DATA SHARING ADDENDUM

DATASET

This data processing addendum (the "**Addendum**"), forms a part of the Terms of Service (the "**ToS**") entered into by and between O.G Data Network Ltd., a company incorporated under the laws of the State of Israel ("**OG**"), and You (the "**Customer**") (with OG on the one hand and the Customer on the other hand may also be referred to herein as a "**Party**", and collectively they may also be referred to as the "**Parties**").

By entering into the Principal Agreement, the Parties enter into this Addendum. For the purposes of this Addendum only, any reference to any Party shall also refer to such Party's Affiliates, as the term Affiliate is defined below.

By virtue of the Principal Agreement, OG may share certain Agreement Personal Data (as this term is defined below) with Customer. Therefore, each Party wishes ensure that the other Party fulfils its obligations under Applicable Privacy Laws in connection with the Agreement Personal Data, and otherwise agree to set out the responsibilities in relation thereto (as the terms Applicable Privacy Laws and Agreement Personal Data are defined below).

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. "**Agreement Personal Data**" shall mean any Personal Data Processed by any Party pursuant to or in connection with the Principal Agreement.

1.2. "**Affiliate**" shall mean person or entity controlling, controlled by or under the common control with the relevant Party; 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 the Party in question, whether through the ability to exercise voting power, by contract or otherwise.

1.3. "**Applicable Privacy Laws**" shall mean all laws and regulations, including the laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Agreement Personal Data.

1.4. "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

1.5. "**Controller**" means the entity which determines the purposes and means of the Processing of Agreement Personal Data.

1.6. "**Controller to Controller Standard Contractual Clauses**" shall mean the Controller to Controller standard contractual clauses available at the following link:

https://operia.io/wp-content/uploads/2021/11/Operia_Controller_to_Controller_Standard_Contractual_Clauses_091121.pdf.

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. "**International Organization**" means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

1.11. "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an alias, an identification number, location data, a postal address, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.12. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Agreement Personal Data transmitted, stored or otherwise Processed.

1.13. "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.14. "**Processor**" means the entity which Processes Personal Data on behalf of the Controller, including, as applicable, any "service provider" as this term is defined by the CCPA.

1.15. "**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 Controller to Controller Standard Contractual Clauses.

1.16. "**Business**", "**Service Provider**", "**Third Party**" and "**Sale**" shall have the meanings ascribed to them in the CCPA.

2. Acknowledgement and Compliance

2.1. By virtue of the Principal Agreement, the Parties acknowledge that in respect of Agreement Personal Data Processed pursuant to the Principal Agreement the Parties

are separate Controllers and separate Businesses, as defined under any Applicable Privacy Laws.

2.2. Each Party shall determine the purposes and means of Processing of Agreement Personal Data thereby independently. Accordingly, the Parties shall neither Process Agreement Personal Data as joint controllers, nor as Controller and Processor, Business and Service Provider, or Business and Third Party, under Applicable Privacy Laws.

2.3. **Schedule 2.3** to this Addendum sets out certain details regarding the sharing of Agreement Personal Data between the Parties under the Principal Agreement.

2.4. It is clarified, that the Agreement Personal Data is not intended to include special categories of personal data, within the meaning of this term is the GDPR. Accordingly, Customer undertakes that in case that it locates special categories of personal data within the Agreement Personal Data transferred to it by OG, it shall (i) delete such data immediately and refrain from using it for any purpose whatsoever and (ii) notify OG so that it can remove such data from its own database.

2.5. Each Party shall comply with its respective obligations under Applicable Privacy Laws in the Processing of Agreement Personal Data.

3. Data Security

Customer shall implement appropriate technical and organisational measures to secure the Agreement Personal Data, consistent with best practice standard of care. Without derogating from the generality of the aforesaid, as a minimum requirement, Customer commits to implement and apply the technical and organisational measures set forth in **Schedule 3** to protect the security of the Agreement Personal Data.

4. Restricted Processing

4.1. The Parties hereby enter into the Controller to Controller Standard Contractual Clauses. In the event of any conflict or inconsistency between this Addendum and the Controller to Controller Standard Contractual Clauses, the Controller to Controller Standard Contractual Clauses shall prevail.

4.2. The Controller to Controller Standard Contractual Clauses entered into by and between the Parties pursuant to Section 4.1 above, shall apply to any Restricted Processing that will be carried out by either Party.

4.3. Should a change in, or a decision of a competent authority under, an Applicable Privacy Law, require to make changes to the Controller to Controller Standard Contractual Clauses in order to validate Restricted Processing under Applicable Privacy Laws, each Party shall cooperate in good faith with the other Party to re-negotiate the terms of the Controller to Controller Standard Contractual Clauses in light of such change or decision, so as to ensure compliance with any Applicable Privacy Laws.

4.4. For avoidance of doubt, this Section **Error! Reference source not found.** shall not apply in respect of Processing of Agreement Personal Data that are allowed by EU Privacy

Laws without entering into the Controller to Processor Standard Contractual Clauses or an agreement incorporating the Controller to Controller Standard Contractual Clauses.

5. Cooperation

In any event where a Party receives correspondence, inquiry or a complaint from a third party that relates to the Processing of Agreement Personal Data by the other Party, the following provisions shall apply:

5.1. The Party receiving such correspondence, inquiry or a complaint shall promptly notify the other Party of such correspondence, inquiry or a complaint, providing it with all details related to such correspondence, inquiry or a complaint.

5.2. The Parties shall cooperate in good faith in order to respond to the correspondence, inquiry or a complaint in accordance with the requirements of the Applicable Privacy Laws.

6. Survival

This Addendum shall survive termination or expiry of the Principal Agreement. Upon termination or expiry of the Principal Agreement, each Party may continue to Process Agreement Personal Data, provided that such Processing complies with Applicable Privacy Laws and the provisions of this Addendum.

7. Miscellaneous

7.1. Nothing in this Addendum reduces either Party's obligations under the Principal Agreement or Applicable Privacy Laws in relation to the protection of Agreement Personal Data or permits either Party to Process (or permit the Processing of) Agreement Personal Data in a manner which is not explicitly authorized by the Principal Agreement.

7.2. Subject to the provisions of Section 7.1 above, 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 Principal Agreement, the provisions of this Addendum shall prevail.

7.3. Without derogating from the provisions of Clauses 17 (Governing law applicable to the clauses) and 18 (Choice of forum and jurisdiction) of the Controller to Controller Standard Contractual Clauses:

7.3.1. 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 Principal Agreement;

7.3.2. The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity.

7.4. If any provision of this Addendum is held by a court of competent jurisdiction to be unenforceable, 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.

7.5. Any notice or other document to be given under this Addendum shall be in writing and shall be deemed to have been duly given if sent via email, delivered by hand or sent by recorded delivery to the other Party at the address noted in the preamble to the Principal Agreement. Any such notice or other documents shall be deemed to have been received by the addressee 7 (seven) days following the date of dispatch if the notice or other document is sent by registered post, or in the following business day after the day in which the notice is received by personal delivery or sent via email.

Schedule 2.3 to the Addendum

DESCRIPTION OF THE SHARING OF AGREEMENT PERSONAL DATA

Data subjects

The personal data transferred concern the following categories of data subjects:

Individuals who published personal data in publicly available webpages.

Purposes of the transfer(s)

The transfer is made for the following purposes:

For the provision of license and/or services by OG to Customer pursuant to the Principal Agreement.

Categories of data

The personal data transferred concern the following categories of data:

Name, number of contacts, general description, country location, position, workplace, education data, professional experience, membership in social groups, language proficiency, recommendations, professional certificates, social activities, participation in projects and participation in volunteer activities.

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

Recipients and categories of recipients specified in the public-facing privacy policy of the Customer, as shall be from time to time.

Sensitive data

The personal data transferred concern the following categories of sensitive data:

Not applicable.

Nature of the transfer

The personal data transferred will be processed as part of the License pursuant to the Principal Agreement.

Schedule 3

Minimum technical and organizational requirements:

1. **Information security program**. A written security program is implemented, maintained and complied with. As part of the program, Customer 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.** Customer tests and maintained 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 for the in this Schedule.

8. **Security awareness and privacy training**. An 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.