DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is incorporated by reference into the Master Software as a Service (SaaS) Agreement ("**SaaS Agreement**") entered by and between the Customer and Intenseye to reflect the Parties' agreement with regard to the Processing of Personal Data by Intenseye on behalf of the Customer.

In this DPA, the Customer is hereinafter referred to as "**Data Controller**"; and Intenseye is hereinafter referred to as "**Data Processor**".

Capitalized terms not defined herein shall have the meanings assigned to such terms in the SaaS Agreement.

By signing the SaaS Agreement, the Customer accepts this DPA.

1. DEFINITIONS AND INTERPRETATION

"Applicable Law" means all applicable and binding privacy and data protection laws and regulations, including such laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Canada and the United States of America, as applicable to the Processing of Personal Data under the SaaS Agreement including (without limitation) the GDPR, the UK GDPR, and the US State Privacy Laws, as applicable to the Processing of Personal Data hereunder and in effect at the time of Intenseye's performance hereunder.

"CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. seq. (as amended).

"Data Breach" any accidental or unlawful destruction, loss, alteration, compromise, disclosure of, or access to Personal Data, stored, transmitted or otherwise processed in the context of the SaaS Agreement attributable to Intenseye.

"Data Controller" is the party that determines the purposes and means of the Processing of Personal Data, and for purposes of this DPA, means Customer.

"Data Processor" is the party that Processes Personal Data on behalf of the Data Controller, and for purposes of this DPA, means Intenseye.

"Data Subject" is the identified or identifiable natural person that the Personal Data is related to.

"GDPR" means the General Data Protection Regulation (EU) 2016/679.

"Personal Data" means any Customer Data that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person, which is Processed by Intenseye on behalf of the Customer, under this DPA and the SaaS Agreement between the Customer and Intenseye.

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

"Sensitive Data" means Personal Data that is protected under Applicable Law and requires unique treatment, such as "special categories of data", "sensitive data" or other materially similar terms under Applicable Law, which may include any of the following depending on the Applicable Law: (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) financial and credit information including credit or debit card number; (c) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (d) genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, (e) data relating to criminal convictions and offenses; and/or (f) account passwords in unhashed form.

"Services" means the services Intenseye provides under the SaaS Agreement.

"Standard Contractual Clauses" means Annex to the Commission Implementing Decision (EU) 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.

"Sub-processor" means any third party that is engaged by Intenseye to Processes Personal Data under the instruction or supervision of Intenseye.

"UK GDPR" means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

"US State Privacy Laws" means all applicable comprehensive state privacy laws that govern the Processing of Personal Data in effect in the United States of America, which may include, without limitation, the CCPA, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

2. DETAILS OF DATA PROCESSING

2.1. Roles of the Parties. The Parties acknowledge and agree that regarding the Processing of Personal Data, the Customer is the Data Controller and Intenseye is the Data Processor.

2.2. Data Controller's Processing of Personal Data. Data Controller, in its use of the Services, and Data Controller's instructions to Data Processor, shall comply with Applicable Law. Data Controller shall establish and have all required legal bases in order to collect, Process and transfer to Data Processor the Personal Data, and to authorise the Processing and (if necessary) transfer by Data Processor, and for Data Processor's Processing activities under the SaaS Agreement. Data Controller accepts and declares that none of the Personal Data it transfers to Data Processor is subject to any legal dispute and it possesses all legal rights stipulated under the Applicable Law and any other contract or document that may be binding for Data Controller in order to Process and transfer such Personal Data as contemplated hereunder.

2.3. Data Processor's Processing of Personal Data. Data Processor, when Processing on the Data Controller's behalf under the SaaS Agreement, shall Process Personal Data for the following purposes:

(i) Processing in accordance with the SaaS Agreement and this DPA;
(ii) Processing for Data Controller as part of its provision of the Services;
(iii) Processing to comply with the Data Controller's reasonable and documented instructions, where such instructions are consistent with the terms of the SaaS Agreement regarding the manner in which the Processing shall be performed;
(iv) Processing as required under the applicable law, and/or as required by a court of competent jurisdiction or other competent governmental authority, provided that Data Processor shall inform Data Controller of the legal requirement before Processing, unless such law or order prohibit such disclosure on important grounds of public interest.

2.4. Purpose Limitation. Data Processor will Process Personal Data in order to provide the Services in accordance with the SaaS Agreement. **Schedule 1** ***(Details and Description of Processing)*** of this DPA further specifies the nature and purpose of the Processing, the Processing activities, the duration of the Processing, the types of Personal Data and categories of Data Subjects.

2.5. Sensitive and Biometric Data. The Parties agree that Services are not intended for the Processing of Sensitive Data and/or biometric data. Data Controller shall not provide or otherwise make available any Sensitive Data and/or

biometric data to Data Processor, and Data Processor shall not have any liability in connection with any Sensitive Data and/or biometric data provided by Data Controller in violation of this Section.

2.6. California Specific Terms. To the extent that Data Processor's Processing of Personal Data is subject to the CCPA, this section shall also apply. Data Controller discloses or otherwise makes available Personal Data to Data Processor for the limited and specific purpose of Data Processor providing the Services to Data Controller in accordance with the SaaS Agreement and this DPA. Data Processor shall: (i) comply with its applicable obligations under the CCPA; (ii) provide the same level of protection as required under the CCPA; (iii) notify Data Controller if it can no longer meet its obligations under the CCPA; (iv) not sell or share (as such terms are defined in the CCPA) any Personal Data Processed hereunder nor take any action that would cause any Transfer of Personal Data to or from Data Processor under the SaaS Agreement or this DPA to qualify as "selling" or "sharing" such Personal Data under the CCPA; (v) not retain, use, or disclose Personal Data for any purpose (including any commercial purpose) other than to provide the Services under the SaaS Agreement or as otherwise permitted under the CCPA; (vi) not retain, use, or disclose Personal Data outside of the direct business relationship between Data Controller and Data Processor; and (vii) unless otherwise permitted by the CCPA, not combine Personal Data with personal information that Data Processor (a) receives from, or on behalf of, another person, or (b) collects from its own, independent consumer interaction. Data Controller may: (1) take reasonable and appropriate steps agreed upon by the Parties to help ensure that Data Processor Processes Personal Data in a manner consistent with Data Controller's CCPA obligations; and (2) upon notice, take reasonable and appropriate steps agreed upon by the Parties to stop and remediate unauthorized Processing of Personal Data by Data Processor.

3. OBLIGATIONS OF DATA PROCESSOR

3.1. Data Processor shall:

a. not Process any Personal Data other than in accordance with the Data Controller's instructions (including the instructions as set out in **Schedule 1** ***(Details and Description of Processing)***, unless otherwise required under Applicable Law and SaaS Agreement signed between the Parties;

b. keep all Personal Data strictly confidential and ensure, prior to the disclosure of Personal Data to its employees, subcontractors or employees of subcontractors, that these persons are bound by confidentiality obligations;

c. only store the Personal Data for as long as the Data Controller requires and correct, anonymize, block or delete the relevant Personal Data at the Data Controller's instructions (in such cases, Data Processor shall not be liable for being unable to perform the Services in full compliance with the SaaS Agreement and its annexes directly due to Data Controller's referred instruction);

d. ensure that Data Processor's employees that Process or access Personal Data have a need to do so in order to carry out their duties in connection with the SaaS Agreement;

e. ensure that any person who is authorised by Data Processor to Process Personal Data (including its staff, agents, and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty);

f. taking into account the nature of the Processing, assist the Data Controller by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to requests for exercising the data subject's rights laid down the Applicable Law; and

g. comply with all relevant obligations applicable to Data Processors under the Applicable Law.

4. TECHNICAL AND ORGANIZATIONAL MEASURES

4.1. Data Processor shall adopt and maintain technical and organizational measures designed to protect Personal Data and prevent any unlawful Processing of or access to Personal Data. Such technical and organizational measures may at least include measures as set out in **Schedule 2** ***(Technical and Organizational Measures)*** depending on the nature of the Personal Data transferred and the Processing conducted by the Data Processor.

4.2. Data Processor shall ensure that the technical and organizational measures as set out in **Schedule 2** ***(Technical and Organizational Measures)*** are appropriate or otherwise consistent with industry standards, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for rights and freedoms of persons, that, where appropriate, may include, pseudonymization, encryption, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services, etc.

5. NOTIFICATION OF DATA BREACH

5.1. Upon becoming aware of a Data Breach, Data Processor shall:

(i) notify Data Controller without undue delay, and where feasible, in any event no later than 72 hours from becoming aware of the Data Breach;

(ii) provide timely information relating to the Data Breach as it becomes known or as is reasonably requested by Data Controller; and

(iii) promptly take reasonable steps to investigate any Data Breach. Data Processor's notification of or response to a Data Breach under this DPA shall not be construed as an acknowledgment by Data Processor of any fault or liability with respect to the Data Breach.

5.2. The notification will include sufficient details including the time of the event, the nature and scale of such event, the nature and scope of Personal Data records concerned, measures taken or to be taken to mitigate the consequences of the Data Breach, etc.

5.3. Data Processor shall without delay take all reasonable measures to reduce and recover the negative impact of a Data Breach as it relates to Data Processor's impacted systems.

6. SUB-PROCESSORS

6.1. Data Processor may respectively engage Sub-processors in connection with the provision of the Services and has Data Controller's general authorization for the engagement of Sub-processor(s) from an agreed list.

6.2. Data Processor shall maintain and regularly update a list of its Sub-processors ("Sub-processor List"). Data Processor's current list of Sub-processors used to process Personal Data can be viewed on https://www.intenseye.com/privacy-policy . The Sub-processor List includes the identities of the Sub-processors and their entity's country. Data Controller is deemed to authorize Data Processor's Sub-processors upon first use of the Services. Data Controller is encouraged to consult the Sub-processor List periodically to stay informed of current Sub-processors. To receive notifications of new Sub-processors, the Data Controller must email privacy@intenseye.com with the subject line "Subscribe to New Subprocessors." Once subscribed, Data Processor will notify Data Controller of any new Subprocessor before allowing such Sub-processor to Process Data Controller Personal Data. Data Processor will provide notice of its intent to engage a new Sub-processor by updating the Sub-processor List or via email (as applicable). Data Controller will have ten (10) days from the date notice is provided by Data Processor to submit a legitimate, good-faith objection to the new Subprocessor, in which case, it must provide reasonable grounds for the objection. In the event of such an objection, the Data Processor and Data Controller will collaborate in good faith to address the grounds for the objection.

6.3. Notwithstanding Section 6.2, Data Processor reserves the right to replace a Sub-processor at any time if immediate action is necessary to provide the Services. In such cases, the Data Processor shall notify Data Controller of the

replacement as soon as reasonably possible in accordance with the procedure in Section 6.2 above, and Data Controller may exercise its right to object to the replacement Subprocessor in accordance with the procedure in Section 6.2 above.

6.4. Data Processor will be liable for the actions and omissions of its Sub-processors undertaken in connection with Data Processor's performance under this DPA to the same extent Data Processor would be liable if performing the Services directly.

7. INTERNATIONAL TRANSFERS OF PERSONAL DATA

7.1. Each party shall comply with the provisions of the SaaS Agreement, this DPA, and Applicable Law with regards to the international transfer of Personal Data..

7.2. If Personal Data originating in the European Economic Area, Switzerland, and/or the United Kingdom is transferred by Data Controller to Data Processor in a country that has not been found to provide an adequate level of protection under Applicable Law, the parties agree that the transfer shall be governed by Module Two's obligations in the Standard Contractual Clauses, as supplemented by Schedule 3 attached hereto, the terms of which are incorporated herein by reference. Each party's signature to this Agreement shall be considered a signature to the Standard Contractual Clauses to the extent that the Standard Contractual Clauses apply hereunder.

8. DATA SUBJECT RIGHTS

8.1. Data Processor shall provide all reasonable assistance to ensure that Data Controller is able to fulfill its legal obligations when a Data Subject exercises his or her rights under the Applicable Law.

8.2. If Data Processor receives a request from a Data Subject that expressly references, or clearly relates to, Data Controller, Data Processor shall promptly inform Data Controller. Data Processor may direct the Data Subject to contact Data Controller, but Data Processor shall not otherwise respond to the request without the consent of Data Controller.

9. AUDIT RIGHTS

9.1. Data Processor shall make available to Data Controller on request all information reasonably required to demonstrate compliance with the obligations regarding the protection of Personal Data under this DPA.

9.2. Subject to this Section, no more than once per year, upon Data Controller's request, Data Processor shall allow for and contribute to audits, including inspections, by Data Controller or an auditor mandated by Data Controller in relation to the Processing of the Personal Data by Data Processor under the SaaS Agreement and the DPA. Any audit must be: (i) conducted during Data Processor's regular business hours; (ii) with reasonable advance notice to Data Processor; (iii) carried out in a manner that prevents unnecessary disruption to Data Processor's operations; and (iv) subject to reasonable confidentiality procedures. In addition, any access to Data Processor's facilities, networks, and/or systems will be carried out by Data Processor acting in reasonable cooperation with Data Controller or its auditor). The expenses of an audit shall be borne by Data Controller.

9.3. Notwithstanding the above, information and audit rights of Data Controller pursuant to this Section only arise to the extent that compliance cannot be adequately demonstrated in accordance with this clause or the SaaS Agreement does not otherwise give them information and audit rights to ensure that Data Processor meets the relevant requirements of Applicable Law. In addition, Data Processor shall not be liable to disclose any information that (i) it is obligated to keep confidential under Applicable Law, (ii) is confidential information, intellectual property and/or trade secrets of a third party, and (iii) is confidential information, intellectual property and/or trade secrets of Data Processor and is not directly related to the Services provided to Data Controller by Data Processor under the SaaS Agreement.

10. DATA PROTECTION IMPACT ASSESSMENT

Data Processor shall provide reasonable assistance to Data Controller with any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, as required under Applicable Law, in each case solely in relation to Processing of Personal Data by and taking into account the nature of the Processing and information available to Data Processor.

11. TERM AND TERMINATION

This DPA shall remain in force until the termination of the SaaS Agreement. Parties agree that following termination of this DPA, Data Processor shall, at the choice and by means and costs of the Data Controller, delete all Personal Data, or return all Personal Data and the copies thereof to Data Controller or a third party designated by the Data Controller, except where storage of copies is legally required.

12. GENERAL

All other terms and conditions of the SaaS Agreement remain in full force and effect. In the event of any conflict between certain provisions of this DPA and the provisions of the SaaS Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the SaaS Agreement solely with respect to the Processing of Personal Data.

Schedule 1 to DPA
DETAILS AND DESCRIPTION OF PROCESSING

Categories of Data Subjects whose Personal Data is Processed or transferred:
The categories of Data Subjects whose Personal Data are Processed or transferred are determined and controlled by Data Controller and may include the following:

1. *Employees including temporary workers, contractors, and job applicants,*
2. *Consumers,*
3. *Website and digital asset users,*
4. *Employees of suppliers, partners, subcontractors and other business contacts, group companies and affiliates, especially in cases where such employees use the Facilities which the Service Software is integrated to.*

Categories of Personal Data:
The categories of Personal Data are determined and controlled by Data Controller and may include the following:

1. *Personal details - including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, mobile phone (opt-in), and email,*
2. *Account and Profile Information – display name, profile photo, job title, set preferences,*
3. *Service use – Log, device and cookie data obtained via the use of Service Software by Authorized Users,*
4. *Customer support – Information regarding a problem with a Service, Services provided and related information, including details of the Services supplied, and contracts,*
5. *Video footage – CCTV video footage and images to provide the Services,*
6. *Other – Any other Personal Data that may be provided or otherwise uploaded to the Services by Data Controller at its own discretion, including any incident reports and related data such as incident images.*

Sensitive data:
Data Controller is prohibited from providing Data Processor with Sensitive Data and/or biometric data, and Data Processor will not intentionally process Sensitive Data and/or biometric data.

The frequency of the transfer:
Personal Data will be transmitted when new accounts are created in the Service Software and when errors are reported. The Personal Data is transferred on a continuous basis. The Service Software works 24/7, analyzing real-time streaming. However, only unsafe acts and conditions are stored, while other Personal Data are disposed of immediately.

Nature of Processing:
The Personal Data Processed or transferred will be subject to the following Processing activities:

1. *Receiving Personal Data, including collection, accessing, retrieval, recording, and data entry*
2. *Holding Personal Data, including storage, organization and structuring*
3. *Using Personal Data, including analyzing, consultation, testing, and training the artificial intelligence utilized by Data Processor to provide Services to Data Controller*
4. *Updating Personal Data, including correcting, adaptation, alteration, alignment and combination*
5. *Taking steps to protect Personal Data, including restricting, encrypting, and security testing*
6. *Sharing Personal Data, including disclosure, dissemination, allowing access or otherwise making available Personal Data in accordance with the SaaS Agreement and the DPA.*
7. *Returning Personal Data to Data Controller or a third party upon Data Controller's request*
8. *Erasing Personal Data, including destruction and deletion*

Purpose(s) of the data transfer and further Processing
The purpose of Processing Personal Data is described in the SaaS Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
Personal Data such as general details are kept up to date as long as Data Controller continues to use Service Software. Retention period will be determined by Data Controller via the Service Software, provided that such period will not be less

than thirty (30) days. If necessary, such Personal Data may be retained for compliance with a legal obligation. If, for some reason there needs to be a user to be removed, it can be deleted manually via the Software Service or via Data Processor's support personnel. Upon expiration or termination of the SaaS Agreement, Data Processor will delete Personal Data as requested.

Subject-matter and duration of the processing for transfers to subprocessors

The subject-matter of processing of Personal Data is defined in the SaaS Agreement. The duration of Processing shall be for the term designated under this Schedule.

Schedule 2 to DPA
TECHNICAL AND ORGANIZATIONAL MEASURES

This Schedule 2 describes technical and organizational security measures taken by Data Processor for the purposes of data privacy and security. The technical and organizational measures will be implemented in accordance with industry standard practices and Data Processor's SOC 2 Type II certification.

1. Information Security Policies and Standards

1.1. Data Processor will implement security requirements that are designed to maintain the integrity, confidentiality, resilience and availability of Personal Data, which may include (but are not limited to) the following:

1.1.1. Measures designed to prevent unauthorized persons from gaining access to Personal Data processing systems (physical access control);

1.1.2. Measures designed to prevent Personal Data Processing systems being used without authorization (logical access control);

1.1.3. Measures designed to ensure that:

1.1.3.1 Data Processor personnel entitled to use a Personal Data processing system gain access only (i) through an internal and documented process, (ii) to such Personal Data that they are entitled to access in accordance with their access rights and the purposes of the Processing, and (iii) for the time necessary for Processing the Personal Data, and

1.1.3.2 in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control);

1.1.4. Measures designed to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage (data transfer and storage control);

1.1.5. Measures designed to ensure the establishment of an audit trail for access to key systems that Process Personal Data by Data Processor personnel to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing (entry control);

1.1.6. Measures designed to ensure that Personal Data are Processed solely in accordance with Data Controller's Instructions (control of instructions);

1.1.7. Measures designed to ensure that Personal Data are protected against accidental destruction or loss, and measures designed to support access to Personal Data and / or restoration of Personal Data in the event of a physical or technical incident impacting availability (availability control); and

1.1.8. Measures designed to ensure that Personal Data collected for different purposes can be Processed separately (separation control).

1.2. These measures will be kept up to date and revised whenever relevant changes are made to any information system that uses or houses Personal Data, or to how that system is organized.

1.3. These measures will be routinely reviewed to evaluate efficacy and areas for improvement and where relevant adopt and apply changes as part of a continuous improvement programme.

2. Physical Security

2.1. Data Processor will maintain commercially reasonable security systems at all Data Processor facilities that contain an information system that uses or houses Personal Data. Data Processor will reasonably and appropriately restrict physical access to such facilities.

2.2. Physical access control will be implemented for all data centers.

3. Organizational Security

3.1. Data Processor will ensure that it has implemented security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.

3.2. All Data Breaches will be managed in accordance with appropriate incident response procedures.

4. Network Security

Data Processor will implement measures designed to maintain network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection systems, access control lists and secure routing protocols.

5. Access Control

5.1. Only authorised staff will be permitted to grant, modify or revoke Data Processor personnel access to an information system that uses or houses Personal Data.

5.2. User administration procedures for Data Processor personnel will be adopted which define user roles and their privileges, how access is granted, changed and terminated; addresses appropriate segregation of duties; and defines the logging/monitoring requirements and mechanisms.
5.3. All employees of Data Processor will be assigned unique User-IDs.
5.4. Access rights will be implemented adhering to the “least privilege” approach.
5.5. Data Processor will implement commercially reasonable physical and electronic security measures designed to protect passwords.

6. Virus and Malware Controls

Data Processor will install and maintain industry standard (which will comprise the latest version or engine) anti-virus and malware protection software on key Data Processor systems that Process Personal Data. The anti-virus software will be updated regularly.

7. Personnel

7.1. Data Processor will implement a security awareness program to train Data Processor personnel about their security obligations. This program will include training about data classification obligations, physical security controls, security practices and Data Breach reporting.
7.2. Data Processor will have clearly defined roles and responsibilities for its employees. Screening is implemented before employment with terms and conditions of employment applied appropriately.
7.3. Data Processor personnel will strictly follow established security policies and procedures. Disciplinary process will be appropriately applied if employees breach Data Processor’s established security policies and procedures.

Schedule 3 to DPA
SUPPLEMENTAL TERMS FOR THE STANDARD CONTRACTUAL CLAUSES

This Schedule 3 forms part of the DPA and supplements the Standard Contractual Clauses.

The parties agree that the following terms shall supplement the Standard Contractual Clauses:

1. **Supplemental Terms.** The parties agree that: (i) a new Clause 1(e) is added the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses also apply mutatis mutandis to the Parties' processing of personal data that is subject to the Swiss Federal Act on Data Protection. Where applicable, references to EU Member State law or EU supervisory authorities shall be modified to include the appropriate reference under Swiss law as it relates to transfers of personal data that are subject to the Swiss Federal Act on Data Protection."; (ii) a new Clause 1(f) is added to the Standard Contractual Clauses which shall read: "To the extent applicable hereunder, these Clauses, as supplemented by Annex III, also apply mutatis mutandis to the Parties' processing of personal data that is subject to UK Data Protection Laws (as defined in Annex III)."; (iii) the optional text in Clause 7 is deleted; (iv) Option 1 in Clause 9 is struck and Option 2 is kept, and data importer must notify data exporter of any new subprocessors in accordance with Section 6 of the DPA; (v) the optional text in Clause 11 is deleted; and (vi) in Clauses 17 and 18, the governing law and the competent courts are those of Ireland (for EEA transfers), Switzerland (for Swiss transfers), or England and Wales (for UK transfers).

2. **Annex I.** Annex I to the Standard Contractual Clauses shall read as follows:

A. List of Parties

Data Exporter: Data Controller
Address: As set forth in the Notices section of the SaaS Agreement.
Contact person's name, position, and contact details: As set forth in the Notices section of the SaaS Agreement.
Activities relevant to the data transferred under these Clauses: The Services.
Role: Controller (Module Two); Processor (Module Three).

Data Importer: Data Processor.
Address: As set forth in the Notices section of the SaaS Agreement.
Contact person's name, position, and contact details: As set forth in the Notices section of the SaaS Agreement.
Activities relevant to the data transferred under these Clauses: The Services.
Role: Processor.

B. Description of the Transfer:

See Schedule 1 of the DPA.
C. Competent Supervisory Authority: The supervisory authority mandated by Clause 13. If no supervisory authority is mandated by Clause 13, then the Irish Data Protection Commission (DPC), and if this is not possible, then as otherwise agreed by the parties consistent with the conditions set forth in Clause 13.

D. Clarifying Terms: The parties agree that: (i) the certification of deletion required by Clause 8.5 and Clause 16(d) of the Clauses will be provided upon data exporter's written request; (ii) the measures data importer is required to take under Clause 8.6(c) of the Clauses will only cover data importer's impacted systems; (iii) the audit described in Clause 8.9 of the Clauses shall be carried out in accordance with Section 9 of the DPA; (iv) the termination right contemplated by Clause 14(f) and Clause 16(c) of the Clauses will be limited to the termination of the Clauses; (v) unless otherwise stated by data importer, data exporter will be responsible for communicating with data subjects pursuant to Clause 15.1(a) of the Clauses; and (vi) the information required under Clause 15.1(c) of the Clauses will be provided upon data exporter's written request.

3. **Annex II.** Annex II of the Standard Contractual Clauses shall read as follows:

Data importer shall implement and maintain technical and organizational measures designed to protect personal data in accordance with Schedule 2 of the DPA.

Pursuant to Clause 10(b), data importer will provide data exporter assistance with data subject requests in accordance with the DPA.

4. Annex III. A new Annex III shall be added to the Standard Contractual Clauses and shall read as follows:

The UK Information Commissioner's Office International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**UK Addendum**") is incorporated herein by reference.

Table 1: The start date in Table 1 is the effective date of the DPA. All other information required by Table 1 is set forth in Annex I, Section A of the Clauses.

Table 2: The UK Addendum forms part of the version of the Approved EU SCCs which this UK Addendum is appended to including the Appendix Information, effective as of the effective date of the DPA.

Table 3: The information required by Table 3 is set forth in Annex I and II to the Clauses.

Table 4: The parties agree that neither party may end the UK Addendum as set out in Section 19.