Israeli Privacy Addendum

“Data Protection Laws” shall also include the Privacy Protection Law, 1981 and the regulations promulgated thereunder.

“Data Transfers” If data is being transferred to a Subprocessor outside of Israel territory, Customer Personal Data shall be transferred to the approved Subprocessor in accordance with and subject to the provisions of the Privacy Protection Regulations (Transfer of Information to Databases Outside the State), 2001.

“**Industry-standard technical and organizational measures required for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality and integrity of Personal Data”**, shall include, at minimum:

1.Service Provider shall maintain and implement sufficient and appropriate (based on the type of Customer Personal Data and its sensitivity) environmental, physical and logical security measures with respect to Customer Personal Data and to Service Provider’s system's infrastructure, data processing system (including the system in which the Customer Personal Data is processed), communication means, terminals, system architecture, hardware and software, in order to prevent penetration and unauthorized access to Customer Personal Data or to the system or communication lines between Customer and Service Provider. Systems on which Customer Personal Data is processed shall be located in a secure location, which may be accessed only by properly authorized employees.

2.The Service Provider will separate, to the extent and level reasonably possible, between the database systems which enable access to Customer Personal Data and other computer systems used by the Service Provider. The Service Provider shall update the database systems on a regular basis, including the computer material required for their operation; no use will be made of systems whose manufacturer does not support their security aspects, unless an appropriate security solution is provided.

3.Service provider shall list all components (hardware and software) used to process Customer Personal Data, including computer systems, communication equipment, and software. Service Provider shall use such list to continuously monitor such components and identify weaknesses and risks for the purpose of implementing appropriate security measures to mitigate them.

4.Service Provider maintains procedures to restrict and limit access to Customer Personal Data, as well as procedures relating to backup and recovery procedures of security related data as required under the Security Regulations.

5.Service Provider shall record the access to the Customer Personal Data, including recording the exit or entry of any employee for or into the facilities where the Customer Personal Data is processed, as well as any equipment brought in or taken out of such facilities.

6.Service Provider shall implement automatic control mechanisms for verifying access to systems containing Customer Personal Data, which shall include, inter alia, the user identity, date and time of access attempt, the system component attempted to be accessed, type and scope of access and if access was granted or denied.

Service Provider shall periodically monitor the information from the control mechanisms, list issues and irregularities and the measures taken to handle them. Control records shall be maintained for a minimum of 24 months. Service Provider records and any related reports and measures will be shared with Customer, upon request, and to extent required under Privacy Law, such records shall be backed-up by Service Provider.

7.Service Provider declares and undertakes that it has a valid SOC2 certification and that it will continue to hold it, comply with and continue to meet its requirements throughout the term of the Terms.

8.The Service Provider will not transfer Customer Personal Data through a public communications network or via the internet, without using industry-standard encryption methods.