ProBackup Data Processing Addendum

(On the basis of the Commission Standard Contractual Clauses)

Between

The Customer accepting the standard terms and conditions of ProBackup (link) 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
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 entire duration of the Services agreement concluded between the parties, including for a sixty (60) day notice period following a notification of termination. After such notice period, ProBackup deletes all files and data belonging to the controller from its servers.

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 are hosted in the European Union in an ISO 27001, ISO 27017, and ISO 27018 compliant environment via Amazon Web Services ('**AWS'**).

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** and encrypted **at rest**. The connections made to ProBackup are encrypted using Transport Layer Security ('**TLS**') and Secure Shell ('**ssh**').

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 takes regular snapshots of its databases and securely copies those snapshots to a separate data center for restoration purposes. Backups are also encrypted.

Customer Data is stored cross-regionally with AWS in the European Union for safeguarding availability.

D. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and uthorization 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 G Suite user account denoting their system identity. The user accounts are required to have

(a) a unique username,
(b) a unique strong password of at least 8 characters, and
(c) a two-factor authentication (2FA) mechanism.

Authentication is performed by Google's account management system, details of which can be found at https://gsuite.google.com/security. ProBackup leverages G Suite'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 G Suite account authentication system (described above) thereby consolidating authentication controls into a single user account system that is centrally managed by the security team.

When authentication to G Suite 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 encrypted protocols such as TLS or ssh (see above).

G. Measures for the protection of data during storage

Customer Data is stored cross-regionally with AWS. Data backups are encrypted. Customer data is encrypted at rest (see above).

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

Access to ProBackup is mediated by a staffed front office and programmable door control access. All doors remain locked or staffed under normal business conditions. The security team may provide approval to unlock doors for short periods of time in order to accommodate extenuating physical access needs.

Internet-based security cameras are positioned to record time-stamped video of ingress/egress. These files are stored off-site.

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

To prevent and minimize the potential for threats to ProBackup's systems, baseline configurations are required prior to deployment of any user, network, or production equipment. Baseline configurations are in place for wireless security settings in order to ensure strong encryption and replace vendor

default settings as part of deployment of network devices. Systems are centrally managed 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 with dedicated security personnel reporting to the CEO.

Policies and Procedures are regularly updated 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

ProBackup shall remove all data related to a customer within ten (10) days after the cancellation of their (trial) subscription.

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:

Sub-processor name	ActiveCampaign, LLC
Address	EU-REP.Global GmbH, Attn: ActiveCampaign Hopfenstr. 1d 24114 Kiel, Germany
Contact person's name, position and contact detail	activecampaign@eu-rep.global
Description of the processing activities	ProBackup is using ActiveCampaign to send transactional and promotional emails to their customers. For more info see https://www.activecampaign.com/legal/privacy-policy

Sub-processor name	Amazon
Address	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855 Luxembourg
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 ProBackup's functioning. Amazon Web Services' servers are located in Luxembourg. https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Sub-processor name	Google Workspace
Address	Google Cloud EMEA Limited 70 Sir John Rogerson's Quay, D02 R296 Dublin 2, Dublin, Ireland

Contact person's name, position and contact detail	https://support.google.com/a/?visit_id=637854582622180889-2874424361&rd=2#topic=4388346
Description of the processing activities	ProBackup uses Google Workspace for email management. https://policies.google.com/terms https://www.google.com/drive/terms-of-service/
Sub-processor name	Intercom Software UK Limited
Address	Level 9 The Warehouse 207-211 Old S London, EC1V 9NR United Kingdom
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 customer support management. https://www.intercom.com/legal/privacy
Sub-processor name	Postmark, trademark of ActiveCampagin
Address	AC PM LLC 1 N Dearborn Street, Suite 500 Chicago, IL 60602, United States
Contact person's name, position and contact detail	privacy@activecampaign.com
Description of the processing activities	ProBackup is using postmark app to send emails to their customers. The data processing agreement is available to the controller upon request to processor.

Sub-processor name	Sentry, trademark of Functional Software, Inc.
Address	Functional Software, Inc. 45 Fremont Street, 8th Floor, San Francisco CA 94105, United States
Contact person's name, position and contact detail	compliance@sentry.io.
Description of the processing activities	ProBackup uses Sentry to track issues and error logs. https://sentry.io/legal/dpa/

Sub-processor name	Stripe Payments Europe Ltd.
Address	Stripe Payments Europe Ltd., C/O A&L Goodbody, Ifsc, North Wall Quay, Dublin D01 H104, Ireland
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 their online payments and manage their customer billing details.