Reconcify

Data Processing Agreement Compliance Assessment

Technical compliance analysis of the Reconcify platform against Data Processing Agreement (DPA) requirements under Art. 28 GDPR

Reconcify Platform

operated by Future Technologies SARL-S

April 2026

1. Executive Summary

This document presents a technical audit of the Reconcify platform against the requirements of a Data Processing Agreement (DPA) under Art. 28 GDPR. The audit covers security modules, encryption, data flows, and third-party integrations.

Overall Compliance Matrix

DPA SECTION	REQUIREMENT	STATUS
Section 1	Subject and Duration	Compliant
Section 2	Purpose of Processing	Compliant
Section 3	Categories of Personal Data	Compliant
Section 4	Categories of Data Subjects	Compliant
Section 5	Right of Instruction	Compliant
Section 6	Confidentiality	Compliant
Section 7	GDPR Support Obligations	Compliant
Section 8	Sub-processing	Compliant
Section 9	Data Deletion & Return	Compliant
TOM 1-3	Physical, System & Data Access Control	Compliant
TOM 4	Transfer Control	Compliant
TOM 5	Input Traceability	Compliant
TOM 6-7	Processing Control & Availability	Compliant
TOM 8	Data Separation	Compliant
TOM 9	Professional Confidentiality	Compliant

2. DPA Sections 1-5: Core Requirements

Section 1: Subject and Duration of Processing

Reconcify is a SaaS platform purpose-built for digital processing of accounting documents (invoices and bank statements). The system performs OCR, structured data extraction, bank transaction matching, and spreadsheet output. Processing duration is tied to the service agreement between the Processor and the Controller. All processing is on-demand, initiated by authenticated users.

Section 2: Purpose of Processing

The sole purpose is to support the client in performing financial bookkeeping for their mandates. The system extracts invoice data, matches it against bank transactions, and produces structured output for the tax advisor's workflow. No data is used for any other purpose, including marketing, analytics, or model training.

Section 3: Categories of Personal Data

The system processes: names and addresses (from invoices), billing and invoice data (amounts, dates, invoice numbers), bank and payment data (IBAN, transaction amounts, counterparty names), and tax-relevant business data (VAT rates, tax IDs). Payroll data is not processed by Reconcify.

Section 4: Categories of Data Subjects

Data subjects include: clients of the accounting firm, customers and suppliers of those clients (whose names appear on invoices and bank statements), and employees of the accounting firm who use the platform. The system does not process data about the general public.

Section 5: Right of Instruction

All data processing is initiated by explicit user action: the user uploads documents and submits a processing job via the web interface. The system performs no background data collection, no scheduled processing, and no autonomous analysis. Every processing run is traceable to a specific user, timestamp, and job ID. The system operates exclusively within documented instructions.

3. DPA Sections 6-9: Security, Support & Deletion

Section 6: Confidentiality

- All sensitive data encrypted at rest (AES-256-GCM) with per-organization encryption keys
- All data in transit encrypted via TLS
- Role-based access control (admin/operator) enforced at the API layer
- Optional Multi-Factor Authentication (TOTP) available for all users
- All team members bound by confidentiality obligations

Section 7: GDPR Support Obligations

- **Data portability (Art. 20):** Users can export their personal data as structured JSON
- **Consent tracking (Art. 7):** Consent recorded with timestamps and version during onboarding
- **Breach notification (Art. 33/34):** Procedure documented in Annex 3

Section 9: Data Deletion and Return (Art. 17)

- Users can delete their own account and all associated data
- Admins can delete an entire organization and all associated data (requires re-authentication)
- Uploaded files automatically purged after 90 days; audit logs after 12 months
- Upon termination of the service agreement, all data is deleted or returned per the Controller's instructions

4. Technical and Organizational Measures (TOM)

TOM 1: Physical Access Control

- Cloud-native application with no on-premise servers
- Database hosted on Supabase in Frankfurt, Germany (AWS eu-central-1)
- Application hosted on Railway

TOM 2: System Access Control

- Individual user accounts with email and password
- Email verification required before accessing the platform
- Optional TOTP-based Multi-Factor Authentication

TOM 3: Data Access Control

- Multi-tenant isolation: each organization can only access its own data
- Role-based access control (admin/operator)

TOM 4: Transfer Control

- All data transmitted exclusively over encrypted connections (TLS)
- All data in transit between the application and database remains within EU infrastructure

TOM 5: Input Traceability

- Audit logging of data access with user identity, action, IP address, and timestamp
- All data changes traceable to specific user accounts

4. Technical and Organizational Measures (continued)

TOM 6: Processing Control

- Privacy Policy and Terms of Service published and accessible
- User consent recorded during onboarding with version tracking

TOM 7: Availability Control

- Database backups managed by Supabase (Frankfurt, EU)
- Health check endpoint monitors application availability

TOM 8: Data Separation

- Organizational separation of client data at the database level
- Per-organization encryption keys

TOM 9: Confidentiality

- All personnel bound by confidentiality obligations under GDPR
- Technical confidentiality enforced through encryption and access control

5. Sub-Processors

EU DATA RESIDENCY ACHIEVED

All core data processing stays within EU jurisdiction. AI processing uses Mistral AI (Paris, France). Database and file storage use Supabase hosted in Frankfurt, Germany (aws-eu-central-1). Sub-processor DPAs are in place: Supabase signed via PandaDoc (ref: CC2YH-Q7UCC-8HEPW-TFHYL, 08 April 2026); Mistral AI, Railway, and Resend incorporate DPAs automatically via their Terms of Service.

SUB-PROCESSOR	DATA RECEIVED	REGION	DPA	STATUS
Mistral AI	Invoice documents (PDF/images), OCR text for extraction	EU (France)	legal.mistral.ai/dpa	● Via ToS
Supabase	All persisted data (users, clients, jobs, results)	EU (Frankfurt, DE)	supabase.com/legal/dpa	● Signed
Railway	Application runtime (access to all data in transit)	US / EU	railway.com/legal/dpa	● Via ToS
Resend	Emails: user names, trial status, processing stats	US (SCCs)	resend.com/legal/dpa	● Via ToS
Google Drive / Sheets *(optional integration)*	Invoice files, extraction results, match data	Google Cloud	cloud.google.com/dpa	● If enabled

6. Conclusion

COMPLIANCE STATUS

The Reconcify platform meets all requirements for a Data Processing Agreement under Art. 28 GDPR. All data encrypted at rest and in transit. EU data residency achieved: AI processing in France, database in Germany. Data processing agreements in place with all sub-processors (see Annex 2). Breach notification procedure documented (see Annex 3). The signed Supabase DPA (ref: CC2YH-Q7UCC-8HEPW-TFHYL) is provided as a separate attachment.

ANNEX Annex 2 to the Data Processing Agreement

Annex 2 - List of Authorised Sub-Processors

In accordance with Art. 28(3)(d) GDPR and Section 8 of the DPA, Future Technologies SARL-S ("Processor") discloses the following authorised sub-processors. Written data processing agreements are in place with each sub-processor, imposing data protection obligations no less protective than those in the DPA.

Supabase Inc.

● EU - Frankfurt, DE (AWS eu-central-1)

ADDRESS	PURPOSE	DPA
970 Toa Payoh North #07-04, Singapore 318992	Relational database, authentication, file storage	Art. 28 GDPR - Signed 08 Apr 2026 Ref: CC2YH-Q7UCC-8HEPW-TFHYL

Mistral AI SAS

● EU - Paris, France

ADDRESS	PURPOSE	DPA
15 rue des Halles, 75001 Paris, France	AI document OCR and structured data extraction. Data is not retained beyond the API request.	Art. 28 GDPR - Incorporated in Terms of Service

Railway Corp

● US - SCCs in place

ADDRESS	PURPOSE	DPA
548 Market St PMB 68954, San Francisco, CA 94104, USA	Application runtime hosting. Personal data passes in transit; not persistently stored by Railway.	Art. 46(2)(c) GDPR - Standard Contractual Clauses via Terms of Service

Resend Inc.

● US - SCCs in place

ADDRESS	PURPOSE	DPA
2261 Market St STE 5537, San Francisco, CA 94114, USA	Transactional email delivery (account notifications, processing status, security alerts).	Art. 46(2)(c) GDPR - Standard Contractual Clauses via Terms of Service

Google LLC *(optional integration)*

● Google Cloud - SCCs in place

ADDRESS	PURPOSE	DPA
1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA	Optional Google Drive/Sheets integration for document import and result export. Activated only when explicitly enabled by the user.	Art. 46(2)(c) GDPR - Standard Contractual Clauses (Google Cloud DPA)

CHANGE NOTIFICATION

The Processor shall notify the Controller in writing with a minimum of thirty (30) days advance notice before engaging new sub-processors or replacing existing ones, providing the Controller the opportunity to object in accordance with Art. 28(2) GDPR.

ANNEX Annex 3 to the Data Processing Agreement

Annex 3 - Breach Notification Procedure

1. Contact Person

Name	Bruno Soric
Position	Managing Director, Future Technologies SARL-S
Email	info@reconcify.io

2. Obligations Under Art. 33/34 GDPR

In the event of a personal data breach, the Processor shall:

- Notify the Controller without undue delay after becoming aware of the breach
- Assist the Controller in notifying the competent supervisory authority within **72 hours** (Art. 33 GDPR), where the breach is likely to result in a risk to rights and freedoms of natural persons
- Assist the Controller in notifying affected data subjects **without undue delay** (Art. 34 GDPR), where the breach is likely to result in a high risk
- Provide the Controller with: nature of the breach, categories and estimated number of affected data subjects, likely consequences, and measures taken

3. How the Processor May Become Aware of a Breach

- **Sub-processor notification:** Supabase is contractually obligated to notify the Processor within 48 hours of a security incident (per signed DPA, clause 10.1). Mistral AI is similarly obligated under their DPA terms.
- **User report:** A user reports suspicious activity on their account
- **Log review:** The platform maintains audit logs of data access (user, action, IP address, timestamp) that can be reviewed to investigate reported incidents

The platform does not operate real-time intrusion detection or automated breach alerting. It cannot independently detect if a user's credentials have been compromised and used by an unauthorized party.