ProBackup Data Processing Addendum

(On the basis of the Commission Standard Contractual Clauses)

Version 2026-11-23 — replaces the version of 2024-11-25

Between

The Customer accepting the ProBackup Terms of Service (https://www.probackup.io/terms-of-service) as required when accessing and using the ProBackup Services,

The "controller" as defined below,

And

ProBackup, a business line and the trade name owned and operated by Pro Backup BV, a company created under the laws of Belgium, with principal place of business at Kroonwinningstraat 113, 3500 Hasselt, Belgium, inscribed in the Crossroads Bank for Enterprises under the number 0555.782.383,

The "processor" as defined below,

Hereinafter jointly referred to as the "Parties" or each separately as a "Party".

Whereas,

The parties have concluded a software-as-a-service agreement for services provided by the processor enabling the controller to make back-ups of its files and data processed under certain cloud applications (the "Services"),

The processor provides the controller with the necessary storage space in the cloud in order to store backed-up data and files,

Now therefore, the Parties agree as follows,

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

SECTION II — OBLIGATIONS OF THE PARTIES

Clause 5

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 6

Obligations of the Parties

6.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or the applicable Union or Member State data protection provisions.

6.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

6.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

6.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

6.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

6.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least thirty (30) business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby — in the event the processor has factually disappeared, ceased to exist in law or has become insolvent — the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

6.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 6.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 7

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 7(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
3. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
4. the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 8

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor.

8.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

1. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. the likely consequences of the personal data breach;
3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

8.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III — FINAL PROVISIONS

Clause 9

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

1. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
2. the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679;
3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 6.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I: LIST OF PARTIES

Controller(s):

Shall be the natural or legal person agreeing to the General Terms and Conditions of ProBackup as set out in the heading of this data processing addendum. Controller shall be responsible for sharing information with processor on the persons responsible at its organisation for data protection matters.

Processor:

Name	Pro Backup BV
Address	Kroonwinningstraat 113, 3500 Hasselt, Belgium
Contact person's name, position and contact details	Willem Dewulf, CEO — +46790207459, will@probackup.io

ANNEX II: DESCRIPTION OF THE PROCESSING

A. Categories of data subjects whose personal data is processed

- Controller may submit personal data to the Services, the extent of which is determined and controlled by controller in its sole discretion, and which may include, but is not limited to personal data relating to the following categories of data subjects: members of controller's organisations, contact persons, controller's users authorized by controller to use the Services and other individuals.

B. Categories of personal data processed

- Controller determines the types of data processed in the Services. Controller's data fields can be configured as part of the implementation of the Services or as otherwise permitted in the Services. Identified representatives of controller determine what personal data is processed based on their use of the Services.

C. Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

- Controller may not submit sensitive personal data to the Services, unless otherwise agreed upon in writing. In that case, controller has the responsibility to process the data in accordance with Articles 9 and 10 GDPR and, as the case may be, as further regulated by applicable national legislation.

D. Nature of the processing

- Controller's personal data processed by the processor will be subject to the following basic processing activities: (1) use of controller's personal data to provide the Services and to provide assistance to technical support, (2) storage and backup of controller's personal data in data centres, and (3) computer processing of controller's personal data, including data transmission, data retrieval, data access.

E. Purpose(s) for which the personal data is processed on behalf of the controller

- The processor will process personal data as necessary to provide the Services pursuant to the General Terms and Conditions and as further instructed in writing by the controller in its use of the Service.

F. Duration of the processing

- Except as otherwise directed by the controller, personal data processed in the context of the Services is stored for the duration of the Services agreement concluded between the parties. The agreement ends when a free trial ends without a paid subscription being taken, when a cancelled subscription reaches the end of its paid term, or when the subscription is terminated for non-payment. Within ten (10) days after it ends, backups stop and ProBackup automatically and permanently deletes all backed-up data, attachments and related metadata of the controller. Until then the controller can

reverse the cancellation or export its data. On written request, ProBackup deletes the data sooner.

G. For processing by (sub-)processors, also specify subject matter, nature and duration of the processing

- Processing by (sub-)processors is further detailed under Annex IV and shall only be performed to provide the Services.

ANNEX III: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The Services run on Amazon Web Services ("AWS"), in data centres covered by AWS's ISO 27001, ISO 27017, ISO 27018 and SOC 2 reports. Application servers and metadata databases run in the AWS EU (Ireland) region (eu-west-1). Backed-up content (records and attachments) is stored in the AWS region the controller selects when it creates its account: EU (Ireland, the default), Germany, United Kingdom, United States, Canada, Brazil, Australia, Singapore or Israel. A controller that selects EU or Germany keeps its backed-up content in the European Union. Backed-up content is not replicated to other regions. ProBackup holds a SOC 2 Type 2 report covering Security, Availability and Confidentiality.

In compliance with its obligations under the applicable data protection laws, processor takes the following technical and organisational measures:

A. Measures of pseudonymisation and encryption of personal data

Customer Data is encrypted in transit with Transport Layer Security ("TLS") and at rest with AES-256 (Amazon S3 server-side encryption; Amazon RDS storage encryption with AWS KMS keys). OAuth tokens to the controller's SaaS applications are stored in encrypted form.

B. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

ProBackup maintains an information security program, which includes:

(a) having a formal risk management program, (b) conducting periodic risk assessments of systems and networks, (c) monitoring for security incidents and maintaining a remediation plan, (d) a written information security policy and incident response plan that explicitly addresses and provides guidance to its personnel in furtherance of the security, confidentiality, integrity, and availability of Customer Data, (e) penetration testing performed by a qualified third party, and (f) having resources responsible for information security efforts.

C. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

ProBackup keeps encrypted automated database backups with point-in-time recovery (7 days) and daily encrypted logical exports (14 days). A restore is tested at least once a year. Backed-up content is stored in Amazon S3, which keeps copies across several physically separate Availability Zones within the selected region and is versioned.

D. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures to ensure the security of the processing

ProBackup implements the following measures:

(a) cross-checking of vulnerability databases with all systems and software packages that support critical ProBackup services, (b) the use of automated source code scanners on

every code commit, (c) code reviews on every security-sensitive code commit, (d) vulnerability scanning on ProBackup services, and (e) penetration testing by an independent provider.

ProBackup evaluates the severity of every detected vulnerability in terms of the likelihood and potential impact of an exploit. It develops mitigation strategies and schedules accordingly.

E. Measures for user identification and authorization

Each individual having access to a ProBackup-controlled system, requires a Google Workspace user account denoting their system identity. The user accounts are required to have

(a) a unique username, (b) a unique strong password that meets ProBackup's password policy, and (c) a two-factor authentication (2FA) mechanism.

Authentication is performed by Google's account management system. ProBackup leverages Google Workspace's facilities for detecting malicious authentication attempts. Repeated failed attempts to authenticate may result in the offending user account being locked or revoked.

Whenever available, third-party systems must be configured to delegate authentication to ProBackup's Google Workspace account authentication system (described above) thereby consolidating authentication controls into a single user account system that is centrally managed. When authentication to Google Workspace is not available, unique strong passwords must be created and stored in a ProBackup approved password management system. Passwords must be paired with at least two-factor/multi-factor authentication ("MFA").

F. Measures for the protection of data during transmission

Customer Data is encrypted in transit using TLS (see section A).

G. Measures for the protection of data during storage

Customer Data is stored encrypted at rest in the AWS region selected by the controller (see the introduction and section A). Database backups are encrypted.

H. Measures for ensuring physical security of locations at which personal data are processed

ProBackup has no offices or servers of its own. Customer Data is stored in AWS data centres; the sub-processors listed in Annex IV process parts of it as described there. AWS is responsible for the physical and environmental security of its data centres, and ProBackup reviews AWS's independent audit reports (SOC 2, ISO 27001) at least once a year.

ProBackup's workforce is fully remote and works on laptops subject to ProBackup's endpoint security requirements, including full-disk encryption, malware protection, automatic screen lock and timely security patching. Devices are recorded in an asset inventory with an assigned owner.

I. Measures for ensuring events logging

All access to information security management systems at ProBackup are monitored and logged. At a minimum, log entries include date, timestamp, action performed, and the user ID or device ID of the action performed. The level of additional detail to be recorded by each audit log will be proportional to the amount and sensitivity of the information stored and/or processed on that system. All logs are protected from change.

J. Measures for ensuring system configuration, including default configuration

Production infrastructure is defined and changed through version-controlled configuration and deployment pipelines. Network access to production databases is restricted by default-deny firewall rules to ProBackup's private AWS network and a small number of named systems. Staff laptops follow ProBackup's endpoint security baseline (see section H). Systems are monitored and configured to detect and alert on suspicious activity.

K. Measures for internal IT and IT security governance and management

IT Security Governance and Management structures and processes are designed to ensure compliance with data protection principles at their effective implementation. ProBackup maintains a formal information security program. Senior management has assigned an Information Security Officer role that coordinates the security and privacy program and reports to management. Policies and procedures are reviewed at least annually and require management approval.

L. Measures for ensuring data minimisation

More information about how ProBackup processes personal data is set forth in the Privacy Policy available at https://probackup.io/privacy-policy.

M. Measures for ensuring data quality

More information about how ProBackup processes personal data is set forth in the Privacy Policy available at https://probackup.io/privacy-policy.

N. Measures for ensuring limited data retention

Customer Data is deleted automatically as described in Annex II F. A backup that the controller deletes in the application is removed within ten (10) days; trial backups are removed immediately. Deleted data can remain in encrypted, access-restricted infrastructure backups until those expire automatically: up to 2 days for object-storage versions and up to 15 days for database backups and exports. These copies are used only for disaster recovery. Records that ProBackup must keep by law, such as invoices, are kept for the legal retention period.

O. Measures for ensuring accountability

More information about how ProBackup processes personal data is set forth in the Privacy Policy available at https://probackup.io/privacy-policy.

P. Measures for allowing data portability and ensuring erasure

ProBackup provides web user interfaces (UIs) and data export facilities to provide customers access to their data. ProBackup's customers can exercise their rights of the Privacy Policy by sending an e-mail to info@probackup.io.

For more information on the ProBackup security measures, please contact info@probackup.io

ANNEX IV: LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors.

Backed-up content (the records and attachments the Services copy from the controller's cloud applications) is stored with Amazon Web Services, in the region the controller selects (see Annex III), and passes through Cloudflare in transit. Parts of it can reach other sub-processors only in three cases: a user sends it to ProBackup support (support email, chat and the AI models that help draft answers); it appears in an error report sent to Sentry; or ProBackup staff read it to diagnose a support case the controller raised. The other sub-processors process account, billing, support and usage data about the controller's users.

Each sub-processor processes personal data for the duration of the Services agreement (Annex II F), or for the shorter period stated below. Where a sub-processor processes personal data outside the European Economic Area, the transfer is covered by the Standard Contractual Clauses in its data processing agreement or, where the sub-processor is certified, by the EU-U.S. Data Privacy Framework.

ProBackup's AI support assistant, ReplyPen, is operated by ProBackup itself on Amazon Web Services in Frankfurt (eu-central-1); the AI models it uses are listed below.

A user who chooses to sign in with Google or Microsoft shares their identity with that provider under their own agreement with it; for sign-in, those providers are not sub-processors of ProBackup.

Sub-processor name	ActiveCampaign, LLC
Address	EU-REP.Global GmbH, Attn: ActiveCampaign, Hopfenstr. 1d, 24114 Kiel, Germany
Location	United States
Contact person's name, position and contact detail	activecampaign@eu-rep.global
Description of the processing activities	ProBackup uses ActiveCampaign to send product and promotional emails to its customers' users (name, email address, email engagement). https://www.activecampaign.com/legal/dpa

Sub-processor name	Amazon Web Services EMEA SARL
Address	Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg

Location	The AWS region selected by the controller for backed-up content; EU (Ireland), eu-west-1, for the application and its databases; EU (Frankfurt), eu-central-1, for ProBackup's support tooling
Contact person's name, position and contact detail	https://aws.amazon.com/contact-us/compliance-support/
Description of the processing activities	Amazon Web Services provides the server infrastructure for the Services: hosting, storage of all Customer Data, databases, sign-in (Amazon Cognito) and logging. AWS EMEA SARL is the AWS contracting entity and its registered address is in Luxembourg; the data sits in the regions above (see Annex III). https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf

Sub-processor name	Anthropic Ireland, Limited
Address	6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland
Location	United States
Contact person's name, position and contact detail	privacy@anthropic.com
Description of the processing activities	ProBackup staff use Anthropic's Claude models to review support email and the account information needed to answer it. From 1 December 2026 this runs under Anthropic's Commercial Terms and Data Processing Addendum (Claude Team), under which Anthropic does not use this data to train its models. https://www.anthropic.com/legal/data-processing-addendum

Sub-processor name	Automat-IT Malam Team Ltd.
Address	Derech Menachem Begin 121, 6701203 Tel Aviv-Yafo, Israel
Location	Israel
Contact person's name, position and contact detail	info@automat-it.com

Description of the processing activities	Automat-IT is the reseller through which ProBackup buys Amazon Web Services. It handles AWS billing and partner support and holds administrative access to ProBackup's AWS account, through which it can technically access the Customer Data stored there. Israel has an adequacy decision of the European Commission.
Sub-processor name	Billit NV
Address	Oktrooiplein 1, box 302, 9000 Ghent, Belgium
Location	European Union
Contact person's name, position and contact detail	https://www.billit.be/en/contact/
Description of the processing activities	ProBackup uses Billit to send electronic invoices over the Peppol network (company name, VAT number, billing address, invoice contact).
Sub-processor name	Cello (Powerplay GmbH)
Address	Sumpfmeisenweg 3A, 81249 Munich, Germany
Location	European Union
Contact person's name, position and contact detail	https://cello.so/data-processing-agreement/
Description of the processing activities	ProBackup uses Cello to run its referral programme (user identifier, name and email address of users who take part).
Sub-processor name	ClickUp (Mango Technologies, Inc.)
Address	350 Tenth Avenue, Suite 500, San Diego, CA 92101, United States
Location	United States
Contact person's name, position and contact detail	https://clickup.com/terms/dpa
Description of the processing activities	ProBackup uses ClickUp for internal task management and system alerts, including support cases that need an engineer (account identifiers, email address, case description).

Sub-processor name	Cloudflare, Inc.
Address	101 Townsend Street, San Francisco, CA 94107, United States
Location	Global network
Contact person's name, position and contact detail	https://www.cloudflare.com/cloudflare-customer-dpa/
Description of the processing activities	Cloudflare provides DNS, DDoS protection and a proxy in front of ProBackup's websites and API. All traffic between users and the Services, including Customer Data, passes through Cloudflare's network, where the encrypted connection is terminated and re-encrypted towards ProBackup.

Sub-processor name	Functional Software, Inc. (Sentry)
Address	45 Fremont Street, 8th Floor, San Francisco, CA 94105, United States
Location	United States
Contact person's name, position and contact detail	compliance@sentry.io
Description of the processing activities	ProBackup uses Sentry to track application errors: error reports with user identifier and email address, and recordings of a sample of web-application sessions, with all text, form inputs and images masked. https://sentry.io/legal/dpa/

Sub-processor name	GitHub, Inc.
Address	88 Colin P. Kelly Jr. Street, San Francisco, CA 94107, United States
Location	United States
Contact person's name, position and contact detail	https://github.com/customer-terms/github-data-protection-agreement
Description of the processing activities	ProBackup stores its source code and its internal support knowledge base on GitHub. The knowledge base holds pseudonymised support cases, which can include a user's email address.

Sub-processor name	Google Cloud EMEA Limited (Google Workspace)
Address	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Ireland
Location	Global
Contact person's name, position and contact detail	https://support.google.com/a/
Description of the processing activities	ProBackup uses Google Workspace for email, including support email, and internal documents. https://cloud.google.com/terms/data-processing-addendum

Sub-processor name	Google Cloud EMEA Limited (Vertex AI)
Address	70 Sir John Rogerson's Quay, Dublin 2, D02 R296, Ireland
Location	European Union
Contact person's name, position and contact detail	https://cloud.google.com/terms/data-processing-addendum
Description of the processing activities	ProBackup's AI support assistant uses Google's Gemini models through Vertex AI in the EU to draft answers to support requests (the request and the account information needed to answer it). Google does not store or train on this data, except that prompts flagged by its abuse filters may be kept for up to 90 days in the EU.

Sub-processor name	Intercom Software UK Limited
Address	Level 9, The Warehouse, 207-211 Old Street, London, EC1V 9NR, United Kingdom
Location	United States
Contact person's name, position and contact detail	Get in touch with the DPO through the messenger or by emailing dataprotection@intercom.io.
Description of the processing activities	ProBackup uses Intercom for in-app customer support (contact details, conversations). https://www.intercom.com/legal/data-processing-agreement

Sub-processor name	Mixpanel, Inc.

Address	San Francisco, CA, United States; EU representative: Mixpanel S.L., Avenida Diagonal 442, 08037 Barcelona, Spain
Location	United States
Contact person's name, position and contact detail	compliance@mixpanel.com
Description of the processing activities	ProBackup uses Mixpanel for product analytics (user identifier, email address, product usage events).

Sub-processor name	OpenAI Ireland Limited
Address	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland
Location	European Union
Contact person's name, position and contact detail	https://openai.com/policies/data-processing-addendum/
Description of the processing activities	ProBackup's AI support assistant uses OpenAI models with EU data residency and zero data retention to draft answers to support requests (the request and the account information needed to answer it). OpenAI does not store or train on this data.

Sub-processor name	PostHog, Inc.
Address	2261 Market Street #4008, San Francisco, CA 94114, United States
Location	European Union (Frankfurt)
Contact person's name, position and contact detail	privacy@posthog.com
Description of the processing activities	ProBackup's AI support assistant reports its own errors to PostHog's EU cloud; an error report can include the name or email address of the person who wrote to support.

Sub-processor name	Postmark (AC PM LLC, an ActiveCampaign company)
Address	AC PM LLC, 1 N Dearborn Street, Suite 500, Chicago, IL 60602, United States

Location	United States
Contact person's name, position and contact detail	privacy@activecampaign.com
Description of the processing activities	ProBackup uses Postmark to send transactional emails to its customers' users, such as sign-in codes, backup reports and invoices. https://postmarkapp.com/dpa

Sub-processor name	Segment (Twilio Inc.)
Address	101 Spear Street, 5th Floor, San Francisco, CA 94105, United States
Location	United States
Contact person's name, position and contact detail	https://www.twilio.com/en-us/legal/data-protection-addendum
Description of the processing activities	ProBackup uses Segment to collect product usage events and route them to its analytics tools (user identifier, name, email address, events).

Sub-processor name	Stape Europe OÜ
Address	Sepapaja tn 6, 15551 Tallinn, Estonia
Location	European Union
Contact person's name, position and contact detail	https://stape.io/eu-dpa
Description of the processing activities	ProBackup uses Stape to measure sign-ups and purchases for its advertising, server to server (email address, name, IP address, browser and ad-click identifiers). Stape forwards these events, with the email address hashed, to Google Ads, Meta, Microsoft Advertising and OpenAI Ads.

Sub-processor name	Stripe Payments Europe Limited
Address	C/O A&L Goodbody, IFSC, North Wall Quay, Dublin D01 H104, Ireland
Location	European Union and United States

Contact person's name, position and contact detail	You can reach Stripe's appointed Data Protection Officer (DPO) via email at dpo@stripe.com
Description of the processing activities	ProBackup uses Stripe to process online payments and manage customers' billing details. https://stripe.com/legal/dpa

Sub-processor name	Yuki (Visma)
Address	The Yuki Company (Visma), Netherlands
Location	European Union
Contact person's name, position and contact detail	https://www.yukisoftware.com/en-es/privacy-policy/
Description of the processing activities	ProBackup uses Yuki for its accounting: invoices and the billing details on them.

Sub-processor name	ZeroBounce (Hertza, L.L.C.)
Address	10 E. Yanonali Street, Santa Barbara, CA 93101, United States
Location	European Union
Contact person's name, position and contact detail	GDPR@zerobounce.net
Description of the processing activities	ProBackup uses ZeroBounce to check that the email address entered at sign-up can receive email.