

Fraudfinder Ltd – Privacy Notice (2026 Edition)

Last updated: 12 August 2026

1. Who We Are

Fraudfinder Ltd ("Fraudfinder", "we", "us") is a private limited company registered in England and Wales (Company No. 10531940) with its registered office in London, UK. We provide AI-powered document-fraud-detection and risk-analysis technology through our portal, APIs, and authorised partners (the "Platform").

For data-protection purposes, Fraudfinder acts:

- as a Processor when handling documents and data supplied by our business clients; and
- as a Joint Controller with those clients in relation to aggregated analytics, fraud-pattern intelligence, and AI-model training derived from those documents.

You can contact us at support@fraudfinderaai.com for any privacy-related query.

2. The Data We Process

We process personal data contained in financial and utility documents uploaded by our clients or their end-users. Typical categories include:

Service	Description	Categories of Personal Data
Document Fraud Check	Assess authenticity of financial and utility documents.	Document images, extracted text, account numbers, names, and metadata.
Data Extraction	Retrieve and structure transactions from bank statements.	Name, account holder, sort code, account number, financial transactions.
Growth Add-on Package	Premium features: API access, archive, and transaction extractions.	As above plus usage metadata.
Enterprise Add-on Package	Growth features + optional ID Checks, AI Training Opt-Out, and Data Deletion on demand.	Identity and financial data, as applicable.
ID Check (Sumsb)	Identity verification through our partner Sumsb.	ID images, extracted text, facial or liveness data processed by Sumsb.
Confirmation of Payee (Creditsafe)	Confirms account name vs bank details.	Name, account number, sort code, IBAN (if applicable).

We also collect technical data (IP address, device type, browser, usage logs) for security and service monitoring.

3. How We Use Personal Data

We use personal data to:

- Deliver, maintain, and improve our Services.

- Detect, prevent, and investigate fraud or misuse.
- Develop and improve our fraud-detection models using submitted documents. Customers may opt out of model training via the relevant Add-on Package.
- Provide customer support and account management.
- Comply with legal and regulatory obligations.

Lawful Bases (Article 6 UK GDPR)

- Contractual necessity – processing required to deliver the fraud-detection Services, including analysing documents and generating results.
- Legitimate interests – security, fraud prevention, analytics, maintaining and improving fraud-detection models using customer-submitted documents (unless the customer has opted out via the relevant Add-on Package).
- Consent – for optional marketing communications.
- Legal obligation – where disclosure is required by law or regulator.

4. Joint-Controller Activities

For aggregated and AI-training purposes, Fraudfinder and each business client jointly determine:

- what categories of anonymised data contribute to model training;
- how that data is aggregated or pseudonymised; and
- the safeguards applied.

Fraudfinder is solely responsible for managing the AI-model environment, and the client remains responsible for the legality of initial data collection. Derived datasets, machine-learning weights, and related analytics are owned exclusively by Fraudfinder. All AI-model development and operation takes place within Fraudfinder's own environment hosted in the United Kingdom (see Section 5).

5. Sharing and Sub-Processors

We engage carefully selected sub-processors for hosting, processing, and communications:

Category	Supplier	Purpose
Hosting & Infrastructure	Amazon Web Services (UK/EEA)	Cloud hosting, secure data storage, and operation of our AI fraud-detection models.
OCR Text Extraction	Google Cloud (Netherlands, EEA)	Optical character recognition (text extraction) from submitted documents.
Identity Verification	Sumsb (EU)	ID checks for clients who enable this feature.
Confirmation of Payee	Creditsafe (UK)	Validating bank-account ownership for clients who enable this feature.
Messaging	Twilio – SendGrid (Global)	Transactional email notifications (email addresses only).
Security & Delivery	Cloudflare (Global edge network)	CDN, DNS and DDoS/WAF protection (data in transit only).

Monitoring	Sentry (EEA/US)	Application error and performance monitoring (diagnostic/technical data only).
------------	-----------------	--

All sub-processors are bound by written data-processing agreements consistent with UK GDPR Article 28. A current sub-processor registry is available on request.

6. International Transfers

All client documents and the personal data they contain are stored and processed within the United Kingdom and EEA. Limited operational data (such as email addresses used for transactional notifications, and technical diagnostic data) may be processed outside the UK/EEA by the suppliers identified in Section 5; where this occurs it is safeguarded by ICO/EU-approved Standard Contractual Clauses or an applicable adequacy decision.

7. Data Retention

Client Data is retained for up to six years from the date of upload unless deleted sooner on request. Enterprise clients may delete data on demand at any time, including programmatically via the API. Aggregated or anonymised data used for model training may be retained indefinitely, as it no longer constitutes personal data.

8. Security

Fraudfinder applies controls aligned with ISO 27001 and NCSC guidance, and is Cyber Essentials certified:

- AES-256 encryption at rest and TLS 1.2+ in transit;
- role-based access control and multi-factor authentication;
- continuous monitoring and annual independent penetration testing;
- daily backups and tested disaster-recovery plans.

9. Your Rights

Individuals have the following rights under UK data-protection law:

- Access – receive a copy of your data.
- Rectification – correct inaccurate information.
- Erasure – request deletion where legally possible.
- Restriction – limit processing in specific circumstances.
- Portability – receive your data in a structured format.
- Objection – object to processing based on legitimate interests.
- Complaint – lodge a complaint with the Information Commissioner’s Office (ICO) at ico.org.uk.

Requests can be sent to support@fraudfinderaid.com. Fraudfinder is registered with the ICO under registration reference ZA230074.

10. Automated Decision-Making and AI

Fraudfinder's models analyse submitted documents and generate a recommendation (Accept, Consider, or High Risk) together with the specific indicators detected. Recommendations assist clients in identifying potentially fraudulent documents; decisions are not made solely by automated means, and clients are expected to include human review before taking adverse action. We continuously test models for accuracy and fairness and do not use outputs for profiling individuals for marketing or credit purposes.

11. Marketing and Communications

We may send service-related or administrative emails that you cannot opt out of, and optional marketing communications that require consent. You can withdraw marketing consent at any time via unsubscribe links or by contacting us.

12. Changes to This Notice

We may update this Privacy Notice to reflect operational or legal changes. The latest version will always appear at fraudfinderai.com/privacy and the revision date will be updated.

13. Contact Us

For all privacy queries or to exercise your rights:

Email: support@fraudfinderai.com

Post: Fraudfinder Ltd, 71-75 Shelton Street, WC2H 9JQ, London, United Kingdom