

Data Processing Agreement

Last updated September 10, 2026

This Data Processing Agreement ("DPA") is entered into by and between the Subscriber and Xelpmoc Design and Tech Limited, a public limited company incorporated under the Companies Act, 2013 and having its registered office at No. 57, 13th Cross, Novel Business Park, Hosur Road, Anepalya, Adugodi, Bangalore – 560030, Karnataka, India ("Company"). This DPA forms part of, and is incorporated by reference into, the General Terms of Subscription between the Company and the Subscriber (the "Agreement"), and supplements the Company's Privacy Policy. This DPA applies to the extent the Company processes Personal Data on behalf of the Subscriber, as a service provider or processor, in connection with the Services.

This DPA is a standard document that applies uniformly to all Subscribers by reference in the Agreement, in the same way as the Privacy Policy. It becomes effective on the date the Subscriber accepts the Agreement and remains in effect for as long as the Company processes Personal Data on the Subscriber's behalf. Capitalised terms used but not separately defined in this DPA have the meanings given to them in the Agreement or the Privacy Policy.

Definitions

In addition to the terms defined in the Agreement and the Privacy Policy, for purposes of this DPA:

- **Applicable Data Protection Laws.** means the CCPA and the other U.S. State Privacy Laws (each as defined in the Privacy Policy), and any other data protection or privacy law applicable to the Company's processing of Personal Data on the Subscriber's behalf under this DPA, in each case as amended, replaced, or supplemented from time to time.
- **Business and Service Provider.** have the meanings given to those terms under the CCPA. As between the Company and the Subscriber, and for the specific

processing activities described in the "Roles of the Parties" section below, the Subscriber acts as a Business and the Company acts as a Service Provider. This DPA does not apply to processing for which the Company acts as a Business in its own right, as described in the "Roles of the Parties" section below and in the Company's CCPA Privacy Notice.

- **Data Subject.** means an identified or identifiable natural person whose Personal Data is processed by the Company on the Subscriber's behalf under this DPA, including an Authorised User, an End Client, or another individual whose information is contained in Subscriber Data or End Client Data (each as defined in the Agreement).
- **Security Incident.** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data processed by the Company on the Subscriber's behalf.
- **Sub-processor.** means a third party engaged by the Company to process Personal Data on the Subscriber's behalf in connection with the Services, as further described in the "Sub-processors" section below.

Roles of the Parties

Where the Company processes Personal Data on the Subscriber's documented instructions to provide the Services, the Company acts as a Service Provider and the Subscriber acts as a Business, each under the CCPA. This includes, in particular: uploading, extracting, analysing, classifying, and otherwise processing documents and data submitted by the Subscriber through the Services, including through the Company's use of Google LLC's artificial intelligence and machine learning API services; storing documents that the Subscriber elects to retain using DocuVault; and retrieving or synchronising data through the Subscriber's connected Google Drive or QuickBooks account, including pushing sales and cost transaction records to, and, where the Subscriber uses the Platform's upload-to-QuickBooks feature, transmitting source document attachments to, the Subscriber's connected QuickBooks account, in each case only as authorised and instructed by the Subscriber. This DPA governs the Company's processing of Personal Data in this capacity.

This DPA does not apply to Personal Data the Company processes as a Business in its own right, including in relation to: creating, administering, authenticating, and billing Subscriber and Authorised User accounts; sending service, administrative, and marketing communications; measuring website and in-app interactions through Google Analytics, Google Ads, Google's Display Network, Taboola, Inc., and Outbrain Inc.; measuring website and in-app interactions, and providing session replay, through PostHog Inc.; monitoring the security, integrity, and performance of the Services across all Subscribers; and complying with the Company's own legal, regulatory, and contractual obligations. The Company's role in respect of that processing is described in the Privacy Policy and the CCPA Privacy Notice, not in this DPA.

Summary of the Company's Obligations as Service Provider

Where this DPA applies, the Company:

- processes Personal Data only on the Subscriber's documented instructions, as described in the "Instructions" section below;
- keeps Personal Data confidential, as described in the "Confidentiality" section below;
- implements the security measures described in the "Security Measures" section below;
- engages Sub-processors only as authorised and subject to flow-down obligations, as described in the "Sub-processors" section below;
- does not use Personal Data to train or improve artificial intelligence or machine-learning models across Subscribers, except as described in the "Artificial Intelligence and Machine Learning Restriction" section below;
- provides reasonable assistance with Data Subject and Consumer rights requests, as described in the "Assistance with Rights Requests" section below;
- notifies the Subscriber of Security Incidents, as described in the "Security Incident Notification" section below;
- deletes or returns Personal Data at the end of the provision of Services, as described in the "Deletion and Return of Data" section below; and

- makes available information, and allows and contributes to audits, as described in the "Audits and Information" section below.

Instructions

The Company shall process Personal Data only on the Subscriber's documented instructions, which are deemed to include the instructions reflected in the Agreement, this DPA, the Privacy Policy, and the Subscriber's configuration and use of the Services, including the Subscriber's decisions to connect a Google Drive or QuickBooks account or to store documents using DocuVault.

Where the Company is required by applicable law to process Personal Data other than on the Subscriber's instructions, the Company shall, unless prohibited from doing so, inform the Subscriber of that legal requirement before carrying out the relevant processing. The Company shall promptly notify the Subscriber if, in the Company's opinion, an instruction from the Subscriber infringes Applicable Data Protection Laws.

Details of Processing

The subject matter, duration, nature and purpose of processing, and the categories of Data Subjects and Personal Data processed under this DPA, are set out in Schedule 1.

Confidentiality

The Company shall ensure that personnel authorised to process Personal Data on the Subscriber's behalf are subject to a duty of confidentiality, whether contractual or statutory, and process Personal Data only to the extent necessary for their role in providing the Services.

Security Measures

The Company shall implement the technical and organisational security measures described in the "Security Measures" section of the Privacy Policy and the "Security" section of the Agreement, having regard to the state of the art, the costs of

implementation, and the nature, scope, context, and purposes of processing, as well as the risk to Data Subjects.

As with the Agreement and the Privacy Policy, the Company does not guarantee that its security measures will be error-free or that unauthorised third parties will never defeat them, and the Company's liability in connection with a failure of its security measures is governed by the "Liability" section below.

Sub-processors

The Subscriber generally authorises the Company to engage the Sub-processors listed in Schedule 2 to process Personal Data in connection with the Services. Google Analytics, Google Ads, Google's Display Network, Taboola, Inc., and Outbrain Inc. and PostHog Inc. are not Sub-processors for purposes of this DPA: as described in the "Roles of the Parties" section above, those technologies are used by the Company in its own capacity as a Business – Google Analytics, Google Ads, Google's Display Network, Taboola, Inc., and Outbrain Inc. receive Personal Data for their own advertising and analytics purposes, while PostHog Inc. processes Personal Data solely as the Company's own analytics service provider under a signed data processing agreement – and the Company's Business role in relation to each of them is addressed in the Privacy Policy and CCPA Privacy Notice, not this DPA.

- Before engaging a new Sub-processor, or replacing an existing one, the Company shall provide the Subscriber with advance notice of at least fifteen (15) days, by posting an updated version of Schedule 2, or by such other reasonably equivalent means as the Company may adopt. If the Subscriber has a reasonable data-protection objection to the new Sub-processor, it may notify the Company of that objection within the notice period, and the parties shall discuss the objection in good faith. If the parties are unable to resolve the objection, the Subscriber's exclusive remedy is to terminate the affected Service in accordance with the Agreement.
- The Company shall impose data-protection obligations on each Sub-processor that are, in substance, no less protective of Personal Data than those set out in this DPA, having regard to the nature of the services the Sub-processor provides. The Company remains liable to the Subscriber for a Sub-processor's acts and

omissions in connection with the processing of Personal Data to the same extent the Company would be liable if performing the Sub-processor's services directly.

Artificial Intelligence and Machine Learning Restriction

The Company will not combine or use Personal Data received from or on behalf of one Subscriber to develop, improve, or train artificial intelligence or machine-learning models for the benefit of other Subscribers or the Company generally, except (i) where the underlying information has first been aggregated or de-identified, or (ii) where the Subscriber has separately and specifically authorised such use.

Where the Company uses a third-party artificial intelligence or machine-learning service, such as Google LLC's API services, to analyse, extract, or verify data from documents on the Subscriber's behalf, the Company requires that Sub-processor to be contractually restricted from using that data to train or improve its own models. Consistent with this requirement, the Company's agreement with Google LLC for these services is governed by Google's enterprise (paid) API terms, which contractually prohibit Google from using such data to train or improve its own models.

Assistance with Rights Requests

Taking into account the nature of the processing, the Company shall provide the Subscriber with reasonable assistance, by appropriate technical and organisational measures, to enable the Subscriber to respond to a verified request from a Data Subject or Consumer to exercise rights available under Applicable Data Protection Laws, including rights to know, access, correct, or delete Personal Data, or to opt out of a sale, sharing, or targeted advertising. If the Company receives such a request directly from a Data Subject or Consumer in relation to Personal Data it processes on the Subscriber's behalf, the Company may direct the individual to submit the request to the Subscriber, and shall promptly inform the Subscriber of the request, unless prohibited by law from doing so.

Security Incident Notification

If the Company becomes aware of a Security Incident affecting Personal Data it processes on the Subscriber's behalf, the Company shall notify the Subscriber without undue delay after becoming aware of the incident, consistent with the notification commitment in the "Security" section of the Agreement, and shall provide the Subscriber with information reasonably available to the Company regarding the nature and scope of the incident, to the extent the Company may lawfully do so and without prejudice to any ongoing investigation. The Company shall take reasonable steps to mitigate the effects of a Security Incident and to prevent its recurrence.

Deletion and Return of Data

On termination or expiry of the Agreement, the Company shall delete or return Personal Data it processes on the Subscriber's behalf in accordance with the "Data Retention and Deletion" section of the Privacy Policy and the "Consequences of Termination" item in the "Subscription Period, Billing and Termination" section of the Agreement, including the distinct retention treatment of Output and of documents the Subscriber has elected to store using DocuVault, subject in each case to any retention required by applicable law or expressly agreed in writing. In summary, and as more fully described in those sections: account deletion results in the immediate, permanent deletion of substantially all Personal Data the Company processes on the Subscriber's behalf, subject to a narrow set of records (historical purchase and usage data, and support correspondence) retained for audit and product-improvement purposes, and subject to DocuVault's distinct 30-day Trash-and-restore mechanism for manually deleted documents.

Audits and Information

The Company shall make available to the Subscriber information reasonably necessary to demonstrate the Company's compliance with this DPA, and shall allow for, and contribute to, audits, including inspections, conducted by the Subscriber or an independent auditor mandated by the Subscriber. Such an audit may be conducted no more than once in any twelve (12)-month period, absent a Security Incident affecting the Subscriber's Personal Data or a specific requirement of a regulator with jurisdiction over the Subscriber, on at least thirty (30) days' prior written notice, during the Company's normal business hours, subject to reasonable

confidentiality protections, and in a manner that does not unreasonably disrupt the Company's business or compromise the security of other Subscribers' data. The Company does not currently hold, and has no current plans to obtain, a third-party security certification or assessment report (such as a SOC 2 report); audits will accordingly be conducted through the on-site/inspection mechanism described above. If the Company later obtains such a certification, it may offer a summary of that certification in lieu of a full on-site audit.

International Processing

Personal Data may be processed in India, the United States, or other jurisdictions where the Company or its Sub-processors maintain facilities, systems, personnel, or operations, consistent with the "Cross-Border Transfers" section of the Privacy Policy.

This DPA does not address, and the Company does not represent that it satisfies, any cross-border transfer mechanism required under the law of a jurisdiction other than India or the United States, such as the EU General Data Protection Regulation or the UK GDPR. The Company does not currently offer the Services to, and does not knowingly process Personal Data on behalf of, Subscribers, Authorised Users, or End Clients located in the European Union, the United Kingdom, or another jurisdiction whose data protection law would require a separate transfer mechanism, and has no current plans to serve those markets. If that changes, this DPA will need a corresponding transfer-mechanism annex before the Company processes such Personal Data.

Liability

Each party's liability arising out of or in connection with this DPA, including in connection with a Security Incident or a Sub-processor's acts or omissions, is subject to, and shall not exceed, the limitation of liability and indemnification provisions of the Agreement, which are incorporated into this DPA by reference and apply to this DPA as if fully set out herein.

Term and Termination

This DPA takes effect on the date the Subscriber accepts the Agreement and remains in effect for as long as the Company processes Personal Data on the Subscriber's behalf in connection with the Services. This DPA terminates automatically on termination or expiry of the Agreement, without prejudice to any obligation under this DPA that by its nature is expressed or intended to survive termination, including the obligations described in the "Deletion and Return of Data" section above.

Precedence, Governing Law, and General

If there is a conflict between this DPA and the Agreement regarding the Company's processing of Personal Data on the Subscriber's behalf, this DPA prevails to the extent of the conflict. In all other respects, the Agreement continues to apply.

This DPA is governed by, and any dispute arising out of or in connection with it shall be resolved in accordance with, the governing law and dispute resolution provisions of the Agreement, including the agreement to arbitrate under the Arbitration and Conciliation Act, 1996, with its seat at Bangalore.

No amendment to this DPA is effective unless made in accordance with the amendment provisions of the Agreement. If any provision of this DPA is held invalid, illegal, or unenforceable, the remaining provisions continue in full force and effect, and the parties shall discuss in good faith a replacement provision that most closely achieves the intended effect of the original.

Schedule 1: Details of Processing

- **Subject matter.** The Company's provision of the FigureIQ intelligent document processing Services to the Subscriber under the Agreement.
- **Duration.** For as long as the Company processes Personal Data on the Subscriber's behalf under the Agreement, including any period Personal Data is retained after termination under the "Deletion and Return of Data" section above.
- **Nature and purpose of processing.** Uploading, extraction, analysis, classification, indexing, storage (including via DocuVault), transmission, retrieval, and reporting of documents and data submitted by or on behalf of the Subscriber, in each case

to provide the Services, as further described in the "Nature of Services" section of the Privacy Policy.

- **Categories of Data Subjects.** The Subscriber's Authorised Users, and End Clients whose information is contained in documents or data submitted by or on behalf of the Subscriber.
- **Categories of Personal Data.** As described in the "Categories of Personal Data Processed" section of the Privacy Policy, in particular document and project data, and, to the extent contained within documents submitted by the Subscriber, account and registration information, communications information, and Sensitive Personal Data or Information.

Schedule 2: Sub-processors

As of the date of this DPA, the Company engages the following Sub-processors in connection with the Services:

Sub-processor	Function	Location of Processing
Amazon Web Services	Cloud hosting and storage	United States
Google LLC	Google Drive integration (where connected by Subscriber); artificial intelligence and machine learning API services used to analyse, extract, and verify data from documents	United States
Intuit Inc.	QuickBooks two-way data synchronisation, including retrieval of vendor, customer, and configuration records, pushing of transaction records, and, where the Subscriber uses the upload-to-QuickBooks feature, transmission of source document attachments (where connected by Subscriber)	United States
Stripe, Inc.	Payment processing for recurring subscription billing and one-time top-up page purchases	United States
Twilio SendGrid	Delivery of transactional and service-related emails	United States

This list will be updated from time to time in accordance with the "Sub-processors" section above. Each of Amazon Web Services, Stripe, Inc., and Twilio SendGrid's standard data-processing or data-protection addendum is automatically incorporated into the commercial terms the Company has already agreed to, without any separate sign-up step, so no further action is required for these three Sub-processors.

RELATED

[General Terms of Subscription](#) [Privacy Policy](#) [CCPA Privacy Notice](#) [Notice at Collection](#)

[All legal documents](#)