DATA PROCESSING ADDENDUM

This Data Processing Addendum ("Addendum") is entered into by and between Flyp Technologies Inc., dba Uberflip, an Ontario, Canada corporation, having its principal place of business at 370 Dufferin Street, Toronto, Ontario, Canada M6K 1Z8 ("Uberflip") and Customer. Uberflip provides content management services which analyzes a data subject's browsing habits in order to tailor marketing content and advertising, promote engagement and generate leads (the "Uberflip Offering").

This Addendum supplements the Services Agreement (the "Agreement") executed by Uberflip and Customer for the provision of the Uberflip Offering. In the event of any conflict between the Agreement and this Addendum, the terms and conditions of this Addendum shall control. Except to the extent expressly superseded or modified in this Addendum, the terms and conditions of the Agreement will apply to this Addendum and remain in full force and effect.

1. Definitions.

"**Processing**" or "**Process**" means the collection, use, modification, retrieval, disclosure, storage, anonymization, deletion, and/or management of Personal Data.

"**Personal Data**" means information of an identified or identifiable individual transferred by Customer, or its permitted agents, to Uberflip hereunder, and any information derived or otherwise created by Uberflip in connection therewith.

"**Privacy Laws**" means all applicable laws and regulations governing the collection, use disclosure and protection of Personal Data.

2. Data Processing and Security Responsibilities.

In the course of Processing Personal Data in connection with the Uberflip Offering, Uberflip shall comply with Privacy Laws applicable to Uberflip. Without limiting the foregoing, Uberflip shall:

a) only Process Personal Data for the purposes of rendering the Uberflip Offering and as otherwise instructed by Customer in writing from time to time, and not Process any Personal Data in any other manner without the express prior written consent of Customer unless required to do so by applicable law, including applicable laws of Canada, the European Union (EU) or the laws of an EU Member State to which Uberflip is subject;

b) immediately inform the Customer if, in Uberflip's opinion, any instruction received from the Customer infringes any Privacy Laws;

c) not disclose (and not allow any of its employees, or permitted agents or representatives to disclose) in any manner whatsoever any Personal Data to any third party without the prior written consent of Customer unless required to do so under applicable law;

d) where any disclosure, transfer or other Processing of Personal Data is required by applicable law, including applicable laws of Canada, the European Union (EU) or the law of an EU Member State to which Uberflip is subject, promptly notify Customer in writing before complying with any such requirement and comply with all reasonable directions of Customer relating thereto; and

e) immediately notify Customer in writing of any (i) enquiry received from individuals relating to, among other things, the individual's right to access, modify, correct, erase or restrict the processing of Personal Data or to exercise their right of data portability or an objection in accordance with Privacy Laws, (ii) complaint received by Uberflip relating to the Processing of Personal Data, and (iii) order, demand, warrant or any other document purporting to compel the production of any Personal Data, and promptly comply and fully co-operate with all reasonable instructions of Customer with respect to any action taken with respect to such enquiry or complaint;

f) implement appropriate physical, technical, administrative and organizational measures appropriate to the sensitivity of the Personal Data to protect the Personal Data against loss, theft, destruction, damage, alteration and unauthorized or unlawful access, use, disclosure or other processing and provide reasonable assistance to Customer, at Customer's cost, to ensure compliance with Customer's obligations to implement such security measures;

g) limit access to Personal Data only to those employees and authorized agents of Uberflip who need to have access to the Personal Data solely for the purposes of Uberflip rendering the Uberflip Offering;

h) ensure or cause each of the employees and permitted contractors of Uberflip to agree, in writing, to protect the confidentiality and security of the Personal Data in accordance with the terms of this Addendum, and otherwise properly advise and train each of its employees and permitted subcontractor of the requirements of Uberflip under this Addendum and applicable Privacy Law;

i) ensure that each employee or permitted contractor of Uberflip involved in rendering the Uberflip Offering hereunder is screened by way of criminal record check and otherwise to confirm the suitability of the performance of their duties in connection with the Uberflip Offering, including the access to and Processing of Personal Data;

j) ensure that all Personal Data Processed by Uberflip in the course of performing the Uberflip Offering is securely and logically segregated from any other information owned or managed by Uberflip or other third parties, including implementing any necessary access barriers and password authorization procedures in connection therewith;

k) except as otherwise agreed to in writing by Customer only maintain and otherwise process the Personal Data in North America (Canada or the United States);

l) provide all reasonable assistance to Customer in connection with its obligations under Privacy Laws to carry out a data protection impact assessment (and, where required by the Privacy Laws, consulting with the relevant supervisory authority in respect of any such data protection impact assessment).

3. Audit Rights

Uberflip shall provide Customer (or its representatives) with access to all information reasonably necessary to demonstrate compliance with this Addendum, upon 30 days advance notice in writing, and in the event that any such audit, inspection or examination reveals that Uberflip is non-compliant with its obligations under the foregoing provisions, to promptly bring itself into compliance.

4. Sub-Processors.

Customer acknowledges and agrees that Uberflip shall use sub-processors (including Uberflip affiliates) to provide the Offering as set out in the then-current sub-processor list, which is available at www.uberflip.com/legal/sub-processors/ (the "**Sub-processor List**"). Uberflip shall enter into a written agreement with each such sub-processor that imposes obligations on the sub-processor that are substantially similar to those imposed on Uberflip under this Addendum. Uberflip shall only retain sub-processors that Uberflip can reasonably expect to appropriately protect the privacy, confidentiality and security of the Personal Data. Where such sub-processors fail to fulfil their data protection obligations, Uberflip shall remain fully liable to the Customer for the performance of those sub-processor's obligations. Uberflip shall update the Sub-processor List prior to appointing any new sub-processor in addition to or in lieu of those listed on the Sub-processor List. Customer can, at any time, subscribe to be updated if and when the Sub-Processor List is updated pursuant to and in accordance with this Addendum. Customer shall have 30 days from the update to the Sub-processor List to object to the appointment of any new sub-processor(s) by providing detailed reasons for such objection to Uberflip.

5. Security Breach Notification.

a) Uberflip shall notify Customer in writing within 48 hours upon Uberflip becoming aware of, or suspecting any loss, theft, damage or unauthorized or unlawful access to or use, disclosure or other Processing of Personal Data in Uberflip's or its agent's or sub-processor's custody or control ("Privacy Breach");

b) The notice referred to in (a) above shall include, in reasonable detail and to the extent known at the time of such notice, a description of the circumstances of the Privacy Breach and the cause of the Privacy Breach, the date and/or time period during which the Privacy Breach is believed to have occurred or, if neither is known, the approximate period, a description of the Personal Information involved in the Privacy Breach, the number of affected individuals or, if unknown, the approximate number, and a description of the steps taken or to be taken by Uberflip to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm. Uberflip shall provide regular updates to Customer as additional information becomes available;

c) Uberflip shall promptly take all necessary and advisable corrective actions, and shall cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate, rectify or remediate such Privacy Breach. Without limiting the foregoing, Uberflip shall cooperate with Customer in investigating and responding to the foregoing, notifying affected individuals and other parties in accordance with applicable law, and seeking injunctive or other equitable relief against any such person or persons who have violated or attempted to violate the security of Personal Data;

d) promptly upon learning of an actual or suspected Privacy Breach, Uberflip shall, if appropriate, retain a reputable forensics expert to recommend to Uberflip steps necessary to stop any ongoing Privacy Breach, to preserve all records and information related to such activities and to investigate the nature and scope of the incident;

e) in the event that applicable law or contract requires that any individuals, organizations, regulators or other parties be notified of a Privacy Breach involving Personal Data, Customer shall determine whether such notice shall come from Customer or Uberflip. In any event, the content, timing and other details of such notice shall be subject to Customer prior written approval, in Customer sole discretion; and

f) without limitation of the foregoing, Uberflip shall keep and maintain a record of every Privacy Breach in connection with the Uberflip Offering provided by Uberflip and provide a copy of such records to Customer promptly upon request.

6. Termination.

In the event a law, or legal requirement, or privacy or information security enforcement action, investigation, litigation or claim, or any other circumstance, is reasonably likely to adversely affect Uberflip's ability to fulfill its obligations under this Addendum, Uberflip shall promptly notify Customer in writing and Customer may, in its sole discretion and without penalty of any kind to Customer, suspend the transfer or disclosure of Personal Data to Uberflip or access to Personal Data by Uberflip, terminate any further Processing of Personal Data by Uberflip, and terminate the Agreement.

Upon the termination of the Agreement or at such other times as instructed by Customer in writing, immediately return (or, upon the written instruction of Customer, securely dispose of) each and every original and copy in every media of all Personal Data in the possession or control of Uberflip and certify to Customer in writing upon completion of any such delivery or disposal. In the event applicable law does not permit Uberflip to comply with the delivery or destruction of the Personal Data, Uberflip warrants that it shall ensure the strict confidentiality of the Personal Data and that it shall not Process any Personal Data by or on behalf of Customer after termination of the Agreement.

IN WITNESS WHEREOF, the parties' authorized signatories have duly executed this Addendum as of the Effective Date:

Flyp Technologies Inc., DBA Uberflip

By: ___________________________________

Print Name: ___________________________

Title: _________________________________

Date: _________________________________

CUSTOMER

By: ______________________

Print Name: ______________

Title: ____________________

Date: ____________________

Name and/or title of person authorized to receive notices for Customer under this Addendum (if different from above):

____

____

Standard Contractual Clauses (processors)

between

Customer

and

Flyp Technologies Inc., dba Uberflip

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: ________________________________

address: ________________________________

tel: ________________________________

fax: ________________________________

e-mail: ________________________________

Other information needed to identify the organisation (if applicable)

(the data exporter or Customer)

Name of the data importing organisation: Flyp Technologies Inc., dba Uberflip

address: 370 Dufferin St., Toronto ON, M6K 1Z8

tel: 416-900-3830

fax: 416-583-5799

e-mail: accounting@uberflip.com

Other information needed to identify the organisation: n/a

(the data importer or Uberflip)

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 Annex A.

The Clauses form a part of the Data Processing Addendum (the “Addendum”) entered into between data exporter and data importer.

1. DEFINITIONS

For the purposes of the Clauses:

(a) personal data, special categories of data, process/processing, controller, processor, data subject and supervisory authority shall have the same meaning as in Directive 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;

(b) the data exporter means the controller who transfers the personal data;

(c) the data importer means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its 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 Directive 95/46/EC;

(d) 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 its instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 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;

(f) 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 Annex A 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 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this clause 3.2, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 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 3.3, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 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

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 Annex B 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 Directive 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 Annex B and a summary description of the security measures, as well as a copy of any contract for sub-processing Offering 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 subjects as the data importer under the Clauses; and

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

5. OBLIGATIONS OF THE DATA IMPORTER

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 Annex B 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 Annex B 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; and

(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 its 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. COOPERATION 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 law of the Member State in which the data exporter is established, namely that Member State listed below in respect of each data exporter.

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 Clauses.

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 fulfil 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 that Member State listed below in respect of each data exporter.

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(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.

13. ADDITIONAL CLAUSE: STRUCTURE

13.1 The data importer enters into these Clauses with each of the data exporters listed below separately and each such Clauses shall constitute a separate and independent agreement between the data importer and the relevant data exporter. Each such Clauses come into force from and including the date they are countersigned by the data exporter, as indicated below.

13.2 For the avoidance of doubt, if a data exporter wishes to vary the Clauses in force between it and the data importer, such variation shall be effected pursuant to clause 10 and the agreement or consent of any other data exporter is not required.

Annex A

to the Standard Contractual Clauses

This Annex 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 Annex A.

Data exporter

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

The data exporter is the legal entity who has engaged the data importer to provide the Uberflip Offering.

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

The data importer is Flyp Technologies Inc., dba Uberflip, a company established under the laws of Ontario, Canada. Uberflip provides content management services which analyzes a data subject's browsing habits in order to tailor marketing content and advertising, promote engagement and generate leads (the "Uberflip Offering").

Data subjects

The personal data transferred concern the following categories of data subjects (please specify)

Partners, shareholders, employees and/or contractors of Customer who have been supplied with a Uberflip user account and password ("Users").

Customer's end users that interact with the Uberflip Offering ("Audience Members").

Categories of data

The personal data transferred concern the following categories of data (please specify)

With respect to Users:

- First and last name;
- Company email address; and
- Employee identification number.

With respect to Audience Members:

- Information uploaded or posted by Audience Member to the Uberflip Offering;
- Internet Protocol address
- Browser type
- Operating system

	• Engagement data (including page requests, actions performed, pages most read, zoom pattern, search terms, average time spent on pages). • Online behavioural tracking data
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)	Personal data will be collected, used, stored, and analyzed for the purposes of providing the Uberflip Offering. The duration of the processing is the term of the Data Processing Agreement entered into by the data exporter and data importer.
DATA EXPORTER	**DATA IMPORTER**
Name: ______________________________	Flyp Technologies Inc., dba Uberflip

Annex B

to the Standard Contractual Clauses

This Annex B 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 in accordance with clause 4(d) and clause 5(c) (or documents/legislation attached):

Information Security Management Program

Uberflip maintains an information security management program that includes a security policy, change management plan, patch management plan, incident management plan, backup and disaster recovery processes and procedures, business continuity procedures, and risk management standards.

The information security management program is designed to help safeguard data transferred by Customer or its permitted agents to Uberflip, and any information derived or otherwise created by Uberflip in connection therewith, against unlawful loss, access or disclosure, as well as to identify and minimize reasonably foreseeable risks through risk assessment and regular testing.

Administrative Safeguards

Access to Uberflip’s data centers is granted only when needed, and then only for a reasonable amount of time, and is reviewed regularly by engineering management.

Uberflip has implemented specific human resource policies that every new employee must sign and agree to before beginning work at Uberflip:

- Each employee goes through a detailed background check, including criminal record and reference checks..
- Employees are required to sign non-disclosure and confidentiality clauses as part of their employment agreements. These are both for internal technologies used by Uberflip (proprietary information), and any client-facing aspects (privacy policies, personal information on users, etc.).
- Uberflip has internal policies that include: clear desktop policy; clear screen policy; workplace behavior; and workplace safety policies, which are re-signed upon any update to the policies, or at the annual mark of employment.
- IT technical training takes place throughout the onboarding of new employees, and again at the annual mark, which touches on topics such as: data privacy; data retention; and risk management

Technical Safeguards

Uberflip restricts digital access to its collocated data centers:

- Access to the data center network is controlled by VPN, multi-factor authentication, and individual employee SSH keys.

- VPN access control lists and SSH keys are managed by Uberflip's engineering management.
- The data center network is segmented into production and non-production networks, with restrictions on cross-network access, to ensure non-production systems can't access production systems.

Encryption:

- Uberflip encrypts backups of databases and files containing personal information. Access to backups and management of encryption keys is carefully controlled by engineering management.
- Uberflip encrypts credentials and other secrets that could be used to access external systems containing personal data. Management of encryption keys is carefully controlled.

Architecture:

- Uberflip's architecture is designed to require, capture, and store as little personal information as possible.
- Uberflip does not store personal information collected through calls-to-action (CTAs) for any longer than is necessary to submit that information to the customer's marketing automation platform (MAP).

Anonymization; use of data:

- Uberflip removes or anonymizes personal data before production data is used for development, testing, or other internal purposes. The process of removing or anonymizing personal data is automated and centralized. The process is reviewed regularly to ensure new data or changes to data formats are accounted for.
- Uberflip does not share personal data with third parties other than authorized sub-processors.

Physical Safeguards

Uberflip restricts physical access to its collocated data centers:

- Building access is controlled by smart card lock, mantrap, a manned front desk, security guards, and comprehensive video security (all 24 hours a day, 7 days a week).
- Suite access is controlled by smart card and/or biometric locks.
- Rack access is controlled by combination locks.
- Building and suite access control lists are managed by Uberflip's engineering management.
- Access is granted only when needed, for a select time period, and is reviewed regularly by engineering management.
- Guests are not allowed without authorization from engineering management.

Uberflip does not store personal information in its office, and its office network does not have direct access to the data center network. However, physical access to Uberflip's office is also restricted:

- building access is controlled by smart card/passcode locks (24 hours a day, 7 days a week), manned front desk (office hours), passcode alarm (outside office hours), and comprehensive video security (24 hours a day, 7 days a week).

Breach Notification

Uberflip will notify Customer in writing within 48 hours upon Uberflip becoming aware of, or suspecting any loss, theft, damage or unauthorized or unlawful access to or use, disclosure or other processing of personal data in Uberflip’s or its agent’s or sub-processor’s custody or control.

Records and Access

Internal system security logs are aggregated and stored online for a minimum of 3 months.

Security Testing and Continued Evaluation

Uberflip performs regular security testing of the Uberflip Offering to ensure vulnerabilities are identified and mitigated in a timely fashion in line with its risk management standards.

Uberflip conducts periodic reviews of the security of Uberflip’s data center facilities, servers, networking equipment, and host software systems and adequacy of its information security management program as measured against industry security standards as well as its policies and procedures.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organization)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organization)