SUPPLIER: Obie.ai

DATA PROCESSING AGREEMENT

This data processing agreement ("**Data Processing Agreement**") applies to [your business name] (**"Client"**) and the Supplier. The Parties agree as follows:

1 GENERAL

1.1 This Data Processing Agreement is entered into and becomes effective on the date identified on the signature form attached to this Data Processing Agreement.

1.2 To the extent there is any conflict between the Contract and this Data Processing Agreement, the terms of this Data Processing Agreement will prevail so far as the subject matter concerns the processing of Personal Data.

1.3 The Contract, as amended by this Data Processing Agreement supersedes all prior versions of the Contract and all other communications and understandings, whether written or verbal.

2 DEFINITIONS

Agreement means the Contract, as amended by this Data Processing Agreement.

Business Day means a day other than Saturday, Sunday or a day on which banks are authorised to close in Canada for general banking business.

Data Breach has the meaning given in clause 3.4.6.

Data Protection Law means the Data Protection Act 1998, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation and/or regulation which amends, replaces, re-enacts or consolidates them, including the General Data Protection Regulation (EU) 2016/679, as may be in force and applicable, from time to time.

Client means

[your business name and address]

Client Data means all Personal Data processed by the Supplier under or in connection with the performance by the Supplier of its obligations under the Contract.

Personal Data has the meaning given in clause 3.1 of this Agreement.

Regulatory Body means those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled by any applicable law to supervise, regulate, investigate or influence the matters dealt with in the Contract, this Data Processing Agreement or any other affairs of the Client.

Sub-processor means a person or entity subcontracted by the Supplier to process the Client Data in accordance with the Supplier's obligations under or in connection with the Contract on the Supplier's behalf and subject to the Client's instructions.

Supplier means the entity identified as "Supplier" in the signature form attached to this Data Processing Agreement.

3 DATA PROTECTION

3.1 For the purposes of this Agreement, "Personal Data", "data controller", "data processor", "data subject" and "process" shall have the meaning given by the Data Protection Law.

3.2 The Parties agree and acknowledge that the Supplier may be acting as a data processor or sub-processor, as the context admits or requires, in respect of the Client Data.

3.3 The subject-matter of the data processing is the performance of the Contract and the processing will be carried out for the duration of the Agreement. Schedule 1 of this Data Processing Agreement sets out the nature and purpose of the processing, the types of personal data the Supplier processes and the categories of data subjects whose personal data is processed.

3.4 The Supplier will:

3.4.1 process the Client Data in compliance with this Data Processing Agreement, all applicable laws, enactments, regulations, orders, standards and other similar instruments, including but not limited to the Data Protection Law;

3.4.2 process the Client Data only to the extent, and in such a manner, as is necessary for the purposes specified in the Contract and in accordance with Client's written instructions from time to time and shall not process the Client Data for any other purpose with the exception of anonymized queries which are used to train the Supplier's natural language processing component for the benefit of all Supplier clients. Where the Supplier is required by law to process the Client Data, the Supplier will promptly inform the Client of such legal requirement prior to carrying out the processing, unless it is prohibited from doing so by law;

3.4.3 implement and maintain appropriate technical and organisational measures to protect against unauthorised or unlawful processing of the Client Data and against accidental loss or destruction of, or damage to, the Client Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting the Client Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to the Client Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it). Measures implemented by sub-processor Microsoft Azure shall include at least those measures described in Schedule 2 (Security Measures);

3.4.4 ensure that all personnel who have access to and/or process the Client Data have undertaken training in the laws relating to handling Personal Data and procure such personnel to keep the Client Data confidential;

3.4.5 notify the Client within seventy-two (72) hours if it receives any complaint, notice or communication which relates to the processing of the the Client Data, or any request from a data subject exercising any rights pursuant to the applicable Data Protection Law ("**Data Subject Request**"). Supplier shall not respond to a data subject Request without the Client's prior written consent except to confirm that such request relates to the Client, to which the Client hereby agrees. The Supplier shall provide the Client with full cooperation and assistance in relation to any such complaint, notice communication, or request and shall not disclose any of the Client Data to any data subject or to a third party other than at the request of the Client, or as provided for in this Data Processing Agreement;

3.4.6 notify the Client within seventy-two (72) hours if it becomes aware of any unauthorised or unlawful processing, loss of, damage to, disclosure of, access to or destruction of the Client Data ("**Data Breach**") and provide the Client with any co-operation, information and assistance in respect of any Data Breach, reasonably requested by the Client, at the Supplier's own expense, which shall include the following to the extent then known: (i) detailed description of the Data Breach; (ii) the possible cause and consequences for the Data Subjects of the Data Breach; (iii) the categories of Personal Data involved, (iii) a summary of the possible consequences for the relevant data subjects; (iv) a summary of unauthorised recipients of the Personal Data; (v) measures taken by Supplier to mitigate any damage; and (vi) the identify of each affected person.

3.4.7 promptly comply with any request from the Client requiring the Supplier to amend, transfer, return or delete the Client Data, unless otherwise required by law. For the avoidance of doubt, where the Contract is terminated by either Party, the Supplier will, upon the Client's request, irretrievably delete and (at Client's sole option) return to the Client all of the Client Data, and delete all copies of the Client Data, immediately, and provide written confirmation to the Client of the same;

3.4.8 allow the Client and any of its third party auditors on behalf of the Client to access any of the Supplier's premises, the Supplier's personnel and relevant data and records as may be reasonably required in order to undertake verification that the Supplier has complied with obligations set out in this clause 3; and

3.4.9 maintain complete and accurate records and information to demonstrate its compliance with this clause 3.

3.5 The Supplier agrees that it will not transfer any of the Client Data to a country outside the European Economic Area unless the Client Data is transferred to a country approved by the European Commission as providing an adequate level of protection for Personal Data or the transfer is made pursuant to European Commission-approved standard contractual

clauses for the transfer of Personal Data or other appropriate legal data transfer mechanisms are used, which (where necessary) the Client hereby authorises the Supplier to enter into on its behalf. If the legal means by which adequate protection for the transfer is achieved ceases to be valid, the Supplier will work with the Client to put in place an alternative solution. The Supplier currently transfers data to/from Microsoft Azure in the United States, which has EU-US Privacy Shield certification, and the Client agrees to this setup.

3.6 The Supplier may not appoint a Sub-processor or give any Sub-processor access to Client Data, unless:

3.6.1 the Supplier gives the Client at least 30 days written notice (such notice to be communicated in the manner prescribed for giving notice in the Contract) prior to the appointment of the Sub-processor, and such notice provides the identity and location of the sub-processer and a detailed description of the intended processing to be carried out by the sub-processor to enable the Client to evaluate any potential risks to Personal Data;

3.6.2 the contract with the Sub-processor includes terms which are at least as protective of Client Data as those set out in this Data Processing Agreement and comply with the requirements of the applicable Data Protection Law;

3.6.3 as between the Client and the Supplier, the Supplier remains fully liable for all acts or omissions of any Sub-processor appointed by it in connection with this Data Processing Agreement; and

3.6.4 the Sub-processor's contract to process the Client Data terminates automatically on termination of this Agreement for any reason.

4 AUDIT

4.1 Supplier shall, in accordance with Data Protection Law, make available to the Client such information in Supplier's possession or control and provide all assistance in connection with audits of Supplier's premises, systems and documentation as the Client may reasonably request with a view to demonstrating Supplier's compliance with the obligations of data processors under Data Protection Law in relation to its processing of Personal Data.

5 TRANSFERS

5.1 The Client acknowledges and accepts that the provision of the Services under the Contract may require the processing of Personal Data by sub-processors in countries outside the EEA.

5.2 To the extent any processing of Personal Data by Supplier takes place in any country outside the EEA, and the Supplier is registered with the EU-US Privacy Shield, approved by the European Commission (Decision of 12th July 2016) (the "**Privacy Shield**"), the terms of the transfer shall be covered by the Privacy Shield providing that: (a) the Supplier hereby warrants and represents that its Privacy Shield certification is valid as of the effective date of this Agreement; (b) the Supplier shall maintain its adherence to the Privacy Shield throughout the duration of the Contract; and (c) the Supplier shall immediately inform the Client if at any time the Supplier ceases to be Privacy Shield certified during the term of the Contract, for whatever reason.

5.3 To the extent any processing of Personal Data by the Supplier takes place in any country outside the EEA, and the Supplier is not registered with the Privacy Shield, the terms of the transfer shall be governed by the standard contractual clauses for the transfer from controllers to processors (Decision 2010/87/EU) and set out in Schedule 3, which are hereby incorporated into this Agreement.

5.4 If, for whatever reason, the transfer of Personal Data under clauses 5.2 and 5.3 ceases to be lawful, the Supplier shall either: (a) with the Client's prior written consent, implement an alternative lawful transfer mechanism; or (b) allow the Client to terminate the Contract at no additional cost or liability to the Client.

5.5 If, in the performance of this Data Processing Agreeement, Supplier transfers any Personal Data to a sub-processor located, or permits processing of any Personal Data by a sub-processor outside of the EEA (without prejudice to clause 3.7), Supplier shall in advance of any such transfer ensure that a legal mechanism to achieve appropriate safeguards in respect of that processing is in place, such as: (a) the requirement for Supplier to execute or procure that the sub-processor execute standard contractual clauses approved by the EU authorities under EU Data Protection Laws and set out in Schedule 3; (b) the requirement for the sub-processor to be certified under the EU-U.S. Privacy Shield Framework; or (c) the existence of any other specifically approved safeguard for data transfers (as recognised under EU Data Protection Laws) and/or a European Commission finding of adequacy. The Supplier currently transfers data to/from Microsoft Azure in the United States, which has EU-US Privacy Shield certification, and the Client agrees to this setup.

6 TERM AND TERMINATION

6.1 Without prejudice to any rights that have accrued under this Data Processing Agreement or any of its rights or remedies, either Party may terminate this Data Processing Agreement with immediate effect by giving written notice to the other party if the other party commits a material breach of this Data Processing Agreement.

6.2 This Data Processing Agreement shall otherwise continue in full force and effect until expiry or termination of the Contract.

6.3 Termination of this Data Processing Agreement shall not affect the accrued rights, remedies, obligations or liabilities of the Parties existing at termination.

6.4 Any provision of this Data Processing Agreement that expressly or by implication is intended to come into or continue in force on or after termination of this Data Processing Agreement shall remain in full force and effect.

7 GENERAL

7.1 These terms and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with the subject matter or formation of this Data Processing Agreement shall be governed by and interpreted in accordance with the laws of the province of Ontario and the country of Canada.

7.2 The Supplier and the Client irrevocably agree that the courts of the province of Ontario and the country of Canada have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arises out of, or in connection with, this Data Processing Agreement or its subject matter or formation.

7.3 This Agreement is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this Data Processing Agreement. No modification of, amendment to, or waiver of any rights under the Data Processing Agreement will be effective unless in writing and signed by an authorized signatory of each party. This Data Processing Agreement may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this Data Processing Agreement. Each party represents and warrants to the other that the execution and delivery of this Data Processing Agreement, and the performance of such party's obligations hereunder, have been duly authorized and that this Data Processing Agreement is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

Data Processing Agreement - Schedule 1

Details of the Personal Data and processing activities

Subject Matter:
The Personal Data processing is required in order to identify users and provide relevant results and permissions within the scope of the Obie solution.

The purpose(s) of the processing is/are: necessary for the provision of the Services

Data Subjects
The Personal Data concern the following categories of data subjects (please specify):
Current personnel, former personnel, Contractors/consultants/freelancers

Categories of data
The personal data transferred concern the following categories of data (please specify):
Name, Work Email, Slack UserId

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
N/A

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
For the Obie bot user to provide search services to any Client users, and gather analytics on usage that are anonymized for Obie admins.

Duration
The duration of the process will be until expiry/termination of the Contract.

Data Processing Agreement - Schedule 2

Security Measures

Access control to premises and facilities
Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries

Access control to systems
Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators

Access control to data
Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorised input, reading, copying, removal modification or disclosure of data. These measures shall include:

- Differentiated access rights
- Access rights defined according to duties
- Automated log of user access via IT systems
- Measures to prevent the use of automated data-processing systems by unauthorised persons using data communication equipment

Disclosure control
Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include:

- Compulsory use of a wholly-owned private network for all data transfers
- Encryption using a VPN for remote access, transport and communication of data.
- Creating an audit trail of all data transfers

Input control
Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.
Measures should include:

- Logging user activities on IT systems
- Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment
- Ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data have been input;

Job control
Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

Availability control
Measures should be put in place to ensure that data are protected against accidental destruction or loss.
These measures must include:

- Ensuring that installed systems may, in the case of interruption, be restored
- Ensure systems are functioning, and that faults are reported

- Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems

Segregation control
Measures should be put in place to allow data collected for different purposes to be processed separately. These should include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments

Data Processing Agreement - Schedule 3

EU Standard Contractual Clauses

2010 EU Model clauses extracted from 2010/87/EU Annex EU Standard Contractual Clauses for the transfer of personal data to data processors established in third countries which do not ensure an adequate level of data protection

INTRODUCTION

Both parties have agreed on the following Contractual Clauses (the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

AGREED TERMS

1. Definitions

For the purposes of the Clauses:

"**personal data**", "**special categories of data**", "**process/processing**", "**controller**", "**processor**", "**data subject**" and "**supervisory authority**" shall have the same meaning as in EU Data Protection Laws 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

the "**data exporter**" means the entity who transfers the personal data;

the "**data importer**" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of EU Data Protection Laws 95/46/EC;

the "**sub-processor**" means any processor engaged by the data importer or by any other sub- processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

the "**applicable data protection law**" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established; and

"**technical and organisational security measures**" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this Clause, Clause 4.1(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

4.1 The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of EU Data Protection Laws 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

5. Obligations of the data importer

5.1 The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Co-operation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

9. Governing law

The Clauses shall be governed by the laws of the Member State in which the data exporter is established, namely Delaware.

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

11. Sub-processing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub- processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third- party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely Delaware.

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5.1(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data-processing services

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

This agreement has been entered into on the date shown at the beginning of the first page of this agreement.

On behalf of the data exporter:

Name (written out in full): [your name]

Position: [your position]

Address: [your business address]

Signature

On behalf of the data importer:

Name (written out in full): Alex Sopinka

Position: CTO

Address: 175 Longwood Road South, Suite 304A, Hamilton, Ontario, Canada, L8P0A1.

Signature

EU Standard Contractual Clauses – Appendix 1

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data Exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

[description of your business and use of Obie]

Data importer
Data importer processes Personal Data upon the instruction of data exporter in accordance with the terms of the agreement between the data importer and data exporter.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
The data exporter may submit Personal Data to data importer, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:
Current personnel, former personnel, Contractors/consultants/freelancers

Categories of data
The personal data transferred concern the following categories of data (please specify):
The data exporter may submit Personal Data to data importer, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:
Name, Work Email, Slack UserId

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
None

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
The objective of the processing of Personal Data by data importer is to provide the Services, pursuant to the Contract.

DATA EXPORTER
[your business name]
Name: [your name]
Authorised Signature:

DATA IMPORTER
Obie.ai
Name: Alex Sopinka
Authorised Signature:

EU Standard Contractual Clauses – Appendix 2

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer and its sub-processor Microsoft Azure, in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

As per **Data Processing Agreement – Schedule 2 (Security Measures)**

SIGNATURE FORM

This signature form and all those documents identified in the table immediately below (together, the "**Data Processing Agreement**") are entered into on their terms, and the terms of this signature form, between each party undersigned (each a "**Party**" and together, the "**Parties**") as of the Signature Effective Date (as defined below):

Each Party agrees that they:

a) have received, read and understood each of the documents forming part of the Data Processing Agreement, including all documents incorporated either by reference or by links to websites, and all amendments (if any) thereto;

b) are bound by the terms of all such documents;

c) intend to deliver good and adequate consideration; and

d) agree that the **Signature Effective Date** is the date of the last signature, below.

By signing below, each signatory certifies that they have express authority to sign on behalf of the company or other entity entering into the Data Processing Agreement and that they have full knowledge of the content of the Data Processing Agreement.

	SUPPLIER
Name and address of legal entity:	Obie.ai, 175 Longwood Road South, Suite 304A, Hamilton, Ontario, Canada, L8P0A1
Company number:	806788329
First and last name of signatory:	Alex Sopinka
Job title:	CTO
Signature:	
Signature date:	April 18, 2019

	CLIENT
Name and address of legal entity:	[your business name and address]
Company number:	[your company number]
First and last name of signatory:	[your first and last name]
Job title:	[your job title]
Signature:	
Signature date:	