

## PROBAX DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") amends the terms and forms part of the Agreement (defined below) by and between the customer as identified in the Agreement ("**Customer**") and the applicable Probax entity from which Customer is purchasing Cloud Products ("**Probax**") and will be effective on the later of (i) the effective date of the Agreement; or (ii) the date both parties execute this DPA in accordance with Section 1 below ("**Effective Date**"). All capitalized terms not defined in this DPA have the meanings set forth in the Agreement.

### 1. Instructions and Effectiveness

1.1. This DPA has been pre-signed on behalf of Probax. To enter into this DPA, Customer must:

- (a) be a customer of the Cloud Products;
- (b) complete the signature block below by signing and providing all relevant information; and
- (c) submit the completed and signed DPA to Probax.

1.2. This DPA will only be effective (as of the Effective Date) if executed and submitted to Probax accurately and in full accordance with Section 1. Where Customer makes any deletions or other revisions to this DPA, this DPA will be null and void.

1.3. Customer signatory represents to Probax that he or she has the legal authority to bind Customer and is lawfully able to enter into this DPA.

### 2. Data Protection

2.1 **Definitions:** In this DPA, the following terms have the following meanings:

- (a) "**Agreement**" means the contract in place between Customer and Probax in connection with the purchase of Cloud Products by Customer.
- (b) "**Applicable Data Protection Law**" means U.S. Data Protection Law and European Data Protection Law that are applicable to the processing of personal data under this DPA.
- (c) "**Cloud Products**" means the software, platform, infrastructure, or other "as a service" solutions that the Customer has subscribed to.
- (d) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") have the meanings given in European Data Protection Law.
- (e) "**Customer Personal Data**" means any personal data provided by (or on behalf of) Customer to Probax in connection with the Services, all as further described in Exhibit A, Annex 1(B), Part A of this DPA.
- (f) "**End Users**" means an individual the Customer permits or invites to use the Cloud Products. For the avoidance of doubt: (a) individuals invited by End Users, (b) individuals under managed accounts, and (c) individuals interacting with a Cloud Product as Customer's customers are also considered End Users.
- (g) "**Europe**" means for the purposes of this DPA, the Member States of the European Economic Area ("**EEA**"), the United Kingdom ("**UK**") and Switzerland.

- (h) **“European Data Protection Law”** means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (**“EU GDPR”**); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the EU GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (**“UK Data Protection Law”**); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) the Swiss Federal Data Protection Act and its implementing regulations (**“Swiss DPA”**), in each case as may be amended, superseded or replaced from time to time.
- (i) **“Privacy Shield Principles”** means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).
- (j) **“Restricted Transfer”** means a transfer (directly or via onward transfer) of personal data that is subject to European Data Protection Law to a country outside Europe that is not subject to an adequacy decision by the European Commission, or the competent UK or Swiss authorities (as applicable).
- (k) **“Security Incident”** means any confirmed breach of security that leads to the accidental, or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data processed by Probax and/or its Sub-processors in connection with the provision of the Service. For the avoidance of doubt, "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- (l) **“Services”** means the provision of the Cloud Products by Probax to Customer pursuant to the Agreement.
- (m) **“special categories of personal data”** or **“sensitive data”** means any Customer Personal Data (i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (ii) that is genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation, and (iii) relating to criminal convictions and offences.
- (n) **“Standard Contractual Clauses”** or **“EU SCCs”** means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
- (o) **“Sub-processor”** means any processor engaged by Probax to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA where such entity processes Customer Personal Data. Sub-processors may include Probax's affiliates or other third parties.
- (p) **“UK Addendum”** means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under S119(A) of the UK Data Protection Act 2018, as may be amended, superseded, or replaced from time to time.
- (q) **“U.S. Data Protection Law”** means those data protection or privacy laws and regulations within the United States, including the California Consumer Privacy Act (as amended) (the **“CCPA”**), as applicable to Customer Personal Data.

- 2.2 **Relationship of the parties:** Where Applicable Data Protection Law provides for the roles of “controller,” “processor,” and “sub-processor”:
- (a) Where Probax processes Customer Personal Data on behalf of Customer in connection with the Services, Probax will process such personal data as a processor or Sub-processor on behalf of Customer (who, in turn, processes such personal data as a controller or processor) and this DPA will apply accordingly. A description of such processing is set out in Exhibit A, Annex 1(B), Part A.
  - (b) Where Probax processes personal data as a controller, as further detailed in Exhibit A, Annex 1(B), Part B, Probax will process such personal data in compliance with Applicable Data Protection Law and only for the purposes that are compatible with those described in Exhibit A, Annex 1(B), Part B. For these purposes, only Sections 2.3 and 2.6 of this DPA will apply, to the extent applicable.
- 2.3 **Description of Processing:** A description of the processing of personal data related to the Services, as applicable, is set out in Exhibit A. Probax may update the description of processing from time to time to reflect new products, features or functionality comprised within the Services. Probax will update relevant documentation to reflect such changes.
- 2.4 **Customer Processing of Personal Data:** Customer agrees that (i) it will comply with its obligations under Applicable Data Protection Law in its processing of Customer Personal Data and any processing instructions it issues to Probax, and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under Applicable Data Protection Law for Probax to process personal data (including but not limited to any special categories of personal data) and provide the Services pursuant to the Agreement (including this DPA).
- 2.5 **Probax Processing of Personal Data:** When Probax processes Customer Personal Data in its capacity as a processor on behalf of the Customer, Probax will process the Customer Personal Data as necessary to perform its obligations under the Agreement, and only in accordance with the documented lawful instructions of Customer (as set forth in the Agreement, in this DPA, or as directed by the Customer or Customer’s End Users through the Cloud Products) (the “**Permitted Purpose**”). Probax will not retain, use, disclose or otherwise process the Customer Personal Data for any purpose other than the Permitted Purpose except where otherwise required by law(s) that are not incompatible with Applicable Data Protection Law, and will not “sell” the Customer Personal Data within the meaning of the CCPA or otherwise. Probax will promptly inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Law.
- 2.6 **Restricted transfers:** The parties agree that when the transfer of personal data from Customer (as “data exporter”) to Probax (as “data importer”) is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, the transfer will be subject to the Standard Contractual Clauses, which are deemed incorporated into and form a part of this DPA, as follows:
- (a) In relation to transfers of Customer Personal Data protected by the EU GDPR and processed in accordance with Section 2.2(a) of this DPA, the EU SCCs will apply, completed as follows:

- i. Module Two or Module Three will apply (as applicable);
  - ii. in Clause 7, the optional docking clause will apply;
  - iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes will be as set out in Section 2.10 of this DPA;
  - iv. in Clause 11, the optional language will not apply;
  - v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
  - vi. in Clause 18(b), disputes will be resolved before the courts of Ireland;
  - vii. Annex I of the EU SCCs is deemed completed with the information set out in Exhibit A to this DPA, as applicable; and
  - viii. Subject to Section 2.8 of this DPA, Annex II of the EU SCCs is deemed completed with the information set out in Exhibit B to this DPA;
- (b) In relation to transfers of personal data protected by the EU GDPR and processed in accordance with Section 2.2(b) of this DPA, the EU SCCs apply, completed as follows:
- i. Module One will apply;
  - ii. in Clause 7, the optional docking clause will apply;
  - iii. in Clause 11, the optional language will not apply;
  - iv. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
  - v. in Clause 18(b), disputes will be resolved before the courts of Ireland;
  - vi. Annex I of the EU SCCs is deemed completed with the information set out in Exhibit A to this DPA, as applicable; and
  - vii. Subject to Section 2.8 of this DPA, Annex II of the EU SCCs is deemed completed with the information set out in Exhibit B to this DPA;
- (c) In relation to transfers of personal data protected by UK Data Protection Law, the EU SCCs: (i) apply as completed in accordance with paragraphs (a) and (b) above; and (ii) are deemed amended as specified by the UK Addendum, which is deemed executed by the parties and incorporated into and forming an integral part of this DPA. In addition, Tables 1 to 3 in Part 1 of the UK Addendum is deemed completed respectively with the information set out in Section 2.9, as well as Exhibits A and B of this DPA; Table 4 in Part 1 is deemed completed by selecting “neither party.” Any conflict between the terms of the EU SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.
- (d) In relation to transfers of personal data protected by the Swiss DPA, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above, with the following modifications:
- i. any references in the EU SCCs to “Directive 95/46/EC” or “Regulation (EU) 2016/679” will be interpreted as references to the Swiss DPA, and references to specific Articles of “Regulation (EU) 2016/679” will be replaced with the equivalent article or section of the Swiss DPA;
  - ii. references to “EU”, “Union”, “Member State” and “Member State law” will be interpreted as references to Switzerland and Swiss law, as the case may be, and will not be interpreted in such a way as to exclude data subjects in Switzerland from

exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs;

- iii. Clause 13 of the EU SCCs and Part C of Annex 1 are modified to provide that the Federal Data Protection and Information Commissioner (“**FDPIC**”) of Switzerland will have authority over data transfers governed by the Swiss DPA. Subject to the foregoing, all other requirements of Clause 13 will be observed;
  - iv. references to the “competent supervisory authority” and “competent courts” will be interpreted as references to the FDPIC and competent courts in Switzerland;
  - v. in Clause 17, the EU SCCs will be governed by the laws of Switzerland; and
  - vi. Clause 18(b) states that disputes will be resolved before the applicable courts of Switzerland.
- (e) It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA), the Standard Contractual Clauses prevail to the extent of such conflict;
- (f) Although Probax does not rely on the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks (“**Privacy Shield**”) as a legal basis for transfers of personal data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for so long as Probax and its covered entities are self-certified to the Privacy Shield, Probax will continue to process personal data in accordance with the Privacy Shield Principles. Probax will promptly notify Customer if it makes a determination that Probax can no longer meet its obligations under the Privacy Shield Principles; and
- (g) If Probax adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to Applicable Data Protection Law) for the transfer of personal data not described in this DPA (“**Alternative Transfer Mechanism**”), the Alternative Transfer Mechanism will apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Law and extends to the territories to which personal data is transferred).

2.7 **Confidentiality of processing:** Probax must ensure that any person that it authorizes to process Customer Personal Data (including Probax’s staff, agents and Sub-processors) will be subject to a duty of confidentiality (whether a contractual duty or a statutory duty) and must not permit any person to process Customer Personal Data who is not under such a duty of confidentiality.

2.8 **Security:** Probax and, to the extent required under the Agreement, Customer must implement appropriate technical and organizational measures in accordance with Applicable Data Protection Law (e.g., Art. 32 GDPR) to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data. Probax’s current technical and organizational measures are described in Exhibit B (“Security Measures”). Customer acknowledges that the Security Measures are subject to technical progress and development and that Probax may

update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

- 2.9 **Sub-processing:** Customer agrees that Probax may engage Sub-processors to process Customer Personal Data on Customer's behalf. The Sub-processors currently engaged by Probax and authorized by Customer are listed at <https://www.probax.io/subprocessors>. Probax will: (i) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect the Customer Personal Data to the standard required by Applicable Data Protection Law (and in substance, to the same standard provided by this DPA); and (ii) remain liable to Customer if such Sub-processor fails to fulfill its data protection obligations with regard to the relevant processing activities under Applicable Data Protection Law.
- 2.10 **Changes to Sub-processors:** Probax must (i) make available an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and (ii) notify Customer if it adds any new Sub-processors at least fourteen (14) days' prior to allowing such Sub-processor to process Customer Personal Data. Customer may object in writing to Probax's appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such an event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the Agreement (including this DPA) for convenience.
- 2.11. **Cooperation obligations and data subjects' rights:**
- (a) Taking into account the nature of the processing, Probax must provide reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, to rectification, to erasure, to restriction, to objection, and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party, in each case in respect of Customer Personal Data that Probax processes on Customer's behalf;
  - (b) In the event that any request, correspondence, enquiry or complaint (referred to under paragraph (a) above is made directly to Probax, Probax acting as a processor will not respond to such communication directly without Customer's prior authorization, unless legally required to do so, and instead, after being notified by Probax, Customer may respond. If Probax is legally required to respond to such a request, Probax will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so; and
  - (c) To the extent Probax is required under Applicable Data Protection Law, Probax will (at Customer's request and expense) provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities, taking into account the nature of processing and the information available to Probax.

- 2.12. **Security incidents:** Upon becoming aware of a Security Incident, Probax will inform Customer without undue delay and provide timely information (taking into account the nature of processing and the information available to Probax) relating to the Security Incident as it becomes known or as is reasonably requested by Customer to allow Customer to fulfill its data breach reporting obligations under Applicable Data Protection Law. Probax will further take reasonable steps to contain, investigate, and mitigate the effects of the Security Incident. Probax's notification of or response to a Security Incident in accordance with this Section 2.12 will not be construed as an acknowledgment by Probax of any fault or liability with respect to the Security Incident.
- 2.13. **Deletion or return of Data:** Upon written request from Customer, Probax will delete or return to Customer all Customer Personal Data (including copies) processed on behalf of the Customer in compliance with the procedures and retention periods outlined in the DPA, Cloud Product Specific Terms or Trust Centre; this requirement does not apply to the extent Probax is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data Probax will securely isolate and protect from any further processing, as further detailed in Exhibit A, Annex 1(B), Part A.
- 2.14. **Audit Rights:** Customer acknowledges that Probax is regularly audited by independent third-party auditors and/or internal auditors including as may be described from time to time at <https://www.probax.io/compliance>. Upon request, and on the condition that Customer has entered into an applicable non-disclosure agreement with Probax, Probax must provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of Customer Personal Data, including responses to information security and audit questionnaires, that are necessary to confirm Probax's compliance with this DPA, provided that Customer cannot exercise this right more than once per calendar year.
- 2.15. **Law enforcement:** If a law enforcement agency sends Probax a demand for Customer Personal Data (e.g., a subpoena or court order), Probax will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Probax may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Data to a law enforcement agency, then Probax will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Probax is legally permitted to do so.

### 3. Relationship with the Agreement

- 3.1. The parties agree that this DPA replaces and supersedes any existing DPA the parties may have previously entered into in connection with the Services.
- 3.2. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA will prevail to the extent of that conflict in connection with the processing of Customer Personal Data. If there is any conflict between the Standard Contractual Clauses and the Agreement (including this DPA), the Standard Contractual Clauses will prevail to the extent of that conflict in connection with the processing of Customer Personal Data governed under the Standard Contractual Clauses.

- 3.3. Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's affiliates under this DPA is subject to the exclusions and limitations of liability set out in the Agreement.
- 3.4. Any claims against Probax or its affiliates under this DPA can only be brought by the Customer entity that is a party to the Agreement against the Probax entity that is a party to the Agreement. In no event will this DPA or any party restrict or limit the rights of any data subject or of any competent supervisory authority.
- 3.5. This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.
- 3.6. This DPA and the Standard Contractual Clauses will terminate simultaneously and automatically upon deletion by Probax of the Customer Personal Data processed on behalf of the Customer, in accordance with Section 2.13 of this DPA.

### Customer Signatures


<b>CUSTOMER</b>	<p>Customer name (Required): _____</p> <p>Address: _____</p> <p>Signature (Required): _____</p> <p>Name (Required): _____</p> <p>Title (Optional): _____</p> <p>Date (Required): _____</p> <p>EU Representative (Required only where applicable): _____</p> <p>Contact details: _____</p> <p>Data Protection Officer (Required only where applicable): _____</p> <p>Contact details: _____</p>
-----------------	--



## Probax Signature

Data Protection Compliance Contact: Sam Meegahage

Contact Details: [compliance@probax.io](mailto:compliance@probax.io)

<b>Probax Pty Ltd</b>	Signature:  Name: Sam Meegahage Title: Chief Operating Officer Date: 24 November 2022
-----------------------	---

## EXHIBIT A

### Description of the Processing Activities / Transfer

<b>Annex 1(A) List of Parties: Data Exporter</b>	<b>Data Importer</b>
<b>Name:</b> Customer	<b>Name:</b> Probax
<b>Address / Email Address:</b> As provided for in the DPA	<b>Address / Email Address:</b> As provided for in the DPA
<b>Contact Person's Name, position, and contact details:</b> As provided for in the DPA	<b>Contact Person's Name, position, and contact details:</b> As provided for in the DPA
<b>Activities relevant to the transfer:</b> See Annex 1(B) below	<b>Activities relevant to the transfer:</b> See Annex 1(B) below
<b>Role:</b> See Annex 1(B)	<b>Role:</b> See Annex 1(B)

## Annex 1(B) Description of processing and transfer (as applicable)

The parties acknowledge that Probax's processing of personal data will include all personal data submitted or uploaded to the Services by Customer from time to time, for the purposes of, or otherwise in connection with, Probax providing the Services to Customer.

Set out below are descriptions of the processing and transfers of personal data as contemplated as of the date of this DPA. Such descriptions are subject to change or may be supplemented pursuant to Section 2.3 of the DPA.

### Part A: Description of processing and transfer (as applicable) for Modules 2 and 3 of the Standard Contractual Clauses (reference to Sections 2.2(a) as well as 2.6(a) DPA)

Hive	
<i>Categories of data subjects</i>	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Services on behalf of the Customer.
<i>Categories of personal data transferred</i>	<p><i>User Account Information, for example:</i></p> <ul style="list-style-type: none"> <li>• Probax identifier associated with user account</li> <li>• Sub-account names</li> <li>• Full name</li> <li>• Email address</li> <li>• Time zone</li> </ul> <p><i>Personal Identification, for example:</i></p> <ul style="list-style-type: none"> <li>• IP address</li> <li>• Location/ Region/ City</li> </ul> <p><i>Employment Information, for example:</i></p> <ul style="list-style-type: none"> <li>• Office / location</li> <li>• Company/organisation</li> </ul>
<i>Sensitive data transferred?</i>	No.
<i>Frequency of the transfer</i>	Continuous.
<i>Nature of the processing</i>	<p>Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.</p> <p><b>Note:</b> Customers utilise Hive to create sub-accounts and implement, monitor and manage all end-customer data protection jobs (within the platform). All data stored and processed is necessary for providing the Services.</p>
<i>Purpose of the data transfer</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Duration of processing</i>	Upon termination, Customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the Customer's current subscription period. Probax retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for all paid plans) after the end of the Customer's current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days.

Scout	
<i>Categories of data subjects</i>	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Services on behalf of the Customer.
<i>Categories of personal data transferred</i>	<p><i>Device identification data, for example:</i></p> <ul style="list-style-type: none"> <li>• Device information</li> <li>• IP address</li> </ul> <p><i>Employment Information and localisation data, for example:</i></p> <ul style="list-style-type: none"> <li>• Office / location</li> <li>• Company/organisation</li> </ul>
<i>Sensitive data transferred?</i>	No.
<i>Frequency of the transfer</i>	Continuous.
<i>Nature of the processing</i>	<p>Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.</p> <p><b>Note:</b> Scout acts as the information collector for Hive. It retrieves data from Veeam regarding job statistics, error messages, log files, and license status.</p>
<i>Purpose of the data transfer</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Duration of processing</i>	Only when installed. When a Customer uninstalls Scout from a device, data will cease to be processed.

<b>Honeycomb Storage (Hot/Cold/Object)</b>	
<i>Categories of data subjects</i>	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Services on behalf of the Customer.
<i>Categories of personal data transferred</i>	<p>Customer data is stored within data protection jobs that Probax recommends be encrypted (configured in Veeam) so no personal data is readable. If unencrypted, the following categories apply:</p> <p><i>User Account Information, for example:</i></p> <ul style="list-style-type: none"> <li>• Identifier associated with user account</li> <li>• Full name</li> <li>• Email address</li> <li>• Time zone</li> </ul> <p><i>Personal Identification, for example:</i></p> <ul style="list-style-type: none"> <li>• Location/ Region/ City</li> <li>• Phone numbers</li> </ul> <p><i>Employment Information, for example:</i></p> <ul style="list-style-type: none"> <li>• Job title / role</li> <li>• Office / location</li> <li>• Company/organization</li> </ul> <p><i>Device identification data, for example:</i></p> <ul style="list-style-type: none"> <li>• Device information</li> <li>• IP address</li> </ul> <p><i>Sensitive personal information, for example:</i></p> <ul style="list-style-type: none"> <li>• health and medical information (if transferred and stored in backup data unencrypted)</li> </ul> <p>Note: other categories of personal data may be transferred if transferred and stored in backup data unencrypted.</p>
<i>Sensitive data transferred?</i>	None (as long as jobs are encrypted).
<i>Frequency of the transfer</i>	Set by the Customer (hourly, daily, weekly, monthly, etc.).
<i>Nature of the processing</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Purpose of the data transfer</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Duration of processing</i>	<p>Customers can delete their replication data at any time.</p> <p>If a customer has ceased business with Probax they can delete their data manually, request the support team to delete it immediately, or wait for the 30-day period past their account expiration and Probax's automated processes will delete the data.</p>

Second Colony DRaaS	
<i>Categories of data subjects</i>	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Services on behalf of the Customer.
<i>Categories of personal data transferred</i>	<p><i>User Account Information, for example:</i></p> <ul style="list-style-type: none"> <li>• Identifier associated with user account</li> <li>• Full name</li> <li>• Email address</li> <li>• Time zone</li> </ul> <p><i>Personal Identification, for example:</i></p> <ul style="list-style-type: none"> <li>• Location/ Region/ City</li> <li>• Phone numbers</li> </ul> <p><i>Employment Information, for example:</i></p> <ul style="list-style-type: none"> <li>• Job title / role</li> <li>• Office / location</li> <li>• Company/organization</li> </ul> <p><i>Sensitive personal information, for example:</i></p> <ul style="list-style-type: none"> <li>• health and medical information (if replicated and stored in protected virtual machine)</li> </ul> <p>Note: other categories of personal data may be transferred if stored and replicated from a protected virtual machine.</p>
<i>Sensitive data transferred?</i>	Yes, depending on what has been stored on a replicated (protected) virtual machine.
<i>Frequency of the transfer</i>	Set by the Customer (continuous, hourly, daily, weekly, monthly, etc.).
<i>Nature of the processing</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Purpose of the data transfer</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Duration of processing</i>	<p>Customers can delete their backup data at any time.</p> <p>If a customer has ceased business with Probax they can delete their data manually, request the support team to delete it immediately, or wait for the 30-day period past their account expiration and Probax's automated processes will delete the data.</p>

<b>Microsoft 365 Backup &amp; Archive</b>	
<i>Categories of data subjects</i>	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Services on behalf of the Customer.
<i>Categories of personal data transferred</i>	<p><i>User Account Information, for example:</i></p> <ul style="list-style-type: none"> <li>• Identifier associated with M365 user account</li> <li>• Full name</li> <li>• Email address</li> <li>• Time zone</li> </ul> <p>All other categories of personal data are encrypted during transit and rest (AES256).</p>
<i>Sensitive data transferred?</i>	No, all sensitive data is encrypted.
<i>Frequency of the transfer</i>	Every 4 hours.
<i>Nature of the processing</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Purpose of the data transfer</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Duration of processing</i>	Upon termination, Customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the Customer's current subscription period. Probax retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the Customer's current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days.

<b>Dropbox Backup &amp; Archive</b>	
<i>Categories of data subjects</i>	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Services on behalf of the Customer.
<i>Categories of personal data transferred</i>	<p><i>User Account Information, for example:</i></p> <ul style="list-style-type: none"> <li>• Identifier associated with M365 user account</li> <li>• Full name</li> <li>• Email address</li> <li>• Time zone</li> </ul> <p>All other categories of personal data are encrypted during transit and rest (AES256).</p>
<i>Sensitive data transferred?</i>	No, all sensitive data is encrypted.
<i>Frequency of the transfer</i>	Daily.
<i>Nature of the processing</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Purpose of the data transfer</i>	Providing the Services, including maintaining and displaying user profiles and Services data during use, authentication of users, and managing access control as well as user permissions.
<i>Duration of processing</i>	Upon termination, Customer accounts are deactivated within 15 days (for monthly subscriptions) and 17 days (for annual subscriptions) after the end of the Customer's current subscription period. Probax retains data for deactivated products for 15 days (for evaluation licenses) or 60 days (for Free, Standard, and Premium product plans) after the end of the Customer's current subscription period. Upon deletion, an archive of the data is kept for an additional 30 days.



**Part B: Description of processing and transfer (as applicable) for Module 1 of the Standard Contractual Clauses (reference to Sections 2.2(b) as well as 2.6(b) DPA)**

<b>All Cloud Products: Probax as a controller</b>	
<i>Categories of data subjects</i>	Customer, Customers' employees, Customers' collaborators, as well as all relevant End Users of the Services on behalf of the Customer.
<i>Categories of personal data transferred</i>	<p><i>Personal data relating to or obtained in connection with the operation, support or use of the Services, e.g.:</i></p> <p>User Account Information, for example pseudonymous Probax IDs, Account IDs, Cloud IDs, Site IDs, Tenant ID.</p> <p><i>Payment and billing information, to the extent it includes personal data</i></p> <p><i>Device and connection information, for example:</i></p> <ul style="list-style-type: none"> <li>• IP address</li> <li>• Cookie information</li> <li>• Device information</li> <li>• Browser information</li> </ul> <p>Note: Personal data provided through various Probax support channels, including for example Probax ID, Account ID, username, contact information and any personal data contained within a summary of the problem experienced or information needed to resolve the support case. If any user generated content is submitted via support tickets, Probax acts as a processor of such personal data and Sections 2.2(a) as well as 2.6(a) DPA apply accordingly.</p>
<i>Sensitive data transferred?</i>	None
<i>Frequency of the transfer</i>	Continuous
<i>Nature of the processing</i>	Collection, storage, and processing of relevant personal data for the purposes identified in this Part B.
<i>Purpose of the data transfer</i>	<p>Personal data will be processed for Probax's legitimate business purposes. This entails in particular the following:</p> <ul style="list-style-type: none"> <li>• To facilitate security, fraud prevention, performance monitoring, business continuity and disaster recovery in order to protect Customers, End Users and Probax.</li> <li>• To engage and to provide support and assistance to Customer and End Users as requested from time to time.</li> <li>• To comply with legal and financial reporting obligations.</li> <li>• To administer the Services, including to calculate usage-based billing.</li> <li>• To derive insights in order to maintain, develop, and improve the Services and support, including for research and development purposes.</li> <li>• To derive insights in order to inform internal business analysis and product strategy.</li> </ul>
<i>Duration of processing</i>	Probax may process personal data for the purposes described above for the duration of the DPA, and for as long as Probax has a legitimate need to retain the personal data for the purposes it was collected or transferred, in accordance with Applicable Data Protection Law.

Last Updated: 24 November 2022

### **Annex 1(C): Competent supervisory authority**

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

## EXHIBIT B

### Technical and Organisational Security Measures

#### 1. Purpose

This Exhibit describes Probax’s security program, security certifications, and physical, technical, organizational and administrative controls and measures to protect Customer Data from unauthorized access, destruction, use, modification or disclosure (the “**Security Measures**”). The Security Measures are intended to be in line with the commonly-accepted standards of similarly-situated cloud service providers (“**industry standard**”). The Security Measures apply to all Probax Cloud Products that are available under the Agreement.

#### 2. Updates and Modifications

The Security Measures are subject to technical progress and development and Probax may update or modify the Security Measures from time to time, provided that such updates and modifications do not materially degrade or diminish the overall security of the Cloud Products, as described in this document.

#### 3. Definitions

Any capitalised terms used but not defined in this document have the meanings set out in the Agreement. The term “**Customer Data**” means any data, content or materials provided to Probax by or at the direction of Customer or its End Users via the Cloud Products, including from Third-Party Products.

#### 4. Security Measures

The Security Measures are described in the following table: <b>Measure</b>	<b>Description</b>
<i>Measures of pseudonymisation and encryption of personal data</i>	<p><b>Data Encryption</b></p> <p>Probax has and will maintain: (i) an established method to encrypt Customer Data in transit and at rest; (ii) an established method to securely store passwords following industry standard practices; and (iii) use established key management methods.</p> <p>Any Customer Data is encrypted in transit over public networks using TLS 1.2 or greater, with Perfect Forward Secrecy (PFS) to protect it from unauthorized disclosure or modification.</p> <p>Data drives on servers holding Customer Data and attachments use full disk, industry-standard, AES-256 encryption at rest.</p>
<i>Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services</i>	<p><b>Security Program</b></p> <p>Probax will maintain a security management program that includes but is not limited to:</p> <ul style="list-style-type: none"> <li>(a) executive review, support and accountability for all security related policies and practices;</li> <li>(b) a written information security policy and framework that meets or exceeds industry standards and that, as a baseline, includes (i) defined information security roles and responsibilities, (ii) a formal and effective risk mitigation program and (iii) a service provider security management program;</li> <li>(c) periodic risk assessments of all Probax owned or leased systems processing Customer Data;</li> <li>(d) prompt review of security incidents affecting the security of Probax systems processing Customer Data, including determination of root cause and corrective action;</li> </ul>

	<p>(e) a formal controls framework based on, among other things, formal audit standards such as the SOC 2 Type II report;</p> <p>(f) processes to document non-compliance with the security measures;</p> <p>(g) processes to identify and quantify security risks, develop mitigation plans, which must be approved by Probax’s Chief Operating Officer (or one of their delegates), and track the implementation of such plans; and</p> <p>(h) a comprehensive security testing methodology that consists of diverse and independent approaches that, when combined, are reasonably designed to maximize coverage for a varied and diverse set of attack vectors.</p> <p>Probax will periodically (and, in any event, no less frequently than annually) review, test and, where applicable, update such security management program.</p> <p><b>Security Incident Notification</b>          Probax will notify Customer of Security Incidents in accordance with the Probax Data Processing Addendum.</p> <p><b>Employee Screening, Training, Access and Controls</b>          Probax will maintain policies and practices that include the following controls and safeguards applied to Probax staff who have access to Customer Data and/or provide Support and Services to Customer:</p> <p>(a) pre-hire background checks (including criminal record inquiries) on Probax job candidates, which are conducted by a third-party background check provider and in accordance with applicable Laws and generally accepted industry standards;</p> <p>(b) periodic security awareness training;</p> <p>(c) a disciplinary policy and process to be used when Probax staff violate Probax’s security policies;</p> <p>(d) access to Probax IT systems only from approved Probax-managed devices with appropriate technical security controls (including two-factor authentication);</p> <p>(e) controls designed to limit access to Customer Data to only those Probax staff with an actual need-to-know such Customer Data. Such controls include the use of a formal access management process for the request, review, approval and provisioning for all Probax staff with access to Customer Data; and</p> <p>(f) separation of duties to prevent a single Probax employee from controlling all key aspects of a critical transaction or business process related to Customer Data or systems.</p> <p><b>Other matters</b>          See the items below titled “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,” and “Measures for the protection of data during storage”.</p>
<p><i>Measures for ensuring the ability to restore the</i></p>	<p><b>Resilience Program</b></p>

<p><i>availability and access to personal data in a timely manner in the event of a physical or technical incident</i></p>	<p>During the Agreement Term, Probax’s business continuity and disaster recovery plans (collectively, the “BCDR Plans”) will address at least the following topics:</p> <ul style="list-style-type: none"> <li>(a) the availability of human resources with appropriate skill sets;</li> <li>(b) the availability of all IT infrastructure, telecommunications capabilities and any other technology used or relied upon by Probax in the provision of the Products;</li> <li>(c) Probax’s plans for storage and continuity of use of data and software;</li> <li>(d) clear recovery time objectives (RTOs) and recovery point objectives (RPOs);</li> <li>(e) mechanisms for the geographic diversity or back-up of business operations;</li> <li>(f) the potential impact of cyber events and Probax’s ability to maintain business continuity in light of such events, as well as a framework and procedure to respond to and remediate such events;</li> <li>(g) the management of data corruption incidents; and</li> <li>(h) procedures and frequency of testing of the BCDR Plans.</li> </ul> <p>Probax will periodically (and, in any event, no less frequently than annually) review, test and, where applicable, update the BCDR Plans.</p>
<p><i>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing</i></p>	<p><b>Compliance Program</b> Probax will maintain a compliance program that includes independent third-party audits and certifications</p> <p><b>Vulnerability Management</b> Probax will maintain the following vulnerability management processes:</p> <p><u><i>Vulnerability Scanning and Remediation.</i></u> Probax employs processes and tools in line with industry standards to conduct frequent vulnerability scanning to test Probax’s network and infrastructure and application vulnerability testing to test Probax applications and services. Probax applies security patches to software components in production and development environments as soon as commercially practicable in accordance with our Vulnerability Management Policy.</p> <p><u><i>Identifying Malicious Threats.</i></u> Probax employs processes and tools in line with industry standards to identify malicious actors and prevent them from accessing Customer Data or Probax systems that process Customer Data. These include, but are not limited to, maintaining software that attempts to identify and detect attempted intrusions, behaviours consistent with Internet-based attacks, and indicators of potential compromise. Probax will maintain a security incident and event management system and supporting processes to notify appropriate personnel in response to threats.</p> <p><u><i>Vulnerability Testing.</i></u> Probax conducts internal vulnerability testing, as described here. This includes our bug bounty program. We make the results of these internal tests publicly available and commit to making bug fixes in line with our Vulnerability Management Policy.</p> <ul style="list-style-type: none"> <li>b) Probax will use commercially reasonable efforts to address identified security vulnerabilities in our Cloud Products and our infrastructure in accordance with the Vulnerability Management Policy. The parties</li> </ul>

	<p>acknowledge that Probax may update the Vulnerability Management Policy from time to time in its discretion, provided such updates do not result in a material derogation of the Vulnerability Management Policy.</p>
<p><i>Measures for user identification and authorisation</i></p>	<p>Probax cloud users can authenticate using username and password, or external IdPs (incl. via SAML, Google, Microsoft and Apple). All credentials are hosted in the application database, which is encrypted at rest. Passwords are stored using a secure hash + salt algorithm.</p> <p>Administrators are able to configure and enforce password complexity and MFA requirements for managed accounts via Hive</p>
<p><i>Measures for the protection of data during transmission</i></p>	<p>See the item above titled “Measures of pseudonymisation and encryption of personal data”</p>
<p><i>Measures for the protection of data during storage</i></p>	<p><b>Data Hosting Facilities</b>            Probax uses Amazon Web Services (AWS) for all cloud hosted infrastructure needed to deliver Cloud Products to our Customers. AWS provides technical, operational, and contractual measures needed to protect Customer data. More information can be found at <a href="https://aws.amazon.com/compliance/data-protection">https://aws.amazon.com/compliance/data-protection</a>.</p> <p><b>Tenant Separation</b>            Probax will use established measures to ensure that Customer Data is kept logically segregated from other customers' data when at-rest.</p> <p><b>Data Encryption</b>            See the item above titled “Measures of pseudonymisation and encryption of personal data”</p>
<p><i>Measures for ensuring physical security of locations at which personal data are processed</i></p>	<p>See the item above titled “Measures for the protection of data during storage”.</p>
<p><i>Measures for ensuring events logging</i></p>	<p>Audit logging is available via API.</p>
<p><i>Measures for ensuring system configuration, including default configuration</i></p>	<p>See the item above titled “Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services”.</p>
<p><i>Measures for internal IT and IT security governance and management</i></p>	<p>See the item above titled “Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services”.</p>
<p><i>Measures for certification/assurance of processes and products</i></p>	<p>See the item above titled “Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing”.</p>
<p><i>Measures for ensuring data minimisation</i></p>	<p>See “What information we collect about you” section of the Probax Privacy Policy.</p>
<p><i>Measures for ensuring data quality</i></p>	<p>See the items above titled “Measures of pseudonymisation and encryption of personal data”, “Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services”, and “Measures for the protection of data during storage”.</p>

	In addition, Customer and its Users have the ability to update any Customer Data provided to Probax using in-built product functionality.
<i>Measures for ensuring limited data retention</i>	<p><b>Data Retention and Destruction Standard</b></p> <p>Probax maintains a Data Retention and Destruction Standard, which designates how long we need to maintain data of different types. The Data Retention and Destruction Standard is guided by the following principles:</p> <ul style="list-style-type: none"> <li>• Records should be maintained as long as they serve a business purpose.</li> <li>• Records that serve a business purpose, or which Probax has a legal, regulatory, contractual or other duty to retain, will be retained.</li> <li>• Records that no longer serve a business purpose, and for which Probax has no duty to retain, should be disposed. Copies or duplicates of such data should also be disposed. To the extent Probax has a duty to retain a specified number of copies of a Record, such number of copies should be retained.</li> <li>• Probax’s practices implementing this Standard may vary across departments, systems and media, and will of necessity evolve over time. These practices will be reviewed under our company-wide policy review practices.</li> </ul>
<i>Measures for ensuring accountability</i>	See the item above titled “Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing”.
<i>Measures for allowing data portability and ensuring erasure</i>	<p><b>Data Export</b></p> <p>Probax allows Customer to export its Customer Data from the Cloud Products.</p> <p><b>Secure Deletion</b></p> <p>Probax will maintain a process reasonably designed to ensure secure destruction and deletion of any and all Customer Data as provided in the Agreement. Such Customer Data will be securely destroyed and deleted by Probax so that: (a) Customer Data cannot be practicably read or reconstructed, and (b) the Probax systems that store Customer Data are securely erased and/or decommissioned disks are destroyed.</p>