PPL SCHEDULE TO ZOLL ITAMAR DATA PROCESSING ADDENDUM

This PPL Schedule supplements and forms an integral part of the Data Processing Addendum between Processor and Controller (the "**DPA**") where the latter expressly incorporates this PPL Schedule by reference, and shall apply if and to the extent Processor Processes, on behalf of Controller, Personal Data that originates from Israel or is otherwise subject to the PPL in the course of Controller's use of the Services. Capitalized terms not defined herein shall have the meanings given to them in the DPA.

This PPL Schedule shall prevail over any conflicting terms of the DPA and, where applicable, the Agreement, but shall not otherwise modify either, and shall be interpreted to give effect to the Parties' intent to comply with the PPL.

1. **Definitions**

For the purposes of this PPL Schedule, the following terms shall have the meanings set forth below:

1.1. The terms "**Authorized User**", "**Data Security Procedure**", "**Database Systems**", "**Monitoring Mechanism**", "**Risk Assessment**" and "**Security Incident**" have the same meanings as under Israel's Protection of Privacy Regulations (Data Security) 5777-2017 (the "**Regulations**"); "Database Controller" and "**Holder**" have the same meanings as under the PPL.

1.2. "**Database**" means a collection of Personal Data Processed by digital means by Processor solely on behalf of Controller.

2. **Access to Controller's Database Systems**

Processor shall not have access to Controller's Database Systems. Personal Data shall instead be provided to Processor through the Services directly by Controller or the Data Subjects.

3. **Authorized Processing**

The DPA shall apply to the Processing of Personal Data hereunder, with the following terms construed as follows: "Controller" means "Database Controller"; "Data Protection Laws" means the PPL; "DPA" means the DPA as supplemented and modified by this PPL Schedule; and "Processor" means "Holder".

4. **Cross-Border Data Transfers**

Processor shall not transfer, nor permit the transfer of, Personal Data originating from Israel to a jurisdiction outside of Israel unless such transfer is performed in accordance with Israel's Protection of Privacy Regulations (Transfer of Data to Databases Abroad) 5761-2001.

5. **Implementation of Data Security Obligations**

Without limiting any provision of this PPL Schedule, Processor represents and warrants that it:

5.1. Holds a valid certification under the ISO/IEC 27001:2022(E) standard (the "**Standard**"), which applies to its Processing of Personal Data hereunder and shall remain valid throughout the term of the DPA, and that it complies, and shall continue to comply, with the requirements of the Standard, including all relevant controls listed in Annex A thereto, as interpreted and detailed in Israel's Registrar of Databases' Directive No. 03/2018 on 'Applicability of the Protection of Privacy Regulations (Data Security) 5777-2017 to Organizations Certified Under the ISO/IEC 27001 Standard';

5.2. Has established and maintains a Data Security Procedure, shall ensure only those portions strictly necessary for the performance of their duties are disclosed to its Authorized Users, and shall assess the need for updates to such procedure as required by the Regulations;

5.3. Shall ensure that up-to-date documentation detailing the Database structure and the inventory of Processor's Database Systems involved in the Processing of Personal Data is maintained in a manner that limits access to its Authorized Users strictly to the extent necessary for the performance of their duties;

5.4. Shall conduct Risk Assessments and penetration tests on its Database Systems involved in the Processing of Personal Data, discuss their findings and, where necessary, implement corrective measures and update its Data Security Procedure, all as and to the extent required under the Regulations;

5.5. Shall ensure that the records produced by its Monitoring Mechanism are retained for the duration required by law, and that the measures implemented to control access to the Personal Data and to its Database Systems involved in its Processing include, to the extent possible, identification by physical means under the exclusive control of each Authorized User;

5.6. Shall hold periodic discussions regarding any Security Incidents involving the Personal Data and assess the need to update its Data Security Procedure accordingly, all as and to the extent required under the Regulations;

5.7. Shall restrict the connection of portable devices to its Database Systems involved in the Processing of Personal Data, and shall ensure the implementation of reasonable safeguards to protect any Personal Data copied onto such devices, all in accordance with the requirements set forth in the Regulations;

5.8. Shall ensure that reasonable measures are used to authenticate and verify the authorization of its Authorized Users accessing Personal Data remotely via the internet or other public network, including, to the extent required under the Regulations, physical authentication means under each Authorized User's exclusive control;

5.9. Has established and maintains procedures to ensure that backup copies of the data collected or generated pursuant to the provisions set forth in Regulation 17 of the Regulations, to the extent applicable to its Processing of Personal Data, can be restored to their original state at any time.

6. **Compliance Reporting**

Without limiting Processor's audit obligations under the DPA, Processor shall, upon written request, report to Controller at least annually on the manner in which it performs its obligations under this PPL Schedule and the Regulations, as they apply to its Processing of Personal Data.