Data Processing Agreement

Version 2.0. Effective 25 August 2026 for accounts created on or after that date. For existing accounts, this version applies from 1 October 2026 in accordance with Section 13.3. This version replaces the Data Processing Agreement dated 1 January 2023 and, once it validly applies to a given Customer's account in accordance with Section 13.3, supersedes that version for that account.

The previous version remains available at Data Processing Agreement v1.0. This DPA forms part of the SimpleBackups Terms and Conditions, version 2.0, which are published alongside it.

This Data Processing Agreement (**"DPA"**) forms part of the SimpleBackups Terms and Conditions (the **"Agreement"**) between the customer identified in the applicable account or order (**"Customer"**) and Union Lab SRL, a Belgian company registered under enterprise number 0772.884.914, with its registered office at Avenue Paule 10, 1150 Woluwe-Saint-Pierre, Belgium, operating the SimpleBackups service (**"SimpleBackups"**).

This DPA applies where SimpleBackups processes Customer Personal Data on Customer's behalf. It applies from the later of the effective date above and the date Customer accepts the Agreement. No additional signature is required. A countersigned copy is available on request at privacy@simplebackups.com.

1. Definitions

In this DPA:

“Customer Personal Data” means Personal Data processed by SimpleBackups on Customer’s behalf through the Services. It includes Personal Data contained in the databases, files, storage locations or connected applications selected by Customer for backup, synchronization or restore (**“Backup Data”**), and related connection, configuration, job and log data (**“Configuration Data”**). Customer Personal Data may include special categories of Personal Data within the meaning of Article 9 GDPR (including health data) where Customer’s own sources, databases or connected applications contain such data; SimpleBackups does not select or classify the contents of Customer’s sources and processes any such special-category data strictly on Customer’s documented instructions and subject to Section 12.

“Data Protection Laws” means laws applicable to the processing of Customer Personal Data under the Agreement, including the GDPR, the UK GDPR and UK Data Protection Act 2018, the Swiss Federal Act on Data Protection, and the CCPA, in each case as applicable and amended from time to time.

“GDPR” means Regulation (EU) 2016/679.

“CCPA” means the California Consumer Privacy Act of 2018, as amended.

“Services” means the backup, storage, synchronization, snapshot and restore services provided by SimpleBackups under the Agreement.

“Subprocessor” means a third party appointed by SimpleBackups to process Customer Personal Data on Customer’s behalf in connection with the Services.

“Controller”, **“Processor”**, **“Data Subject”**, **“Personal Data”**, **“Personal Data Breach”** and **“Processing”** have the meanings given in applicable Data Protection Laws. References to a **“Supervisory Authority”** include, where the context requires, the UK Information Commissioner’s Office.

2. Roles, scope and instructions

2.1 Roles. For Customer Personal Data, Customer is the Controller or a Processor acting for another Controller, and SimpleBackups is Customer’s Processor or Subprocessor. Each party shall comply with the Data Protection Laws applicable to it

in that role. The characterisation of SimpleBackups' role for any given category of data or any given tool or provider engaged by SimpleBackups is determined by the actual purpose of the relevant processing, and not by internal labelling; Section 2.6 and Exhibit C apply this principle.

2.2 Instructions. SimpleBackups shall process Customer Personal Data only on Customer's documented instructions, unless required to do so by European Union or Member State law applicable to SimpleBackups or, where the UK GDPR applies, by applicable United Kingdom law. If legally permitted, SimpleBackups shall inform Customer before processing required by law. The Agreement, this DPA, Customer's use and configuration of the Services, and any applicable Order Form are Customer's documented instructions.

2.3 Unlawful instructions. SimpleBackups shall immediately inform Customer if, in its opinion, a Customer instruction infringes applicable Data Protection Laws. SimpleBackups may suspend the affected processing while the parties clarify or amend the instruction.

2.4 Processing details. The subject matter, duration, nature and purpose of processing, and the categories of Personal Data and Data Subjects, are described in Exhibit A.

2.5 Customer responsibilities. Customer is responsible for the lawfulness of its instructions, the accuracy and quality of Customer Personal Data, providing required notices, and establishing a lawful basis for the processing, including, where applicable, an Article 9(2) GDPR condition for any special category of Personal Data Customer causes to be processed through the Services. Customer shall comply with the restricted-workload requirements in Section 12.

2.6 SimpleBackups as Controller. This DPA does not apply when SimpleBackups processes account, billing, relationship, website or service-telemetry data as an independent Controller for customer administration, billing, security, fraud prevention, legal compliance, and service improvement. This independent-Controller processing does not include Backup Data. Configuration Data remains Customer Personal Data to the extent SimpleBackups processes it on Customer's behalf to provide the Services. Where SimpleBackups uses a general-purpose software, analytics, artificial-

intelligence or collaboration tool, the tool is treated as a Subprocessor under this DPA, and listed as such in Exhibit C, to the extent it is used to provide, maintain, secure or support the Services on a specific Customer's behalf and processes Customer Personal Data for that purpose; it is treated as falling outside this DPA only to the extent it is used exclusively for SimpleBackups' own independent-Controller purposes described in this Section 2.6 and does not process Customer Personal Data for that purpose. Independent-Controller processing is described in the SimpleBackups Privacy Policy.

3. Personnel and confidentiality

3.1 SimpleBackups shall ensure that persons authorized to process Customer Personal Data are bound by confidentiality obligations and receive access only as necessary to provide, secure or support the Services.

4. Security

4.1 SimpleBackups shall implement and maintain the technical and organizational measures required by Article 32 GDPR and, as applicable, Article 32 UK GDPR, taking into account the state of the art, implementation costs, the nature, scope, context and purposes of processing, and the risks to individuals, designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

4.2 The measures in effect on the effective date are summarized in Exhibit B. SimpleBackups may update those measures as the Services evolve, provided that the updates do not materially reduce the overall level of protection for Customer Personal Data.

4.3 Customer is responsible for configuring the Services appropriately for its risk, including selecting suitable processing and storage locations, retention, access permissions, backup encryption and restore-testing arrangements.

5. Subprocessors

5.1 General authorization. Customer generally authorizes SimpleBackups to engage the Subprocessors listed in Exhibit C.

5.2 Notice. SimpleBackups shall inform affected Customer account contacts by email at least thirty (30) days before a new or replacement Subprocessor begins processing Customer Personal Data. SimpleBackups shall also update Exhibit C.

5.3 Objections. Customer may object during the notice period on reasonable grounds relating to the protection of Customer Personal Data. The parties shall work in good faith to address the objection. If SimpleBackups cannot provide a commercially reasonable alternative, Customer may terminate the affected Services and receive a pro-rata refund of prepaid fees for the unused terminated period.

5.4 Subprocessor obligations. SimpleBackups shall enter into a written agreement with each Subprocessor imposing the same data-protection obligations as this DPA to the extent applicable to the Subprocessor's processing, and shall confirm, for each Subprocessor listed in Exhibit C, that such an agreement is in force and operatively incorporated into SimpleBackups' own account with that Subprocessor. SimpleBackups shall remain responsible to Customer for the Subprocessor's performance of those obligations as required by applicable Data Protection Laws.

5.5 Customer-directed providers. A storage destination, integration or other provider connected by Customer and contracted directly by Customer is not a SimpleBackups Subprocessor. Customer instructs SimpleBackups to transmit data to that provider and is responsible for its selection and use.

6. International transfers

6.1 SimpleBackups is established in Belgium and is directly subject to the GDPR. Transfers from SimpleBackups to a Subprocessor in a country not covered by an applicable adequacy decision shall be protected as required by applicable Data

Protection Laws, including, where appropriate, through the European Commission's Standard Contractual Clauses, the UK International Data Transfer Agreement or UK Addendum, or another lawful transfer mechanism.

6.2 For each Subprocessor listed in Exhibit C that processes Customer Personal Data outside the EEA or United Kingdom, Exhibit C states the transfer mechanism relied upon (an applicable adequacy decision, the relevant Standard Contractual Clauses module, the UK Addendum or IDTA, or another lawful mechanism). Further supporting documentation is available on request.

6.3 Where Customer selects or connects a processing or storage destination outside the EEA or United Kingdom, Customer instructs SimpleBackups to make that transfer and is responsible for ensuring that its instruction is lawful. This Section 6.3 does not relieve SimpleBackups of its own obligations under Sections 2.2 and 2.3, or of any obligation directly applicable to SimpleBackups under Chapter V GDPR or the corresponding provisions of the UK GDPR; SimpleBackups' execution of Customer's instruction under this Section 6.3 remains subject to those obligations.

6.4 If a restricted transfer from SimpleBackups to Customer requires a transfer mechanism under applicable Data Protection Laws, the parties shall complete the applicable transfer terms separately. Nothing in this DPA designates Union Lab SRL as a third-country data importer; for Customer Personal Data, SimpleBackups' role is that of Processor or Subprocessor as described in Section 2.

6.5 If SimpleBackups receives a legally binding request from a public authority for Customer Personal Data, it shall, to the extent legally permitted, notify Customer and disclose only the Customer Personal Data it is legally required to disclose.

7. Data Subject requests and regulatory assistance

7.1 Taking into account the nature of the processing, SimpleBackups shall provide reasonable assistance through appropriate technical and organizational measures to help Customer respond to requests from Data Subjects.

7.2 If SimpleBackups receives a request from a Data Subject relating to Customer Personal Data, it shall forward the request to Customer and shall not respond except on Customer's instructions or as required by law.

7.3 Taking into account the nature of processing and the information available to SimpleBackups, SimpleBackups shall provide reasonable assistance with Customer's obligations concerning security, breach notifications, data protection impact assessments and prior consultation with Supervisory Authorities.

7.4 Assistance is provided through the Services and SimpleBackups' standard documentation where reasonably sufficient. No fee shall apply to assistance necessary for SimpleBackups to comply with its mandatory obligations under this DPA or applicable Data Protection Laws, or to assistance required as a result of a Personal Data Breach or other non-compliance caused by SimpleBackups or a Subprocessor. Beyond such mandatory assistance, additional assistance may be charged at SimpleBackups' then-current professional-services rates to the extent permitted by applicable law, and SimpleBackups shall inform Customer before incurring a charge.

8. Personal Data Breaches

8.1 SimpleBackups shall notify Customer without undue delay and, in any event, within seventy-two (72) hours after becoming aware of a Personal Data Breach affecting Customer Personal Data. Such notification may be made on the basis of information available at the time, and SimpleBackups shall supplement it with further information as it becomes available, on a progressive basis consistent with the phased-disclosure approach Article 33(4) GDPR contemplates for controllers. For the avoidance of doubt, a Personal Data Breach occurring at a Subprocessor and affecting Customer Personal Data shall be treated as a Personal Data Breach for purposes of this Section 8.

8.2 SimpleBackups shall provide information reasonably available to it that Customer requires to meet applicable breach-notification obligations and shall take reasonable steps to contain, investigate and mitigate the breach, and shall cooperate with, and

provide reasonable assistance to, Customer's own investigation and regulatory notifications.

9. Return and deletion

9.1 During the term, Customer may retrieve or delete Customer Personal Data using available Service functionality and its connected storage destination.

9.2 Following termination or expiration of the Agreement, and at Customer's choice, SimpleBackups shall delete or return Customer Personal Data under its control in accordance with the schedule in Exhibit A (Retention and deletion), and shall delete existing copies, unless applicable law requires their retention or Customer has not made an election, in which case SimpleBackups shall delete Customer Personal Data by default. Copies maintained in routine backups are rendered inaccessible for further processing promptly upon deletion or return and are permanently deleted at the next applicable backup-cycle rotation, and remain protected by this DPA until deletion.

9.3 Section 9 does not govern backup files held by a storage provider contracted directly by Customer. Customer is responsible for retrieving or deleting those files.

10. Information and audits

10.1 SimpleBackups shall make available information reasonably necessary to demonstrate compliance with Article 28 GDPR and Article 28 UK GDPR, as applicable, including relevant current certifications, audit materials and security documentation.

10.2 Customer shall first use the information made available under Section 10.1; reliance on certifications, audit reports or other assurance materials as a first step does not displace Customer's underlying right to audit or inspect under this Section 10. If the information made available under Section 10.1 is not reasonably sufficient, Customer may conduct an audit itself or through an independent auditor that is not a SimpleBackups competitor, subject to the following safeguards:

- no more than once in any twelve-month period, except that this limit does not apply where the audit is reasonably necessary following a Personal Data Breach affecting Customer Personal Data, where Customer has a reasonable, documented suspicion of material non-compliance with this DPA, or where a Supervisory Authority requires it;
- at least thirty (30) days' written notice, save that this notice period shall be reduced to a reasonable shorter period where a genuine urgency exists, including in the circumstances described in the preceding bullet, or where a shorter period is legally required;
- during normal business hours, under appropriate confidentiality obligations, and without unreasonable disruption;
- limited to systems, records and processing relevant to Customer Personal Data; and
- at Customer's reasonable and proportionate cost, including SimpleBackups' reasonable time at its then-current professional-services rates, unless the audit identifies a material breach of this DPA by SimpleBackups, in which case SimpleBackups shall bear its own costs of the audit.

10.3 SimpleBackups is not required to disclose information that would compromise another customer's security or confidentiality, expose privileged material, or create a security risk. The parties shall use a reasonable alternative method to provide necessary assurance; SimpleBackups shall not invoke this Section 10.3 to avoid providing assurance reasonably necessary to demonstrate compliance with Article 28 GDPR and Article 28 UK GDPR, as applicable.

11. California

11.1 Where the CCPA applies to Customer Personal Data, SimpleBackups acts as a service provider or contractor. SimpleBackups shall not sell or share Customer Personal Data, retain, use or disclose it outside the direct business relationship except to provide the Services or as otherwise permitted by the CCPA, or combine it with Personal Data from other sources except as permitted by the CCPA.

11.2 SimpleBackups certifies that it understands and shall comply with the restrictions in Section 11.1. It shall notify Customer if it determines that it can no longer comply. Customer may take reasonable and appropriate steps required by the CCPA to stop and remediate unauthorized use of Customer Personal Data.

12. Restricted workloads

12.1 The standard self-service Services are not designed for protected health information subject to HIPAA, payment-card data subject to PCI DSS, or special categories of Personal Data under Article 9 GDPR, in each case without the additional approval and configuration described in this Section 12.

12.2 Customer shall not use the standard self-service Services for a restricted workload described in Section 12.1 unless an Order Form or other written agreement signed or expressly approved by SimpleBackups identifies the supported workload, the categories of restricted data and Data Subjects involved, the approved processing and storage regions, the required technical configuration (which may include customer-managed encryption, mandatory streaming, a dedicated processing environment, and a region lock), the applicable retention schedule, and any enhanced security, support-access or incident-notification commitments applicable to that Order Form. Any approval is limited to that workload and configuration.

12.3 Customer remains responsible for establishing a lawful basis and, where required, an Article 9(2) condition or other legal authorization for the processing. SimpleBackups' approval of an Order Form under this Section 12 constitutes contractual permission for SimpleBackups to process the described workload and configuration on Customer's documented instructions; it does not constitute a determination, representation or warranty by SimpleBackups that Customer's own processing is lawful, that Customer holds a valid Article 9(2) condition, or that SimpleBackups has performed any diligence on Customer's underlying legal basis. The standard self-service Services do not include a HIPAA Business Associate Agreement.

12.4 Where an Order Form under this Section 12 includes a fixed initial breach-notification commitment shorter than the general standard in Section 8.1, that commitment applies to the Customer Personal Data covered by that Order Form in place of Section 8.1, subject to confirmation of its operational feasibility before the Order Form is issued.

13. General

13.1 Order of precedence. If this DPA conflicts with the Agreement on the processing of Customer Personal Data, this DPA controls, and an Order Form issued under Section 12 controls over this DPA for the specific workload and configuration it describes. An applicable mandatory transfer mechanism controls over all of the foregoing.

13.2 Liability. Each party's liability arising from this DPA is subject to the limitations and exclusions in the Agreement. If the Agreement does not state an aggregate cap, each party's aggregate liability arising from this DPA shall not exceed the fees paid or payable by Customer for the Services during the twelve (12) months preceding the event giving rise to liability. Nothing limits liability to the extent a limitation is prohibited by applicable law.

13.3 Changes. SimpleBackups may update this DPA to reflect changes to the Services, Subprocessors or applicable law. SimpleBackups shall give affected Customers at least thirty (30) days' notice of a material change, specifying the effective date on which the updated DPA will apply to that Customer's account in place of any prior version, including the Data Processing Agreement dated 1 January 2023 where applicable. An update shall not materially reduce the overall protection of Customer Personal Data during the current subscription term.

13.4 Notices. Notices under this DPA may be sent to Customer's account email address and to SimpleBackups at **privacy@simplebackups.com**.

13.5 Privacy contact. Questions about this DPA may be directed to SimpleBackups' Privacy Contact at **privacy@simplebackups.com**. References in this DPA, the Agreement, any Order Form or related documentation to a privacy contact, privacy

lead or similar role at SimpleBackups are references to an internal privacy-function contact point and do not represent that SimpleBackups has designated a Data Protection Officer under Article 37 GDPR or Article 37 UK GDPR unless SimpleBackups has expressly confirmed such a designation in writing.

13.6 Confidentiality; permitted disclosure. Each party shall keep confidential the terms of this DPA and any non-public information disclosed under it, except that Customer may disclose this DPA, any Order Form, and any security or compliance documentation SimpleBackups provides under Section 10, to Customer's own professional advisers, auditors, insurers and regulators, and to Customer's own customers or business partners to the extent reasonably necessary for Customer to perform its own due-diligence, disclosure or regulatory obligations, in each case subject to reasonable confidentiality protections.

13.7 Governing law. This DPA is governed by Belgian law, without prejudice to any mandatory transfer terms. The courts of Brussels, Belgium have exclusive jurisdiction, to the extent permitted by applicable law.

Exhibit A: Details of processing

Item	Description
Subject matter	Provision of the backup, storage, synchronization, snapshot and restore Services selected and configured by Customer.
Duration	The term of the Agreement and the deletion period below.
Nature and purpose	Receiving, accessing, copying, temporarily processing, compressing, encrypting, transmitting, storing, monitoring, retrieving and restoring Customer Personal Data as necessary to provide and secure the Services.
Frequency	On the schedules configured by Customer and when Customer initiates an on-demand backup, synchronization, download or restore.
Categories of Data Subjects	Individuals whose Personal Data is contained in the sources selected by Customer, and Customer personnel or users represented in Configuration Data.

Item	Description
Categories of Personal Data	Personal Data contained in Customer-selected databases, files, storage locations and connected applications, which may include special categories of Personal Data under Article 9 GDPR (including health data) depending on the sources Customer selects; connection and authentication information; job configuration, logs and operational metadata. SimpleBackups does not select or classify the contents of Customer's sources.
Restricted data	The standard self-service Services are subject to Section 12. Restricted data, including special categories of Personal Data under Article 9 GDPR, protected health information subject to HIPAA, and payment-card data subject to PCI DSS, may be processed only under the written approval and configuration described in Section 12 and the applicable Order Form.
Retention and deletion	Backup content: retained per Customer's configured retention settings and deleted or overwritten according to that configuration; on termination, deleted within the period stated in the applicable Order Form or, absent an Order Form, within ninety (90) days. Account data, encrypted connection credentials and Configuration/job metadata: soft-deleted immediately on account closure, with permanent erasure within ninety (90) days. Temporary worker files: deleted on job completion. Operational and security logs (including SolarWinds and Sentry): retained for twelve (12) months and deleted thereafter in the ordinary course. SimpleBackups' internal control-plane backups (encrypted): retained on a twelve (12) month lifecycle; residual copies of deleted account data may persist within these encrypted backups until lifecycle expiry, remaining protected under this DPA until deletion. Support records (Intercom) and AI-tooling data (Anthropic, OpenAI): retained per the applicable provider's standard terms.

Customer obligations: Customer determines the sources, purposes, schedules, destinations, regions and retention settings and is responsible for its instructions and lawful basis.

Exhibit B: Technical and organizational measures

SimpleBackups maintains measures appropriate to the Services and risk, including:

- **Security governance:** documented information-security responsibilities, risk management, access control, incident response, business continuity and secure-development practices. At the effective date, Union Lab SRL's information security management system is independently certified to ISO/IEC 27001:2022 (certificate no. 270012023665, issued by ISO Assured Ltd, valid 29 November 2025 to 29

November 2026) for the provision of cloud-based backup solutions. The current certificate and the corresponding Statement of Applicability (F-IMS26, issue 3, dated 24 November 2025) are available on request.

- **Encryption:** encrypted network connections are used for supported service communications. Backup files stored in SimpleStorage are encrypted at rest by the storage layer. Customer-controlled backup encryption is available for supported backup types; where enabled, the completed stored backup cannot be decrypted without Customer's private key, which SimpleBackups does not hold or have the ability to recover.
- **Access control:** access to production systems and Customer Personal Data is limited according to role and need, protected by multi-factor authentication for administrative and privileged access, and subject to confidentiality obligations. Direct access to production infrastructure and databases is limited to SimpleBackups' two co-founders; support personnel are limited to scoped, application-level support tooling without direct database access.
- **Data minimization:** the application control plane is designed to process job configuration and operational information rather than backup-file content. Serverless workers process Backup Data only to perform the configured job.
- **Processing and temporary data:** supported streaming workflows can transfer backup output through compression and optional Customer-controlled encryption without persisting a complete plaintext backup file. Other workflows may use temporary working files. Temporary resources are subject to job-cleanup and infrastructure-lifecycle controls.
- **Tenant separation:** logical controls separate customer accounts and data in the multi-tenant Services. Temporary processing resources use job or tenant separation appropriate to the workload.
- **Logging and monitoring:** production systems use operational and security logging, monitoring and alerting. Logs are designed to avoid secrets and backup-file content, but may include identifiers and job metadata needed to operate and troubleshoot the Services.
- **Availability and recovery:** SimpleBackups maintains internal backup, continuity and recovery processes appropriate to the Services, including restore testing of production databases on an approximately quarterly cadence.

- **Security evaluation:** security controls are reviewed through the information security management system, including through annual internal and external ISO/IEC 27001:2022 audits. Relevant infrastructure-provider assurance materials are considered as part of supplier management.
- **Deletion:** Customer-configured retention controls apply to backup files. Account and temporary processing data are deleted or made inaccessible under documented application and infrastructure lifecycle processes, per the schedule in Exhibit A.

Exhibit C: Service Subprocessors

This table lists third parties engaged by SimpleBackups that may process Backup Data or Configuration Data on Customer's behalf, applying the functional test in Section 2.6 to determine which tools are included. Providers used only for SimpleBackups' independent Controller activities, such as billing, sales, accounting or general website analytics, are described in the Privacy Policy instead. For each Subprocessor, this table sets out the provider, its function, its processing location, and the applicable international-transfer mechanism. Extended detail for each Subprocessor listed below (specific categories of data processed, retention practices, and architectural notes) is set out in a separate SimpleBackups Subprocessor Detail Schedule, made available to Customers on request at privacy@simplebackups.com. The same Subprocessors and processing locations appear in both documents; only the level of detail differs.

Last updated: 25 August 2026.

Subprocessor	Service / Purpose of Processing	Processing Location	International Transfer Mechanism
Amazon Web Services EMEA SARL (Luxembourg) and affiliates	Application control plane; SimpleStorage object storage selected by Customer	Control plane: United States. SimpleStorage: European Union (Sweden) by default, or United States if selected by Customer.	Not a Restricted Transfer where SimpleStorage is limited to the EU region. For the United States control plane: EU Standard Contractual Clauses, Module Three (Processor-to-Processor).

Subprocessor	Service / Purpose of Processing	Processing Location	International Transfer Mechanism
Hetzner Online GmbH	Serverless backup workers and temporary processing resources	European Union (Finland/Germany) by default; United States where selected by Customer and legally available.	No Restricted Transfer where processing is limited to the EEA. Processing of EEA Personal Data in the United States is permitted only where an applicable transfer mechanism under Chapter V GDPR is in place.
Contabo GmbH	Workers for Australia-region workloads, where selected by Customer	Australia	EU Standard Contractual Clauses (Module Three, Processor-to-Processor), executed between Contabo GmbH and Contabo Australia Ltd.
DigitalOcean, LLC	Legacy serverless worker for certain existing accounts	United States	EU-U.S. Data Privacy Framework (including UK Extension) and Swiss-U.S. Data Privacy Framework; EU Standard Contractual Clauses and UK Addendum as a fallback where applicable. Module Two or Module Three, as applicable to Customer's role.
Wasabi Technologies, LLC	Object storage supporting internal systems	European Union (Amsterdam)	Not a Restricted Transfer where processing is limited to the EEA.
Pusher Limited	Realtime job and status communications	United States by default; European Union available	EU Standard Contractual Clauses: Module Two where Customer acts as Controller; Module Three where Customer acts as Processor. UK Standard Contractual Clauses, as applicable.
Cloudflare, Inc.	Network delivery and security (anycast)	Global anycast network	Standard Contractual Clauses and/or Data Privacy Framework, as applicable.

Subprocessor	Service / Purpose of Processing	Processing Location	International Transfer Mechanism
ActiveCampaign, LLC (Postmark)	Transactional and backup-job notification email	United States	EU-U.S. Data Privacy Framework (including UK Extension) and Swiss-U.S. Data Privacy Framework; EU Standard Contractual Clauses and UK Addendum as a fallback where applicable. Module Two or Module Three, as applicable to Customer's role.
Intercom, Inc.	Customer support communications and materials submitted for support	European Union and United States	EU-U.S., Swiss-U.S. and UK-U.S. Data Privacy Framework; EU Standard Contractual Clauses and UK Addendum as a fallback where applicable. Module One for Account Data; Module Two or Module Three for Customer Personal Data, as applicable to Customer's role.
Functional Software, Inc. (Sentry)	Application error monitoring	European Union	Not a Restricted Transfer where processing is limited to the EEA.
SolarWinds Worldwide, LLC (Papertrail/Loggly)	Application and job-log management	United States	EU Standard Contractual Clauses, Module Two, together with the UK Addendum and Swiss Addendum, as applicable, under the executed SolarWinds Customer Data Processing Addendum.
OpenAI, L.L.C. / OpenAI Ireland Limited	Internal engineering and support assistance	European Union/Switzerland data: OpenAI Ireland Limited. Other Customer Personal Data: United States	EU Standard Contractual Clauses or applicable adequacy decision for EEA/Swiss data. UK Standard Contractual Clauses and UK Addendum for UK data.

Subprocessor	Service / Purpose of Processing	Processing Location	International Transfer Mechanism
Anthropic PBC	Internal engineering and support assistance	United States	EU Standard Contractual Clauses or applicable adequacy decision for EEA/Swiss data. UK Standard Contractual Clauses and UK Addendum for UK data.
Slack Technologies, LLC	Internal operations communication	United States	Salesforce Processor Binding Corporate Rules, where applicable; otherwise EU Standard Contractual Clauses, Module Two or Module Three, as applicable to Customer's role, together with the UK Addendum.
Google Ireland Limited (Google Workspace)	Support and administrative correspondence	Global infrastructure	EU Standard Contractual Clauses and UK Addendum, as applicable.

Customer-selected storage destinations and integrations are governed by Section 5.5.