we do not knowingly collect personal data from, children.

13. Changes to this Policy

We may update this Policy from time to time to reflect changes in our service or legal requirements. We will post the updated version here with a new "last reviewed" date, and where a change is material, we will take reasonable steps to notify our business customers directly.

14. Contact us

Questions, requests, or concerns about this Policy or how we handle personal data can be directed to:

Two Roads srl

21 Champ d'Al Vau, 1380 Lasne, Belgium

VAT: BE644.745.142

Email: privacy@gotoalfred.com