Alfred

LEGAL DOCUMENT

Data Processing Addendum

Annex to the Alfred Terms and Conditions · Complete version

Version 1.5 · November 2026 · Prepared by Go To Alfred srl

Table of contents

Table of contents 1
1. Definitions 3
2. Subject Matter, Duration, and Roles of the Parties 4
3. Alfred's Obligations 4
4. Customer's Obligations 5
5. Confidentiality 6
6. International Data Transfers 6
7. Sub-processors 6
8. Alfred's AI Sub-processor: Anthropic 7
9. Bring-Your-Own-AI Option 7
10. Notification Sub-processor: Resend 8
11. Data Subject Requests 8
12. Audits 9
13. Term, Deletion, and Return of Data 9
14. Liability 9
15. Precedence and Governing Law 9
16. Acceptance 10
17. Annex 1: Details of Processing 10
Categories of Data Subjects 10
Categories of Personal Data 10
Purpose and Nature of Processing 10
Duration of Processing 11
Frequency 11
18. Annex 2: List of Sub-processors 11
19. Annex 3: Technical and Organisational Security Measures 12
Access Control 12

Encryption 12
Credential and Connector Safety 13
Cost and Usage Controls 13
Human Oversight 13
Organisational Measures 13

This Data Processing Addendum ("DPA") is entered into between the customer identified in the applicable Order Form or account registration ("Customer") and Alfred, a product of Go To Alfred srl ("Alfred", "we", "us"), and forms part of, and is incorporated by reference into, the Alfred Terms and Conditions (the "Agreement") accepted by Customer. Capitalised terms not defined in this DPA have the meaning given to them in the Agreement. This is the complete version of the DPA, and the binding one. Alfred also publishes a shorter public summary on its website; where the two differ, this complete version prevails.

Alfred entity: Go To Alfred srl, with registered office at 21 Champ d'Al Vau, 1380 Lasne, Belgium, currently being incorporated (en constitution), its BCE/KBO number to follow ("Alfred", "Company", "Processor").

1. Definitions

1.1 "GDPR" means Regulation (EU) 2016/679 (General Data Protection Regulation) and, where applicable, its Belgian implementing legislation (Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens).

1.2 "Data Protection Laws" means the GDPR together with any other applicable data protection and privacy legislation in force from time to time in the European Union, the European Economic Area, and their member states, including the United Kingdom GDPR and Data Protection Act 2018 where applicable.

1.3 "Personal Data", "Data Subject", "Processing", "Controller", "Processor", "Sub-processor" and "Personal Data Breach" have the meanings given to them in the GDPR.

1.4 "Customer Personal Data" means Personal Data contained in emails, attachments, CRM/ERP and invoicing records, files read from file-storage services Customer connects, and related metadata that Customer or its users submit to, or that is processed by, the Alfred platform in the course of Customer's use of the Services, including Personal Data relating to Customer's own customers, prospects, suppliers and other correspondents (as Data Subjects).

1.5 "Services" means the Alfred platform made available to Customer under the Agreement: email triage, AI-assisted drafting of replies for human approval, Ask Alfred (answers about a contact drawn from connected systems), the management dashboard, and the related CRM, ERP, invoicing and file-storage connectors.

1.6 "Sub-processor" means any third party engaged by Alfred to Process Customer Personal Data in order to provide the Services, including the AI providers and infrastructure providers listed in Annex 2.

1.7 "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, as approved by the European Commission (Commission Implementing Decision (EU) 2021/914 of 4 June 2021), as may be updated or replaced from time to time, and the equivalent UK Addendum issued by the UK Information Commissioner's Office.

1.8 "File-Storage Data Agreement" means the separate agreement an administrator of Customer accepts before a file-storage service (such as Dropbox, OneDrive or SharePoint) can be connected, which governs the Processing of file content.

1.9 "Connector Page" means the page "What Alfred does in each system" referred to in the Agreement, describing what the Services read and write in each connected system.

2. Subject Matter, Duration, and Roles of the Parties

2.1 This DPA applies whenever Alfred Processes Customer Personal Data on behalf of Customer in connection with the Services. The subject matter, duration, nature and purpose of the Processing, and the categories of Data Subjects and Personal Data, are set out in Annex 1.

2.2 The parties acknowledge that, in respect of Customer Personal Data, Customer is the Controller (or, where Customer itself acts as a processor for its own customers, a Processor acting on its customers' instructions) and Alfred is the Processor. Alfred will Process Customer Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country, unless required to do otherwise by Union or Member State law to which Alfred is subject, in which case Alfred shall inform Customer of that legal requirement before Processing, unless that law prohibits this on important grounds of public interest.

2.3 The Agreement, this DPA, the File-Storage Data Agreement where accepted, Customer's configuration choices within the Services (including which systems are connected, which categories of data, folders, users and teams each may use, whether notes are written back to a connected system, whether Web search is switched on, the choice between Alfred's own AI provider account and a Customer-provided account under Section 9, and any other account settings), and Customer's use of the approval-queue workflow together constitute Customer's complete documented instructions to Alfred for the purposes of Article 28(3)(a) GDPR.

2.4 This DPA remains in effect for as long as Alfred Processes Customer Personal Data under the Agreement.

2.5 Where Customer connects a file-storage service, the File-Storage Data Agreement applies in addition to this DPA and prevails on the Processing of file content.

3. Alfred's Obligations

3.1 Alfred shall Process Customer Personal Data only for the purposes described in Annex 1 and strictly in accordance with Customer's documented instructions, unless otherwise required by applicable law.

3.2 Alfred shall ensure that persons authorised to Process Customer Personal Data (including employees and contractors) are bound by appropriate confidentiality obligations.

3.3 Alfred shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as further described in Annex 3, including encryption of connector credentials at rest (via envelope encryption through a managed key-management service), per-tenant isolation of Customer data enforced by the database, role-based access control, and audit logging of administrative access, including any access by Alfred's staff to Customer's account.

3.4 Alfred shall not engage another processor (a Sub-processor) without Customer's prior general written authorisation, as set out in Section 7.

3.5 Taking into account the nature of the Processing, Alfred shall assist Customer, insofar as reasonably possible and taking into account the information available to Alfred, in fulfilling Customer's obligations to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR, and in complying with Customer's obligations under Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments, and prior consultation).

3.6 Alfred shall notify Customer without undue delay, and in any event within 48 hours of becoming aware, after confirming a Personal Data Breach affecting Customer Personal Data, and shall provide reasonable information to assist Customer in meeting any obligation to notify a supervisory authority or affected Data Subjects under Articles 33 and 34 GDPR.

3.7 At Customer's choice, on termination of the Services, Alfred shall delete or return all Customer Personal Data, and delete existing copies, unless applicable law requires storage of the Personal Data, in accordance with Section 11.

3.8 Alfred shall make available to Customer all information reasonably necessary to demonstrate compliance with the obligations in this Section 3, and shall allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer, subject to Section 10.

4. Customer's Obligations

4.1 Customer shall ensure that its instructions to Alfred, and its use of the Services, comply with Data Protection Laws, including that it has a valid legal basis for the Processing of Customer Personal Data and, where required, has provided appropriate notices to and, where necessary, obtained consent from Data Subjects.

4.2 Customer is solely responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired it, and for ensuring that its connection of third-party mailboxes, CRM, and ERP systems to the Services is authorised.

4.3 Customer shall not instruct Alfred to Process any special category of Personal Data (Article 9 GDPR) or Personal Data relating to criminal convictions and offences (Article 10 GDPR) through the Services unless the parties have agreed additional safeguards in writing.

5. Confidentiality

Alfred shall ensure that access to Customer Personal Data is limited to personnel who need such access to perform the Services, and that such personnel are subject to confidentiality obligations, whether contractual or statutory.

6. International Data Transfers

6.1 Alfred's own infrastructure and database hosting for the Services runs on Railway's EU region, so Customer Personal Data processed and stored within the core Alfred platform remains within the European Union.

6.2 Certain Sub-processors listed in Annex 2 (Anthropic, Resend and Atlassian) process data in, or transfer data to, the United States. Where Alfred transfers Customer Personal Data outside the EEA or the UK, whether directly or via a Sub-processor, such transfer is made either (a) on the basis of an applicable adequacy decision, or (b) under Standard Contractual Clauses, incorporated by reference into this DPA and, where relevant, into Alfred's own agreements with the applicable Sub-processor, together with any additional safeguards those Sub-processors have adopted (including certification under the EU-U.S. Data Privacy Framework, where applicable).

6.3 Alfred shall, on Customer's written request, provide copies of the relevant transfer mechanism documentation (or a summary sufficient for Customer's own records) for any Sub-processor to which Customer Personal Data is transferred outside the EEA or UK.

7. Sub-processors

7.1 Customer provides Alfred with a general written authorisation to engage the Sub-processors listed in Annex 2 as of the effective date of this DPA.

7.2 Alfred shall inform Customer, by posting an updated version of Annex 2 or by direct notice (email or in-app notice) to Customer’s account administrator, of any intended addition or replacement of a Sub-processor at least 14 days before granting that Sub-processor access to Customer Personal Data, thereby giving Customer the opportunity to object.

7.3 If Customer reasonably objects to a new Sub-processor on legitimate data protection grounds, the parties shall discuss in good faith a reasonable alternative. If no resolution is reached within 30 days, Customer may, as its sole remedy, terminate the Services affected by the new Sub-processor, without penalty, by written notice to Alfred.

7.4 Alfred remains fully liable to Customer for the acts and omissions of its Sub-processors to the same extent Alfred would be liable if performing the Services of each Sub-processor directly, and shall impose data protection obligations on each Sub-processor that are no less protective than those set out in this DPA.

7.5 The current list of Sub-processors is set out in Annex 2.

8. Alfred's AI Sub-processor: Anthropic

8.1 By default, the Services use Anthropic PBC ("Anthropic") as a Sub-processor to provide the AI model that triages incoming emails, drafts reply suggestions, answers questions in Ask Alfred, reads the tone of incoming emails for the management dashboard, reads files from the folders Customer selects in a connected file-storage service, and transcribes scanned documents attached to emails. Anthropic Processes the content needed for each of these (the relevant email, file or question, and any connected-system context assembled by Alfred) for the sole purpose of generating that output, under Alfred's own commercial account with Anthropic.

8.2 Alfred's use of Anthropic is governed by Anthropic's Commercial Terms of Service, which automatically incorporate Anthropic's own Data Processing Addendum, including Standard Contractual Clauses for any transfer of data outside the EEA/UK.

8.3 Where Customer's plan includes Web search and Customer's administrator has switched it on, a user's question about a business contact may be answered with a search of the public web, run through a search provider of Anthropic's choosing. Searches concern business contacts only (companies, and self-employed professionals using their own business web domain), never people in a private capacity; no data from Customer's connected systems is placed in the search; the results are shown to that user marked as unverified, and are not stored.

Anthropic Data Processing Addendum / Commercial Terms:
https://www.anthropic.com/legal/commercial-terms

9. Bring-Your-Own-AI Option

9.1 Customer may elect, via its account settings, to have AI processing performed through Customer's own Anthropic, OpenAI, Mistral or Google Gemini account rather than Alfred's ("BYOK AI"). Where Customer elects BYOK AI, Customer (not Alfred) is the party that contracts directly with that provider and accepts its terms for that Processing; the provider

ceases to be Alfred's Sub-processor for that Processing and instead Processes data as Customer's own processor.

9.2 Regardless of whether Customer elects BYOK AI, Alfred's own servers and infrastructure continue to receive, store, and route the underlying email and connected-system context in order to operate the Services, and this DPA continues to apply in full to that Processing by Alfred.

9.3 One step is an exception: a scanned document attached to an email (one with no text layer) is always transcribed through Alfred's own Anthropic account, under Section 8, whichever AI provider Customer has chosen.

9.4 Web search runs on Customer's own Anthropic account where Customer has connected one. It is not available with another AI provider, and in that case no search is made through Alfred's own account.

10. Notification Sub-processor: Resend

10.1 The Services use Resend (Plus Five Five, Inc.) ("Resend") as a Sub-processor to send transactional notification emails to Customer's account administrators and users (for example, approval-queue alerts and connector-failure notices). Resend does not process the content of Customer's own customer-facing email correspondence; only Alfred-generated system notifications.

10.2 Alfred's use of Resend is governed by Resend's Data Processing Addendum, which incorporates Standard Contractual Clauses for transfers from the EEA, UK, and Switzerland, and which is entered into automatically upon Alfred's acceptance of Resend's Terms of Service.

Resend Data Processing Addendum: https://resend.com/legal/dpa

Resend Sub-processor list: https://resend.com/legal/subprocessors

10.3 Under its DPA, Resend deletes Customer-related data within 90 days of the termination of Alfred's account with Resend.

11. Data Subject Requests

If Alfred receives a request directly from a Data Subject seeking to exercise their rights under Data Protection Laws in respect of Customer Personal Data, Alfred shall not respond to that request itself (save to acknowledge receipt) and shall, without undue delay, forward the request to Customer, who remains responsible for responding. Alfred shall provide reasonable assistance, using the functionality of the Services where possible, to enable Customer to respond.

12. Audits

On no less than 30 days' written notice, and no more than once per calendar year (except following a confirmed Personal Data Breach), Customer or its appointed independent auditor may request evidence of Alfred's compliance with this DPA, which Alfred shall provide in the form of the most recent available security documentation, completed security questionnaire, or, where reasonably necessary, a scheduled inspection during business hours. Audits are subject to reasonable confidentiality protections and shall be conducted so as to minimise disruption to Alfred's business and other customers. Customer shall bear its own costs of any audit.

13. Term, Deletion, and Return of Data

13.1 This DPA remains in force for as long as Alfred Processes Customer Personal Data under the Agreement.

13.2 On termination or expiry of the Agreement, and at Customer's written election, Alfred shall, within 30 days, either delete or return (in a commonly used, machine-readable format) all Customer Personal Data held within the Alfred platform, save to the extent applicable law requires continued retention, in which case Alfred shall isolate and protect that data from further Processing.

13.3 Deletion timelines applicable to Sub-processors (for example, Resend's 90-day post-termination deletion window, described in Section 10.3) apply in addition to, and independently of, Alfred's own deletion of data within its own infrastructure.

14. Liability

Each party's liability arising out of or in connection with this DPA is subject to the limitations and exclusions of liability set out in the Agreement. Nothing in this DPA relieves either party of its own direct obligations and liabilities under Data Protection Laws.

15. Precedence and Governing Law

15.1 In the event of a conflict between this DPA and the Agreement, this DPA prevails to the extent of the conflict, insofar as it concerns the Processing of Personal Data. In the event of a conflict between this DPA and the Standard Contractual Clauses (where applicable), the Standard Contractual Clauses prevail.

15.2 This DPA is governed by Belgian law and subject to the exclusive jurisdiction of the courts of Belgium, consistent with the governing law clause of the Agreement.

16. Acceptance

This DPA is accepted by Customer, together with the Agreement, at the time Customer registers for the Services, or under Customer's Order Form, and applies automatically for as long as the Agreement is in force. The version accepted, and when, is shown to Customer's administrators in the Services (System settings, Legal documents), where the version in force is always available. Customer may request a countersigned copy for its own records by contacting Alfred at the address below.

Contact for privacy and data protection matters: info@gotoalfred.com

17. Annex 1: Details of Processing

Categories of Data Subjects

— Customer's own customers, prospects, suppliers and other correspondents, whose Personal Data appears in emails, CRM records, ERP and invoicing records, and files in the folders Customer makes available.

— Customer's employees and authorised users who use the Services (account holders, agents in the approval queue, administrators).

Categories of Personal Data

— Contact details (name, email address, phone number, postal address) contained in emails and connected CRM/ERP records.

— Correspondence content (email subject lines and body text, attachments).

— Commercial data relevant to the customer relationship (contract terms, order history, invoice and payment status, delivery/shipment records).

— Metadata (timestamps, message headers, sender/recipient addresses).

— Content of files in the folders of a connected file-storage service that Customer selects.

— Information Alfred derives from the above to provide the Services: which contact or company an email or a folder relates to, short internal notes of an exchange, and Alfred's reading of an email's tone for the management dashboard (shown with the sentence it is based on, never turned into a score for a person).

No special categories of Personal Data (Article 9 GDPR) are intentionally processed by the Services; Customer is responsible for not routing such data through the Services except where separately agreed in writing (see Section 4.3).

Purpose and Nature of Processing

Triage of inbound business email; reading messages sent from a connected mailbox, only to check whether a message Alfred prepared has gone out and whether a follow-up is still needed; AI-assisted drafting of replies and new emails, including follow-ups on earlier exchanges, each sent only after a user approves it; answers to users' questions about a contact in Ask Alfred, including, where switched on, a search of the public web about a business contact; recording a short internal note of an exchange in a connected CRM, ERP or invoicing system, only once the related reply has been approved by a user and sent, and where Customer has not switched this off (where no reply is sent, the note is kept within the Services and not written to the connected system); creating or closing a task when a user asks or approves a reply; reading files in selected folders to identify which contact they relate to, to inform drafts and to attach a file to an approved reply; and company-level figures on the management dashboard. Files in a file-storage service are only read, never created, changed, moved or deleted. What is read and written in each system is described on the Connector Page.

Duration of Processing

For the duration of the Agreement, plus any post-termination retention/deletion period described in Section 13.

Frequency

Continuous, for as long as Customer's mailbox and connected systems remain linked to the Services.

18. Annex 2: List of Sub-processors

Sub-processor	Purpose	Location / transfer basis	Reference
Anthropic PBC	AI processing described in Section 8, including Web search where switched on (default, unless Customer elects BYOK AI, subject to Section 9.3)	United States; SCCs / DPF	anthropic.com/legal/commercial-terms
Plus Five Five, Inc. (Resend)	Transactional notification emails to Customer's users (for example approval-queue and connector alerts)	United States; SCCs / DPF	resend.com/legal/dpa
Railway Corporation	Application hosting and database infrastructure (EU region)	European Union	railway.com

Sub-processor	Purpose	Location / transfer basis	Reference
Amazon Web Services	Encryption key management for connector credentials, and encrypted off-platform storage of database backups (EU region)	European Union	aws.amazon.com/compliance/gdpr-center
Sentry	Error monitoring: application exceptions and error-level log entries	European Union	sentry.io/legal
Atlassian	Support ticketing: support requests submitted from within the Services, including their content	United States; SCCs	atlassian.com/legal

Mollie B.V. (payment processing) and Billit (invoicing) handle the billing-contact details of Customer's own administrator, for Alfred's own subscription billing. They do not receive Customer Personal Data submitted to the Services, and are named here for completeness rather than as Sub-processors of that data.

19. Annex 3: Technical and Organisational Security Measures

Access Control

— Role-based access control within the Services (Administrator / Team Leader / User), with access to each mailbox, connected system and file-storage folder granted per user or team.

— Database-level enforcement of per-tenant data isolation, not solely reliant on application-layer logic.

— Separate, audited access path for Alfred's own staff. Acting inside a customer account requires a stated reason, ends after 30 minutes, and is recorded in that account's audit trail, visible to its administrators.

— Optional multi-factor authentication, required per role by the administrator, and single sign-on through Customer's identity provider, set up with Alfred's team.

Encryption

— Connector credentials (mailbox, CRM, ERP, invoicing and file-storage logins) encrypted at rest using AWS KMS envelope encryption, scoped per tenant and per connector. User passwords are stored only as one-way hashes.

— Data in transit encrypted via TLS.

Credential and Connector Safety

— Automatic suspension of a connector after repeated consecutive authentication failures, with administrator alerting.

— Deploy-safety checks confirming code actually running in production matches what was intended to be deployed.

— Inbound emails and files are checked for hidden instructions aimed at the AI; a file with hidden text is never used, and an email with suspected instructions is flagged to the administrators.

— A file that looks like a password or key store is never used in a draft or attached to a reply.

Cost and Usage Controls

— Every AI call attributed to the account it serves and logged, with a safety limit that stops drafting if an account's AI use far exceeds what its plan covers.

Human Oversight

— No message (reply or new email) is sent without explicit review and approval by a user within the Services, and nothing is written to a connected system without a user's approval: a short internal note of an exchange is written only with a reply a user has approved and sent, and an administrator can switch notes off per connector.

Organisational Measures

— Confidentiality obligations on personnel with access to Customer Personal Data.

— Staging environment separate from production for testing changes before deployment.

— Daily encrypted database backups held outside the hosting provider, in the EU.