DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its schedules and appendices ("DPA") forms part of the Uberflip Services Agreement (the "Agreement") or other written or electronic agreement 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. This DPA shall apply to the Agreement to the extent that Uberflip processes Personal Data (as defined below) in the provision of Uberflip's services, which includes the services listed on Appendix 3 to the Standard Contractual Clauses ("SCCs") of this DPA (the "Services") and reflects the parties' agreement with regard to the Processing of Personal Data.

By signing this DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Uberflip processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

The Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

1. Definitions.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Uberflip, but has not signed its own Order Form with Uberflip and is not a "Customer" as defined under this DPA.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations. "Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Customer" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.

"Customer Data" means what is defined in the Agreement as "Customer Data" or "Your Data", provided that such data is electronic data and information submitted by or for Customer to the Services.

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, the United States, and Canada, applicable to Uberflip in the Processing of Personal Data under the Agreement, as amended from time to time.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"GDPR" means the 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), including as implemented or adopted under the laws of the United Kingdom.

"Personal Data" means any information relating to an identified or identifiable natural person where such data is Customer Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

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

"Sub-processor" means any Processor engaged by Uberflip.

"Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR or, for the United Kingdom, the Information Commissioner's Office ("ICO").

2. Data Processing and Security Responsibilities.

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and Uberflip is the Processor. Customer acknowledges and agrees that Uberflip will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of Uberflip as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

2.3 Uberflip Processing of Personal Data. Uberflip shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Customer in its use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4 Uberflip recognizes that it is a Service Provider for the Customer and acknowledges that it understands its responsibilities under the CCPA. Uberflip collects Personal Information of California consumers as instructed by the Customer and in accordance with their instructions. Uberflip does not engage in the sharing, disclosing or selling personal information of individual consumers as defined within the CCPA

2.5 Details of the Processing. The subject-matter of Processing of Personal Data by Uberflip is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and

purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2, Details of the Processing.

3. RIGHTS OF DATA SUBJECTS

Data Subject Request. Uberflip shall, to the extent legally permitted, promptly notify Customer if Uberflip receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Taking into account the nature of the Processing, Uberflip shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Uberflip shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Uberflip is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Uberflip's provision of such assistance.

4. UBERFLIP PERSONNEL

4.1 Confidentiality. Uberflip shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

4.2 Reliability. Uberflip shall take commercially reasonable steps to ensure the reliability of any Uberflip personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. Uberflip shall ensure that access to Personal Data is limited to those personnel who need to have access in order to render the Services in accordance with the Agreement.

4.4 Data Protection Officer. Uberflip has appointed a data protection officer. The appointed person may be reached at dpo@uberflip.com.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. Customer acknowledges and agrees that (a) Uberflip's Affiliates may be retained as Sub-processors; and (b) Uberflip may engage third-party Sub-processors in connection with the provision of the Services. Uberflip has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 List of Current Sub-processors and Notification of New Sub-processors. Uberflip shall make available to Customer, the current list of Sub-processors for the Services publicly on its website at https://www.uberflip.com/legal/sub-processors/ (the **"Sub-Processor list"**) with a mechanism to subscribe to notifications for any updates to the Sub-Processor List including the addition or removal of Sub-processors. Uberflip shall update its Sub-Processor List prior to authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

5.3 Objection Right for New Sub-processors. Customer may object (on reasonable grounds pursuant to applicable Data Protection Laws and Regulations) to Uberflip's use of a new Sub-processor by notifying Uberflip promptly in writing within fifteen (15) days of update to the Sub-Processor List in accordance with the mechanism set out in Section 5.2. In the event Customer objects to a new Sub-

processor, as permitted in the preceding sentence, Uberflip will use reasonable efforts to make available to Customer, a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If within sixty (60) calendar days, Customer, acting reasonably, is still not satisfied with the steps taken by Uberflip to meet Data Protection Laws and Regulations, Customer may terminate only those Services which cannot be provided by Uberflip without the use of the objected-to new Sub-processor by providing written notice to Uberflip.

5.4 Liability. Uberflip shall be liable for the acts and omissions of its Sub-processors to the same extent Uberflip would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. SECURITY

6.1 Controls for the Protection of Customer Data. Uberflip shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data as set out in Uberflip's Data Security Policy located at https://www.uberflip.com/legal/ under "Data Security Policy". Uberflip regularly monitors compliance with these measures. Uberflip will not materially decrease the overall security of the Services during a subscription term.

6.2 Third-Party Audits. Uberflip's security operations are audited annually by a third-party. Upon Customer's written request but at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Uberflip shall make available to Customer that is not a competitor of Uberflip (or Customer's independent, third-party auditor that is not a competitor of Uberflip) a copy of Uberflip's then most recent third-party audits as applicable.

6.3 Data Protection Impact Assessment. Upon Customer's request, Uberflip shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Uberflip.

7. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

Uberflip maintains security incident management policies and shall notify Customer without undue delay, but no later than 48 hours after becoming aware of material accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, which is transmitted, stored or otherwise Processed by Uberflip or its Sub-processors (a "Security Breach Incident"). Uberflip shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Uberflip deems necessary and reasonable in order to remediate the cause of such a Security Breach Incident to the extent the remediation is within Uberflip's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

8. TERMINATION; RETURN AND DELETION OF PERSONAL DATA

8.1 In the event a law, legal requirement, 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 DPA, Uberflip shall promptly notify Customer in writing. The parties shall negotiate in good faith, alternative Processing, and if no other alternative processing is commercially reasonable to Uberflip, Uberflip may immediately suspend any processing and/or terminate, in whole or in part, the Agreement and this DPA.

8.2 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. In the event applicable law does not permit Uberflip to comply with the delivery or destruction of the Personal Data, Uberflip shall ensure the strict confidentiality of the Personal Data and shall not Process any Personal Data by or on behalf of Customer after termination of the Agreement.

9. EUROPEAN SPECIFIC PROVISIONS

9.1 GDPR. Uberflip will Process Personal Data in accordance with the GDPR requirements directly applicable to Uberflip in the provision of its Services.

9.2 Data Protection Impact Assessment. Uberflip shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 6.3 of this DPA, to the extent required under the GDPR.

9.3 Transfer mechanisms for data transfers. Subject to the additional terms in Schedule 1, the Standard Contractual Clauses set forth in Schedule 2 to this DPA apply to the Services listed in Appendix 3 to the Standard Contractual Clauses (the "SCC Services"). The SCCs apply to transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries where such transfer would be prohibited by Data Protection Laws and Regulations in the absence of the SCCs. For the avoidance of doubt, the SCCs shall apply where such transfer is to a country which has not been found to ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations, or for which another scheme approved by the European Commission cannot be relied upon.

List of Schedules
Schedule 1: Transfer Mechanisms for European Data Transfers
Schedule 2: Details of Processing
Schedule 3: Standard Contractual Clauses

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

Flyp Technologies Inc., d.b.a. Uberflip	CUSTOMER
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
	Name and/or title of person authorized to receive notices for Customer under this Addendum (if different from above):

SCHEDULE 1: TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

ADDITIONAL TERMS FOR SCC SERVICES

1. **Customers covered by the Standard Contractual Clauses.** The SCCs and the additional terms specified in this Section apply to (i) Customer which is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom and, (ii) its Authorized Affiliates. For the purpose of the SCCs and this Section 2, the aforementioned entities shall be deemed "data exporters".

2. **Instructions.** This DPA and the Agreement are Customer's complete and final documented instructions to Uberflip for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 8(1) of the SCCs, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with this DPA, the Agreement and applicable Order Form(s); (b) Processing initiated by Users in their use of the SCC Services and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of this DPA, the Agreement or Order Form(s).

3. **Data Exports from the United Kingdom under the SCCs.** In case of any transfers of Personal Data under the SCCs from the United Kingdom, to the extent such transfers are subject to Data Protection Laws and Regulations applicable in the United Kingdom ("UK Data Protection Laws"), (i) general and specific references in the SCCs to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 shall hereby be deemed to have the same meaning as the equivalent reference in the UK Data Protection Laws; (ii) References in the SCCs to "the law of the Member State in which the data exporter is established" shall hereby be deemed to mean "the law of the United Kingdom"; and (iii) any other obligation in the SCCs determined by the Member State in which the data exporter is established shall hereby be deemed to refer to an obligation under UK Data Protection Laws.

4. Appointment of new Sub-processors and List of current Sub-processors. Pursuant to Clause 9(a) of the SCCs, Customer acknowledges and expressly agrees that (a) Uberflip Affiliates may be retained as Sub-processors; and (b) Uberflip and Uberflip Affiliates respectively may engage third-party Sub-processors in connection with the provision of the SCC Services. Uberflip shall make available to Customer the current list of Sub-processors in accordance with Section 5.2 of this DPA.

5. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 9(a) of the SCCs, Customer acknowledges and expressly agrees that Uberflip may engage new Sub-processors as described in Sections 5.2 and 5.3 of the DPA.

6. Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be provided by Uberflip to Customer pursuant to Clause 9(c) of the SCCs may have all commercial information, or clauses unrelated to the SCCs or their equivalent, removed by Uberflip beforehand; and, that such copies will be provided by Uberflip, in a manner to be determined in its discretion, only upon request by Customer.

7. Audits and Certifications. The parties agree that the audits described in Clause 8(9)(c) and Clause 8(9)(d) of the SCCs shall be carried out in accordance with the following specifications:

   Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Uberflip shall make available to Customer that is not a competitor of Uberflip (or Customer's independent, third-party auditor that is not a competitor of Uberflip) information regarding the compliance with the obligations set forth in this DPA in the form of third-party audit reports and/or

certifications to the extent Uberflip makes them generally available to its customers. Customer may contact Uberflip at dpo@uberflip.com to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Uberflip for any time expended for any such on-site audit at the Uberflip then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Uberflip shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Uberflip. Customer shall promptly notify Uberflip with information regarding any noncompliance discovered during the course of an audit.

8. Sensitive Data. The parties agree that the Services are not to be used for the transfer and processing of sensitive data that is described in Cause 8(7) of the SCCs.

9. Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the SCCs) and the SCCs in Schedule 3, the SCCs shall prevail.

SCHEDULE 2 - DETAILS Of PROCESSING

Categories of data subjects whose personal data is transferred

- Partners, shareholders, employees and/or contractors of Customer who have been supplied with an Uberflip user account and password ("Users").
- Business relationship management contacts ("Customer Contacts").
- Customer's end users that interact with the Uberflip Services ("Audience Members").

Categories of personal data transferred

With respect to Customer Contacts

- First and Last name
- Company email address
- Optional: Phone number, other contact information or personal data that Customer wishes to transmit to the Services

With respect to Users:

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

With respect to Audience Members:

- Information uploaded or posted by Audience Member to the Services
- Internet Protocol address
- Browser type
- Operating system version
- Engagement data (including page requests, actions performed, pages most read, zoom pattern, search terms, average time spent on customer owned pages).
- Online behavioural tracking data on designated pages by users/customers
- Marketing Automation Platform (MAP) / Customer Relationship Management (CRM) data provided by the customer / controller. This may include contact information and firmographic information related to customer end-users or organizations that was collected independently from Uberflip.

Description of the Processing

Measuring and improving the engagement, and interest of a website visitor in the marketing activities on behalf of Uberflip Customers *in order to create customized marketing experiences to present to website visitors by identifying the proper content to present based on:*

- *where they may be in the purchasing funnel.*
- *company that they may represent*
- *interest in related goods and services*
- *previously collected information on the website visitor that the organization may have in their possession*

Duration of Processing

Personal data will be collected, used, stored, and analyzed for the purposes of providing the Uberflip Services. The duration of the processing is the term of the Data Processing Agreement entered into by the data exporter and data importer.

SCHEDULE 3: EU STANDARD CONTRACTUAL CLAUSES

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or

return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union

([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data exporter accepts the data importer's auditor report(s) as providing all information for demonstrating compliance with the obligations set out in these clauses The data exporter may request for and contribute to an audit of processing activities covered by these Clauses if there are indications of non-compliance. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor if there are indications of non-compliance with the Clauses. Audits may include inspections at the premises or physical facilities, when and where appropriate, of the data importer and shall, where appropriate, be carried out with reasonable notice of no shorter than 30 business days. The data exporter agrees to cover all costs of this audit.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list published on Uberflip's website at https://www.uberflip.com/legal/sub-processors/. The data exporter may be notified electronically by subscribing to notifications to the web page for any intended changes to the list. The importer shall specifically inform the

data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 calendar days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object on reasonable grounds of non-compliance with these Clauses.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as a competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Republic of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. **LIST OF PARTIES**

MODULE TWO: Transfer controller to processor

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: . . . . . .

Address: . . . . . .

Contact person's name, position and contact details: . . . . . .

Activities relevant to the data transferred under these Clauses: . . . . . .

Signature and date: . . . . . .

Role (controller/processor): . . . . . .

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Flyp Technologies Inc, dba Uberflip

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

Contact person's name, position and contact details: Angus Chan, Manager, Data Privacy, dpo@uberflip.com

Activities relevant to the data transferred under these Clauses: The data importer is Flyp Technologies Inc., dba Uberflip, a company established under the laws of Ontario, Canada. The Uberflip Content Experience Platform provides content management services which analyzes a data subject's browsing habits on specific web properties identified by its customers, in order to tailor marketing content and advertising, promote engagement and generate leads. The Uberflip SnapApp Platform enables marketers to discover the criteria for a sales-ready lead and execute marketing programs with interactive assets, prospect insights, and tracking and reporting of results across stages of the process (the "Services").

Signature and date: . . . . . .

Role (controller/processor): Processor . . . . . .

B. **DESCRIPTION OF TRANSFER**

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

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

Business relationship management contacts ("Customer Contacts").

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

. . . . . .

Categories of personal data transferred

With respect to Customer Contacts

- First and Last name
- Company email address
- Optional: Phone number, other contact information or personal data that Customer wishes to transmit to the Services

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 Services
- Internet Protocol address
- Browser type
- Operating system version
- Engagement data (including page requests, actions performed, pages most read, zoom pattern, search terms, average time spent on customer owned pages).
- Online behavioural tracking data on designated pages by users/customers
- Marketing Automation Platform (MAP) / Customer Relationship Management (CRM) data provided by the customer / controller. This may include contact information and firmographic information related to customer end-users or organizations that was collected independently from Uberflip.

. . . . . .

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable. The Uberflip platform is not intended to store, process or transfer sensitive data.

. . . . . .

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Data transfer happens on multiple intervals throughout the day based on the activities of the customer and how popular the sites where the Uberflip platform is deployed

. . . . . .

Nature of the processing

Measuring and improving the engagement, and interest of a website visitor in the marketing activities on behalf of Uberflip Customers

. . . . . .

Purpose(s) of the data transfer and further processing

Create customized marketing experiences to present to website visitors by identifying the proper content to present based on:

- *where they may be in the purchasing funnel.*
- *company that they may represent*
- *interest in related goods and services*
- *previously collected information on the website visitor that the organization may have in their possession*

. . . . . .

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data will be collected, used, stored, and analyzed for the purposes of providing the Uberflip Services. The duration of the processing is the term of the Data Processing Agreement entered into by the data exporter and data importer.

. . . . . .

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Sub-processors provide technical infrastructure for the Uberflip platform; database and event logging; performance management, data visualization, and analytic assistance.

. . . . . .

C. **COMPETENT SUPERVISORY AUTHORITY**

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

Uberflip maintains a description of its technical and organisational measures to ensure the security of customer data on its website located under Data Security Policy at https://www.uberflip.com/legal/. These measures include the following:

Measures of pseudonymisation and encryption of personal data

- Uberflip encrypts backups of databases and files containing customer information. Access to backups and management of encryption keys is controlled by engineering management. Encryption is based on AES256 and managed through AWS Key Management Service in the Canadian Region.
- Uberflip encrypts credentials and other secrets that could be used to access external systems containing personal data.
- If using Uberflip authentication, passwords are hashed using SHA256.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- *Uberflip uses data mirrors and database replication across AWS Canada Region.*
- *Uberflip encrypts backups of databases and files containing personal information. Access to backups and management of encryption keys is carefully controlled by engineering management.*
- Access and role based controls are in place to permit only authorized individuals from accessing production data.
- Access and role based controls are available within the platform for customers to restrict access to content and functionality.
- Uberflip systems and infrastructure is only accessible via an SSL VPN with multi-factor authentication ("MFA"), and individual SSH keys.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- *Uberflip by mirroring and replicating data in near-real-time protects the service from physical, or technical incidents.*
- *Backups are performed periodically each day.*
- *Uberflip undergoes annual backup and restoration testing to ensure processes/procedures in place to mitigate against the unavailability of an entire cloud region.*

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- *Automated tooling and systems are in place to detect and notify the organization of anomalies such as network, access, and storage.*
- *Changes to the environments require approvals and change tickets that include reviewed changes.*
- *Annual penetration test is conducted using an independent 3rd party.*
- *Uberflip undergoes an annual SOC2 Type II audit conducted by a 3rd party to ensure that organization measures are effective for the security of the processing under its controls.*

Measures for user identification and authorisation

- Uberflip manages access to corporate systems through a central application portal.
- Additional VPN authorization is required to access production systems.

- Customers may use SAML based identity providers for identification and authenticating users to access and manage the Service.

Measures for the protection of data during transmission

- *Uberflip platform encrypts data in transit using at minimum TLS1.2*

Measures for the protection of data during storage

- *Data is encrypted using AES256 encryption.*
- *Databases and file systems / object stores (e.g. AWS S3) are encrypted.*
- *Backup files are encrypted.*

Measures for ensuring physical security of locations at which personal data are processed

- *Uberflip uses Amazon Canada AWS for its cloud infrastructure provider that provides physical security for the platform. Please see https://aws.amazon.com/compliance/data-center/controls/ for more information.*

Measures for ensuring events logging

- *Logging of events, configuration and alerts is reviewed as part of our SOC2 Type II annual audit. Network and systems configuration for logging within the Cloud environments are managed through scripts and change control requiring approvals for changing systems and settings.*
- *Uberflip infrastructure security event logs are collected in a central system and protected from tampering. Logs are stored for a minimum of 15 months*
- *All VPCs leverage advanced threat detection tools to monitor and alert for suspicious activities and potential malware.*

Measures for ensuring system configuration, including default configuration

- *Systems configuration, defaults and controls over the configuration is part of our SOC2 Type II audit. Uberflip uses automation and templates to deploy and update configuration without direct personnel involvement. Automation and templates are controlled through Source Change Control and only specific personnel have the authority to merge and deploy changes to Uberflip's production environment.*

Measures for internal IT and IT security governance and management

- *Administrative access and user access are regularly reviewed. Uberflip annual SOC2 Type II audit reviews the effectiveness of its IT and Security governance activities.*

Measures for certification/assurance of processes and products

- *Uberflip engages in an annual SOC2 Type II audit conducted by a 3rd party for certification/assurances of processes and products.*

Measures for ensuring data minimisation

- *Data collection is based on the goals of the product for determining content engagement contact/lead generation, as well as securing the products and services Uberflip offers. A publicly available Data Dictionary is available for viewing that discloses what is being collected and for the identified purposes.*
- *Uberflip's users/customers can configure settings to define information they require to collect such as within their CTA forms.*

Measures for ensuring data quality

- *Data is provided by website visitor activity (browser); visiting pages, completing fields and forms. Where the website visitor is providing information directly, Uberflip customers may tailor rules and verification steps. Customers can correct information that has been transferred to Uberflip through updating their MAP or CRM.*

- *Customers are responsible for the quality of the content that is being provided to Uberflip to process and distribute. Replacement and modification is supported within the platform.*
- *Platform changes are quality controlled through peer reviews, regression tested; a separate quality control team is also part of Uberflip's SDLC*

Measures for ensuring limited data retention

- *Uberflip maintains data for as long as there is a business relationship with the customer; data may also be removed by request of the customer and when appropriate by the data subject.*
- *Features are available within the product to allow customers to remove/delete data based on a request from an individuals.*
- *Data that is collected within Call to Action (CTA) forms are stored for a minimal amount of time to confirm transfer to customer systems.*
- *Automated systems are set to rotate backups at a set interval.*

Measures for ensuring accountability

- *Uberflip has a manager of data privacy to ensure products and services meet commitments for respecting customer and their audience data.*
- Product Roadmap is reviewed for security and privacy concerns.
- Training and acceptance of company policies including privacy, confidentiality and appropriate use is required annually by all employees.
- Tracking of changes made to production environments

Measures for allowing data portability and ensuring erasure

Uberflip permits customers to download content and analytical reports surrounding the engagement of their marketing materials. As Uberflip is not a content creation platform, the customer will already be in possession of the materials we are displaying and managing. The platform provides features for customers to control their content and manage/erase data collected on individuals without requiring its direct assistance.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

Uberflip is able to make requests of its sub-processors, if required, to provide assistance to the controller. In the majority of instances, Uberflip controls the data that is flowing to its sub-processors and can access the information to assist the controller. We review critical sub-processors on an annual basis to ensure security controls are in place.

Transfers to sub-processors are done so in an encrypted manner when travelling across the internet using TLS 1.2 and implement encryption at rest based on the sensitivity of data.