

PAXTON AI, INC.

DATA PROCESSING ADDENDUM

Last Updated: October 15, 2026

This Data Processing Addendum (“DPA”) forms part of and is incorporated by reference into the Terms of Service or other written agreement (the “Agreement”) between Paxton AI, Inc. (“Paxton”) and the customer accepting the Agreement (“Customer”). Capitalized terms used but not defined in this DPA have the meanings given in the Agreement. The standard DPA applies without a separate signature to the extent specified in the Terms.

This DPA applies to the extent Paxton Processes Customer Personal Data on Customer’s behalf in providing the Services. It does not change the Parties’ separate legal responsibilities or expand Paxton’s rights to use Customer Data, Output, or Google API Data.

Customer must not submit Protected Health Information (“PHI”) on behalf of a HIPAA covered entity or business associate without a separate written business associate agreement (“BAA”). If executed, the BAA governs Processing of such PHI.

1. DEFINITIONS

“Customer Personal Data” means Personal Data within Customer Data or Output, or in related content-bearing derivatives such as prompts, chats, extracted text, embeddings, search indexes, and content-bearing logs, that Paxton Processes on Customer’s behalf in providing the Services. Business-contact, account, billing, transaction, and service-usage information that Paxton Processes as an independent controller for genuine account administration, security, fraud prevention, billing, service analytics, or legal compliance is excluded only to the extent it does not contain Customer content or data otherwise Processed on Customer’s behalf. Paxton’s independent processing of such information is described in its Privacy Policy.

“Data Protection Law” means applicable United States federal and state privacy and data-protection laws governing Customer Personal Data. It does not include HIPAA except as addressed in a separately executed BAA, or non-U.S. data-protection law except as expressly addressed in a separate written addendum. Applicable Google API requirements are addressed separately in this DPA and the Agreement.

“Data Subject” means the individual to whom Customer Personal Data relates.

“Deidentified Data” means information derived from Customer Personal Data that cannot reasonably be used to identify, or be linked to, Customer, any particular individual, or household and is maintained subject to applicable deidentification requirements.

“Google API Data” means information received through a Customer-authorized Google API connection and information aggregated, anonymized, or derived from it, to the extent subject to applicable Google API data-use requirements, whether or not the information constitutes Personal Data.

“Permitted Purpose” means Processing Customer Personal Data as reasonably necessary to host, store, organize, index, retrieve, analyze, summarize, and transmit Customer Data and Output; process prompts, chats, OCR text, and related content-bearing derivatives; generate and deliver requested Output; authenticate users and administer accounts; provide support; maintain, secure, troubleshoot, and optimize the Services for Customer; prevent fraud, abuse, and Security Incidents; and comply with applicable law.

“Personal Data” has the meaning given under applicable Data Protection Law.

“PHI” has the meaning assigned under the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”).

“Process” (and “Processing”) means any operation performed on Customer Personal Data, including collection, storage, retrieval, use, disclosure, transmission, deletion, and destruction.

“Security Incident” means a confirmed unauthorized acquisition of, access to, use of, disclosure of, alteration of, destruction of, or loss of Customer Data or Output in Paxton’s possession or control that materially compromises its confidentiality, integrity, or availability. Unsuccessful scans, pings, attempted intrusions, and similar events that do not compromise such information are excluded. This definition does not narrow any notification or reporting obligation imposed by applicable law, an applicable BAA, or Google API requirements.

2. PROCESSING INSTRUCTIONS

Paxton will Process Customer Personal Data only for the Permitted Purpose, to fulfill its obligations under the Agreement, and as required by applicable law. Customer instructs Paxton to perform that Processing by entering into the Agreement and enabling the applicable Services. Customer discloses Customer Personal Data for the limited and specified Permitted Purpose.

Paxton may use data derived from Customer Personal Data to improve the Services only after conversion into Deidentified Data, as permitted by the Agreement and Section 6. This

permission does not authorize a use of Google API Data prohibited by applicable Google policies, including the use of anonymized or derived Google API Data for prohibited model training or advertising.

To the extent applicable under Data Protection Law, Paxton acts as Customer's processor, service provider, or contractor with respect to Customer Personal Data. Except for permitted processing under this DPA and applicable law, Paxton will not: (a) sell or share Customer Personal Data; (b) retain, use, or disclose it outside the limited and specified Permitted Purpose or the direct business relationship; or (c) combine it with personal information from other sources in a manner prohibited by applicable Data Protection Law.

Where the California Consumer Privacy Act ("CCPA") applies, Paxton will comply with obligations applicable to service providers or contractors, provide the level of protection required by that law, and reasonably assist Customer with applicable requests and compliance responsibilities. If Customer reasonably believes Paxton's Processing violates this DPA or Data Protection Law, Customer may provide written notice, and Paxton will take reasonable and appropriate steps to stop and remediate confirmed unauthorized Processing.

3. CUSTOMER RESPONSIBILITIES

Customer represents that it has the rights, permissions, notices, authorizations, and other legal bases necessary to provide and use Customer Personal Data through the Services. Customer remains responsible for its lawful instructions, applicable privacy-law obligations, responding to Data Subject requests, and determining whether a BAA or additional international processing terms are required for its use case.

4. PAXTON OBLIGATIONS

Paxton will Process Customer Personal Data only as permitted under this DPA and the Agreement; ensure personnel authorized to access it are subject to appropriate confidentiality obligations; implement commercially reasonable safeguards; provide assistance required under Sections 8, 9, 10, and 11 and applicable law; and notify Customer if Paxton determines it can no longer meet the obligations of this DPA. Access to Google API Data is separately limited by the Google-specific user authorization and human-access conditions described in the Privacy Policy and applicable Google requirements.

5. SUBPROCESSORS

Customer generally authorizes Paxton to engage subprocessors to provide the Services. Paxton maintains its current list of subprocessors at <https://www.paxton.ai/legal/subprocessor-list>. The list identifies subprocessors and their functions and may change as the Services evolve. Paxton will enter into written agreements with subprocessors requiring confidentiality, security, permitted-purpose, and data-protection obligations appropriate to their functions, including any specific restrictions required by the CCPA or other applicable Data Protection Law. Paxton remains responsible for the data-protection obligations it delegates to subprocessors in connection with the Services, subject to the Agreement's liability limitations and mandatory law.

Where applicable Data Protection Law requires advance notice and an opportunity to object to a new subprocessor, Paxton will provide the legally required notice through a standardized account-email, in-product, or other designated notification method, with an opportunity to raise a reasonable data-protection objection before the new subprocessor begins covered Processing. Paxton will consider a timely, legally valid objection in good faith and provide any response or remedy required by applicable law.

6. ARTIFICIAL INTELLIGENCE AND GOOGLE API DATA

The Services may use third-party artificial intelligence model providers, document-processing providers, and cloud infrastructure providers. To the extent these providers Process Customer Personal Data on Paxton's behalf, they may do so only for the Permitted Purpose and are subject to applicable contractual confidentiality, security, and data-use restrictions. Paxton requires its third-party AI model providers to contractually prohibit the use of Customer Data, Output, and related content-bearing derivatives to train, fine-tune, or otherwise improve their generalized artificial intelligence or machine learning models.

Paxton uses OpenAI's Zero Data Retention (ZDR) controls for eligible API processing. These controls limit OpenAI's retention of customer content submitted to and generated through applicable API endpoints, subject to the technical limitations and exceptions associated with those controls. ZDR does not govern Paxton's own retention of Customer Data and Output to provide the Services or the retention practices of other subprocessors.

Paxton does not use identifiable Customer Personal Data to train or fine-tune its own generalized artificial intelligence models. Paxton may use Deidentified Data to maintain and improve the Services as permitted by the Agreement. Paxton will use reasonable measures designed to prevent reidentification and will not attempt to reidentify Deidentified Data except as permitted by law to test or validate deidentification.

Google Drive Sync. If Customer or an Authorized User enables Paxton's Google Drive synchronization integration, information obtained through that integration, including copies, extracted content, and derived information ("Google Drive Data"), is subject to the applicable Google API Services User Data Policy and Google Workspace Limited Use requirements.

Paxton and its subprocessors will use and transfer Google Drive Data only for purposes permitted by those requirements and will not use or permit its use for prohibited AI model training or improvement, advertising, sale to data brokers, or other prohibited purposes. Applicable Google requirements also govern human access, service-provider transfers, and data portability.

These restrictions apply only to Google Drive Data and information derived from it, including after disconnection for as long as Paxton retains such information. They do not extend to other Customer Data or Output solely because Customer uses Google Drive Sync. Other information received through Google APIs remains subject to the requirements applicable to those APIs.

7. SECURITY

Paxton maintains a commercially reasonable information security program designed to protect Customer Personal Data against unauthorized access, disclosure, alteration, and destruction. At a minimum, this program includes the measures in Schedule 2, which Paxton may update from time to time provided the updates do not materially reduce the overall level of protection. Additional Google-specific safeguards apply to Google API Data to the extent required by applicable Google policies.

8. SECURITY INCIDENTS

If Paxton becomes aware of a Security Incident, it will notify Customer without unreasonable delay and within any time period required by applicable Data Protection Law or an applicable BAA. Paxton will investigate and take commercially reasonable steps to mitigate harm and provide reasonably available information. Separately, Paxton will provide any notification or reporting required by applicable Google API terms. No provision of this DPA limits notice required by law merely because an event falls outside the defined contractual term "Security Incident." Notification does not constitute an admission of fault or liability.

9. DATA SUBJECT REQUESTS

If Paxton receives a Data Subject request relating to Customer Personal Data, it may direct the request to Customer. Customer remains responsible for responding to such requests. Taking into account the nature of Processing and information available to Paxton, Paxton will provide reasonable assistance, including through existing self-service functionality, for legally valid requests to access, correct, delete, or exercise other rights in Customer Personal Data, to the extent required by applicable Data Protection Law.

10. RETURN AND DELETION

Customer is responsible for retaining copies of Customer Personal Data using the download or export functionality available during the subscription term. Except as required by applicable Data Protection Law, applicable Google API portability rules, an applicable BAA, or a separate written agreement, Paxton is not obligated to provide post-termination access, custom exports, data conversion, migration assistance, or recovery of deleted information.

Following termination or expiration, Paxton may delete Customer Personal Data from active production systems in accordance with its retention practices. Where applicable Data Protection Law requires Paxton to return or delete Customer Personal Data at Customer's direction at the end of the Services, Paxton will do so as required by that law, subject to legally permitted or required exceptions. Customer may communicate such a direction using the available self-service functionality or a designated privacy/support channel. Paxton need not create a bespoke export format except to the extent required by law or another governing agreement.

Residual information in backups may remain until the ordinary backup expiration or deletion cycle, to the extent permitted by applicable law, and will remain protected under this DPA while retained. Paxton may retain information for applicable legal obligations, valid legal holds, security, or dispute-resolution purposes only where required or permitted by applicable law and governing agreements.

For as long as Paxton uses or stores Google API Data, Paxton will comply with the data-portability obligations of the applicable Google APIs Terms of Service and Google data-use rules. This Google-specific obligation does not create a universal post-termination export right for unrelated Customer Data or Output.

11. COMPLIANCE AND ASSESSMENTS

Upon reasonable written request, no more than once in any twelve-month period unless applicable law requires otherwise or following a Security Incident, Paxton will provide information reasonably necessary to demonstrate compliance with this DPA. The default method is provision of available standardized documentation, security summaries, certifications, independent assessment reports, or other generally available evidence. Paxton may use a qualified independent assessor and may provide that assessor's report to satisfy a legally required assessment where permitted by law.

Where applicable Data Protection Law requires a right to take reasonable and appropriate verification steps or to conduct reasonable assessments or audits, Customer may exercise that right on reasonable advance notice, subject to reasonable confidentiality, security, scope, and timing safeguards. The Parties will use available independent evidence before seeking any additional assessment. If such evidence is legally insufficient, Paxton will reasonably cooperate with a proportionate further assessment by Customer or a qualified independent assessor to the extent required by law. Paxton need not disclose trade secrets, information about other customers, or information compromising security, or provide production-system access, except to the extent legally unavoidable with appropriate safeguards. Neither Party is required to undertake duplicative or disproportionate measures beyond those imposed by law.

12. NON-U.S. DATA

This DPA does not itself provide a transfer mechanism under the GDPR, UK GDPR, Swiss Federal Act on Data Protection, or other non-U.S. data-protection law. Customer must not initiate Processing requiring additional international transfer mechanisms or processor terms unless Paxton has approved it in writing and the Parties have entered into an applicable data-protection or transfer addendum. This provision does not displace laws independently applicable to either Party.

13. LIMITATION OF LIABILITY

The limitations of liability in the Agreement apply to this DPA. To the extent permitted by applicable law, Paxton is not liable for claims resulting from Processing in accordance with Customer's lawful instructions, Customer's violation of law, or Customer's failure to obtain required rights, permissions, or consents. Mandatory statutory rights or liability that cannot lawfully be limited remain unaffected.

14. ORDER OF PRECEDENCE

If this DPA conflicts with the Agreement, this DPA governs solely with respect to Processing Customer Personal Data. If this DPA conflicts with an applicable separately executed BAA, the BAA governs solely for PHI. These priority provisions do not override applicable mandatory Data Protection Law or the additional Google API requirements applicable to Google API Data, including nonpersonal derived information.

15. UPDATES TO THIS DPA

Updates to this DPA are governed by the amendment and notice provisions of the Agreement. Material changes apply to existing paid subscriptions at the time provided in the Agreement unless a sooner change is required by law or another applicable obligation. Paxton will post the updated DPA at [DPA URL] with a revised “Last Updated” date. Prior versions remain applicable to Customers until a valid amendment becomes effective for their subscriptions.

SCHEDULE 1 — DETAILS OF PROCESSING

Categories of Data Subjects. Customer personnel and Authorized Users; Customer clients; opposing parties; witnesses; experts; medical providers; employees; family members; and others whose information appears in Customer Data, Output, or related content-bearing derivatives.

Categories of Customer Personal Data. Names, contact information, personal identifiers, and other information contained in litigation files, pleadings, correspondence, contracts, medical records, medical billing records, expert reports, prompts, chats, generated Output, OCR and extracted text, embeddings, search indexes, case files, integration records, and content-bearing logs, to the extent Processed on Customer’s behalf.

Sensitive Personal Data. Customer Personal Data may include health-related, financial, identification, and other sensitive information appearing in legal matters. PHI submitted on behalf of a covered entity or business associate requires a separately executed BAA.

Nature and Purpose of Processing. Providing, maintaining, securing, troubleshooting, and supporting the Services; generating requested Output; and improving the Services through permitted Deidentified Data, subject to the additional restrictions on Google API Data.

Duration. During the subscription and any period of lawful post-termination Processing, subject to Section 10 and applicable agreements.

SCHEDULE 2 — TECHNICAL AND ORGANIZATIONAL MEASURES

Paxton maintains risk-based safeguards, which it may update provided they do not materially decrease overall protection:

Access controls. Role-based access limited to personnel with an authorized business need, supported by identity and access-management controls.

Encryption. Customer Personal Data is encrypted in transit and at rest using industry-standard methods appropriate to the Services.

Authentication. Unique credentials and authentication controls for systems Processing Customer Personal Data.

Monitoring and incident response. Production logging and monitoring, documented incident-response procedures, and processes for investigating and mitigating Security Incidents.

Business continuity. Routine backups and documented service-recovery procedures for disruptions.