

UPFLEX CLIENT DATA PROCESSING ADDENDUM

Last Updated: 25 April 2022

[Need a signed copy? Please email your request to privacy@upflex.com]

This Data Processing Addendum (“**DPA**”) is incorporated into and forms part of your (“**Client**”) Agreement with Upflex, Inc. (“**Company**”), (the “**Agreement**”).

1. **Scope, Order of Precedence, and Term**

- (a) This DPA applies when Personal Data is processed in connection with the Services.
- (b) In the event of a conflict between this DPA and the Agreement, the DPA will control to the extent necessary to resolve the conflict. In the event the parties use an International Data Transfer Mechanism and there is a conflict between the Transfer Mechanism and this DPA, the Transfer Mechanism will control.
- (c) The effective date of this DPA is the date of the Agreement, or the date that Client first begins using Company Products or Services, whichever is earlier. This DPA is coterminous with the Agreement, except for obligations that survive past termination as specified below.

2. **Definitions**

In this DPA, the following terms have the meanings set forth below. In the event of a conflict between the definitions in this DPA and any applicable Data Protection Law, the definition provided by the Law in question will control. Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

“Affiliate” means (i) for Client, any entity that directly or indirectly Controls, is Controlled by, or is under common Control with Client and (ii) for Company, any entity that is Controlled by Company.

“Control” means ownership of, or the power to vote, more than fifty percent (50%) of the outstanding shares of any class of voting security, control in any manner over the election of a majority of the directors, or of individuals exercising similar functions, or the power to exercise a controlling influence over the management of another entity.

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing Personal Data.

“Client” means the individual or entity that has entered into the Agreement with Company and one that has agreed to incorporating this DPA into the Agreement.

“Client Data” means any data, file attachments, text, images, reports, personal data, or other content that is uploaded or submitted to an online Service by Client or Users and is Processed by Company on behalf of Client.

“Data Protection Laws” means any and all data protection and privacy laws applicable to the processing of Personal Data under the Agreement.

“Data Subject” means a living, natural person who is or can be identified directly or indirectly by reference to an identifier such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

“EU Data Protection Law” means all data protection laws and regulations applicable to Europe, including (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the “**GDPR**”); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i)

and (ii); (iii) in respect of the United Kingdom any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy; and (iv) in respect of Switzerland any applicable national legislation that replace or converts into domestic law the GDPR or any other law relating to data and privacy.

“Company Personnel” means any individual authorized by Company to Process Client Data.

“Parties” or **“Party”** means Client and/or Company as applicable.

“Personal Data” means any information relating to an identified or identifiable natural person (‘data subject’) or household; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

“Process” or **“Processing”** means any operation or set of operations which is performed upon Personal Data, whether or not it is performed via automatic means such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, obfuscation, or destruction.

“Processor” means a natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of a Controller.

“Professional Service” means consulting, implementation, or training services for Products and Services as described in a Purchase Order or Statement of Work.

“Security Breach” means any accidental, unauthorized, or unlawful breach of security that leads to the destruction, loss, alteration, unauthorized disclosure of, or access to, Client Data on systems managed or otherwise controlled by Company.

“Security Incident” means a security event that does not lead to the destruction, loss, alteration, unauthorized disclosure of, or access to, Client Data on systems managed or otherwise controlled by Company.

“SCCs” means the Standard Contractual Clauses approved by the European Commission or Swiss Federal Data Protection Authority (as applicable).

“Services” means the Support and Maintenance Services, Professional Services, Software as a Service, and any other online service or application provided or controlled by Company and made available for Client’s use online and specified in an applicable Purchase Order.

“Software as a Service (SAAS)” means the Upflex Platform which is a method of software delivery and licensing in which software is accessed online via a subscription, rather than bought and installed on individual computers. subscription services that can be accessed online or through a product interface, including Company’s Cloud Services Platform (including software made available through Company’s Cloud Services Platform), software-as-a-service offerings, network services, data feeds, or any other offering and any related applications, content, technology, or information, made available by Company online and provided under an Order.

“Subprocessor” means any individual or entity (including any third party but excluding Company) appointed by or on behalf of Company to process Personal Data pursuant to the Agreement.

“Supervisory Authority” means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR.

“Support and Maintenance Services” means the Product or Service maintenance and technical support services provided by Company under an Agreement or Purchase Order as described in the Agreement.

“Technical and Organizational Measures” or **“TOMs”** means the functions, processes, controls, systems, procedures, and measures that Company implements to promote secure processing and storage of Personal Data, address and prevent data breaches, and facilitate compliance with relevant Data Protection Laws. See

Annex II.

“**User**” means any individual authorized or invited by Client or another User to access and use the Services under the terms of the Agreement.

3. Roles and Responsibilities

(a) Role of the Parties. **Annex I** lists the parties’ statuses as Controller, Joint Controller, Processor, or Subprocessor under relevant Data Protection Laws for each processing activity. The parties agree and understand that Section 3 will apply to them according to their role as indicated in **Annex I**.

(b) Controller

(i) Controller is responsible for the accuracy of Client Data and the legality of the means by which it acquires Client data.

(ii) Controller’s instructions to process Client Data will comply with all applicable Data Protection Laws and be duly authorized, with all necessary rights, permissions, and authorizations secured.

(iii) Company as Controller. Company may collect Personal Data directly from Data Subjects (which may be duplicative of Client Data) in accordance with Company’s internal policies and publicly posted Privacy Notice available at: <https://upflex.com/legal/privacy-policy/>, and nothing in this DPA will prohibit Company from Processing such Personal Data as a Controller under Data Protection Laws.

(c) Processor

(i) Processor, and any person who is authorized by it, will process Client Data only: (a) as instructed by Client or as initiated by Users via a Service; (b) only to the extent necessary to provide Services or to prevent or address technical issues with a Service; (c) to prevent or address violations of the Agreement or this DPA; (d) to comply with Client’s instructions to the extent they are consistent with the terms of the Agreement and applicable law; (e) to comply with appropriate obligations of confidentiality; and/ or (f) in accordance with the rights and duties attached to the Client Data.

(ii) Processor will not disclose Client Data to a third party for monetary or other consideration except as otherwise permitted under this DPA or the Agreement.

(d) Client Responsibilities. Client shall:

(i) be responsible for its secure use of the Services (including account authentication and configuration, securing data when in transit to and from the Services, and any appropriate backup and encryption steps);

(ii) implement appropriate TOMs relating to its use of the Services in a manner which enables Client to comply with applicable laws and regulations and maintain appropriate security, protection, deletion and backup of Personal Data; and

(iii) control the type and substance of Client Data, set User permissions to access Client Data, and be responsible for reviewing and evaluating whether the documented functionality of the Services meets Client’s required security and privacy obligations.

4. Subprocessing

(a) Use of Subprocessors. Client hereby permits Company to engage Sub-processors to process Client Data and approves of the Supplier Affiliates and third parties listed in **Annex III** as Subprocessors. Client shall treat such list as strictly confidential and proprietary information of the Company.

(i) Such Subprocessors will treat all Client Data as confidential and will be permitted to access Client Data only to deliver the services that Company has retained them to provide in connection with the services, and they are prohibited from using Client Data for any other purpose.

(ii) Company will:

- ❖ Enter into a written agreement with each Subprocessor containing data protection obligations that provide at least the same level of protection for Client Data as those in this DPA, to the extent applicable to the nature of the services provided by such Subprocessor;
 - ❖ Restrict the Sub-processor's access to Client Data only to what is necessary to maintain or provide the services to Client; and
 - ❖ Remain responsible for such Subprocessor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-processor that cause Company to breach any of its obligations under this DPA.
- (b) Liability for Subprocessors. Each party will be liable for the acts and omissions of its Subprocessors to the same extent it would be liable if performing the services of the Subprocessor directly under the DPA.
- (c) Objection to Subprocessors. Client agrees to register and subscribe to [Sub-processor list](#) to be notified of any new or updated Subprocessor, including details of the Processing to be undertaken by the Subprocessor.
- (i) In the event that Client reasonably objects to a Sub-processor and notifies Company in writing, Company will notify Client of any available alternatives to change the Services or receive the Services from an alternate Subprocessor, together with any applicable charges or changes to terms, but only to the extent that qualified alternatives are available.
- (ii) If an alternative Subprocessor that is acceptable to Client is not available within a reasonable time, then Client may terminate the Services which cannot be provided by Company without the objectionable Sub-processor, provided that Client shall not receive a refund of any prepaid fees for such Services due to the termination. Company will work with Client in good faith to make available a change in the provision of the Services which avoids the use of that proposed Subprocessor.

5. Data Subject Rights

- (a) Data Subject Rights. As part of the Services, Company may provide Client with a number of self-service features that Client may use to retrieve, correct, delete or restrict the use of Client Data, which Client may use to assist it in connection with its obligations under Data Protection Laws with respect to responding to requests from Data Subjects via Client's account. In addition, Company will, taking into account the nature of the processing, provide reasonable assistance to Client to the extent possible to enable Client to comply with its data protection obligations with respect to Data Subject rights under Data Protection Laws.
- (b) If Client does not have access to such Personal Data through its use of the Services to respond to such request, Company will provide Client with commercially reasonable cooperation and assistance in relation to responding to a Data Subject's request for access to that individual's Personal Data to the extent legally permitted. Client will be responsible for any costs arising from Company's provision of such assistance.
- (c) In the event that any such request is made to Company directly, Company will not respond to such communication except as necessary (for example, to direct the Data Subject to contact Client or if legally required) without Client's prior authorization. If Company is required to respond to such a request, Company will promptly notify Client and provide Client with a copy of the request unless Company is legally prohibited from doing so. For the avoidance of doubt, nothing in the Agreement (including this DPA) will restrict or prevent Company from responding to any Data Subject or Supervisory Authority requests in relation to Personal Data for which Company is a Controller.

6. Cooperation

- (a) Data Protection Impact Assessment. To the extent required under applicable Data Protection Laws, and under strict confidentiality, Company will (taking into account the nature of the processing and the information available to Company) provide all reasonably requested information regarding the Services to enable Client to carry out data protection impact assessments or prior consultations with Supervisory Authorities as required by Data Protection Laws.
- (b) Legal Disclosure Requests. If either party receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, such request will be immediately forwarded to the other party to allow the party an opportunity to engage in any legal processes it deems appropriate with respect to the protection or disclosure of Personal Data.

(c) Audits.

- (i) Company will respond to all reasonable requests for information made by Client to confirm Company's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, by making additional information available regarding its information security program upon Client's written request to compliance@upflex.com provided that Client will not exercise this right more than once per calendar year.
- (ii) Once per year, upon Client's written request and on a confidential basis, Company will, within a reasonable time following such request, make available to Client (or Client's independent third party auditor that is not a competitor of Company) information regarding Company's compliance with the obligations set forth in the DPA, which may be in the form of third party audit reports and certifications, to the extent that Company has such current reports or certifications and generally makes them available to Clients.
- (iii) Client agrees that it will provide at least 30 days written notice for any audit activities. Before the commencement of any audit, Company and the Client will agree upon the scope, purpose, timing, and duration of the audit.
- (iv) Client will reimburse Company for any time expended and expenses incurred for any audit at Company's standard Professional Services rates.

7. Data Transfers and Exports

- (a) The Parties acknowledge and agree that the Processing of Client Data by Company may involve an international transfer of Client Data from Client to Company ("**International Transfer**").
- (b) Standard Contractual Clauses. With respect to any International Transfer from the European Economic Area, the United Kingdom, and Switzerland that would be prohibited by applicable Data Protection Laws in the absence of a lawful data transfer mechanism, the Parties agree that the SCCs issued by the European Commission under decision 2010/87/EU will be in effect between the Parties. If Standard Contractual Clauses are established for the United Kingdom and Switzerland, each respective national standard contractual clauses will be in effect between the Parties for transfers from the United Kingdom or Switzerland respectively.
- (c) The SCCs will apply to Client Data that is transferred outside the European Economic Area ("**EEA**"), either directly or via onward transfer to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).
- (d) The Standard Contractual Clauses will not apply to Client Data that is not transferred, either directly or via onward transfer outside the EEA. Notwithstanding the foregoing the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply if Company has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for the lawful transfer of personal data (as defined in the GDPR) outside the EEA.

8. Security

- (a) Company will not assess the type or substance of Client Data to identify whether it contains Client Data or is subject to any specific legal requirements.
- (b) Company has implemented and maintains appropriate TOMs that are designed to protect Client Data from Security Incidents and to preserve the security and confidentiality of Client Data in accordance with Company's security standards described in Annex II.
- (c) For any Services for which Company obtains third party certifications or audits, upon request, Company will provide a copy of Company's most recent third-party certification or audit as applicable, which Company generally makes available to its Clients at the time of the request.
- (d) Updates to TOMs. Client is responsible for reviewing the information made available by Company relating to data security and for making an independent determination as to whether the Services meet Client's requirements and legal obligations under Data Protection Laws. Client acknowledges that the TOMs may

change through the adoption of new or enhanced security technologies and development and as a result Company may update or modify the TOMs from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to Client.

- (e) Security Breach Response. Client agrees and acknowledges that Company's notification of or response to a Security Breach will not be construed as an acknowledgment by Company of any fault or liability with respect to the Security Incident.
- (f) Upon becoming aware of a Security Breach that results in unlawful exposure, destruction, or loss of access that is likely to affect the rights and freedoms of data subjects, Company will: (a) notify Client without undue delay, and where feasible, in any event no later than 48 hours from becoming aware of the Security Breach; (b) provide timely information relating to the Security Breach as it becomes known or as is reasonably requested by Client; and (c) investigate and, as necessary, take appropriate steps to mitigate or remediate in accordance with Company's Security policies and procedures.

9. General

(a) Modification to the DPA Terms. The parties agree to mutually determine and execute appropriate modifications to the terms of this DPA which do not materially alter the economics or allocation of risk established by the Agreement: (i) if required to do so by a Supervisory Authority or other government or regulatory entity [with appropriate jurisdiction]; (ii) if necessary to comply with Data Protection Law; or (iii) to implement or adhere to revised SCCs which may be issued under Data Protection Law.

(b) Waiver. Unless otherwise expressly stated herein, this DPA may be modified only by a written agreement executed by an authorized representative of each Party. The waiver of any breach of this DPA will be effective only if in writing, and no such waiver will operate or be construed as a waiver of any subsequent breach.

(c) Relationship with the Agreement. Any claims brought under this DPA will be subject to the terms and conditions of the Agreement.

- (i) This DPA will remain in effect for as long as Company carries out Client Data processing operations on behalf of Client or until termination of the Agreement (and all Client Data has been returned or deleted in accordance with Section 9(d) below).
- (ii) This DPA will replace any existing data processing agreement or similar document that the Parties may have previously entered into in connection with the Services.

(d) Return or Deletion of Data.

(i) Upon termination or expiration of the Agreement, Company will (at Client's written request) delete or return to Client all Personal Data in Company's possession or control. The Client acknowledges that Company may retain deidentified or anonymized data for research purposes.

(ii) This requirement will not apply to the extent Company is required by applicable law to retain some or all of the Client Data or to Client Data Company has archived in its backup systems. In this case, Company will archive the data and implement reasonable measures to prevent the Personal Data from any further processing and eventually delete in accordance with Company's retention and deletion policies, unless otherwise required by applicable law.

(e) Severability. If any provision of this DPA is held to be unenforceable, then that provision is to be construed either by modifying it to the minimum extent necessary to make it enforceable (if permitted by law) or disregarding it (if not permitted by law), and the rest of this DPA is to remain in effect as written. Notwithstanding the foregoing, if modifying or disregarding the unenforceable provision would result in failure of an essential purpose of this DPA, the entire DPA will be considered null and void.

(f) Notices. Unless otherwise expressly stated herein, the parties will provide notices under this DPA in accordance with the Agreement, provided that all such notices may be sent via email.

(g) Governing Law and Jurisdiction. Unless prohibited by Data Protection Laws, this DPA is governed by the laws stipulated in the Agreement and the Parties to this DPA hereby submit to the choice of jurisdiction and venue stipulated in the Agreement, if any, with respect to any dispute arising under this DPA.

(h) Enforcement. Regardless of whether Client or its Affiliate(s) or a third party is a Controller of Client Data, unless otherwise required by law: (a) only Client will have any right to enforce any of the terms of this DPA against Company; and (b) Company's obligations under this DPA, including any applicable notifications, will be to only Client.

10. Limitation of Liability

(a) Each Party's and all of its Affiliates' liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) will be subject to the exclusions and limitations of liability set forth in the Agreement to the extent permissible by applicable law.

(b) Any claims made against Company or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) will be brought solely by the Client entity that is a party to the Agreement.

(c) Variations in Data Protection Laws. If any variation is required to this DPA as a result of a change in or subsequently applicable Data Protection Law, then either Party may provide written notice to the other Party of that change in law. The Parties will then discuss and negotiate in good faith any variations to this DPA necessary to address such changes, with a view to agreeing and implementing those or alternative variations as soon as practicable, provided that such variations are reasonable with regard to the functionality and performance of the Services and Company's business operations.

(d) Reservation of Rights. Notwithstanding anything to the contrary in this DPA: (i) Company reserves the right to withhold information the disclosure of which would pose a security risk to Company or its Clients or is prohibited by applicable law or contractual obligation; and (ii) Company's notifications, responses, or provision of information or cooperation under this DPA are not an acknowledgement by Company of any fault or liability.

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) 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 Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 –Module Two: Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 – Module Two: Clause 18(a) and (b).
- (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

[INTENTIONALLY OMITTED]

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 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 (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:

- (a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (b) 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;
- (c) 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
- (d) 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 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. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (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

- (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. The data 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 [Specify time period] 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.
- (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 right

- (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.
- (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

- (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

- (a) 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

- (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 [for Module Three:, if appropriate in consultation with the controller]. 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

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 [for Module Three: and the controller] 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

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

- (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 Ireland.
- (c) The 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

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: The Client as defined in the Client's Upflex Platform Account (on behalf of itself and any affiliated entities).

Address: The Client's address as set out in the Client's Upflex Platform Account.

Activities relevant to the data transferred under these Clauses: **Client operations including business registration on upflex.com and the Upflex App and making bookings via the Upflex Platform.**

Role (controller/processor): **Controller**

Data importer(s):

1. Name: **Upflex, Inc.**

Address: **833 Broadway, Floor 2, New York, NY 10003 USA**

Contact person's name, position and contact details: **Denise Farnsworth, Chief Privacy Officer and Data Protection Officer, privacy@upflex.com**

Activities relevant to the data transferred under these Clauses: **Client operations including business registration on upflex.com and the Upflex App and making bookings via the Upflex Platform.**

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

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred. **The categories of data subjects are Data exporter's employees, consultants, and other contingent workers.**

Categories of personal data transferred. **Data exporter may submit personal data through the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include those categories listed in the Privacy Notice. Examples include business contact information and location data.**

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures. **Location data is processed and transferred for the purpose of providing the Service via the Upflex Platform and is used only for the purpose of providing the Service and is transferred only to those service providers that support provision of the Service with equivalent technical measures and role-based restrictions. All security measures previously listed are applicable to this sensitive data, including role-based restrictions, record retention policy, and encryption.**

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

Nature of the processing. **Software as a service application and platform licensed by Upflex to data exporter.**

Purpose(s) of the data transfer and further processing. **Provide the Services; improve the Services; integrity, safety, and security; and marketing (with consent)**

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period. **For the duration of the contract that is the basis for providing the Services, plus 90 days, or when the employee, consultant, or contingent worker relationship with data exporter is terminated.**

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing. **All sub-processors are services providers that directly support delivery of the Upflex Platform, which includes the transfer of personal data via the Upflex Platform or other technology associated with the Upflex Platform for the duration of the delivery of the Services.**

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

Irish Data Protection Commissioner

ANNEX II

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

MODULE TWO: Transfer controller to processor

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.

Upflex Security Plan

This document provides a description of the technical and organizational security measures implemented by Upflex. Upflex will maintain appropriate administrative, physical, and technical safeguards (“Security Safeguards”) for protection of the security, confidentiality and integrity of Personal data provided by Client in connection with the Standard Contractual Clauses. Upflex’s Security Safeguards are described below and may be updated from time to time and made reasonably available by Upflex.

Security Safeguards include the following:

- **Domain: Organization of Information Security**
 - **Security Roles and Responsibilities.** Upflex personnel with access to data are subject to confidentiality obligations.
 - **Risk Management Program.** Upflex performs a risk assessment where appropriate before processing the data.
- **Domain: Asset Management**
 - **Asset Handling**
 - Upflex classifies the Personal data it processes for Client to help identify it and to allow for access to it to be appropriately restricted (e.g., through usernames, passwords, and encryption).
 - Upflex has procedures for disposing of printed materials that contain Personal data.
 - Upflex maintains an inventory of all hardware on which Personal data is stored.
- **Domain: Human Resources Security**
 - **Security Training**
 - Upflex informs its personnel about relevant security procedures and their respective roles. Personal data also informs its personnel of possible consequences of breaching the security rules and procedures.
- **Domain: Physical and Environmental Security**
 - **Physical Access to Facilities.** Upflex limits access to facilities where information systems that process Client Data are located to identified authorized individuals.
 - **Protection from Disruptions.** Upflex uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

- **Component Disposal.** Upflex uses industry standard processes to delete Client Data when it is no longer needed.
- **Domain: Communications and Operations Management**
 - **Operational Policy.** Upflex maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal data.
 - **Data Recovery Procedures**
 - On a regular and ongoing basis, Upflex creates backup copies of Client Data from which Personal data may be recovered in the event of loss of the primary copy.
 - Upflex stores copies of Client Data and data recovery procedures in a different place from where the primary computer equipment processing the Client Data is located.
 - Upflex has specific procedures in place governing access to copies of Client Data.
 - **Malicious Software.** Upflex has anti-malware controls to help avoid malicious software gaining unauthorized access to Client Data, including malicious software originating from public networks.
 - **Data Beyond Boundaries**
 - Upflex encrypts Client Data that is transmitted over public networks.
 - **Event Logging**
 - Upflex logs the use of its data-processing systems.
 - Upflex logs access and use of information systems containing Client Data, registering the access ID, timestamp, and certain relevant activity.
- **Domain: Information Security Incident Management**
 - **Incident Response Process**
 - Upflex maintains an Incident Response Plan.
 - Upflex maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and remediation steps, if applicable.
- **Domain: Business Continuity Management**
 - Upflex's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Client Data in its original state from before the time it was lost or destroyed.

- **Access Control to Processing Areas**

Processes to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the Personal data are processed or used, to include:

- establishing secure areas,
- protection and restriction of access paths,
- securing the mobile/cellular telephones,
- data processing equipment and personal computers,
- all access to the data centers where Personal data are hosted is logged, monitored, and tracked,
- the data centers where Personal data are hosted is secured by a security alarm system, and other appropriate security measures, and

- the facility is designed to withstand adverse weather and other reasonably predictable natural conditions, is secured by around-the-clock guards, keycard and/or biometric access (as appropriate to level of risk) screening and escort-controlled access and is also supported by on-site back-up generators in the event of a power failure.

Access Control to Data Processing Systems

Processes to prevent data processing systems from being used by unauthorized persons, to include:

- identification of the terminal and/or the terminal user to the data processor systems,
- automatic time-out after 10 minutes or less of user terminal if left idle, identification and password required to reopen,
- issuing and safeguarding of identification codes,
- password complexity requirements (minimum length, expiry of passwords, etc.), and
- protection against external access by means of an industrial standard firewall.

Access Control to Use Specific Areas of Data Processing Systems

Measures to ensure that persons entitled to use data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Personal data cannot be read, copied, or modified or removed without authorization, to include by:

- implementing binding employee policies and providing training in respect of each employee's access rights to the Personal data,
- effective and measured disciplinary action against individuals who access Personal data without authorization,
- release of data to only authorized persons,
- implementing principles of least privileged access to information which contains Personal data strictly on the basis of "need to know" requirements;,,
- production network and data access management governed by VPN, two factor authentication, and role-based access controls,
- application and infrastructure systems log information to centrally managed log facility for troubleshooting, security reviews, and analysis; and
- policies controlling the retention of backup copies which are in accordance with applicable laws which are appropriate to the nature of the data in question and corresponding risk.

Transmission Control

Procedures to prevent Personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Personal data by means of data transmission facilities is envisaged, to include:

1. use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels,
2. implementation of VPN connections to safeguard the connection to the internal corporate network,
3. constant monitoring of infrastructure (e.g., ICMP-Ping at network level, disk space examination at system level, successful delivery of specified test pages at application level), and
4. monitoring of the completeness and correctness of the transfer of data (end-to-end check).

Storage Control

When storing any Personal data Upflex must back the Personal data up as part of a designated backup and recovery processes in encrypted form, using a commercially supported encryption solution and all data defined as Personal data stored on any portable or laptop computing device or any portable storage medium is likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key for symmetric encryption and a 1024 (or larger) bit key length for asymmetric encryption.

Input Control

Measures to ensure that it is possible to check and establish whether and by whom Personal data has been input into data processing systems or removed, to include:

1. authentication of the authorized personnel,
2. protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data,
3. utilization of user codes (passwords),
4. proof established within data importer's organization of the input authorization, and
5. ensuring that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are locked.

Availability Control

Measures to ensure that Personal data are protected from accidental destruction or loss, to include infrastructure redundancy and regular backups performed on database servers.

Segregation of Processing

Procedures to ensure that data collected for different purposes can be processed separately, to include:

1. separating data through application security for the appropriate users,
2. storing data, at the database level, in different tables, separated by the module or function they support,
3. designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately, and
4. barring live data from being used for testing purposes as only dummy data generated for testing purposes may be used for such.

Onsite Control

When present on Client's premises, all employees and subcontractors (if applicable) will comply with all reasonable rules, regulations, practices, and procedures (including, without limitation, security-related arrangements) generally prescribed by Client and use Client property only for the purposes set forth in an Agreement and will return all such property to Client upon completing the applicable services.

Vulnerability management program

A program to ensure systems are regularly checked for vulnerabilities and any detected are immediately remedied, to include:

1. all networks, including test and production environments, regularly scanned (at least quarterly);
2. penetration tests are conducted regularly, and vulnerabilities are remedied immediately, and.
3. Client is, on request, permitted to carry out (or to appoint a third party to carry out) penetration testing on the same systems at least once per year.

Data Destruction

In the event of expiration or termination of the Agreement by either side or otherwise on request from Client following receipt of a request from a data subject or regulatory body:

1. all Client data and documentation shall be securely returned to Client in a format agreed by Client - e.g., as system logs, updated databases etc. - or (at Client's discretion) securely destroyed within 30 days and Upflex will certify such destruction,
2. all Client data (whether constituting Personal data or not) shall be purged from all Upflex and/or third-party storage devices including backups within one (1) month of termination or receipt of a request from Client, unless Upflex is otherwise required by law to retain a category of data for longer periods. Personal data will ensure that all such data which is no longer required is destroyed to a level where it can be assured that it is no longer recoverable, and
3. all information about systems such as network diagrams, IP address ranges, system inventories, User Ids and passwords shall be purged by Upflex within one (1) month and Upflex shall procure that any of its third-party service providers undertake in writing to do the same.

Standards and Certifications

Data storage solutions and/or locations have at least SOC 1 (SSAE 16) or SOC 2 reports – equivalent or similar certifications or security levels will be examined on a case-by-case basis.

ANNEX III

LIST OF SUB-PROCESSORS

Transfer controller to processor.

The controller has authorised the use of the following sub-processors:

1. Name: Stripe, Inc

Address: 185 Berry Street, Suite 550, San Francisco, CA 94107, United States

Contact person's name, position and contact details: Emma Redmond, Global Privacy and Data Protection Lead, privacy@stripe.com

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Payment gateway

2. Name: Amazon Web Services, Inc

Address: 410 Terry Avenue North, Seattle, WA 98109-5210, United States

Contact person's name, position and contact details: AWS General Counsel, privacyshield@amazon.com, Fax: 206-266-7010

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Cloud-based service provider

3. Name: Data Studio (Google)

Address: 1600 Amphitheatre Parkway Mountain View, CA 94043, United States

Contact person's name, position and contact details: Keith Enright, Chief Privacy Officer, enterprise-dpo@google.com

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Upflex uses Data Studio for Booking Analytics, processing employee first and last name, email address, and location data for this purpose.

4. Name: Intercom, Inc

Address: 55 2nd Street, 4th Floor, San Francisco, CA 94105, United States

Contact person's name, position and contact details: Data Protection Officer, legal@intercom.io

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Communication provider (chat support, help center)

5. Name: Google

Address: 1600 Amphitheatre Parkway Mountain View, CA 94043, United States

Contact person's name, position and contact details: Keith Enright, Chief Privacy Officer, enterprise-dpo@google.com

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Data storage in Google Drive (Enterprise version)

6. Name: Hubspot, Inc

Address: 25 First Street, 2nd Floor, Cambridge, MA 02141, United States

Contact person's name, position and contact details: Nicholas Knoop, Data Protection Officer, HubSpot, Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141 USA

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Cloud-based CRM and email service

7. Name: Twilio, Inc

Address: 101 Spear Street, 1st Floor, San Francisco, California 94105, United States

Contact person's name, position and contact details: Twilio Privacy Team, Office of the Data Protection Officer, privacy@twilio.com

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Cloud-based SMS Notification Service (Twilio), Cloud-based Email Notification Service (SendGrid)

8. Name: Mixpanel, Inc

Address: One Front Street, 28th Floor, San Francisco, CA 94111, United States

Contact person's name, position and contact details: Peter Day, Head of Global Privacy, peter.day@mixpanel.com

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Product Analytics

9. Name: Auth0, Inc

Address: 10800 NE 8th Street Suite 700 Bellevue, WA 98004, United States

Contact person's name, position and contact details: Auth0 Privacy Office - Legal Department, 10800 NE 8th Street, Suite 600, Bellevue, WA 98004, U.S.A. privacy@auth0.com

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Identity Management