DATA PRIVACY, DATA PROTECTION AND SECURITY REQUIREMENTS

This Data Privacy, Data Protection and Security Requirements Exhibit ("**Exhibit**") forms a part of the Client Terms of Service provided via the Upflex Platform to you ("**Client**" or "**you**"), or other terms and conditions between the parties that govern the Services. (the "**Agreement**"). The parties understand, acknowledge, and agree this Exhibit is hereby incorporated into the Agreement.

The purpose of this Exhibit is to establish minimum privacy, data protection and security standards and related requirements for Upflex, Inc. ("**Upflex**") in connection with its performance of Services in accordance with the Agreement. Capitalized terms that are not defined in this Exhibit shall have the meaning ascribed to them in the Agreement or under Data Protection Law.

1. <u>Definitions</u>

(a) "**Data Protection Laws**" means all data protection and privacy laws applicable to a party and its Processing of Personal Data under the Agreement, including, where applicable and without limitation, (i) EU Regulation 2016/674 ("**EU GDPR**"); (ii) its incorporation into the laws of England and Wales, Scotland and Northern Ireland by virtue of Section 3 of the UK European Union (Withdrawal) Act 2018 ("**UK GDPR**"); (iii) the Swiss Federal Act on Data Protection ("**FADP**"); (iv) United States federal and/or state data protection or privacy statutes, including but not limited to the California Consumer Protection Act of 2018 ("**CCPA**") and the California Privacy Rights Act of 2020 ("**CPRA**"); in each case, as may be amended, superseded or replaced from time to time; and/or (iv) any other data protection and privacy laws applicable to a party and its Processing of Personal Data in connection with the Agreement.

(b) "**Model Clauses**" means (i) where the GDPR or Swiss FADP applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); or (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR with the UK International Data Protection Transfer (IDTA) Addendum (or the stand-alone version of the IDTA where applicable) that was effective on, 21 March 2022. ("**UK SCCs**").

(c) "**Client Data**" means any data of any type which is provided by Client to Upflex or accessed or collected by Upflex on behalf of Client in connection with providing the Services or otherwise performing Upflex's obligations under the Agreement, including without limitation information which Client inputs, or provides to Upflex for inputting, into the Services.

(d) "**Client Personal Data**" means the personal data of any type, as a subset of Client Data, that could identify an individual, whether alone or when combined with any other data, as defined by the applicable Data Protection Laws.

(e) "**Security Best Practices**" means security procedures that are at the highest of the following: (i) privacy & IT security best practices of any standards agreed upon by the parties (e.g., ISO, SANS); (ii) the privacy and security requirements mandated by Data Protection Laws; and (iii) the security requirements, obligations, specifications, and event reporting procedures set forth in this Exhibit.

(f) "**Security Incident**" means, any (i) loss or misuse (by any means) of Client Data; (ii) Client Personal Data Breach; and/or (iii) other act or omission that compromises or may compromise the security, confidentiality, or integrity of Client Data, or any system of, or system used by, Client or its employees, contractors, shareholders, customers, clients and/or suppliers.

(g) "**Security Policies**" means statements and guidelines for securing Client Data pertaining to Security Best Practices and mandating compliance with applicable laws and regulations.

(h) "**Security Procedures**" means statements of the step-by-step actions taken to achieve and maintain compliance with Security Best Practices.

(i) "**Security Technical Controls**" means any specific hardware, software, or administrative mechanisms necessary to enforce Security Best Practices in accordance with the terms of this Agreement as methods for addressing security risks to information technology systems and relevant physical locations or implementing related policies. Security Technical Controls specify technologies, methodologies, implementation procedures, and other detailed factors or other processes to be used to implement Security Policy elements relevant to specific groups, individuals, or technologies.

(j) "**Services**" means those services, including without limitation Processing, that Upflex performs for or on behalf of Client pursuant to the Agreement.

The terms "**Data Controller**", "**Data Processor**", "**Personal Data Breach**", "**Personal Data**" and "**Processing**" have the meaning given to them in the applicable Data Protection Laws. The term "Data Controller" shall also include a "business" as defined in the CCPA and the CPRA or analogous terms in the applicable Data Protection Laws, and the term "Data Processor" shall also include a "service provider" as defined in the CCPA and CPRA or analogous terms in the applicable Data Protection Laws.

2. <u>Privacy</u>

(a) <u>Role of the Parties</u>. As between Upflex and Client, Client is the Data Controller of Client Personal Data, and Upflex shall Process Client Personal Data only as a Data Processor acting on behalf of Client and, with respect to the CCPA/CPRA, as a "service provider" as defined therein.

(b) <u>General Obligations</u>. Upflex agrees, warrants, represents, and undertakes to Client that it shall:

(i) Process the Client Personal Data only in accordance with applicable Data Protection Laws, including, without limitation, the obligations under Articles 32 to 36 of the EU GDPR (considering the nature of Processing), and applicable compliance standards, including, without limitation PCI DSS Standards;

(ii) Process the Client Personal Data only in accordance with Section 2(c) of this Exhibit (Details of Processing) and only on documented instructions from Client, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by applicable Data Protection Laws to which the Upflex is subject; in such a case, the Upflex shall inform Client of that legal requirement before Processing, unless such laws prohibit such information on important grounds of public interest;

(iii) Ensure that persons authorized to Process the Client Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iv) Assist Client in helping to ensure compliance with all applicable Data Protection Laws;

(v) Considering the nature of the Processing, assist Client by implementing appropriate technical and organizational measures, including, at the very least, such measures contained in Section 3 (Security) of this Exhibit and assist Client in ensuring compliance with its obligation to respond to data subject's rights requests laid down in Data Protection Laws; and

(vi) Make available to Client all information necessary to demonstrate compliance with all applicable Data Protection Laws including, without limitation, the obligations laid down in Article 28 of the GDPR, and allow for and contribute to audits, including inspections, conducted by Client or another auditor that is agreed upon by both parties.

(c) <u>Details of Processing</u>.

(i) Subject matter: The subject matter of the Processing under this Exhibit is Client Personal Data.

(ii) Frequency and duration: The frequency and duration of the Processing under this Exhibit is the term of the Agreement.

(iii) Nature and purpose of Processing: Upflex shall Process Client Personal Data only to provide the Services.

(iv) Categories of data subjects: Former, present and/or prospective employees, contractors, shareholders, customers, clients and/or suppliers.

(d) Subprocessing. Client agrees that to provide the Services, Upflex may engage subprocessors to Process Client Personal Data. Client specifically authorizes the engagement of those subprocessors listed at: at https://upflex.com/legal/subprocessor-list/ ("**Subprocessor List**"). Where Upflex engages any subprocessors pursuant to this Section:

(i) Upflex will restrict the subprocessors' access to Client Personal Data only to what is necessary to assist Upflex in providing or maintaining the Services and will prohibit the subprocessor from accessing Client Personal Data for any other purpose. Upflex will enter into a written agreement with the subprocessor imposing data protection obligations no less protective of Client Personal Data as this Exhibit to the extent applicable to the nature of the services provided by such subprocessor. Upflex will remain responsible and fully liable for the compliance of any subprocessors with the obligations of this Exhibit and for any acts or omissions of the subprocessor that cause Upflex to breach any of its obligations under this Exhibit.

(ii) Upflex will provide thirty (30) days' prior notice via the Subprocessor List if it intends to make any changes to its subprocessors. Client may object in writing to Upflex's appointment of a new subprocessor during this 30-day notice period, provided that such objection is based on reasonable grounds relating to data protection. In such an event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties cannot agree to a mutually acceptable resolution within ten (10) days, Client shall have the right to immediately terminate the Agreement without any further liability or fees.

(e) Selling and Sharing Prohibited. Upflex acknowledges and confirms that it does not receive any Client Personal Data as consideration for any Services or other items that Upflex provides to Client. Upflex shall not have, derive, or exercise any rights or benefits regarding Client Personal Data. Upflex must not sell or share any Client Personal Data as the terms "selling" and "sharing" are defined in the CCPA and CPRA. Upflex must not collect, share, or use any Client Personal Data except as necessary to perform the Services for Client. Upflex represents and warrants that it understands the rules, requirements, and definitions of the CCPA and CPRA and agrees to refrain from taking any action that would cause any transfers of Client Personal Data to or from Upflex to qualify as "selling personal information" or "sharing personal information" under the CCPA and CPRA.

(f) Return or Deletion of Client Data. Upon termination or expiration of the Agreement, or earlier request by Client, Upflex shall promptly delete (or return, if requested by Client) all Client Data in its possession or control (including, without limitation, all copies and regardless of its format), confirming in writing to Client once deleted. This requirement shall not apply to the extent Upflex is required by mandatory applicable law to retain Client Data where Upflex shall immediately inform Client of such requirement before retention. To the extent Client Data must be retained by Upflex for mandatory applicable legal purposes, such Client Data shall be considered and remain the Confidential Information of Client and the confidentiality obligations under the Agreement shall continue indefinitely.

(g) Extra-territorial Data Transfers. To the extent that Upflex Processes any Client Personal Data that is protected by Data Protection Laws applicable to the European Union, the United Kingdom and/or Switzerland, and such Client Personal Data is being transferred to a country that does not provide an adequate level of protection under applicable Data Protection Laws, the parties agree that Upflex shall provide an adequate protection and/or appropriate safeguards for such Client Personal Data by complying with the following transfer mechanisms:

(i) *Model Clauses*. Upflex agrees to abide by and Process the Client Personal Data in compliance with the Model Clauses, which are immediately incorporated by reference and form an integral part of this Exhibit. For the purposes of the Model Clauses, the parties agree that:

(a) With regards to transfers of Client Personal Data protected by the EU GDPR or Swiss FADP, the EU SCCs shall apply as follows:

(i) Module Two will apply (as applicable);

(ii) in Clause 7, the optional docking clause will not apply;

(iii) in Clause 9, Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in Section 2(d) of this Exhibit;
(iv) in Clause 11, the optional language will not apply;
(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the laws of the Republic of Ireland;
(vi) in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland;
(vii) in Annex I, Part A of the EU SCCs, Upflex is a "data importer" and "processor." Client (or, if relevant, a subsidiary of Client) is the "data exporter" and "controller."
(viii) in Annex I, Part B of the EU SCCs, the relevant information is specified in Section 2(c) and 2(f) of this Exhibit (Details of Processing and Return or Deletion of Client Personal Data);
(ix) For transfers to subprocessors, the subject matter, nature, and duration of the processing is set forth at Section 2(d) of this Exhibit (Subprocessing);
(x) in Annex I, Part C of the EU SCCs: The Irish Data Protection Commission will be the competent supervisory authority; and
(xi) Section 3 (Security) of this Exhibit serves as Annex II of the EU SCCs.

(b) With regards to transfers of Client Personal Data protected by the UK GDPR, the UK SCCs shall apply as follows:
(i) The EU SCC Module Two will apply (as applicable);
(ii) Sections 2g(i)(a)(ii)-(iv) of this Exhibit shall apply;
(iii) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR;
(iv) references to "EU", "Union" and "Member State law" are all replaced with "UK"; Clause 13(a) and Part C of Annex II of the EU SCCs are not used; references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Information Commissioner and the courts of England and Wales;
(v) Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the EU SCCs is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts"; and
(vi) To extent that and for so long as the EU SCCs as implemented in accordance with this section cannot be used to lawfully transfer Client Personal Data in compliance with the UK GDPR, the UK SCCs shall be incorporated by reference and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant Annexes of the UK SCCs shall be populated using the information contained in this Exhibit;
(vii) For purposes of Table 2 in the IDTA and IDTA Addendum, Personal data received from the Importer will be combined with personal data collected by the Exporter, but the Exporter is an independent Controller, so Module 4 does not apply.

(c) It is not the intention of either Party to contradict or restrict any of the provisions set forth in the Model Clauses and, accordingly, if and to the extent the Model Clauses conflict with any provision of the Agreement (including this Exhibit) the Model Clauses shall prevail to the extent of such conflict.

The Parties further agree that Upflex shall, upon Client's request, (i) assist Client in assessing, on a case-by-case basis, whether the country to which the Client Personal Data is being transferred provides an adequate level of protection; and (ii) where the applicable transfer mechanism does not in itself offer an

adequate level of protection, what contractual, technical and/or organizational supplementary measures have been adopted.

3. Security

Upflex represents, warrants, and undertakes that it has established and for so long as Upflex Processes Client Data it will always enforce, an ongoing program of Security Policies, Security Procedures, and Security Technical Controls, which reasonably ensures delivery of Security Best Practices and which includes, without limitation, the following:

(a) Information Security:
- (i) a privacy and security incident management program;
- (ii) a privacy and security awareness program;
- (iii) business continuity and disaster recovery plans, including regular testing; and
- (iv) procedures to conduct periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for timely and appropriate remediation.

(b) Physical Access:
- (i) physical protection mechanisms for all information assets and information technology to ensure such assets and technology are stored and appropriately protected;
- (ii) appropriate facility and room entry controls to limit physical access to systems that store or Process Client Data;
- (iii) processes to ensure access to facilities and rooms are monitored and is restricted on a "need to know" basis; and
- (iv) controls to physically secure all Client Data and to securely destroy such information when it is no longer needed in accordance with this Exhibit and the Agreement.

(c) Logical Access:
- (i) appropriate mechanisms for user authentication and authorization in accordance with a "least privilege" policy;
- (ii) controls and auditable logs to enforce and maintain rigorous access restrictions for employees, and subcontractors, including encryption of data transmission and encrypted data during remote access sessions;
- (iii) timely and accurate administration of user account and authentication management;
- (iv) processes to ensure assignment of unique IDs to each person with computer access;
- (v) processes to ensure Upflex-supplied defaults for passwords and security parameters are appropriately managed (e.g., changed periodically etc.);
- (vi) mechanisms to track and log all access to Client Data by unique ID;
- (vii) mechanisms to encrypt or hash all passwords or otherwise ensure all passwords are not stored unsecured in clear text; and
- (viii) processes to immediately revoke accesses of inactive accounts or terminated/transferred users.

(d) Security Architecture and Design:
- (i) a security architecture that reasonably ensures delivery of Security Best Practices;
- (ii) documented and enforced technology configuration standards;
- (iii) encryption of the Client Data in transit and at rest;
- (iv) regular testing of security systems and Security Best Practices;
- (v) a system of effective firewall(s) and intrusion detection technologies necessary to protect Client Data; and
- (vi) database and application layer design processes that ensure web applications are designed to protect the information data that is Processed through such systems.

(e) System and Network Management:

(i) mechanisms to keep security patches current;
(ii) monitor, analyze, and respond to security alerts;
(iii) appropriate network security design elements that provide for segregation of data from other third-party data;
(iv) use and regularly update anti-virus software; and
(v) the integrity, resilience and availability of any software or services utilized to Process the Client Data.

Failure by Upflex to comply with Security Best Practices or its obligations hereunder shall constitute a breach of the Agreement.

Security Audit. Client (or its designated representatives) may, on an annual basis or more frequently as reasonably requested by Client, at Client's expense, conduct an audit to verify that Upflex is operating in accordance with this Exhibit. Such audit(s) may include a review of all aspects of Upflex's performance, including, but not limited to, Upflex's general controls and security practices and procedures. Upflex will cooperate with Client in conducting any such audit, and will allow Client reasonable access, during normal business hours and upon reasonable notice, to all pertinent records, documentation, computer systems, data, personnel, and areas used to Process the Client Data areas as Client reasonably requests to complete such audit. Client will take reasonable steps to prevent the audit from materially impacting Upflex's operations. Upflex shall correct any deviations from Security Best Practices that are identified in any security audit as soon as practicable, but in no event more than five days after receiving notice from Client outlining any deviations (provided, however, that if five days is not a practicable cure period, then Upflex may instead present a remediation plan to Client within such five day period that sets forth an achievable and reasonable timeframe, and Upflex must thereafter diligently proceed to correct any deviations in accordance with such plan).

Security Incidents. Upflex shall immediately notify (within 24 hours) Client of any Security Incidents and provide Client with: a detailed description of the Security Incident; the type of data that was the subject of the Security Incident; the identity of each affected person, and the steps Upflex takes to mitigate and remediate such Security Incident, in each case as soon as such information can be collected or otherwise becomes available. Upflex shall use its best efforts to immediately mitigate and remedy any Security Incident and prevent any further Security Incident(s) at its sole expense. Subject to Upflex's applicable legal obligations, Upflex agrees that Client shall have the sole right to determine (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Client's discretion, (ii) the contents of such notice, and (iii) whether any type of remediation may be offered to affected persons, as well as the nature and extent of any such remediation. In the event of a Security Incident involving Client Data in Upflex's possession or otherwise caused by or related to Upflex's acts or omissions, and without limiting Client's other rights and remedies, Upflex will pay all costs and expenses of (i) any disclosures and notification required by applicable law or as otherwise determined as appropriate in Client's reasonable discretion, (ii) monitoring and reporting on the impacted individuals' or entities' credit records if determined in Client's reasonable discretion as reasonable to protect such individuals, and (iii) all other costs incurred by Client in responding to, remediating and mitigating damages caused by such Security Incident.