DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") amends and forms part of the written agreement between Owner and SupportBee, Inc. ("**SupportBee**") (collectively, "**the parties**") for the provision of services to Owner (the "**Agreement**"). This DPA prevails over any conflicting term of the Agreement but does not otherwise modify the Agreement.

1. Definitions

1.1. In this DPA:

a) "**Controller**", "**Data Subject**", "**Processing**", "**Processor**", "**Service Provider**", and "**Supervisory Authority**" have the meaning given to them in Data Protection Law;

b) "**Data Protection Law**" means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and all other Data Protection Laws of the European Union, the European Economic Area ("**EEA**"), and their respective Member States, Switzerland and the United Kingdom ("**UK**"); (ii) the California Consumer Protection Act (California Civil Code § 1798.100) ("**CCPA**"); and (iii) all laws implementing or supplementing the foregoing and any other applicable data protection or privacy laws;

c) "**Data Subject Rights**" means all rights granted to Data Subjects by Data Protection Law, such as the right to information, access, rectification, erasure, restriction, portability, objection, and not to be subject to automated individual decision-making;

d) "**Restricted Data Transfer**" means any international transfer of Personal Data that would be prohibited under Data Protection Law in the EEA or UK without implementation of additional safeguards such as Standard Contractual Clauses.

e) "**Personnel**" means any natural person acting under the authority of SupportBee;

f) "**Personal Data**" means any information that constitutes "personal data" or "personal information" within the meaning of applicable Data Protection Law that SupportBee may access in performing the services under the Agreement.

g) "**Personal Data Breach**" means actual or reasonably suspected unauthorized destruction, loss, control, alteration, disclosure of, or access to, Personal Data for which SupportBee is responsible.

h) "**Sensitive Data**" means any type of Personal Data that is designated as a sensitive or special category of Personal Data, or otherwise subject to additional restrictions under Data Protection Law or other laws to which the Controller is subject;

i) "**Subprocessor**" means a Processor engaged by a Processor to carry out Processing on behalf of a Controller;

j) "**Standard Contractual Clauses**" means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 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 as amended or replaced from time to time; and

k) **"UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner for parties making restricted transfers.

1.2. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

2. Roles

2.1. SupportBee shall process Personal Data only as a Processor acting on behalf of Owner and, with respect to CCPA, as a Service Provider, in each case, regardless of whether Owner acts as a Controller or as a Data Processor on behalf of a third-party Controller with respect to Personal Data.

3. Scope

3.1. This DPA applies to Processing of Personal Data by SupportBee in the context of the Agreement.

3.2. The subject matter, nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set out in **Annex I**, which is an integral part of this DPA.

4. Instructions

4.1. SupportBee must only Process Personal Data on documented instructions of Owner, and is prohibited from Processing Personal Data for any other purpose.

4.2. SupportBee certifies that it will not (a) "sell" (as defined in the CCPA) the Personal Data; (b) retain, use, or disclose the Personal Data for any purpose other than for the specific business purpose of providing the services under the Agreement, including retaining, using, or disclosing the Personal Data for a commercial purpose other the provision of the services; or (c) retain, use, or disclose the Personal Data to any person other than as necessary to provide the services or outside of the direct business relationship between the parties.

4.3. Owner's instructions are documented in **Annex I**, the Agreement, and any applicable statement of work.

4.4. Owner may issue additional instructions to SupportBee as it deems necessary to comply with Data Protection Law.

5. Owner Responsibilities

5.1 Owner is responsible for the lawfulness of Personal Data processing under or in connection with the services. Owner shall (i) have provided, and will continue to provide all notices and have obtained, and will continue to obtain, all consents, permissions and rights necessary under applicable Data Protection Law for SupportBee to lawfully process Personal Data for the purposes contemplated by the Agreement (including this DPA); (ii) make appropriate use of the services to ensure a level of security appropriate to the particular content of the Personal Data; (iii) have complied with all Data Protection Law applicable to the collection of Personal Data and the transfer of such Personal Data to SupportBee and its Subprocessors; and (iv) ensure its processing instructions comply with applicable laws (including applicable Data Protection Law).

6. Subprocessing

6.1. SupportBee must obtain Owner's general prior written authorization to engage Subprocessors. Owner hereby authorizes SupportBee to engage the Subprocessors listed at https://supportbee.notion.site/GDPR-DPA-Subprocessors-90990fd2a49443bb85a431cf2ee85f0e?pvs=4.

6.2. SupportBee must inform Owner at least thirty (30) days prior to any intended change of Subprocessor, thereby giving Owner the opportunity to object such change.

6.3. SupportBee must obtain sufficient guarantees from all Subprocessors that they will implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Law and this DPA.

6.4. SupportBee must enter into a written agreement with all Subprocessors which imposes substantially similar obligations on the Subprocessors as this DPA imposes on SupportBee.

6.5 SupportBee must provide a copy of SupportBee's agreements with Subprocessors to Owner upon request. SupportBee may redact commercially sensitive information before providing such agreements to Owner.

7. Restricted Data Transfers

7.1. To the extent required by Data Protection Law in the EEA, by signing this DPA Owner and SupportBee agree to be bound by module 2 (Controller-to-Processor) of the Standard Contractual Clauses, which are hereby incorporated by reference and completed as follows: the "data exporter" is Owner; the "data importer" is SupportBee; the optional docking clause in Clause 7 is implemented; Clause 9(a) option 1 is implemented and the time period therein is specified as thirty (30) days; the optional redress clause in Clause 11(a) is struck; Clause 13, (a) paragraph 2 is implemented; Clause 17 option 1 is implemented and the governing law is the law of the Republic of Ireland; the court in Clause 18(b) are the Courts of the Republic of Ireland; Annex 1, 2 and 3 to module 2 of the Standard Contractual Clauses are **Annex I** and **II** to this DPA respectively.

7.2. To the extent required by Data Protection Law in the UK, by signing this DPA, Owner and SupportBee agree to be bound by the UK Addendum. Part 1, table 1 of the UK Addendum will be deemed to be completed like its equivalent provisions in the Standard Contractual Clauses (module 2) in Annex I, Section 1. For the purpose of Part 1, Table 2 of the UK Addendum, the Approved EU SCCs are the Standard Contractual Clauses (module 2) incorporated by reference into this DPA pursuant to Section 7.1 of this DPA. For the purpose of Part 1, Table 3, Annex 1, 2 and 3 to the Standard Contractual Clauses (module 2) are **Annex I** and **II**, and Section 6.1 of this DPA respectively. For the purpose of Part 1, Table 4, the party that may end the UK Addendum in accordance with Section 19 of the UK Addendum is the importer. For the purposes of any transfers covered by the Data Protection Law in the UK, the Standard Contractual Clauses (module 2) will be deemed to be amended as set out in Part 2 of the UK Addendum.

8. Personnel

8.1. SupportBee must implement appropriate technical and organizational measures to ensure that Personnel do not Process Personal Data except on the instructions of Owner.

8.2. SupportBee must ensure that all Personnel authorized to Process Personal Data are subject to a contractual or statutory obligation of confidentiality.

8.3. SupportBee must regularly train Personnel regarding the protection of Personal Data.

9. Security and Personal Data Breaches

9.1. SupportBee must implement technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing, including:

a) encryption of Personal Data;

b) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing;

c) measures to detect Personal Data Breaches in a timely manner;

d) measures to restore the availability and access to Personal Data in a timely manner in the event of an incident;

e) Processes for regularly testing, assessing and evaluating the effectiveness of the security measures; and

f) as appropriate, and without limiting the foregoing, the measures listed in **Annex II**.

9.2. SupportBee must inform Owner without undue delay after becoming aware of a Personal Data Breach. SupportBee must, either in the initial notice or in subsequent notices as soon as the information becomes available, inform Owner of the nature of the Personal Data Breach, the categories and number of Data Subjects, the categories and amount of Personal Data, the likely consequences of the Personal Data Breach, and the measures taken or proposed to be taken to address the Personal Data Breach and mitigate possible adverse effects. If SupportBee's notice or subsequent notices are delayed, they must be accompanied by reasons for the delay.

9.3. SupportBee's notification of or response to a Personal Data Breach under Section 9.2 will not be construed as an acknowledgement by SupportBee of any fault or liability with respect to the Personal Data Breach.

9.4. SupportBee must document all Personal Data Breaches, including at least the information referred to in Section 9.2, and provide a copy to Owner upon request.

10. Assistance

10.1.SupportBee must assist Owner, including by implementing appropriate technical and organizational measures, with the fulfilment of Owner's own obligations under Data Protection Law, including:

a) complying with Data Subjects' requests to exercise Data Subject Rights;

b) replying to inquiries or complaints from Data Subjects;

c) replying to investigations and inquiries from Supervisory Authorities;

d) conducting data protection impact assessments, and prior consultations with Supervisory Authorities; and

e) notifying Personal Data Breaches.

10.2.Unless prohibited by Data Protection Law, SupportBee must inform Owner without undue delay if SupportBee:

a) receives a request, complaint or other inquiry regarding the Processing of Personal Data from a Data Subject or Supervisory Authority;

b) receives a binding or non-binding request to disclose Personal Data from law enforcement, courts or any government body;

c) is subject to a legal obligation that requires SupportBee to Process Personal Data in contravention of Owner's instructions; or

d) is otherwise unable to comply with Data Protection Law or this DPA.

10.3.Unless prohibited by Data Protection Law, SupportBee must obtain Owner's written authorization before responding to, or complying with any requests, orders, or legal obligations referred to in Section 10.2.

11. Audit

11.1. SupportBee will make available to Owner upon request all information as necessary to demonstrate compliance with the obligations of Data Protection Law and this DPA and allow for and contribute to audits, including inspections, conducted by a Supervisory Authority, Owner or another auditor as reasonably requested by Owner.

11.2. If Owner's requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Owner's audit request and SupportBee confirms there are no known material changes in the controls audited, Owner agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

11.3. Any Owner-requested audits are at Owner's expense. Owner shall reimburse SupportBee for any time expended by SupportBee or its Subprocessors in connection with any Owner-requested audits or inspections at SupportBee's then-current professional services rates, which shall be made available to Owner upon request.

12. Liability

12.1. The total combined liability of either party and its Affiliates towards the other party and its Affiliates, whether in contract, tort or any other theory of liability, under or in connection with Agreement and this DPA combined, will be limited to limitations on liability or other liability caps agreed to by the parties in the Agreement.

13. Confidentiality

13.1. SupportBee must keep all Personal Data and all information relating to the Processing thereof, in strict confidence.

14. Analytics

14.1 Owner acknowledges and agrees that SupportBee may create and derive from Processing related to the services anonymized and/or aggregated data that does not identify Owner or any natural person, and use, publicize or share with third parties such data to improve SupportBee's products and services and for its other legitimate business purposes.

15. Term and Duration of Processing

15.1. The Processing will last no longer than the term of the Agreement.

15.2. Upon termination of the Processing, SupportBee must, at Owner's choice, delete or return all Personal Data and must delete all remaining copies within ninety (90) days after confirmation of Owner's choice.

15.3. This DPA is terminated upon SupportBee's deletion of all remaining copies of Personal Data in accordance with Section 17.2.

16. Modification of this DPA

16.1. This DPA may only be modified by a written amendment signed by both Owner and SupportBee.

17. Invalidity and Severability

17.1. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

Accepted and agreed to by the authorized representative of each party:

Owner	**SupportBee**
Authorized Signature	Authorized Signature HANA
Name	Name Hana Mohan –
Title	Title President
Date	Date Feb 06, 2026

ANNEX I

A. LIST OF PARTIES

Owner is the controller and the data exporter and SupportBee is the processor and the data importer.

B. DESCRIPTION OF TRANSFER

Subject Matter	SupportBee's provision of the services to Owner.
Duration of the Processing	Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Data Protection Law.
Nature and Purpose of the Processing	SupportBee will process Owner Personal Data for the purposes of providing the data governance services to Owner in accordance with the DPA.
Frequency of the Processing	As and when the services are accessed.
Categories of Data	Name, email address, IP address, phone number, slack id and information necessary to deliver notifications to Owner's customers, including the contents of notifications and delivery information.
Special Categories of Data Processed	The services are not intended to Process special categories of data.
Data Subjects	Owner's end customers and Owner personnel (employee, contractors, etc.)

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is the Irish Data Protection Commission.

ANNEX II

SupportBee shall implement and maintain the controls listed in this Annex II in accordance with industry standards generally accepted by information security professionals as necessary to reasonably protect Personal Data during storage, processing and transmission.

Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data Processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are Processed, include: (a) establishing security areas, restriction of access paths; (b) establishing access authorizations for employees and third parties; (c) access control system (ID reader, magnetic card, chip card); (d) key management, card-keys procedures; (e) door locking (electric door openers etc.); (f) security staff, janitors; (g) surveillance facilities, video/CCTV monitor, alarm system; and (h) Securing decentralized data Processing equipment and personal computers.

Virtual access control

Technical and organizational measures to prevent data Processing systems from being used by unauthorized persons include: (a) user identification and authentication procedures; (b) ID/password security procedures (special characters, minimum length, change of password); (c) automatic blocking (e.g. password or timeout); (d) monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts; (e) creation of *one* master record per user, user-master data procedures per data Processing environment; and (f) encryption of archived data media.

Data access control

Technical and organizational measures to ensure that persons entitled to use a data Processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include: (a) internal policies and procedures; (b) control authorization schemes; (c) differentiated access rights (profiles, roles, transactions and objects); (d) monitoring and logging of accesses; (e) disciplinary action against employees who access Personal Data without authorization; (f) reports of access; (g) access procedure; (h) change procedure; (i) deletion procedure; and (j) encryption.

Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include: (a) encryption/tunneling; (b) logging; and (c) transport security.

Control of instructions

Technical and organizational measures to ensure that Personal Data are Processed solely in accordance with the instructions of the Controller include: (a) unambiguous wording of the contract; (b) formal commissioning (request form); and (c) criteria for selecting the Processor.

Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include: (a) backup procedures; (b) mirroring of hard disks (e.g. RAID technology); (c) uninterruptible power supply (UPS); (d) remote storage; (e) antivirus/firewall systems; and (f) disaster recovery plan.

Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be Processed separately include: (a) separation of databases; (b) "internal client" concept / limitation of use; (c) segregation of functions (production/testing); and (d) procedures for storage, amendment, deletion, transmission of data for different purposes.