DATA PROCESSING ADDENDUM

This data processing addendum (the "**Addendum**"), forms a part of the general terms and conditions (the "**Agreement**") of the platform (the "**Platform**"), owned and powered by Winn.AI Labs Ltd., a company organized under the laws of Israel ("**Company**").

This Addendum shall apply to any Processing of Personal Data which Company will perform as part of the provision of the License to the Corporation (the "**Licensee**", the Licensee and the Company may also be referred to herein as a "**Party**", and collectively they may also be referred to as the "**Parties**") under the Agreement (the "**Services**").

This Addendum shall be an inseparable part of the Agreement. Capitalized terms not defined herein will have the meaning set forth in the Agreement. For the purposes of this Addendum, the term "Company" shall include Company and/or its Affiliates.

By virtue of the Agreement, Company may Process Agreement Personal Data on behalf of the Corporation.

1. Definitions

In this Addendum, the following words and phrases shall (unless the context otherwise requires) have the meanings set out beside them:

1.1. "**Affiliate**" shall mean a person or entity controlling, controlled by or under the common control with Company or Licensee (as applicable); the term "control", for the purpose of this definition, shall mean direct or indirect possession of the power to direct or cause the direction of the management or policies of Company or Licensee (as applicable), whether through the ability to exercise voting power, by contract or otherwise.

1.2. "**Agreement Data Subject**" shall mean natural persons to which Agreement Personal Data relate.

1.3. "**Agreement Personal Data**" shall mean any Personal Data Processed by Company or any Subcontractor pursuant to or in connection with the Agreement.

1.4. "**Applicable Laws**" shall mean European Union or a Member State law and any other applicable law with respect to the activities contemplated by the Agreement.

1.5. "**Applicable Privacy Laws**" shall mean EU Privacy Laws, US Privacy Laws, and, to the extent applicable, the data protection or privacy laws of any other country.

1.6. "**Controller to Processor Standard Contractual Clauses**" means the Controller to Processor standard contractual clauses as adopted by Commission Implementing Decision (EU) 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.

1.7. "**EEA**" means the European Economic Area.

1.8. "**EU Privacy Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each EU member state and as amended, replaced or superseded from time to time, including by the GDPR and laws, rules and guidelines implementing or supplementing the GDPR.

1.9. "**GDPR**" shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

1.10. "**Restricted Processing**" shall mean (1) the transferring of Agreement Personal Data outside the EEA or to an International Organization, and (2) any Processing of Agreement Personal Data that was transferred to any country outside the EEA or to an International Organization; in each case, where such transferring or Processing of Agreement Personal Data would be prohibited by Applicable Privacy Laws in the absence of Standard Contractual Clauses.

1.11. "**Sell**", "**Sale**" or "**Selling**" of Agreement Personal Data, shall mean selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Agreement Personal Data to a third party for monetary or other valuable consideration.

1.12. "**Subcontractor**" shall mean any person appointed by or on behalf of Company to Process Agreement Personal Data on behalf of Licensee in connection with the Agreement, excluding any employee of Company or of any such appointed person.

1.13. "**US Privacy Laws**" shall mean the applicable state, local, and/or federal privacy laws, including but not limited to the California Consumer Protection Act.

1.14. "**European Commission**", "**Controller**", "**Data Subject**", "**International Organisation**", "**Member State**", "**Personal Data**", "**Personal Data Breach**" and "**Processing**" shall have the meanings ascribed to them in the GDPR.

2. Authorization and Compliance

2.1. By virtue of the Agreement, Licensee is considered as the "Controller" and Company is considered as the "Processor" with regards to the Agreement Personal Data.

2.2. **Schedule 2.2** to this Addendum sets out certain details regarding Company's Processing of Agreement Personal Data, as required by article 28(3) of the GDPR. Company may make reasonable changes to Schedule 2.2 as it considers necessary to meet those requirements.

2.3. Licensee shall, in its use of the Services, Process Agreement Personal Data in accordance with the requirements of all Applicable Laws, including Applicable Privacy Laws. Without derogating from the generality of the above, Licensee bears the exclusive responsibility for assessing the lawfulness of the Processing of Agreement Personal Data, as well as the lawfulness of the transfer of Agreement Personal Data to Company to Process Agreement Personal Data for the provision of the Services.

2.4. Company shall only Process Agreement Personal Data on behalf of and in accordance with Licensee's documented instructions. Licensee's instructions for the Processing of Agreement Personal Data shall comply with Applicable Laws.

2.5. Company acknowledges and confirms that it does not receive or Process any Agreement Personal Data as consideration for any services or other items that Company provides to Licensee under the Agreement. Company commits to refrain from Selling any Agreement Personal Data Processed hereunder, without Licensee's prior written consent, nor taking any action that would cause any

transfer of Agreement Personal Data to or from Company under the Agreement or this Addendum to qualify as Selling of such Agreement Personal Data.

2.6. The Parties agree that Company shall Process Agreement Personal Data (i) in accordance with this Addendum and the Agreement, which set out the Licensee's instructions to Company in relation to the Processing of Agreement Personal Data, and/or (ii) on documented instructions from Licensee, unless prohibited to do so by Applicable Laws to which Company is subject. To the extent that Company believes that an instruction given by Licensee does not comply with any Applicable Law, it shall refuse to comply with such instruction even if Licensee insists on it in spite of the notification of Company.

3. Company's Personnel

3.1. Company shall ensure that access to Agreement Personal Data is strictly limited to those individuals who need to know or access the relevant Agreement Personal Data and as strictly necessary for the purpose of the Agreement.

3.2. Company shall take all steps reasonably necessary to ensure that the individuals who may have access to Agreement Personal Data on its behalf (i) are informed of the confidential nature of Agreement Personal Data; and (ii) are subject to confidentiality undertakings or appropriate statutory obligations of confidentiality.

4. Subcontractors

4.1. Licensee acknowledges that (i) Company's Affiliates may be retained as Subcontractors; and (ii) Company and Company's Affiliates may engage third-party Subcontractors in connection with the provision of the Services.

4.2. Company shall ensure that the arrangement between Company and any Subcontractor is regulated by a written agreement or other written instrument governed by EU Member State law, imposing on the Subcontractor undertakings that guarantee at least the same level of protection for Agreement Personal Data as those set out in this Addendum.

4.3. **Schedule 4.3** lists Subcontractors that are currently engaged by Company to Process Agreement Personal Data on behalf of Licensee. At least thirty (30) days before Company engages a new Subcontractor, Company will update the Licensee of that change, providing it with the details of the new Subcontractor and the services to be provided thereby. If Licensee has a legitimate reason under Applicable Privacy Laws to object to the new Subcontractor's Processing of Agreement Personal Data, Licensee may terminate the Agreement (limited to the Services for which the new Subcontractor is intended to be used) on written notice to Company. Such termination shall take effect at the time determined by the Licensee, which shall be no later than thirty (30) days from the date of Company's notice to Licensee informing Licensee of the new Subcontractor. If Licensee does not terminate the Agreement within this thirty (30) day period, Licensee is deemed to have accepted the new Subcontractor.

4.4. Within the thirty (30) day period from the date of Company's notice to Licensee informing Licensee of the new Subcontractor, Licensee may request that the Parties discuss a resolution of the objection. Such discussions shall not extend the period

for termination and do not affect Company's right to use the new Subcontractor after the thirty (30) day period.

5. Rights of Agreement Data Subject

5.1. Without derogating from the generality of the above, Company shall (i) notify Licensee without undue delay of any request raised by an Agreement Data Subject in relation to Agreement Personal Data concerning him or her to Company; and (ii) refrain from responding to any such request, except on a written instruction of Licensee or as required by Applicable Law to which Company is subject.

5.2. Taking into account the nature of the Processing of Agreement Personal Data by Company, Company shall assist Licensee by reasonably appropriate technical and organisational measures, insofar as this is possible and reasonable, for the fulfilment of Licensee's obligations to respond to a request raised by an Agreement Data Subject in relation to Agreement Personal Data concerning him or her. Company may refer requests of Agreement Data Subjects received in relation to Agreement Personal Data concerning them and the Agreement Data Subjects making them, directly to the Licensee for its treatment of such requests.

6. Personal Data Breaches

6.1. Company will notify Licensee of any Personal Data Breach affecting Agreement Personal Data without undue delay after becoming aware of the Personal Data Breach, and reasonably assist Licensee in relation to any Personal Data Breach notifications Licensee is required to make under the GDPR.

6.2. Unless the Personal Data Breach is entirely not under the responsibility of Company, Company will take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach, to the extent mitigation is within Company's reasonable control.

6.3. For avoidance of doubts, Licensee, at its sole discretion, shall determine whether, when and what information to notify any Data Subject or a supervisory authority regarding a Personal Data Breach and take all risks regarding the completeness of such information.

7. Data Security

7.1. Company has implemented and will apply the technical and organizational measures set forth in **Schedule 7.1** to protect the security of Agreement Personal Data. Licensee has reviewed such measures and agreed that as to the Services the measures are appropriate taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing of Agreement Personal Data.

7.2. Company may change the measures in Schedule 7.1 at any time without notice so long as it maintains a comparable or better level of security.

8. Restricted Processing

8.1. The Parties hereby enter into the Controller to Processor Standard Contractual Clauses Clauses with the following modifications: (i) Clause 7 – Docking Clause – is not used; in Clause 9 option 2 (General Written Authorization) will apply,

notification period will be 30 days; In Clause 11 the optional language will not apply; In Clause 17 governing law will be the Ireland law; In Clause 18 disputes shall be resolved by the courts of Ireland. In Annex I Licensee is the 'Data exporter', Company is the 'Data importer'; the 'Data subjects', 'Categories of data', 'Frequency of the transfer', 'Nature of processing', 'Purpose', 'Retention period' and 'Subject matter, nature and duration of the processing' are as described in this Addendum. The competent supervisory authority' is the Data Protection Commission of Ireland; (ii) Schedule 2.2 to this Addendum shall apply as Annex I of the Controller to Processor Standard Contractual Clauses; (iii) Schedule 7.1 to this Addendum shall apply as Annex II of the Controller to Processor Standard Contractual Clauses; and (iv) Schedule 4.3 to this Addendum shall apply as Annex III of the Controller to Processor Standard Contractual Clauses.

8.2. In the event of any conflict or inconsistency between this Addendum and the Controller to Processor Standard Contractual Clauses, the Controller to Processor Standard Contractual Clauses shall prevail.

8.3. Other Controllers, whose use of the Services has been authorised by Licensee under the Agreement, also enter into the Controller to Processor Standard Contractual Clauses with the Company. In such case, Licensee will enter into the Controller to Processor Standard Contractual Clauses on behalf of other Controllers.

8.4. For avoidance of doubt, Articles 8.1 and 8.2 shall not apply in respect of Restricted Processing that are allowed by Applicable Privacy Laws without entering into the Controller to Processor Standard Contractual Clauses or an agreement incorporating the Controller to Processor Standard Contractual Clauses.

9. Data Protection Impact Assessment and Prior Consultation

If, pursuant to Applicable Privacy Laws, Licensee is required to perform a data protection impact assessment or prior consultation, at Licensee's request, Company shall provide such documents as are generally available for the Services. Any additional assistance shall be mutually agreed between the Parties.

10. Records

Each Party is responsible for its compliance with its own documentation requirements, in particular maintaining records of processing activities where required under the Applicable Privacy Laws. Each Party shall reasonably assist the other Party in its documentation requirements.

11. Deletion or Return of Agreement Personal Data

11.1. Subject to Article 11.2, upon a written request of the Licensee at any time and upon the suspension or termination fo the Services (each a "**Termination Event**"), the Company shall, at the Licensee's option, promptly (i) delete all Agreement Personal Data in its possession or control, along with all copies, extracts and other objects or items in which it may be contained or embodied; or (ii) return to Licensee by secure file transfer in such format as requested by Licensee all Agreement Personal Data in its possession or control and delete all such Agreement Personal Data, along with all copies, extracts and other objects or items in which it may be contained or embodied.

11.2. The obligations of Company to delete Agreement Personal Data pursuant to Article 11.1 above shall be subject to any obligations of Company under Applicable Laws requiring the storage of Agreement Personal Data; *provided, however*, that Company shall (i) only retain such Agreement Personal Data to the extent and for such period as required by such Applicable Laws; and (ii) ensure the confidentiality of all such Agreement Personal Data and that such Agreement Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

11.3. Company shall provide written certification to Licensee that it complied with the provisions of this Article 11 above within 7 (seven) days of the occurrence of a Termination Event.

12. Information Rights

Company shall make available to Licensee any information reasonably necessary to Licensee to demonstrate compliance with this Addendum.

13. Audit Rights

Company will allow for and contribute to audits to demonstrate compliance with this Addendum in accordance with the following provisions:

13.1. Licensee shall provide at least six (6) weeks' prior written notice to Company of a request to audit, provided that any such request shall occur no more than once in any twelve (12) calendar month period.

13.2. Upon receipt of the request under Article 13.1 above, Company will inform Licensee if Company has conducted an audit of its data protection and data security procedures in the preceding twelve (12) calendar month period, in which case Licensee agrees to exercise any right it may have to conduct an audit under this Addendum or under the Standard Contractual Clauses (if they apply) by instructing Company to provide Licensee with a summary of such most recent relevant audit report, which shall be considered Company's confidential information.

13.3. To the extent that the Licensee requested an audit under Article 13.1 and Company has not performed an audit pursuant to Article 13.2 during the twelve (12) calendar month period prior to the request, the audit shall be conducted by a mutually agreed upon independent third party auditor who is engaged and paid by Licensee, and is under a non-disclosure agreement requiring the auditor to maintain the confidentiality of all Company's confidential information and all audit findings. All audits shall be conducted during normal business hours, at Company's principal place of business or other location(s) where Agreement Personal Data is Processed. Any such audit will result in the generation of an audit report, which shall be considered Company's confidential information. At Licensee's written request, Company will make available to Licensee a summary of the relevant audit report.

13.4. The scope of any audit will be limited to Company's policies, procedures, systems and controls relevant to the Processing of Agreement Personal Data.

13.5. If the Standard Contractual Clauses apply, nothing in this Article varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or Agreement Data Subject's rights under the Standard Contractual Clauses.

14. Miscellaneous

14.1. This Addendum shall continue to be in force until the termination of the Agreement.

14.2. With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the Parties, including the Agreement, the provisions of this Addendum shall prevail.

14.3. The Parties hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

14.4. If any provision of this Addendum is held by a court of competent jurisdiction to be unenforceable under Applicable Law, then such provision shall be excluded from this Addendum and the remainder of this Addendum shall be interpreted as if such provision was so excluded and shall be enforceable in accordance with its terms; *provided, however*, that in such event this Addendum shall be interpreted so as to give effect, to the greatest extent consistent with and permitted by Applicable Law, to the meaning and intention of the excluded provision as determined by such court of competent jurisdiction.

Schedule 2.2 to the Addendum

Data exporter

The data exporter is the entity identified as the Licensee in the Addendum, which receives a license to use the data importer's Platform.

Data importer

The data importer is the owner and licensor of a platform which enables real time relevant information and feedback during a call through a third party real-time communication software, with the aim to enhance sales performances.

Nature and purpose of the data processing

The provision of the Services pursuant to the Agreement.

Categories of data subjects

The group of individuals affected by the Processing of Personal Data under the Agreement includes customers, potential customer and employees of the data exporter.

Categories of data

The types of personal data that may be collected, processed and/or used under the Agreement may include the following: full name, email address, telephone number, personal data included in conversation summaries and in call transcripts, field of business, areas of business interests, job title, workplace, field of occupation, direct manager, subordinate employees, sales targets, compliance with sales targets, sales data, business calendar data, profile picture, session statistics, geolocation (based on IP address), IP address, browser and device information, referral page. In some situations, the data exporter may transmit to the data importer recordings of business calls, which may contain personal data.

Special categories of data

None.

Processing operations and subject matter of processing

Personal data will be subject to the processing activities which the data importer will be required to perform in order to provide the Services to the data exporter.

Duration of the data processing

Agreement Personal Data shall be processed by the data importer for the duration of the Agreement.

Schedule 4.3 to the Addendum

Sub Processor	Description of processing
MongoDB Atlas	Managed database services
Google Cloud	Cloud services
HI4AI	Data labelling services
OpenAI	User content analysis

Schedule 7.1 to the Addendum

Minimum technical and organizational requirements:

1. **Information security program**. A written security program is implemented, maintained and complied with. As part of the program, Company will: (i) implement an audit program to test and, if necessary, remediate identified gaps of all security controls at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing Agreement Personal Data; (ii) conduct, in line with ISO27001 or similar standards, an annual risk assessment that assesses the threats and vulnerabilities associated with systems; and (iii) produce (pursuant to the results of (i) and (ii)) a documented risk assessment and, where appropriate, risk remediation plan.

2. **Security official**. A designated management level or above security official is responsible for the development, implementation, and ongoing maintenance of the information security program. The appointed official has appropriate recognized information security credentials and qualifications.

3. **Access control**. Access rights are assigned according to the principle that employees and third parties are only granted the level of access they need to perform their activities (need-to-know principle). Access rights are granted according to defined (role-based) permissions. The access rights granted are reviewed regularly. Rights that are no longer required are withdrawn immediately.

4. **Physical access control**. Secure areas are defined on the basis of information security and data protection requirements and protected against unauthorized access by appropriate physical safeguards, defined based on the protection needs of the information located or accessed within them.

5. **Incident response plan**. Policies and procedures are implemented, designed to detect, respond to, and otherwise address incidents, including specific points of contact in the event of an incident, and procedures to: (i) monitor and detect actual and attempted attacks on, or intrusions into, the processing systems, (ii) identify and respond to suspected or known incidents, (iii) immediately mitigate the harmful effects of any incidents without detriment to measures or actions necessary to determine the seriousness of the breach.

6. **System Testing and Maintenance.** Company tests and maintain systems to protect data including, without limitation: (i) installing of critical security patches for operating systems and applications within thirty (30) days of publication, and within three (3) months for other types of patches and updates, (ii) installing the latest recommended versions of operating systems, software and firmware for all system components, and (iii) ensuring that up-to-date system security agent software includes malware protection set to receive automatically updated (at least daily) patches and virus definitions.

7. **Audit logging**. Hardware, software, or procedural mechanisms are implemented and maintained to record and examine activity in processing systems that contain or use electronic information, including appropriate logs and reports concerning the security requirements set forth in this Schedule.

8. **Security awareness and privacy training**. Ongoing security and privacy awareness and training program is maintained for all employees (including management, employees, contractors and other agents), which includes training on how to implement and comply with the information security program and setting forth disciplinary measures for violation of the security program. Security and privacy awareness training are conducted at least annually.