BEEKEEPER

DATA PROCESSING AGREEMENT

Between

BEEKEEPER (“Beekeeper” and “Processor”)

and

[COMPANY NAME]

Address,

City, Country (“Customer”)

collectively referred to as “Party” or “Parties”.

This Data Processing Agreement (“DPA”) is incorporated into and forms an integral part of Beekeeper’s Frontline Success System Subscription Agreement and any other agreement signed by the Parties (the “Agreement”) related to Customer's use of Beekeeper’s Frontline Success System when the processing of Personal Data is required under such Agreement. In case the Customer executes Beekeeper’s Frontline Success System Subscription Agreement i with an authorized third-party (such as a Beekeeper authorized reseller) and neither with Beekeeper nor a Beekeeper Associated Company, any reference herein to the “Agreement” shall refer to the standard Beekeeper’s Frontline Success System Subscription Agreement, as modified from time-to-time and set-out at beekeeper.io/legal.

The Processor entering into this DPA is the Beekeeper Associated Company as follows: (i) if Customer’s principal office is in North America, then Beekeeper shall mean “Beekeeper USA, Inc.”; (ii) if Customer’s principal office is in Germany, then Beekeeper shall mean “Beekeeper GmbH”; (iii) if neither (i) nor (ii) apply, then Beekeeper shall mean “Beekeeper AG”; or (iv) if a Beekeeper entity is identified on the Agreement and is contrary to (i)-(iii) herein, then the Agreement shall control.

Customer enters into this DPA on its own behalf and, to the extent required under applicable Data Protection Laws, on behalf of Controller’s Associated Companies. However, this DPA only applies if, and to the extent the Processor processes Personal Data for which such Associated Companies may be considered a “controller” under the Data Protection Laws. In providing the Service to Controller pursuant to the Agreement, Beekeeper Processes Controller Data on behalf of Controller; therefore, the Parties agree to comply with the following provisions with respect to any Personal Data.

This DPA applies to the Parties as well as to Beekeeper’s Associated Companies, Sub-processors, and Staff, who Process Personal Data in connection with the Agreement.

1. DPA definitions

For the purposes of this DPA all capitalized terms defined herein shall have the meaning set forth below:

"Applicable Law" means as it relates to Controller, Applicable Law means all controlling statutes, regulations, ordinances and administrative rules and orders (that have the effect of law) within the jurisdictions in which Controller operates. As it relates to Beekeeper, Applicable Law means all controlling statutes, regulations, ordinances and administrative rules and orders (that have the effect of law) in Switzerland, the European Union, and the United States of America.

"Associated Companies" means an entity that directly or indirectly controls, is controlled by, or is under common control with, a party to the DPA. For purposes of the foregoing, "control" means the ownership of (i) greater than fifty percent (50%) of the voting power to elect directors of the entity, or (ii) greater than fifty percent (50%) of the ownership interest in the entity. "Associated Companies" also means a cooperative: a user-owned and controlled business from which benefits are derived and distributed equitably on the basis of use or as a business owned and controlled by the people who use its services. For those Controller Associated Companies that require the Services to be hosted within separate tenants, additional Fees may apply unless otherwise indicated on the Order Form.

"Authorized Users" means those employees, agents, and independent contractors of Controller and/or its Associated Companies who are authorized by Controller to use the Services, as further described in the Agreement and who accept the then current End User Terms and Privacy Policy.

"Authorized User Data" means the Personal Data and other information Authorized Users provide to Beekeeper and/or input by Controller into the Service solely for the purpose of creating an account for an Authorized User, but excludes Customer Data and Beekeeper Data.

"Beekeeper" means the Beekeeper Associated Company as follows: (i) if Controller's principal office is in North America, Beekeeper shall mean "Beekeeper USA, Inc."; (ii) if Controller's principal office is in Germany, Beekeeper shall mean "Beekeeper GmbH; (iii) if neither (i) nor (ii) apply, Beekeeper shall mean "Beekeeper AG"; or (iv) if a Beekeeper entity is identified on the Order Form and is contrary to (i)-(iii) herein, the Order Form shall control.

"Beekeeper Data" means (i) such information or data provided by Beekeeper to Controller as part of the Services; (ii) Controller's configuration and Authorized User's use of the Services (inclusive of metadata, communication logs, and transaction logs) which shall be, and be permitted to, de-identified or pseudonymized and shall neither identify Controller nor any Authorized User; nor include any Personal Data; (iii) aggregated anonymized insights on the usage of the Services, and (iv) any Feedback from Controller or Authorized Users to Beekeeper relating to the Services (provided such do not include any Controller Data or Controller Confidential Information).

"Controller" means the Customer and Customer's Associated Companies (if any), which determines the purposes and means of the Processing of Personal Data.

"Controller Data" means all data included in Customer Data and Authorized User Data.

"Customer Data" means the data and information (i) provided by Customer to Beekeeper in connection with this Agreement; and (ii) inputted by Customer, Authorized Users, or Beekeeper on Customer's behalf arising from, or otherwise for the purpose of using, the Services or facilitating Customer's use of the Services; but excluding Authorized User Data and Beekeeper Data.

"Confidential Information" means any information of any type in any form that (i) is disclosed to or observed or obtained by one Party from the other Party (or from a person the recipient knows or reasonably should assume has an obligation of confidence to the other Party) in the course of, or by virtue of, this DPA and (ii) either is designated as confidential or proprietary in writing at the time of such disclosure or within a reasonable time thereafter (or, if disclosure is made orally or by observation, is

designated as confidential or proprietary orally by the person disclosing or allowing observation of the information) or is of a nature that the recipient knew or reasonably should have known, under the circumstances, would be regarded by the owner of the information as confidential or proprietary. The details of the Frontline Success System, Services, Beekeeper Data, and the results of any performance or security tests of the Services, constitute Beekeeper's Confidential Information. Customer Data is the Confidential Information of Controller. the term "Confidential Information" specifically shall not include information that: (i) is or becomes publicly known, not under seal by a court of competent jurisdiction, other than through any act or omission of the receiving Party; (ii) was in the other Party's lawful possession before the disclosure and was not acquired directly or indirectly from the other Party; (iii) is lawfully disclosed to the receiving Party by a third party not having an obligation of confidence of the information to any person or body of which the recipient knew or that, under the circumstances, the recipient reasonably should have assumed to exist; or (iv) is independently developed by the receiving Party, which independent development can be shown by written evidence.

"Data Breach" means any known unauthorized or unlawful destruction, deletion, loss, alteration, disclosure, or loss of access to Personal Data.

"Data Protection Laws" means the applicable set of laws and regulations that govern the collection, processing, storage, and transfer of Authorized Personal Data arising from the European General Data Protection Regulation (GDPR), the Swiss Data Protection Act (DPA), or United States state privacy statutes including the California Privacy Rights Act.

"Data Subject" means the Authorized User entrusting the Controller with its Personal Data subject to the Data Protection Laws to whom Personal Data relates.

"Data Subject Request" means a request from an Authorized User to exercise their rights under the Data Protection Laws, such as the right to access, correct, delete, or restrict the processing of their personal data.

"Disaster Recovery Policy" means the Beekeeper Disaster Recovery Policy currently in place as may be amended by Beekeeper from time to time.

"End User Terms" means the Frontline Success System End User Terms of Service at beekeeper.io/legal, as updated from time to time.

"Effective Date" means the effective date as indicated on an Order From referencing the Agreement; or, if no Order Form is created, the date that Controller begins to use the Services.

"Feedback" means comments, suggestions, or other feedback provided by Controller or Authorized Users to Beekeeper related to the Services or any of its features. Feedback may be provided in writing, verbally, or through any other means of communication.

"Fees" means Subscription Fees and any additional fees or expenses as set out in an Order Form.

"Frontline Success System" means Beekeeper owned, licensed, or otherwise authorized to use internal communications software applications, including as described in the recitals of the Agreement, provided by Beekeeper to Controller and Authorized Users solely for use as part of the Services.

"Hosting Services" means the provision, administration, and maintenance of servers and related equipment, the provision of bandwidth at the hosting facility, and the operation of the Frontline Success System for access and use by Authorized Users pursuant to the Agreement.

"New Optional Feature" means a new feature of the Frontline Success System that Controller can choose to activate within the Service or request activation from Processor.

“Order Form” means an Order Form executed by Controller and Beekeeper pursuant to the Agreement, which details the Services to be provided, applicable Fees, and other applicable requirements.

“Party” means Beekeeper or Controller individually; and collectively referred to as the “Parties”.

“Personal Data” shall have the meaning of all information included in Controller Data relating to an identified or identifiable natural person and any other data that is “personal data”, “personal information”, “personally identifiable information” or such similar term as defined under Data Protection Laws.

“Privacy Policy” means the Beekeeper privacy policy at beekeeper.io/privacy-policy, as updated from time to time.

“Processing” (including “Process” and “Processes”) means any action or set of actions that is performed on Personal Data or Controller Data, whether or not by automatic means. This includes actions such as collection, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing, or destroying.

“Service Level Agreement” means the Beekeeper Service Level Agreement at beekeeper.io/legal as posted on the Effective Date.

“Services” means (i) use of the Frontline Success System in accordance with the Agreement, (ii) use of Beekeeper Data; (iii) the Support Services and the Hosting Services, (iv) access to the Beekeeper hosting platform, and (v) any other services that Beekeeper or its employees, agents, or subcontractors are to provide to or for Controller expressly identified under this DPA or set out in an Order Form; but excludes Third Party Applications and Third Party Features.

"Standard Contractual Clauses" means: (i) where the EU GDPR applies, the standard 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 ("EU SCCs"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR ("UK SCCs"); and (iii) where the Swiss GDPR applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs").

“Staff” means Beekeeper’s and the Beekeeper Associated Companies’ employees, contractors, agents, and consultants who are involved in the activities for the performance of the DPA.

“Subprocessor" means any entity engaged by Processor for the Processing of Personal Data pursuant to its obligations under the DPA. All Subprocessors shall be listed at www.beekeeper.io/legal-library/subprocessors.

“Subscription Fees” means the subscription fees payable by Controller to Beekeeper for the User Subscriptions.

“Supervisory Authority” means an independent public authority that is responsible for ensuring that Data Protection Laws are complied with and whose authority is established by Data Protections Laws.

“Support Services” means the support services provided by Beekeeper in accordance with the Service Level Agreement and any Order Form, in each case with respect to the Services and including the Frontline Success System.

“Third Party Applications” means online applications and offline software products that are provided directly to Controller by third parties and interoperate with the Services.

"Third Party Features" means optional services integrated into the Services provided by one or more third party companies of which Beekeeper does not control (e.g., inline language translation services, provided through Google and Microsoft Bing) as listed at beekeeper.io/legal-library/subprocessors of which such list may be updated from time to time.

"User Subscriptions" means the user subscriptions purchased by Customer for the number of Authorized Users which entitle such Authorized Users to access and use the Services in accordance with the Agreement.

2. Roles and responsibilities

2.1 Appointment of Processor. Controller appoints Processor to Process Personal Data in accordance with the Agreement and this DPA.

2.2 Controller's Responsibilities. Controller shall be solely responsible for compliance with Applicable Laws regarding the use of Service and Processing of Personal Data as expressly directed under the Agreement; including, but not limited to, (i) the lawfulness of disclosing Personal Data to Processor; and (ii) the lawfulness of appointing a Processor to Process Personal Data and Controller Data under such Applicable Law.

2.3 Processor's Responsibilities. Processor shall:

2.3.1 Process Personal Data in accordance with the DPA and the Data Protection Laws; and

2.3.2 Not Process Personal Data for any purpose other than (i) as required for the performance of the Services; (ii) as instructed by Controller or agreed upon by the Parties; or (iii) as imposed by Data Protection Laws or applicable law, in such case, Processor will notify Controller of such additional Processing, unless such notification is prohibited by law.

3. Scope and purposes of Processing

3.1 Purpose. The Processing of Personal Data shall be done to perform the Services and pursuant to the Agreement. The duration, nature, and purpose of the Processing; types of Personal Data and categories of Data Subjects Processed under this DPA, are further specified in Annex 1.

3.2 Scope. Controller instructs Processor to carry out the following Processing activities on Personal Data, provided that Controller or Authorized Users, are:

3.2.1 Carrying out any tasks required for the performance of the Agreement, to perform the Services or improve the services provided by Processor;

3.2.2 Exercising the Processor's rights and obligation under the Agreement, including documenting the Processor's compliance under the Agreement;

3.2.3 Granting access to the platform and providing related support, customer success, and account management services;

3.2.4 Processing Personal Data based on specific requests of Controller (for example, but not limited to, when fulfilling Controller's requests to update Controller Data);

3.2.5 Transferring Personal Data to Sub-processors for the performance of the Agreement;

3.2.6 Transferring Personal Data internationally to fulfill its contractual obligations;

3.2.7 Deleting, rectifying, changing, extracting, or returning, upon Controller's request, Personal Data;

3.2.8 Providing Controller with all information necessary to demonstrate compliance with its obligations;

3.2.9 Supporting Controller during Controller's audits and inspections, conducted either by the Controller, its auditors, or other authorized third parties;

3.2.10 Investigating Data Breaches;

3.2.11 Creating reports or developing specific functionalities for Controller;

3.2.12 Performing pseudonimization, anonymization, randomization, aggregation, and other processing of Customer Data and Authorized Users Data for the provision, improvement, and security of the Services, or generate of Beekeeper Data;

3.2.13 Performing ancillary tasks pursuant to the Agreement;

3.2.14 Fulfilling other requests of the Controller;

3.2.15 Fulfilling tasks related to specific legal requirements.

3.3 Restrictions. Processor is prohibited from (i) Processing Personal Information outside the scope of the Agreement; (ii) selling Personal Information; or (iii) sharing Personal Information with third parties, except relating to Processor's permitted use of Subprocessors or required by Applicable Law.

4. Processor's rights and obligations.

4.1 Staff. Processor shall ensure Processor's Staff engaged in the Processing of Personal Data, are informed of the confidential nature of the Personal Data and have executed confidentiality agreements. Processor shall ensure that Staff access to Personal Data is limited to those individuals assisting in the performance of Processor's rights and obligations under the Agreement, this DPA, and related activities, and on need-to-know and need-to-access principles.

4.2 Suspension of Processing. If Processor believes that an instruction would be in conflict with applicable law, Processor shall inform Controller without undue delay, unless otherwise prohibited by applicable law or competent authority. Processor shall be entitled to suspend the performance of such instructions until the Controller demonstrates the compliance of the instruction or modifies such instruction accordingly.

4.3 Safeguards.

4.3.1 Processor has implemented the following safeguards: (i) internal controls designed to safeguard Personal Data; (ii) technical and organizational measures designed to protect Personal Data in compliance with Data Protection Laws (as decribed in Clause 10),

and (iii), ongoing measures designed to safeguard confidentiality, integrity, availability and the resilience of processing systems and services.

4.3.2 Processor may modify the safeguards so long as the modified safeguards provide at least the same protection for Personal Data as the original safeguard provided.

4.3.3 Processor shall implement a process for regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures to ensure the security of Processing.

4.3.4 When Personal Data is processed by Processor's Staff in home offices, in whole or in part, the Processor shall implement guidelines and security measures for its Staff to follow.

4.4 Data Subject Requests. Processor will use commercial reasonable efforts to support Controller in fulfilling Data Subjects' requests and claims.

4.5 Data Breach.

4.5.1 If a Data Breach should occur, Processor shall endeavor to mitigate potential negative consequences for the Data Subjects.

4.5.2 Processor shall notify Controller, without undue delay, of a Data Breach. Where feasible, notification will occur no later than 72 hours after becoming aware of a Data Breach.

4.5.3 The Data Breach notification to Controller shall include all reasonable information available to Processor at the time, including: (i) the nature of the personal data breach; and (ii) measures taken, being taken or to be taken to address the Data Breach as well as (iii) measures to mitigate its possible adverse effects on Data Subjects.

4.6 Modification of Personal Data. Upon request of the Controller, and where covered by the scope of the Agreement, Processor will use commercially reasonable efforts to correct, extract, or erase Personal Data. Controller will bear any cost caused by such requests.

4.7 At Termination. Upon termination of Agreement, Processor will proceed with the permanent deletion from its systems of Controller Data and, if requested, returning a copy to Controller. Should Controller have specific requests deviating from the Processor's standards in returning or deleting data, Processor shall consider them in good faith and the Controller will bear any cost caused by such specific requests.

4.8 Support. The Processor will use commercially reasonable efforts to provide Controller with the information necessary for Controller to comply with its obligations under Applicable Laws. This includes providing information about the processing of Personal Data and the security measures in place. The Controller will bear any cost caused by such requests pursuant to this clause.

4.9 Regulatory & Legal Requests. The Processor will promptly notify the Controller of any request by a public authority for the transfer of data covered by the Agreement, unless notification is prohibited by law or by a competent authority (this also includes any rules designed to ensure the non-disclosure of investigations performed by a law-enforcement authority). If required, Processor will use commercially reasonable efforts to support the Controller in any discussions with governmental agencies overseeing

Data Protection Laws. Processor will also implement all commercially reasonable suggestions of such agencies to improve the Processing of Personal Data.

5. Controller's rights and obligations

5.1 Irregularities. Controller will notify Processor without undue delay of any defects or irregularities regarding the data protection detected by Controller in the results of Processor's work.

5.2 Data Protection Issues. Controller will notify Processor's point of contact for any Personal Data protection issues arising out of or in connection with the Agreement, as specified in Annex 1 of this DPA.

6. Inquiries by Data Subjects

6.1 Inquiry Process. If an individual directly requests Processor to access, modify, or erase Personal Data, (or understand what categories of Personal Data are maintained and for what purpose), Processor will refer such request to Controller without undue delay. If Controller deems the individual's request legitimate, and qualifies such individual as a Data Subject, Controller will notify Processor without undue delay and complete a Beekeeper Customer Data Request ("CDR") incorporating the specific requests for the Processor. The CDR will support fulfilling Data Subject's requests based on the Controller's agreed instructions.

6.2 Timing. Processor shall endeavor to fulfill the CDR request in a timely manner and in any case within twenty-five (25) days. The Processor may reasonably extend the deadline in the following cases: (i) in the specific cases foreseen by applicable Data Protection Law such as a high number of requests or complex case); or (ii) when the applicable Data Protection Law does not foresee any time limit or a longer than thirty (30) days' time limit for the Controller to respond to the Data Subject's requests. If the Processor decides to extend the deadline, Processor will inform Controller of the decision and the reason for the extension. If Controller considers that the extension is not allowed under applicable Data Protection Law, Controller shall inform the Processor without undue delay and the Party shall review the situation in good faith.

6.3 Responsibilities. Processor is not liable for Controller's compliance with its obligations related to Data Subject's requests, or for the Controller's refusal to fulfill such request. Controller is solely responsible for its decisions about the fulfillment of such requests and will also indemnify Processor against any claim, either from Data Subject or third parties, arising from Controller's refusal to fulfill such requests.

7. Substantiation of Security Measures. Processor will document and, upon Controller's request, substantiate the adoption of security measures in Annex II and its compliance with its obligations pursuant to this DPA.

8. Right to Audit and Inspection

8.1 Annual Audits by Processor. Processor will perform annual audits in accordance with ISO 20017 standards by a third-party and we will provide ISO certification to Controller upon request.

8.2 Controller's Right to Audit. Upon a specific and reasonably justified reason, Controller shall have the right to audit the Processor's compliance with this DPA at any reasonable time during the Term of the Agreement. Controller will share the full audit report and findings with Processor.

8.3 Scope. Controller may limit the scope of the audit to specific Processing activities, or Processor's entire Processing operations. Processor shall provide advanced notice to Processor as to the intended scope of the audit. Processor may deny direct access to repositories and venues where other customers' data are stored and refrain from providing information if it should compromise the confidentiality of Processor's other customers. Physical access to datacenter locations of the Processor is excluded from any audit or inspection.

8.4 Performance. Controller may complete the audit itself or utilize a third-party auditor. All individuals participating in the audit will be required to sign a confidentiality agreement prepared by Processor before performing any inspections in furtherance of the audit. Processor shall have the right to refuse to allow an audit from an auditor who is a competitor of Processor. In such case, Processor shall provide Controller with a written explanation of the reason for the refusal, and Controller may choose to select a different auditor.

8.5 Advanced Notice. Controller shall provide Processor with advanced written notice as to the scope of the audit, the name of the auditor, and the proposed date of the audit (not less than 15 days following Processor's receipt of such notice). Processor shall make commercially reasonable efforts to make its system and personnel available during its regular business hours on Controller's proposed audit date, or upon an alternative mutually agreeable day as close to the proposed date as possible.

8.6 Costs. Controller will be solely responsible for all of its costs, including the costs of third-party auditors, required to perform the audit requested by Controller. Except for Controller requested audits following a Data Breach, Controller will reimburse Processor for its personnel's time and other costs expended when providing support for the audit when such audit requires Processor to expend more than 5 hours of its personnel's time to support such audit.

8.7 Frequency. Absent a Data Breach, Controller may only request an audit to once per calendar year, and the duration of the audit shall not exceed three working business days, unless otherwise agreed.

8.8 Supervisory Authority Audit. Where a data protection authority or another supervisory authority with statutory competence for the Controller conducts an inspection upon request of Controller, clauses 8.2-8.6 shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

8.9 Alternative Independent Audit. As an alternative to Controller's audit, Processor may engage at its discretion (unless prohibited by mandatory law to do so) with an independent and reputable third-party auditor to complete the audit, at Processor's cost. Processor will then share the full audit report and findings with the Controller.

9. Subprocessors

9.1 Use of and Modification of Subprocessors. Controller hereby consents and generally authorizes Processor to use, integrate, increase, reduce, modify, or otherwise change the list of Subprocessors in Annex 1 at any time. Processor shall adapt Annex 1 accordingly. Any increase in the Processing scope by a Subprocessor as described in Annex 1, or the appointment of a new Subprocessor (collectively, "Changes") will become effective for the Controller following Processor providing Controller with at least sixty (60) days' advanced notice of the Changes. The appointment of a new Subprocessor related to a New Optional Feature shall follow the specific process outlined in clause 9.5.

9.2 Objections to Changes in Subprocessors.

9.2.1 Controller may make a good faith and reasonable objection to any Changes when such Change would cause material detrimental change to Controller's interests, such as: (i) a change in statutory regulations that would require Processor to process Personal Data in a way that is not compliant with Controller's instructions; (ii) a change that would increases the risk of a security breach of Personal Data; or (iii) a change that would give the Subprocessor a material competitive advantage over the Controller. Notwithstanding anything to the contrary herein, Controller's consent for changes to Subprocessors cannot be unreasonably withheld.

9.2.2 Controller's objection must be received by Processors within sixty (60) days following Processor providing Controller notice of the Change. The objection must be in writing and describe the Controller's legitimate reason(s) for the objection and suggest corrective steps.

9.3 Acceptance of Change. If Controller does not object to the Change in Subprocessor(s) in accordance with clause 9.2, Controller shall be deemed to have accepted the Change.

9.4 Processor's Right to Cure. If Controller objects to the Change pursuant to the process as provided in clause 9.2, Processor has the right to cure the objection by taking one of the following actions (at Processor's sole discretion):

9.4.1 Not implement the Change;

9.4.2 Take the corrective steps requested by Controller noted in its objection; or

9.4.3 Require Controller to discontinue use of the particular functionality of the Service) Processor shall only reimburse Controller for the removal of such functionality if Controller pays additional separate fees line-itemed on the Order Form for such functionality. Such reimbursement will be calculated on a *pro rata temporis* as of the implementation of the Changes.

9.4.4 If the measures taken by Processor do not resolve Controller's objection under clause 9.2.1, and the Parties fail to reach an amicable solution acting reasonably and in good faith, either Party may terminate the Agreement. Termination will be effective on the day of the effective implementation of the Change.

9.5 Change in Subprocessors for New Optional Feature. The appointment of a new Subprocessor for a New Optional Feature shall become effective once the Processor has provided the Controller with advanced notice of the launch of the New Optional Feature. Annex 1 will be updated accordingly, and Controller's consent for the use of the new Subprocessor shall be obtained when the Controller uses the New Optional Feature.

9.6 Contractual Obligations with Subprocessors. Processor will enter into contracts with all Subprocessors that contain the necessary contractual and technological measures designed to protect the Personal Data. The level of data protection and information security must be at least similar to the level of protection granted by Processor under the DPA and must not be less protective than Applicable Laws.

9.7 Costs Associated with Subprocessors. Processor will bear the costs associated with the use of Subprocessors. However, if Controller requests the Processor to use a specific subprocessor, and Processor is willing and able to provide such a solution, Controller will solely be responsible for the costs (including Processor's internal costs) associated with the use of such subprocessor.

10. Technical and Organizational Measures

10.1 TOMs Implementation. To ensure the protection and safeguard of Personal Data as and to comply with Data Protection Laws, Processor will implement technical and organizational measures ("TOMs") regarding, but not limited to, storage, computing, networking access, transfer, input, order and control as outlined in Annex 2.

10.2 Purpose of the TOMs. The purpose of the TOMs is to protect the Personal Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, abuse, or other processing in violation of the Data Protection Law.

11. Controller Data Transfer. Controller authorizes Processor and its Subprocessors to transfer Personal Data across international borders, including, without limitation, from the European Economic Area, Switzerland, and the United Kingdom to the United States. This international transfer shall be done in compliance with Data Protection Laws and the Processor will implement legally required appropriate safeguards if necessary. These safeguards may include but are not limited to: (i) transferring the Personal Data to a recipient in a country, that subject to a recognized framework, a supervisory authority has determined provides adequate protection for Personal Data; or (ii) transferring Personal Data to a recipient that has executed Standard Contractual Clauses adopted or approved by the competent supervisory authority.

12. Return and Deletion of the Data Upon Termination.

12.1 Termination. Upon expiration of the Term, Processor will no longer respond to data subject requests (CDRs). Processor will only perform the following operations related to Controller's Personal Data: permanently delete Personal Data, and if expressly requested by Controller, extract Personal Data in in a standard machine-readable format.

12.2 Term. The DPA is valid upon signature thereof and will remain in force for as long as the Processor processes Personal Data, or until sixty (60) days following the expiration or termination of the Agreement, whichever occurs first.

13. Miscellaneous.

13.1 Notice. Save of the provisions contained in the Agreement in relation to notices, the following notice process shall apply for notices related under this DPA.

13.1.1 Notices to Processor. Notices to Processor under the DPA shall be sent via recognized overnight courier or by certified mail with return receipt requested to Beekeeper, c/o Beekeeper AG, DPO Team, Hardturmstrasse 181, 8005 Zürich, Switzerland.

13.1.2 Notices to Controller. Notices to Controller in relation to the Processing of Personal Data and the DPA may be sent to the email address of the Controller's DPO or other person of contact as specified in Annex 1. Notices from Processor to the Controller relating to CDRs may be provided directly by email to the person requesting the CDRs for the Controller. Controller consents to receive communications in an electronic form. Such notification shall be deemed to be written notice to the Controller. Controller shall notify Beekeeper of updates to its contact information.

13.1.3 Delivery date. Notices must be in writing and will be treated as delivered on the date on the courier confirmation of delivery, the date shown on the return receipt, or the electronic message transmission date.

13.2 Electronic Signature. The Parties hereby consent to the use of electronic signatures in connection with the execution of this DPA, and further agree that electronic signatures to this DPA shall be legally binding with the same force and effect as manually executed signatures.

13.3 Applicability of the Agreement. For the avoidance of doubt, the clauses set-out in the Agreement shall also apply to the DPA.

13.4 Conflict. To the extent any of the terms of this DPA conflict with the terms of the Agreement, the terms of this DPA shall control.

ANNEX 1
Description of the Transfer and Processing

(A) Catalogue [and classification of sensitivity] of Personal Data to be transferred and processed:

For example: name, surname, email address, phone number

(B) Purpose(s) of the transfer and processing:

For example: provision of SaaS services, onboarding, training, etc.

(C) Categories of Persons Affected:

For example: employees, external contractors, etc.

(D) Subprocessors who may access or receive the Personal Data:

For the complete list of Beekeeper's Subprocessors please refer to our webpage **www.beekeeper.io/legal-library/subprocessors**

(E) Additional useful information (Any agreed definitions may be stated here)

Fill in if required, otherwise leave blank.

(F) Contact Information for Data Protection Inquiries (Data Protection Officer)

BEEKEEPER Data Protection Officer	Contact Number / email dpo@beekeeper.io
CONTROLLER Controller DPO or other person of contact	Contact Number / email

ANNEX 2
Technical and Organizational Measures implemented by the Processor

Documentation of the technical and organizational measures to be implemented by the Processor.

Description of the measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:

1. Measures for pseudonymization and encryption of personal data.

With the current service and product offerings, as we do not process any data outside of the product data storage, we do not utilize pseudonymization measures. However, we have implemented appropriate controls to encrypt data, including Personal Data as defined in our Security White Paper. Application of encryption extends to storage of data on mobile devices and databases hosted in our VPCs (Virtual Private Cloud). Furthermore, where possible, all data transmission channels are also encrypted with secure protocols. Please refer to our Security White Paper for additional information.

2. Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

We have implemented a number of measures to safeguard the confidentiality, integrity, availability and resilience of the service offering, as listed below:

- An Information Security Management System (ISMS) Certified in accordance with ISO 27001/2 control objectives and supplemented by the ISO 27017 & 27018 standards.
- Embedded governance structure and operating procedures for information security operational risk management.
- Use of two factor authentication, and where possible single-sign-on for all employees.
- Secure managed company laptops that are encrypted and protected with anti-malware solutions.
- Segregation of data centers by VPC (Virtual Private Cloud) and multi-AZ deployment.
- Protection of the VPC environment with a segregated security architecture including border firewalls controlled fully by Beekeeper employees. (Security White Paper)
- Limited access to production tenants for authorized Beekeeper employees following Beekeeper's information security policies and need-to-know principle.
- Formalized process to control access to production tenants by defined customer support and/or customer success manager.
- Implementation of privileged access management solution and other technical measures to control (provision and monitor) privileged infrastructure access and access to production.
- Segregation of production, staging and development environments.
- Provisioning of dashboard functionalities for complete onsite user management by the Data controller.
- Provisioning of direct interface to SSO or AD or SFTP solutions for management of authorized users for access. (if deployed by controller).
- Use of the push principle when utilizing any 3rd party service (they cannot initiate data pull).
- Defined 3rd party security risk assessment process.

- Defined and controlled change management process. High level of automation in a microservices environment.
- Encrypted communication with secure algorithms with daily certificate verification.
- Adequate logging of access to Beekeeper production environment.
- Structured governance for monitoring and continuous improvement of the risk and compliance controls.
- Regular training and awareness seminars for all Beekeeper employees:
    I. Mandatory information security training & awareness session every year
    II. Continuous access to security training materials
    III. Annual mandatory role based security training for engineers
    IV. Regular open security sessions for developers (e.g. OWASP sessions)
    V. Information Security onboarding sessions offered quarterly for new joiners
- Implementation of highly resilient backup and data recovery solution
- Continuous monitoring of service availability. Status subscription is available to the controller (status.beekeeper.io)
- Contractually binding service availability commitment of 99.9%
- Measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- Beekeeper performs a quarterly scenario based Business Continuity and Disaster Recovery Tests to assess the recoverability capability of various services.

3. Testing, assessing and evaluating the technical and organizational measures

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures are in place. Beekeeper has implemented a risk management governance structure with the following scope:

- Regular risk meetings between product and risk & compliance teams
- Maintaining an inventory of identified risks
- Annual independent penetration tests performed by externals
- Capability to perform on-demand penetration test when required
- Continuous security vulnerability scanning of the code base
- Testing and quality assurance process incorporated in the development lifecycle
- Regular 3rd party review process
- Defined security incident management policy
- Defined security incident notification policy and process in line with the GDPR framework
- Annual independent ISO internal audit
- Annual independent ISO external audit

4. Vulnerability Management Program and Policy

Our Vulnerability Management Program and respective Policy consists of the following:

- Daily scans (upon code change) of the code base
- Daily scans of our digital certificates
- Continuous NIDS + HIDS monitoring
- Annual penetration tests performed by a 3rd party company
- Anti-malware running on local endpoints and cloud based virtual machines
- Regularly scheduled DAST and ASM
- A Risk Management process to prioritize and remediate known vulnerabilities
- Tool to continuously scan 3rd party libraries for known security vulnerabilities