

GLASSWING AI

Data Processing Addendum

GLOBAL CUSTOMER CONTROLLER-TO-PROCESSOR TERMS

Version 1.0 | Effective date: August 5, 2026

This Data Processing Addendum ("DPA") forms part of the agreement between the customer identified in an applicable Order Form, online purchase, Terms of Service, End User License Agreement, Master Software and Services Agreement or other written agreement ("Customer") and IPivot, Corp. d/b/a Glasswing.ai ("Glasswing") governing Customer's use of the Services (the "Agreement"). This DPA applies when Glasswing Processes Customer Personal Data on Customer's behalf.

ELECTRONIC ACCEPTANCE: This DPA becomes binding when incorporated into an Agreement, executed by the parties, or affirmatively accepted through an authorized electronic process. The person accepting represents authority to bind Customer.

1. Definitions

Capitalized terms not defined in this DPA have the meanings in the Agreement or Applicable Data Protection Law. "Applicable Data Protection Law" means laws applicable to the Processing of Customer Personal Data, including, as applicable, the GDPR, UK GDPR, Swiss FADP and Applicable U.S. State Privacy Laws.

"Customer Personal Data" means Personal Data Processed by Glasswing on behalf of Customer in connection with the Services.

"Data Subject" means An identified or identifiable natural person to whom Customer Personal Data relates.

"GDPR" means Regulation (EU) 2016/679.

"Personal Data" means Information defined as personal data, personal information or a similar regulated concept under Applicable Data Protection Law.

"Process" or "Processing" means Any operation performed on Personal Data, including collection, access, use, storage, storage, disclosure, transmission, analysis, alteration, deletion or destruction.

"Security Incident" means A confirmed breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by Glasswing. Unsuccessful attempts that do not compromise Customer Personal Data are excluded.

"Services" means The Shadow AI Vulnerability Scanning Software, Scanner Service and separately purchased Glasswing products and services identified in the Agreement.

"Subprocessor" means A third party engaged by Glasswing to Process Customer Personal Data on Customer's behalf.

"UK GDPR" means The GDPR as incorporated into United Kingdom law.

2. Roles; Scope; Customer Instructions

Customer is the controller or business and Glasswing is the processor or service provider with respect to Customer Personal Data, except where Applicable Data Protection Law assigns different equivalent roles. If Customer acts as a processor, Glasswing acts as Customer's subprocessor.

Glasswing will Process Customer Personal Data only to provide, secure, support and administer the Services; comply with documented Customer instructions in the Agreement; prevent or address fraud, abuse and security threats; and comply with applicable law. The Agreement, this DPA, Customer's authorized configuration and support requests constitute documented instructions.

Glasswing will notify Customer if, in its reasonable opinion, an instruction infringes Applicable Data Protection Law, unless prohibited by law, and may suspend the affected Processing until the parties resolve the issue. Customer is responsible for the lawfulness of its instructions, notices, consents, legal bases and collection and use of Customer Personal Data.

3. Processing Restrictions

Glasswing will not sell or share Customer Personal Data; retain, use or disclose it outside the direct business relationship with Customer; use it for cross-context behavioral advertising; or combine it with Personal Data received from another source, except as permitted by Applicable Data Protection Law and reasonably necessary to provide, secure or improve the quality of the Services provided to Customer.

Glasswing will not Process Customer Personal Data for a materially different commercial purpose from the limited and specified purposes in Annex 1. Glasswing will provide the level of privacy protection required of a processor, service provider or contractor under Applicable Data Protection Law and will notify Customer if Glasswing determines it can no longer meet those obligations.

4. Confidentiality and Personnel

Glasswing will ensure that personnel authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations, receive privacy and security training appropriate to their responsibilities, and access Customer Personal Data only as necessary for assigned duties.

5. Security

Glasswing will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. The measures are described in Annex 2 and will account for the nature, scope, context and purposes of Processing and the risks to Data Subjects.

Glasswing may update security measures to reflect technological and operational developments, provided the overall level of protection is not materially diminished during the applicable service term.

6. Security Incidents

Glasswing will notify Customer without undue delay after confirming a Security Incident. Notice will include, to the extent known and reasonably available, the nature of the Security Incident, affected data and Data Subjects, likely consequences, measures taken or proposed, and a contact for follow-up. Glasswing may

provide information in phases and will take reasonable steps to contain, investigate and remediate the Security Incident.

Customer is responsible for determining whether notification to a regulator, Data Subject or other person is required. Glasswing will provide reasonable cooperation, considering the nature of Processing and information available to Glasswing. Notification is not an admission of fault or liability.

7. Data Subject Requests and Compliance Assistance

Taking into account the nature of Processing, Glasswing will provide reasonable assistance through appropriate technical and organizational measures to enable Customer to respond to requests concerning access, correction, deletion, portability, restriction, objection and other rights under Applicable Data Protection Law.

If Glasswing receives a request directly from a Data Subject concerning Customer Personal Data, Glasswing will direct the requester to Customer or act on Customer's documented instructions, unless law requires otherwise. Glasswing will reasonably assist Customer with data protection impact assessments, regulatory consultations, cybersecurity audits and risk assessments required by Applicable Data Protection Law, considering the nature of Processing and information available to Glasswing.

8. Subprocessors

Customer grants Glasswing general authorization to engage Subprocessors. Glasswing will maintain a current Subprocessor list and make it available to Customer through the customer portal, website or upon request. Glasswing will provide at least fifteen days' prior notice of a new Subprocessor that will Process Customer Personal Data, except where an emergency replacement is necessary to maintain security or service continuity.

Customer may object during the notice period on reasonable data-protection grounds. The parties will work in good faith to resolve the objection. If no commercially reasonable alternative is available, Customer may terminate the affected Service and receive a prorated refund of prepaid unused fees for that Service. Glasswing will impose written data-protection obligations on each Subprocessor that are no less protective in material respects than those applicable to Glasswing and remains responsible for the Subprocessor's performance to the extent required by Applicable Data Protection Law.

9. International Data Transfers

Glasswing will not transfer Customer Personal Data across national borders except in compliance with Applicable Data Protection Law. Where a transfer requires an approved transfer mechanism, the provisions in Annex 3 apply.

The parties will reasonably cooperate with transfer impact or risk assessments and supplementary measures required by Applicable Data Protection Law. Glasswing will notify Customer, unless prohibited by law, of a legally binding request from a public authority for Customer Personal Data and will challenge requests that Glasswing reasonably believes are unlawful or disproportionate.

10. Return and Deletion

During the service term, Customer may access or export Customer Personal Data to the extent supported by the applicable Service. Following termination or Customer's written request, Glasswing will delete or return

Customer Personal Data within sixty days, unless retention is required by law or the Agreement expressly permits continued retention.

Customer Personal Data in backups may remain until overwritten through Glasswing's ordinary backup cycle, provided it remains protected, isolated from ordinary use and Processed only for restoration, security, legal compliance or deletion. Glasswing may retain de-identified data that cannot reasonably identify Customer or a Data Subject.

11. Audits and Information

Glasswing will make available information reasonably necessary to demonstrate compliance with this DPA, which may include current third-party audit reports, certifications, summaries, policies and security questionnaires. Customer may conduct one audit in any twelve-month period, and additional audits following a Security Incident or regulator request, upon reasonable written notice.

Audits must occur during normal business hours, minimize disruption, protect other customers and Glasswing confidential information, and avoid access to systems or data unrelated to Customer. Customer will bear audit costs unless the audit identifies material noncompliance by Glasswing. Glasswing may require an independent qualified auditor bound by confidentiality. Customer may take reasonable steps to stop and remediate unauthorized Processing.

12. Government and Law-Enforcement Requests

Unless prohibited by law, Glasswing will notify Customer before disclosing Customer Personal Data in response to a compulsory government or law-enforcement request. Glasswing will disclose only the Customer Personal Data legally required and will direct the requesting authority to Customer where appropriate.

13. Applicable U.S. State Privacy Laws

"Applicable U.S. State Privacy Laws" means U.S. state laws applicable to Customer Personal Data that impose controller-processor, business-service-provider or equivalent contractual obligations, including the California Consumer Privacy Act as amended ("CCPA").

For Customer Personal Data subject to the CCPA, Glasswing is a service provider or contractor. The specific business purposes are providing, securing, supporting and administering the Services described in Annex 1. Glasswing will comply with applicable CCPA requirements, provide the same level of privacy protection required of businesses for the Customer Personal Data, enable Customer to respond to consumer requests, permit reasonable compliance monitoring, notify Customer if it can no longer comply, and allow Customer to take reasonable steps to stop and remediate unauthorized use.

Glasswing certifies that it understands and will comply with the restrictions and obligations in this Section.

Any Subprocessor Processing CCPA-covered Customer Personal Data will be bound by a written contract containing the required service-provider or contractor restrictions. This Section supplements, and does not limit, other protections in this DPA.

14. Customer Responsibilities

Customer will use the Services and Process Personal Data in compliance with Applicable Data Protection Law. Customer will not provide Personal Data that is unnecessary for the Services and will not use scanner-

accessibility results as proof of employee AI usage. Customer is responsible for properly configuring identity attribution, retention, content inspection and other optional features.

Unless expressly authorized in the Agreement, Customer will not submit regulated health information, payment-card data, government identification numbers, authentication secrets or special-category data. If Customer purchases and configures a Service intended to Process sensitive content, the applicable Order Form, product documentation and additional safeguards govern that Processing.

15. Liability

Each party's liability arising from this DPA is subject to the exclusions and limitations of liability in the Agreement, except to the extent such limitation is prohibited by Applicable Data Protection Law or would restrict Data Subject rights under incorporated transfer clauses.

16. Order of Precedence; Term; General

This DPA remains effective while Glasswing Processes Customer Personal Data. In a conflict concerning Processing: (a) incorporated EU Standard Contractual Clauses or the UK Addendum control to the extent required by law; (b) this DPA controls; and (c) the Agreement controls thereafter. Except as modified by this DPA, the Agreement remains in effect.

The governing-law, venue, assignment, notices and electronic-acceptance provisions in the Agreement apply to this DPA, except where incorporated transfer clauses require otherwise. Notices to Glasswing concerning this DPA must be sent to IPivot, Corp. d/b/a Glasswing.ai, Attn: Legal, 31241 North Star Way, Valley Center, CA 92082, with a copy to legal@ipivot.ai.

ANNEX 1

DETAILS OF PROCESSING

Subject matter	Processing Customer Personal Data to provide, secure, support and administer the Services purchased or authorized by Customer.
Duration	The Agreement term plus the deletion, backup and legally required retention periods described in this DPA.
Nature of Processing	Collection, transmission, organization, analysis, classification, storage, retrieval, support access, security monitoring, reporting, export, deletion and other operations necessary for the Services.
Business purposes	Providing scanner assessments and purchased products; authenticating users; generating reports; supporting customers; maintaining service security, integrity and availability; troubleshooting; complying with law; and improving service quality using permitted de-identified or aggregated data.
Data Subjects	Customer employees, contractors, authorized users, administrators, security and networking personnel, customer contacts, and other individuals whose Personal Data Customer lawfully submits or makes available through the Services.
Frequency	Continuous or event-driven for hosted products; periodic or customer-initiated for scanner assessments, support and report generation.

Categories of Customer Personal Data

- Account and business-contact information, including name, title, organization, business email and business telephone number.
- Authentication, authorization, account, role, session and audit-log information.
- Endpoint, device and operating-system identifiers and attributes.
- IP addresses, network location, DNS resolver and route information, SNI or hostname test destinations, security-control configuration context and scanner results.
- User, device, department or location attribution supplied or enabled by Customer.
- Service telemetry, feature usage, error, performance, support and diagnostic information.
- For products expressly purchased and configured for authorized content inspection: prompts, responses, uploaded or downloaded content, policy events and related metadata.
- Other Personal Data submitted by Customer in support tickets, configurations, reports or authorized integrations.

Sensitive or Special-Category Data

The Shadow AI Vulnerability Scanning Software is not designed to inspect prompt or file content. Sensitive or special-category data is not intentionally required for base scanner operation. Other Glasswing products may Process sensitive content only when expressly purchased, authorized and configured by Customer. Customer determines the lawful basis and necessity for such Processing.

Customer Instructions

The Agreement, this DPA, Customer's authorized configurations, API and integration settings, support requests and documented instructions accepted by Glasswing.

ANNEX 2

TECHNICAL AND ORGANIZATIONAL MEASURES

The following measures apply as appropriate to the Services, Processing risks and Glasswing's operational environment. Glasswing security personnel must validate these measures before external use of this DPA.

Security governance	Documented security responsibilities, policies, risk management and periodic review of controls.
Identity and access	Role-based access, least privilege, unique accounts, authentication controls, periodic access review and prompt removal of unnecessary access.
Encryption	Industry-standard encryption for Customer Personal Data in transit over public networks and encryption at rest where supported and appropriate to risk.
Network and system security	Segmentation or logical isolation, secure configuration, endpoint protection, firewalling, monitoring and controls appropriate to the environment.
Secure development	Code review, dependency management, testing, change control and remediation practices proportionate to application risk.
Vulnerability management	Risk-based vulnerability identification, prioritization, patching and remediation, with independent testing where appropriate.
Logging and monitoring	Security, administrative and access logging appropriate to the Service, with monitoring and retention based on security and operational needs.
Incident response	Documented detection, escalation, containment, investigation, remediation, recovery and notification procedures.
Availability and recovery	Backup, restoration, service-continuity and disaster-recovery measures appropriate to the Service and purchased commitments.
Data minimization and retention	Collection limited to service purposes; documented retention and secure deletion or disposal practices.
Personnel security	Confidentiality commitments, security awareness and role-appropriate training; screening where lawful and appropriate.
Subprocessor management	Risk-based diligence, written data-protection and security obligations, and ongoing oversight appropriate to services provided.
Physical security	Reliance on hosting-provider and office physical safeguards appropriate to systems and data; controls against unauthorized physical access.
Customer isolation	Logical controls designed to prevent unauthorized access between customer environments.

ANNEX 3

INTERNATIONAL DATA TRANSFERS

A. European Economic Area

Where Customer Personal Data protected by the GDPR is transferred to Glasswing in a country not recognized as providing adequate protection and no other lawful mechanism applies, the Standard Contractual Clauses in the Annex to European Commission Implementing Decision (EU) 2021/914 (EU SCCs) are incorporated by reference.

- Module Two applies when Customer is a controller and Glasswing is a processor; Module Three applies when Customer is a processor and Glasswing is a subprocessor.
- Clause 7 docking applies; Clause 9 uses Option 2 general written authorization with a fifteen-day notice period; the optional language in Clause 11 does not apply.
- For Clause 17, Option 1 applies and the governing law is Ireland. For Clause 18, the courts of Ireland have jurisdiction.
- Annex I.A parties are Customer as data exporter and IPivot, Corp. d/b/a Glasswing.ai as data importer. Annex I.B is Annex 1 of this DPA; Annex II is Annex 2 of this DPA; the competent supervisory authority is determined under Clause 13.
- If the EU SCCs conflict with this DPA, the EU SCCs control for the affected transfer.

B. United Kingdom

For a restricted transfer subject to the UK GDPR, the then-current International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner is incorporated by reference. The parties and transfer information are those in this DPA; the selected EU SCCs are identified above; neither party may terminate the Addendum solely because the Information Commissioner issues a revised form unless the revised form permits termination and applicable law requires it.

C. Switzerland

For transfers subject to the Swiss Federal Act on Data Protection, references in the EU SCCs to the GDPR are interpreted to include the Swiss FADP as applicable; references to EU or Member State law include Swiss law; the competent authority is the Swiss Federal Data Protection and Information Commissioner; and Data Subjects in Switzerland may enforce applicable rights. The EU SCCs otherwise apply with necessary conforming changes.

D. Supplementary Measures

Glasswing will provide information reasonably needed for a transfer impact or risk assessment, implement supplementary technical and organizational measures appropriate to identified risks, and notify Customer if Glasswing can no longer comply with an incorporated transfer mechanism.

ANNEX 4**SUBPROCESSOR AND CONTACT FRAMEWORK**

Glasswing legal entity	IPivot, Corp. d/b/a Glasswing.ai
Address	31241 North Star Way, Valley Center, CA 92082, USA
Privacy/legal contact	legal@ipivot.ai
Subprocessor authorization	General authorization subject to Section 8.
Notice method	Email to Customer's account administrator or notice through the customer portal or designated service channel.
Notice period	At least fifteen days, except emergency replacement for security or service continuity.
Current list	Available through the customer portal, Glasswing website or upon written request to legal@ipivot.ai.