



## DATA PROCESSING AGREEMENT

*Last Updated: February 2026*

This Data Processing Agreement (“**DPA**”) forms part of the Master Subscription Agreement (“**Agreement**”) between Konvu, Inc. (“**Konvu**” or “**Processor**”) and the entity identified in the applicable Order Form (“**Customer**” or “**Controller**”) and supplements the Agreement with respect to the processing of Personal Data by Konvu on behalf of Customer. Konvu may fulfill its obligations under this DPA through its Affiliates (as defined in Section 1 and listed in Annex IV). References to “**Konvu**” in this DPA include its Affiliates to the extent they process Personal Data in connection with the Service, and Konvu, Inc. remains fully liable for the obligations of its Affiliates under this DPA.

This DPA applies to the extent that Konvu processes Personal Data on behalf of Customer in the course of providing the Service under the Agreement. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to matters relating to the processing of Personal Data.

### 1. Definitions

Capitalized terms not defined herein have the meanings given to them in the Agreement. In this DPA:

“**Data Protection Laws**” means all applicable data protection and privacy legislation, including (a) the EU General Data Protection Regulation 2016/679 (“**GDPR**”); (b) the UK General Data Protection Regulation and the Data Protection Act 2018 (“**UK GDPR**”); (c) the Swiss Federal Act on Data Protection (“**Swiss FADP**”); (d) the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“**CCPA/CPRA**”); and (e) any other applicable data protection or privacy laws, in each case as amended, replaced, or superseded from time to time.

“**Personal Data**” means any information that relates to an identified or identifiable natural person and is processed by Konvu on behalf of Customer in connection with the Service, to the extent such information is protected as “personal data,” “personal information,” or similar term under applicable Data Protection Laws.

“**Personal Data Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data processed by Konvu under this DPA.

“**Data Subject**” means the identified or identifiable natural person to whom Personal Data relates.

“**Sub-processor**” means any third party engaged by Konvu to process Personal Data on Konvu’s behalf in connection with the Service.

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with Konvu, Inc., where “control” means ownership of fifty percent (50%) or more of the voting interests of the entity. Konvu’s current Affiliates are listed in Annex IV.

“**Standard Contractual Clauses**” or “**SCCs**” means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in Implementing Decision (EU) 2021/914 of 4 June 2021, Module 2 (Controller to Processor).

**“UK Addendum”** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner under Section 119A(1) of the Data Protection Act 2018, Version B1.0, in force 21 March 2022.

## **2. Scope and Roles**

### **2.1 Processing Roles**

With respect to Customer Data containing Personal Data that Konvu processes in the course of providing the Service, Customer is the Controller and Konvu is the Processor. The subject matter, nature, purpose, duration, and categories of Personal Data and Data Subjects are described in Annex I.

### **2.2 Customer as Processor**

Where Customer acts as a processor on behalf of a third-party controller, the parties agree that Module 3 (Processor to Processor) of the Standard Contractual Clauses shall apply in lieu of Module 2 to the extent required by applicable Data Protection Laws. In such cases, Customer shall ensure that it has obtained all necessary authorizations from the relevant controller for Konvu’s engagement as a sub-processor, and references to “Controller” in this DPA shall be read as references to Customer in its capacity as processor.

### **2.3 Konvu as Independent Controller**

Konvu processes certain data as an independent controller for its own legitimate business purposes, including account administration, billing, service improvement through Aggregated Data (as defined in the Agreement), fraud prevention, and compliance with legal obligations. Such processing is governed by Konvu’s Privacy Policy and is outside the scope of this DPA. For clarity, Konvu’s use of Aggregated Data as described in Section 6.4 of the Agreement is controller processing and is not subject to this DPA.

### **2.4 Customer Obligations**

Customer represents and warrants that: (a) it has complied with and will continue to comply with all applicable Data Protection Laws in connection with its use of the Service, including obtaining any required consents and providing any required notices to Data Subjects; (b) it has a lawful basis for processing the Personal Data and for instructing Konvu to process it as described in this DPA; and (c) it will not provide Konvu with any special categories of personal data (as defined in Article 9 of the GDPR) unless expressly agreed in writing.

## **3. Processing Instructions**

### **3.1 Documented Instructions**

Konvu shall process Personal Data only on documented instructions from Customer, including the instructions specified in this DPA, the Agreement, and any applicable Order Form, unless required to do otherwise by applicable law. If Konvu is required by applicable law to process Personal Data other than on Customer’s instructions, Konvu shall notify Customer of that legal requirement before processing (unless prohibited by law from doing so).

### **3.2 Scope of Instructions**

Customer's instructions for the processing of Personal Data shall comply with applicable Data Protection Laws. Customer instructs Konvu to process Personal Data to the extent necessary to provide the Service in accordance with the Agreement. Additional instructions outside the scope of the Agreement require a separate written agreement and may be subject to additional fees.

### **3.3 Lawfulness of Instructions**

If Konvu reasonably believes that an instruction from Customer infringes applicable Data Protection Laws, Konvu shall promptly notify Customer and may suspend the relevant processing until Customer provides revised instructions. Konvu shall not be liable for any delay or non-performance resulting from such suspension.

## **4. Confidentiality and Personnel**

### **4.1 Confidentiality Obligations**

Konvu shall ensure that all personnel authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Konvu shall ensure that access to Personal Data is limited to personnel who require such access to perform obligations under the Agreement.

### **4.2 Reliability**

Konvu shall take reasonable steps to ensure the reliability of any personnel who have access to Personal Data, including by conducting background checks to the extent permitted by applicable law and ensuring that such personnel have received appropriate training on data protection requirements.

## **5. Security Measures**

### **5.1 Technical and Organizational Measures**

Konvu shall implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, or disclosure. These measures shall be appropriate to the nature, scope, context, and purposes of processing, as well as the risk to the rights and freedoms of Data Subjects. Konvu's current security measures are described in Annex II.

### **5.2 Updates to Security Measures**

Konvu may update its security measures from time to time, provided that such updates do not materially diminish the overall level of protection afforded to Personal Data. Customer acknowledges that security measures are subject to technical progress and development, and that Konvu may update them to reflect changes in technology, industry standards, and the threat landscape.

## **6. Sub-processors**

### **6.1 General Authorization**

Customer grants Konvu a general written authorization to engage Sub-processors to process Personal Data on Konvu's behalf in connection with the Service, subject to the requirements of

this Section 6. The Sub-processors engaged as of the effective date of this DPA are listed in Annex III and at Konvu's Sub-processor page (available at Konvu's Trust Center or upon request).

## **6.2 Notification of Changes**

Konvu shall notify Customer of any intended addition or replacement of Sub-processors by updating its Sub-processor page (available at Konvu's Trust Center) at least ten (10) days prior to the new Sub-processor processing any Personal Data ("**Notice Period**"). Customer may subscribe to Sub-processor change notifications by registering at Konvu's Trust Center or by contacting [privacy@konvu.com](mailto:privacy@konvu.com). It is Customer's responsibility to subscribe to and monitor the Sub-processor page for updates.

## **6.3 Objection Right**

Customer may reasonably object to a new Sub-processor by notifying Konvu in writing within the Notice Period. The objection must be based on reasonable data protection grounds. Upon receipt of an objection, Konvu shall use commercially reasonable efforts to: (a) make available to Customer a change in the Service or recommend a commercially reasonable change to Customer's configuration or use of the Service to avoid processing by the objected-to Sub-processor; or (b) take corrective steps requested by Customer and mutually agreed upon by the parties. If Konvu is unable to provide a commercially reasonable alternative within ten (10) days of receiving the objection, either party may terminate the affected Order Form upon written notice, and Konvu shall refund Customer any prepaid fees for the unused portion of the Subscription Term following the effective date of termination.

## **6.4 Sub-processor Obligations**

Konvu shall: (a) enter into a written agreement with each Sub-processor imposing data protection obligations no less protective than those set out in this DPA; (b) remain fully liable to Customer for the acts and omissions of its Sub-processors to the same extent as if Konvu had performed the processing itself; and (c) conduct appropriate due diligence on Sub-processors before engagement to ensure they are capable of providing the level of protection required by this DPA and applicable Data Protection Laws.

## **6.5 LLM Provider Requirements**

Where a Sub-processor is a large language model provider ("**LLM Provider**") engaged for AI inference in connection with the Service, Konvu shall, in addition to the general obligations in Section 6.4, ensure that: (a) the LLM Provider does not use Personal Data for model training, fine-tuning, or improvement, whether through contractual restrictions, API configurations that prevent data retention, or equivalent technical measures; (b) Personal Data submitted for inference is processed ephemerally and is not retained by the LLM Provider beyond the duration of the inference request; and (c) Customer is notified of the identity of LLM Providers and any material changes thereto in accordance with Section 6.2.

# **7. Data Subject Rights**

## **7.1 Assistance with Requests**

Konvu shall, taking into account the nature of the processing, assist Customer by appropriate technical and organizational measures, insofar as this is possible, to fulfill Customer's obligation to respond to requests from Data Subjects exercising their rights under applicable Data Protection Laws (including rights of access, rectification, erasure, restriction, portability, and objection).

## **7.2 Notification**

If Konvu receives a request from a Data Subject in relation to Personal Data processed on behalf of Customer, Konvu shall promptly redirect the Data Subject to Customer and notify Customer of the request. Konvu shall not respond to the Data Subject directly unless authorized by Customer or required by applicable law.

## **7.3 Costs**

To the extent that Customer's request for assistance under this Section requires resources beyond what is reasonably necessary, Konvu may charge a reasonable fee based on the scope and complexity of the assistance requested, provided that Konvu notifies Customer of such fee in advance.

# **8. Personal Data Breach Notification**

## **8.1 Notification**

Konvu shall notify Customer of a confirmed Personal Data Breach without undue delay, and in any event within forty-eight (48) hours of becoming aware of the breach. Notification shall be made to Customer's designated security contact or, if none is designated, to the email address associated with Customer's account.

## **8.2 Content of Notification**

The notification shall include, to the extent reasonably available: (a) a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records affected; (b) the likely consequences of the breach; (c) a description of the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects; and (d) the identity and contact details of Konvu's point of contact for further information.

## **8.3 Cooperation**

Konvu shall cooperate with Customer and take reasonable commercial steps to assist Customer in investigating, mitigating, and remediating the Personal Data Breach. Konvu shall provide Customer with such additional information as becomes available regarding the breach.

## **8.4 No Admission**

Konvu's notification of a Personal Data Breach shall not be construed as an acknowledgment of fault or liability by Konvu. Nothing in this Section shall limit or waive any rights or remedies either party may have under the Agreement.

# **9. Data Protection Impact Assessments and Prior Consultation**

Konvu shall, taking into account the nature of the processing and the information available to Konvu, provide reasonable assistance to Customer in ensuring compliance with Customer's obligations relating to data protection impact assessments and prior consultation with supervisory authorities, to the extent such obligations apply to Customer's use of the Service and are required under applicable Data Protection Laws.

## **10. Deletion and Return of Personal Data**

### **10.1 Upon Termination**

Upon termination or expiration of the Agreement, Konvu shall, at Customer's election and written request, delete or return all Personal Data processed on behalf of Customer within thirty (30) days of such request, and delete existing copies unless applicable law requires retention. Konvu shall provide written confirmation of deletion upon request.

### **10.2 Retention Exceptions**

Konvu may retain Personal Data beyond the deletion timeline to the extent: (a) required by applicable law or regulation; (b) embedded in backup systems subject to automatic deletion in the ordinary course, provided such backups are deleted no later than ninety (90) days following termination; or (c) reasonably required to enforce the Agreement or establish compliance therewith. Any Personal Data retained under this Section shall remain subject to the protections of this DPA and the Agreement for as long as it is retained.

## **11. Audit Rights**

### **11.1 Information Availability**

Konvu shall make available to Customer such information as is reasonably necessary to demonstrate compliance with this DPA and Article 28 of the GDPR (or equivalent provisions under other applicable Data Protection Laws), subject to the confidentiality obligations of the Agreement.

### **11.2 Third-Party Audit Reports**

Konvu shall, upon Customer's written request (no more than once per twelve-month period), provide Customer with: (a) a summary of Konvu's then-current security program; and (b) any then-current third-party audit reports or certifications (e.g., SOC 2 Type II) to the extent available. Such reports shall be provided subject to the confidentiality obligations of the Agreement and any additional non-disclosure requirements imposed by the auditor.

### **11.3 On-Site Audit**

If Customer reasonably determines that the information provided under Sections 11.1 and 11.2 is insufficient to verify Konvu's compliance with this DPA, Customer may request an audit of Konvu's processing activities. Any such audit shall be: (a) conducted no more than once per twelve-month period; (b) subject to prior mutual agreement on scope, timing, duration, and confidentiality terms; (c) conducted during normal business hours with reasonable advance notice (not less than thirty (30) days); (d) carried out by Customer or an independent third-party auditor selected by Customer and approved by Konvu (such approval not to be unreasonably withheld); and (e) at Customer's expense, unless the audit reveals a material breach of this DPA by Konvu. The audit shall not unreasonably interfere with Konvu's operations.

## **12. International Data Transfers**

### **12.1 Processing Locations**

As of the effective date of this DPA, Konvu processes Personal Data in the United States. Konvu may update its processing locations from time to time, subject to compliance with this Section 12 and the Sub-processor notification requirements of Section 6.



## 12.2 Transfer Mechanisms

To the extent that Konvu's processing of Personal Data involves a transfer of Personal Data from the European Economic Area ("EEA"), the United Kingdom, or Switzerland to a country that has not been recognized as providing an adequate level of data protection, the parties shall rely on the following transfer mechanisms, as applicable:

(a) EU Standard Contractual Clauses: The parties hereby enter into the Standard Contractual Clauses (Module 2: Controller to Processor), as approved by European Commission Implementing Decision (EU) 2021/914. The SCCs are incorporated by reference into this DPA and shall be deemed completed as follows:

- (i) Clause 7 (Docking clause): the optional docking clause is included;
- (ii) Clause 9(a) (Use of sub-processors): Option 2 (General written authorization) applies, with a notice period of ten (10) days as specified in Section 6.2;
- (iii) Clause 11 (Redress): the optional language is not included;
- (iv) Clause 13(a) (Supervision): The supervisory authority of the EU Member State in which Customer is established, or if Customer is not established in the EU, the supervisory authority of the EU Member State in which Customer's EU representative is appointed, shall act as the competent supervisory authority. If neither applies, the Commission nationale de l'informatique et des libertés (CNIL) of France shall act as the competent supervisory authority;
- (v) Clause 17 (Governing law): Option 1 applies; the SCCs shall be governed by the laws of France;
- (vi) Clause 18(b) (Choice of forum and jurisdiction): disputes shall be resolved before the courts of France;
- (vii) Annex I (List of Parties, Description of Transfer, and Competent Supervisory Authority), Annex II (Technical and Organizational Measures), and Annex III (List of Sub-processors) of this DPA shall serve as the corresponding Annexes to the SCCs.

(b) UK International Data Transfer Addendum: For transfers of Personal Data subject to the UK GDPR, the UK Addendum is incorporated by reference into this DPA and shall be deemed completed with the information in Annex I, Annex II, and Annex III. In the event of any conflict between the UK Addendum and the SCCs, the UK Addendum shall prevail for UK transfers.

(c) Swiss Transfers: For transfers of Personal Data subject to the Swiss FADP, the SCCs shall apply with the following modifications: (i) references to the GDPR shall be interpreted as references to the Swiss FADP; (ii) the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner; and (iii) the term "Member State" shall be interpreted to include Switzerland.

(d) EU-U.S. Data Privacy Framework: To the extent that Konvu has self-certified under the EU-U.S. Data Privacy Framework (and, as applicable, the UK Extension and Swiss Extension thereto), such certification may serve as an additional transfer mechanism. If the Data Privacy Framework is invalidated or Konvu's certification lapses, the SCCs shall serve as the fallback transfer mechanism.

## 12.3 Supplementary Measures

Konvu shall implement supplementary technical and organizational measures as described in Annex II to protect Personal Data transferred internationally. If Konvu determines that it can no longer comply with its obligations under the applicable transfer mechanism due to a change in

applicable laws or government practices, Konvu shall promptly notify Customer and the parties shall cooperate in good faith to identify an alternative lawful transfer mechanism.

### 13. California-Specific Provisions

To the extent that the CCPA/CPRA applies to Konvu's processing of Personal Data:

(a) Konvu is a **"Service Provider"** as defined in the CCPA/CPRA. Konvu shall not sell or share (as those terms are defined in the CCPA/CPRA) Personal Data received from Customer.

(b) Konvu shall not retain, use, or disclose Personal Data for any purpose other than providing the Service as specified in the Agreement, or as otherwise permitted by the CCPA/CPRA for service providers.

(c) Konvu shall not combine Personal Data received from Customer with personal information received from other sources or collected from its own interactions with consumers, except as permitted by the CCPA/CPRA.

(d) Konvu grants Customer the right to take reasonable and appropriate steps to help ensure that Konvu uses Personal Data in a manner consistent with Customer's obligations under the CCPA/CPRA, including the audit rights described in Section 11.

(e) Konvu shall notify Customer if it determines that it can no longer meet its obligations under the CCPA/CPRA.

(f) Konvu certifies that it understands and will comply with the restrictions set forth in this Section 13 and the CCPA/CPRA, and will refrain from taking any action that would cause any transfer of Personal Data to Konvu to qualify as a "sale" or "sharing" of personal information under the CCPA/CPRA.

### 14. Term and Termination

This DPA shall become effective on the date of the Agreement and shall remain in effect for as long as Konvu processes Personal Data on behalf of Customer. The DPA shall automatically terminate upon termination or expiration of the Agreement, subject to Section 10 (Deletion and Return) and any provisions that by their nature are intended to survive termination.

### 15. General Provisions

#### 15.1 Governing Law

Except as otherwise specified in the SCCs or UK Addendum for international data transfers, this DPA shall be governed by the laws governing the Agreement.

#### 15.2 Amendments

Konvu may update this DPA from time to time to reflect changes in Data Protection Laws, regulatory guidance, or Konvu's processing activities. Konvu shall provide Customer with at least thirty (30) days' notice of any material changes. If Customer objects to a material change, Customer may terminate the affected Order Form in accordance with the Agreement.

#### 15.3 Severability



If any provision of this DPA is found to be invalid or unenforceable, the remaining provisions shall continue in full force and effect. The invalid provision shall be replaced by a valid provision that most closely approximates the intent of the original provision.

#### **15.4 Entire DPA**

This DPA, together with the Annexes and the Agreement, constitutes the entire agreement between the parties with respect to the processing of Personal Data and supersedes all prior or contemporaneous agreements, proposals, or representations on this subject matter.

**IN WITNESS WHEREOF**, the parties have executed this Data Processing Agreement as of the date last signed below.

**KONVU, INC.**

**CUSTOMER**

---

Signature

---

Signature

---

Name

---

Name

---

Title

---

Title

---

Date

---

Date

## Annex I — Description of Processing

This Annex forms part of the DPA and, where applicable, serves as Annex I to the Standard Contractual Clauses.

### A. List of Parties

Data Exporter (Controller)	Customer, as identified in the applicable Order Form
Data Importer (Processor)	Konvu, Inc., 1111B South Governors Avenue, STE 7673, Dover, Delaware 19904, United States. Konvu may also process Personal Data through its Affiliates listed in Annex IV.
Contact for Data Exporter	As specified in the Order Form or Customer's account
Contact for Data Importer	privacy@konvu.com

### B. Description of Transfer

Subject Matter	Provision of the Konvu AI-powered vulnerability management Service
Nature of Processing	Collection, storage, analysis, retrieval, transmission, and deletion of Personal Data as necessary to provide the Service, including AI-powered vulnerability analysis, triage, and prioritization
Purpose of Processing	To provide the Service in accordance with the Agreement and applicable Order Forms, including: vulnerability detection and assessment; exploitability analysis; triage and prioritization of findings; generation of Service Outputs; and related platform functionality
Duration	For the duration of the Agreement, plus the period required for deletion of Personal Data in accordance with Section 10 of the DPA
Frequency of Transfer	Continuous, as determined by Customer's use of the Service
Retention Period	Until deletion in accordance with the Agreement and this DPA (thirty (30) days following Customer's request upon termination, subject to the retention exceptions in Section 10.2)

### C. Categories of Data Subjects

(a) Customer's employees, contractors, and authorized users of the Service (dashboard users);

(b) Other individuals whose Personal Data may be incidentally present in Customer Data (e.g., identifiers in code snippets retained as vulnerability evidence, or file paths in scanner output).

#### **D. Categories of Personal Data**

(a) Account data: display names, email addresses, and platform roles (e.g., admin, member) of Authorized Users;

(b) Usage and analytics data: IP addresses, browser type, device identifiers, session identifiers, page views, feature interactions, and audit logs generated through use of the Service;

(c) Communication data: email addresses and delivery metadata associated with transactional notifications and product alerts sent by the Service;

(d) Incidental Personal Data: any Personal Data that may be present within code snippets, file paths, or other Customer Data provided to the Service.

No special categories of Personal Data (Article 9 GDPR) are intentionally processed. Customer is responsible for ensuring that special category data is not provided to the Service unless expressly agreed in writing.

#### **E. Competent Supervisory Authority**

The competent supervisory authority shall be determined in accordance with Section 12.2(a)(iv) of this DPA.

## Annex II — Technical and Organizational Measures

This Annex forms part of the DPA and, where applicable, serves as Annex II to the Standard Contractual Clauses. Konvu implements and maintains the technical and organizational security measures summarized below. The full text of each policy, together with supporting evidence and audit reports (including SOC 2 Type II), is available to Customer through Konvu's Trust Center or upon request. Updates to these measures shall not materially diminish the overall level of protection afforded to Personal Data.

### Measure Categories

**Encryption.** Data in transit encrypted via TLS 1.2+; data at rest encrypted via AES-256; key management with automatic rotation per NIST SP 800-57.

**Access Control.** Role-based access control (RBAC), multi-factor authentication for production systems, least-privilege by default, quarterly access reviews, and 24-hour deprovisioning upon termination.

**Infrastructure and Operations.** AWS-hosted infrastructure with network segmentation, intrusion detection, capacity monitoring, data leakage prevention, and documented change management procedures.

**Data Processing.** Data classified by sensitivity (Confidential, Internal, Public). Customer source code processed in ephemeral environments. LLM inference configured to prevent retention. No Customer Data used for model training. Retention schedules enforced per data category.

**Personnel.** Background screening proportional to data access level if applicable by law. Confidentiality agreements. Security awareness training at hire and annually. Disciplinary process for policy violations. Access revoked upon termination per company SLAs.

**Incident Response.** Severity-based triage (S1–S4). Forty-eight (48) hour breach notification. Defined escalation and remediation procedures. Post-incident review.

**Business Continuity.** Disaster recovery plan for service outages and facilities loss. Alternate work facility procedures. Regular backups with documented recovery.

**Secure Development.** Formal change control, version-controlled repositories, segregated environments (production/staging/development), security testing prior to deployment, vulnerability patching within 90 days of discovery.

**Third-Party Management.** Due diligence and risk assessment prior to engagement. Written agreements with security requirements. Annual monitoring and review of supplier security and service delivery.

**Physical Security.** Entry controls, visitor management, environmental threat protection, and surveillance at facilities processing or storing Personal Data.

### Policy Documentation

The following policies are maintained in Konvu's Trust Center and available to Customer upon request:

Policy	Scope
Information Security Policy	Overarching security framework and acceptable use
Access Control Policy	Logical access, RBAC, provisioning, and reviews
Cryptography Policy	Encryption standards and key management
Data Management Policy	Classification, handling, retention, and disposal
Operations Security Policy	Change management, monitoring, and backups
Secure Development Policy	SDLC, testing, and vulnerability management
Incident Response Plan	Detection, triage, notification, and remediation
Business Continuity and Disaster Recovery Plan	Service restoration and alternate facilities
Human Resource Security Policy	Screening, training, and termination procedures
Third-Party Management Policy	Vendor due diligence and ongoing monitoring
Physical Security Policy	Facility access and environmental controls
Risk Management Policy	Risk identification, assessment, and treatment
Information Security Roles and Responsibilities	Security governance and accountability
Asset Management Policy	Asset inventory, handling, and disposal
Anti-Bribery and Anti-Corruption Policy	Ethical conduct and regulatory compliance
Code of Conduct	Employee standards and expected behavior

## Annex III — List of Sub-processors

This Annex forms part of the DPA and, where applicable, serves as Annex III to the Standard Contractual Clauses. The current list of Sub-processors is maintained at Konvu's Trust Center and is available upon request. As of the effective date of this DPA, Konvu engages the following Sub-processors:

Sub-processor	Purpose	Location	Data Processed
Amazon Web Services (AWS)	Cloud infrastructure, compute, storage, and database services	United States	All Customer Data as necessary for Service operation
OpenAI	LLM inference for AI-powered vulnerability analysis	United States	Customer submitted Data for inference (ephemeral; no retention)
Customer.io	Transactional and product alert email delivery	United States	Email addresses, names, and delivery metadata
PostHog	Product analytics and usage tracking	United States	IP addresses, device identifiers, session data, and feature usage
Salesforce	Customer relationship management	United States	Account data, contact names, and email addresses
Help Scout	Customer support ticketing and communications	United States	Names, email addresses, and support ticket content
Konvu SAS (Affiliate)	Engineering, support, and operational services on behalf of Konvu, Inc.	France	Customer Data as necessary for Service operation and support

Konvu will update this list in accordance with the notification and objection procedures described in Section 6 of the DPA. Customer may subscribe to Sub-processor change notifications by contacting [privacy@konvu.com](mailto:privacy@konvu.com).



## Annex IV — List of Affiliates

This Annex lists the Affiliates of Konvu, Inc. that may process Personal Data on behalf of Customer in connection with the Service. Konvu, Inc. remains fully liable for the processing activities of its Affiliates under this DPA.

Entity	Jurisdiction	Corporate Form	Role
Konvu SAS	France	Société par actions simplifiée (SAS)	Sub-processor

This list may be updated by Konvu from time to time. Any Affiliate that processes Personal Data on behalf of Customer shall be subject to the terms of this DPA and shall be listed as a Sub-processor in Annex III.