FAST LEDGER LIMITED

PRIVACY POLICY

Version 1.0 | Effective Date: 22nd April 2026

1. INTRODUCTION AND IDENTITY OF THE DATA CONTROLLER

1.1 Fast Ledger Limited ("Fast Ledger", "we", "us" or "our") is a company incorporated in England and Wales, (company number 15114353), with its registered office at Unit 30 The Business Village, Wexham Road, Slough, England, SL2 5HF. We can be contacted at support@fastledger.co.uk.

1.2 Fast Ledger operates the Fast Ledger cloud-based accounting and business management platform (the "Platform"), accessible at fastledger.info.

1.3 This Privacy Policy explains how we collect, use, share, store and otherwise process personal data in connection with your use of the Platform, our website and any related services we provide. It has been prepared in accordance with the UK General Data Protection Regulation as defined in the Data Protection Act 2018 ("UK GDPR"), the Data Protection Act 2018 ("DPA 2018"), and the Privacy and Electronic Communications Regulations 2003 ("PECR"). In respect of our Spanish Users only, this Privacy Policy also addresses our obligations under Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU GDPR") and the Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales ("LOPDGDD").

1.4 This Privacy Policy applies to: (a) business customers and their authorised users who register for and use the Platform ("Customers"); (b) visitors to our website at fastledger.info; and (c) individuals whose personal data is uploaded to the Platform by Customers.

1.5 Please read this Privacy Policy carefully. If you do not agree with its terms, you should not access or use the Platform.

2. OUR ROLE AS DATA CONTROLLER AND DATA PROCESSOR

2.1 Fast Ledger operates in a dual capacity in relation to personal data:

2.2 Data Controller. We are an independent data controller in respect of personal data we collect and process for our own purposes, including: account registration and management; billing and payment administration; customer support; marketing and communications (where consented); and the improvement and security of the Platform. Our processing in this capacity is described in full in this Privacy Policy.

2.3 Data Processor. We act as a data processor when we process personal data uploaded or inputted by our Customers ("Customer Data") on their behalf, for the purposes of providing the Platform and its features. In this capacity, we process Customer Data only on the documented instructions of the relevant Customer, as set out in our Terms and Conditions of Service and any applicable data processing addendum. Customers, in their capacity as data controllers, are responsible for ensuring that their collection and upload of Customer Data to the Platform is lawful and that appropriate notices have been given to relevant data subjects.

2.4 Where third parties (such as the clients of our accounting or solicitor firm Customers) have their personal data uploaded to the Platform by our Customers, Fast Ledger's obligations as a data processor apply in respect of such data. Such third parties should direct any queries or requests regarding their personal data to the Customer who controls that data in the first instance.

3. WHAT PERSONAL DATA WE COLLECT

3.1 Account and Registration Data. When you register for the Platform, we collect: full name; business name and type; registered address; email address; telephone number; job title or role; and password (stored in encrypted form).

3.2 Billing and Payment Data. We collect billing address, subscription tier and payment method details. Full payment card information is processed by our payment processor and is not stored on our systems.

3.3 Financial and Accounting Data. When you use the Platform, we process the transaction data, bank statements, invoices, receipts, accounting records and other financial information that you upload, input or import via Open Banking connectivity or CSV file upload. This data may include your clients' financial information and may constitute Customer Data over which you are the data controller.

3.4 HMRC and Tax Data. Where you use the Platform's Making Tax Digital integration, we process the tax return data, UTR numbers, VAT registration numbers, business income and expenditure data and other tax-relevant information required to facilitate your HMRC submissions.

3.5 Audio and Transcription Data. Where you use the Transcription Services, we process audio recordings of conversations, meetings and other audio content that you upload or record through the Platform. Audio may include the voices and speech of third parties, including your clients and business contacts. Transcriptions of such audio are also processed and stored.

3.6 Communications and Document Data. Where you use the Platform's communication, email storage and document management features, we process the content of client communications, emails, documents and other materials you store or share via the Platform. Such data will frequently constitute Customer Data and may include the personal data of your clients and business contacts.

3.7 Usage and Technical Data. We automatically collect certain technical information when you access the Platform, including: IP address; browser type and version; device type and operating system; session duration and pages accessed; referring URLs; and error logs. This data is used for security monitoring, debugging and product improvement.

3.8 Communication Data. We collect records of your communications with us, including support requests, feedback and survey responses.

3.9 Cookie Data. We collect data via cookies and similar technologies as described in our Cookie Policy.

4. HOW WE COLLECT PERSONAL DATA

4.1 Directly from you. We collect personal data that you provide to us directly when you register for the Platform, set up your account, configure your Subscription, contact our support team, respond to surveys, or otherwise interact with us.

4.2 Through your use of the Platform. We collect personal data generated through your use of the Platform, including usage data, transaction data imported via Open Banking or CSV upload, audio recordings submitted via the Transcription Services, and communications stored within the Platform.

4.3 From third parties. We may receive personal data about you from: your bank or Open Banking provider (via the bank feed integration); HMRC (in the course of MTD submissions); our payment processor; and analytics service providers.

4.4 From your customers and clients. Personal data relating to your clients and business contacts is uploaded to the Platform by you in your capacity as a data controller. Fast Ledger receives and processes such data in its capacity as data processor on your behalf.

5. LAWFUL BASIS FOR PROCESSING

5.1 We process personal data only where we have a lawful basis for doing so under the UK GDPR (and, where applicable, the EU GDPR). The following table sets out the categories of processing and the lawful basis relied upon:

Processing Activity | Lawful Basis | *Details*

Account registration and management | Contract (Art. 6(1)(b)) | *Necessary to perform the contract with you*

Provision of Platform services | Contract (Art. 6(1)(b)) | *Necessary to deliver the service you have subscribed to*

Billing and payment processing | Contract (Art. 6(1)(b)) | *Necessary to manage your subscription and invoicing*

HMRC/MTD integration and tax submissions | Legal obligation (Art. 6(1)(c)) | *Facilitating your legal tax reporting obligations*

Security monitoring and fraud prevention | Legitimate interests (Art. 6(1)(f)) | *Our legitimate interest in protecting the Platform and users*

Product improvement using anonymised data | Legitimate interests (Art. 6(1)(f)) | *Our legitimate interest in developing and improving the Platform*

Processing of audio/transcription data | Consent (Art. 6(1)(a)) / Contract | *Your consent and/or contractual arrangement with participants*

Marketing communications (existing customers) | Legitimate interests (Art. 6(1)(f)) | *Right to opt out at any time*

Marketing communications (new subscribers) | Consent (Art. 6(1)(a)) | *Only where you have opted in*

Compliance with legal obligations | Legal obligation (Art. 6(1)(c)) | *Including tax, regulatory and judicial requirements*

Customer Data processed on your behalf | Contract with Customer (processor basis) | *On Customer's instructions as data processor*

5.2 Where we rely on legitimate interests as our lawful basis, we have carried out a balancing test to ensure that our legitimate interests are not overridden by the interests or fundamental rights and freedoms of data subjects. You may request further information about any such balancing test by contacting us.

5.3 Where we rely on consent as our lawful basis, you have the right to withdraw that consent at any time without affecting the lawfulness of processing carried out before withdrawal. To withdraw consent, please contact us at support@fastledger.co.uk.

6. PURPOSES FOR WHICH WE USE PERSONAL DATA

We use personal data for the following purposes:

6.1 To create and manage your account and to administer your Subscription.

6.2 To provide, operate, maintain and improve the Platform and all features and services available within it, including accounting tools, bank feed connectivity, HMRC integration, invoice management, stock management, AI transcription, electronic signatures, and communication and document management functionality.

6.3 To process your payments and manage your billing arrangements.

6.4 To facilitate the submission of VAT returns and income tax information to HMRC through the Making Tax Digital integration, acting solely on your instructions.

6.5 To transmit audio recordings to our third-party AI transcription provider (Deepgram, Inc.) for the purpose of generating transcriptions where you use the Transcription Services.

6.6 To monitor and maintain the security of the Platform and to detect, investigate and prevent fraudulent activity, misuse or unauthorised access.

6.7 To respond to your enquiries, support requests and communications.

6.8 To send you service-related communications, including notifications about your Subscription, renewals, updates and changes to this Privacy Policy or our Terms and Conditions.

6.9 To send marketing communications where we are permitted to do so by applicable law, including communications about new features, products or services that may be of interest to you. You may opt out of marketing communications at any time by following the unsubscribe instructions in any such communication or by contacting us.

6.10 To comply with our legal and regulatory obligations, including compliance with HMRC requirements, the Data Protection Legislation, and any orders or requirements of regulatory or judicial authorities.

6.11 To exercise or defend our legal rights in connection with any dispute or legal proceedings.

6.12 To produce anonymised and aggregated statistical data for product development and analysis purposes.

7. SHARING OF PERSONAL DATA — SUB-PROCESSORS AND THIRD PARTIES

7.1 We do not sell, rent or otherwise trade personal data to or with third parties for commercial purposes. We share personal data only in the circumstances set out below.

7.2 Sub-processors. As a data processor of Customer Data, we appoint certain third-party sub-processors who process Customer Data on our behalf. We have entered into appropriate data processing agreements with each of our sub-processors. Our current sub-processors include:

(a) Deepgram, Inc. (United States) — AI transcription of audio data uploaded by Customers using the Transcription Services. International transfer safeguard: Standard Contractual Clauses (UK Addendum and EU SCCs as applicable).

(b) Open Banking service providers (United Kingdom / European Economic Area) — facilitating bank feed connectivity. Such providers are FCA-authorised Account Information Service Providers and are subject to their own regulatory obligations.

(c) Payment processors (United Kingdom / European Economic Area) — processing Subscription payments and managing billing. Payment data is processed in accordance with the Payment Card Industry Data Security Standard (PCI-DSS).

(d) Web hosting and cloud infrastructure providers (United Kingdom / European Economic Area) — hosting the Platform and storing Customer Data.

(e) Analytics providers — aggregated and pseudonymised usage analytics for platform improvement.

7.3 HMRC. Where you use the Making Tax Digital integration, we transmit your tax data to HMRC on your instructions. Such transmission is made at your express direction and HMRC is an independent data controller in respect of the data it receives.

7.4 Legal and regulatory disclosures. We may disclose personal data to regulatory authorities, law enforcement agencies or courts of competent jurisdiction where required to do so by applicable law, regulation or court order.

7.5 Business transfers. In the event of a merger, acquisition, restructuring or sale of all or substantially all of Fast Ledger's business or assets, personal data may be transferred to the relevant acquirer or successor entity, subject to that entity assuming our obligations under this Privacy Policy.

7.6 Professional advisers. We may share personal data with our legal advisers, accountants and insurers on a confidential basis where reasonably necessary for the conduct of our business.

8. INTERNATIONAL TRANSFERS OF PERSONAL DATA

8.1 The United Kingdom and the European Economic Area maintain restrictions on the transfer of personal data to countries that do not ensure an adequate level of data protection. Certain of our sub-processors are located in, or may process data in, countries outside the UK and/or EEA.

8.2 Transfer to the United States — Deepgram. Audio data processed through the Platform's Transcription Services is transmitted to Deepgram, Inc., a company incorporated in the United States. This transfer is made on the basis of Standard Contractual Clauses approved by the European Commission (as incorporated into UK law by the UK Addendum to the International Data Transfer Agreement issued by the ICO). We have assessed the laws and practices of the United States in connection with this transfer and are satisfied that, in combination with the Standard Contractual Clauses and Deepgram's technical and organisational security measures, an adequate level of protection is provided for the personal data transferred.

8.3 All other personal data processed through the Platform is hosted and stored within the United Kingdom or the European Economic Area, unless otherwise notified.

8.4 You may request further information about the safeguards applicable to specific international transfers by contacting us at support@fastledger.co.uk.

9. DATA RETENTION PERIODS

9.1 We retain personal data only for as long as is necessary to fulfil the purposes for which it was collected, having regard to our legal obligations, legitimate business interests and your rights as a data subject. Our principal retention periods are as follows:

(a) Account and registration data: retained for the duration of your Subscription and for a period of six (6) years following termination, to comply with our legal and tax obligations.

(b) Financial and accounting data (including transaction records, invoices and tax return data): retained for a minimum of six (6) years following the end of the relevant tax year, in accordance with HMRC requirements under the Taxes Management Act 1970 and applicable accounting standards.

(c) Audio recordings and transcription data: retained for the duration of your Subscription and for a further period of twelve (12) months following termination, unless you configure a shorter retention period within the Platform or request deletion earlier.

(d) Communications and document data: retained for the duration of your Subscription and for a period of twelve (12) months following termination, or for such longer period as required by applicable law.

(e) Billing and payment data: retained for six (6) years following the relevant transaction, in accordance with our legal obligations under the Value Added Tax Act 1994 and other applicable financial record-keeping requirements.

(f) Usage and technical data: retained for a period of twelve (12) months, unless required for longer for security or legal purposes.

(g) Marketing consent records: retained for the duration of your relationship with us and for a period of three (3) years thereafter, to evidence compliance with applicable law.

9.2 On termination or expiry of your Subscription, we will make your Customer Data available for export for a period of thirty (30) days. Following that period, we will delete or anonymise your Customer Data unless we are required by law to retain it.

9.3 Where we are required by law to retain data for a specific minimum period, we will retain it for that period regardless of any request for earlier deletion, except where permitted by applicable law.

10. DATA SECURITY

10.1 We implement and maintain appropriate technical and organisational security measures to protect personal data against unauthorised or unlawful access, processing, disclosure, alteration, loss or destruction. Our security measures include, without limitation:

(a) encryption of data in transit using Transport Layer Security (TLS);

(b) encryption of data at rest on our servers;

(c) access controls and role-based permissions limiting access to personal data to authorised personnel only;

(d) multi-factor authentication requirements for administrative access;

(e) regular security audits and vulnerability assessments;

(f) personnel training on data protection and information security; and

(g) incident response and data breach notification procedures.

10.2 We require all sub-processors to implement security measures equivalent to or greater than those described in Clause 10.1.

10.3 Notwithstanding the above, no method of transmission over the internet or method of electronic storage is completely secure. We cannot guarantee the absolute security of personal data and encourage you to take your own precautions, including by maintaining strong account passwords and enabling any multi-factor authentication offered through the Platform.

10.4 In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals, we will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, in accordance with our obligations under the UK GDPR. We will also notify affected data subjects where the breach is likely to result in a high risk to their rights and freedoms. For Spanish Users, we will also notify the Agencia Española de Protección de Datos (AEPD) where required under the EU GDPR and LOPDGDD.

11. YOUR RIGHTS AS A DATA SUBJECT

11.1 Under the Data Protection Legislation, you have the following rights in respect of your personal data, which you may exercise by contacting us at support@fastledger.co.uk:

11.2 Right of Access (Subject Access Request). You have the right to request a copy of the personal data we hold about you and information about how we process it. We will respond to

all valid Subject Access Requests within one (1) calendar month of receipt, or within three (3) months where the request is complex or numerous.

11.3 Right to Rectification. You have the right to require us to correct any inaccurate personal data we hold about you, and to complete any incomplete data, without undue delay.

11.4 Right to Erasure (Right to be Forgotten). You have the right to request the deletion of your personal data where: the data is no longer necessary for the purposes for which it was collected; you withdraw consent on which processing is based and there is no other lawful basis; you object to processing and there are no overriding legitimate grounds; or the data has been unlawfully processed. This right is subject to our legal obligations to retain certain data as described in Clause 9.

11.5 Right to Restriction of Processing. You have the right to request that we restrict processing of your personal data in certain circumstances, including where the accuracy of the data is contested, where processing is unlawful but you do not wish the data to be deleted, or where we no longer need the data but you require it for the establishment, exercise or defence of legal claims.

11.6 Right to Data Portability. You have the right to receive personal data you have provided to us in a structured, commonly used and machine-readable format, and to transmit that data to another data controller, where processing is based on contract or consent and is carried out by automated means.

11.7 Right to Object. You have the right to object to our processing of your personal data where that processing is based on legitimate interests, including profiling based on legitimate interests. You also have an absolute right to object to processing for direct marketing purposes. Where you object to processing for direct marketing, we will cease such processing immediately.

11.8 Rights in Relation to Automated Decision-Making and Profiling. You have the right not to be subject to a decision based solely on automated processing (including profiling) which produces legal or similarly significant effects, unless such processing is necessary for the performance of a contract with you or is authorised by applicable law. We do not currently engage in such automated decision-making.

11.9 Right to Withdraw Consent. Where we process personal data on the basis of your consent, you have the right to withdraw that consent at any time. Withdrawal of consent will not affect the lawfulness of processing carried out prior to withdrawal.

11.10 Right to Lodge a Complaint. You have the right to lodge a complaint with the relevant supervisory authority if you believe we have processed your personal data in breach of applicable data protection law. For UK-based data subjects, the relevant authority is the Information Commissioner's Office (ICO), which can be contacted at ico.org.uk or on 0303 123 1113. For Spanish data subjects, the relevant authority is the Agencia Española de Protección de Datos (AEPD), which can be contacted at aepd.es. We would, however, appreciate the opportunity to address your concerns before you approach a supervisory authority and invite you to contact us in the first instance.

12. CUSTOMER DATA AND THIRD-PARTY DATA SUBJECTS

12.1 Where personal data relating to your clients, employees or other third parties is uploaded to the Platform by you in your capacity as a data controller, you are responsible for ensuring compliance with the Data Protection Legislation in respect of such data, including providing appropriate privacy notices to those individuals and establishing a lawful basis for processing.

12.2 Where a third party whose personal data has been uploaded to the Platform by you submits a data subject rights request (for example, a request for access or erasure) to Fast Ledger, Fast Ledger will refer that request to you as the relevant data controller. Fast Ledger

will provide such reasonable assistance as is necessary to enable you to respond to data subject requests in accordance with the Data Protection Legislation.

12.3 You shall indemnify Fast Ledger against all losses, costs, expenses and liabilities arising from any failure by you to comply with your data protection obligations in respect of Customer Data.

13. AUDIO TRANSCRIPTION DATA — SPECIAL OBLIGATIONS

13.1 The use of the Platform's AI Transcription Services involves the processing of audio recordings, which may constitute personal data (and in some circumstances biometric data) of the individuals whose voices are captured. This gives rise to significant obligations under the Data Protection Legislation.

13.2 Before using the Transcription Services to record or process audio that includes the speech of any third party (including clients, colleagues or other meeting participants), you must:

(a) ensure that you have a valid lawful basis under Article 6 UK GDPR (and, where applicable, Article 9 UK GDPR if the recording may capture sensitive personal data) for processing the audio data;

(b) provide clear, timely and adequate notice to all individuals who will be recorded that their voice is being recorded and that the recording will be processed by an AI transcription provider located in the United States;

(c) obtain explicit consent from all individuals who will be recorded where consent is the lawful basis relied upon; and

(d) ensure that any recordings or transcriptions are retained only for as long as necessary and are securely deleted in accordance with your data retention obligations.

13.3 Fast Ledger will transmit audio data to Deepgram, Inc. in the United States for transcription processing. Deepgram acts as a sub-processor of such data and is subject to a data processing agreement incorporating Standard Contractual Clauses. Deepgram's own privacy policy and compliance documentation is available at deepgram.com/privacy.

13.4 Fast Ledger will not use audio recordings or transcriptions for any purpose other than providing the Transcription Services within the Platform, except to the extent anonymised and aggregated data may be used for product improvement purposes.

14. COOKIES AND SIMILAR TECHNOLOGIES

14.1 We use cookies and similar tracking technologies on our website and Platform. Full details of the cookies we use, the purposes for which we use them and how you can manage your cookie preferences are set out in our Cookie Policy, available at fastledger.info/cookies.

14.2 We will not set non-essential cookies without your prior consent, which you may provide or withdraw via the cookie consent banner on our website or within your account settings.

15. EUROPEAN UNION REPRESENTATIVE

15.1 Fast Ledger Limited is a UK-established company. We currently serve customers in Spain, which means that we offer services to data subjects located in the European Union. Pursuant to Article 27 of the EU GDPR, companies established outside the EU that offer goods or services to individuals within the EU are required to designate a representative within the EU.

15.2 Fast Ledger Limited has designated, or is in the process of designating, an EU representative for the purposes of Article 27 EU GDPR. Details of our EU representative will be published on our website at fastledger.info/legal and will be updated as soon as the appointment is complete. Spanish Users and the AEPD may direct EU GDPR-related enquiries to our EU representative once appointed.

15.3 Spanish Users may also direct data protection queries directly to Fast Ledger at support@fastledger.co.uk in the interim. The designation of an EU representative does not limit or exclude Fast Ledger's own data protection obligations under the EU GDPR.

16. CHILDREN'S DATA

16.1 The Platform is designed for use by businesses and individuals acting in the course of their trade or profession. The Platform is not directed at, and should not be accessed or used by, any person under the age of 18 years.

16.2 We do not knowingly collect or process personal data of individuals under the age of 18. If we become aware that we have inadvertently collected personal data from an individual under the age of 18 without appropriate parental or guardian consent, we will take steps to delete such data as soon as reasonably practicable.

16.3 If you are a parent or guardian and believe that a minor has provided us with personal data without your consent, please contact us at support@fastledger.co.uk.

17. DIRECT MARKETING COMMUNICATIONS

17.1 Where you are an existing Customer, we may send you marketing communications by email about our products, services and features that are similar to those you have subscribed to, on the basis of our legitimate interests, unless you have opted out. You may opt out of such communications at any time by clicking the unsubscribe link in any marketing email or by contacting us.

17.2 Where you are not yet a Customer but have provided your contact details to us (for example, via an enquiry form), we will only send you marketing communications where you have given your explicit consent. You may withdraw that consent at any time.

17.3 We will never sell or share your contact details with third parties for their marketing purposes.

17.4 Our marketing communications comply with the Privacy and Electronic Communications Regulations 2003 (PECR) and, in respect of Spanish Users, with the applicable provisions of the Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico (LSSI).

18. CHANGES TO THIS PRIVACY POLICY

18.1 We may update this Privacy Policy from time to time to reflect changes in applicable law, our business practices or the features of the Platform. Where changes are material, we will provide you with prominent notice, which may be by email, in-platform notification or by posting a notice on our website, prior to the change taking effect.

18.2 The date at the top of this Privacy Policy indicates when it was last updated. Your continued use of the Platform following notification of a material change to this Privacy Policy shall constitute your acceptance of the updated policy.

19. LINKS TO THIRD-PARTY WEBSITES AND SERVICES

19.1 The Platform may contain links to, or integrations with, third-party websites, services and applications. This Privacy Policy does not apply to the privacy practices of those third parties. We encourage you to review the privacy policies of any third party whose services you access in connection with the Platform.

19.2 Fast Ledger has no responsibility for, and does not control, the data processing practices of third parties including HMRC, Open Banking providers, Deepgram, payment processors or other integrated services. Your use of such third-party services is subject to those parties' own privacy policies and terms of service.

20. HOW TO CONTACT US AND EXERCISE YOUR RIGHTS

20.1 If you have any questions, concerns or complaints regarding this Privacy Policy or our processing of your personal data, or if you wish to exercise any of your rights as described in Clause 11, please contact us:

By email: support@fastledger.co.uk

By post: Data Protection Enquiries, Fast Ledger Limited, Unit 30 The Business Village, Wexham Road, Slough, England, SL2 5HF

20.2 We will acknowledge receipt of your request within five (5) Business Days and will respond in full within one (1) calendar month of receipt of a valid request, or within three (3) months where the request is complex or numerous, in which case we will notify you of the extended timescale within the initial one-month period.

20.3 Supervisory Authorities. If you are dissatisfied with our response to any data protection concern, you have the right to lodge a complaint with the relevant supervisory authority:

United Kingdom: Information Commissioner's Office (ICO) — ico.org.uk / 0303 123 1113

Spain: Agencia Española de Protección de Datos (AEPD) — aepd.es