Data Processing Addendum

This Data Processing Addendum (this "DPA"), including the attached appendices, forms an integral part and is incorporated by reference into the Master Services Agreement Terms & Conditions available via https://www.operative.com/terms-of-service, as applicable to Operative's provision of the applicable software-as-a-service solutions (the "Services") as provided in the applicable Schedule and related SOWs (together, the "Agreement") between Customer (acting on its own behalf and only to the extent permitted under (and in full compliance with) Applicable Data Protection Laws and Regulations, in the name of and on behalf of its Affiliates), and Operative (acting on its own behalf and on behalf of its Affiliates), if and to the extent Operative Processes Personal Data in the course of providing Services to Customer.

Schedule 1, containing the Standard Contractual Clauses (the "SCCs") is incorporated by reference into the DPA. If Customer wishes to separately execute the Standard Contractual Clauses and its Appendices, please contact legal@operative.com with a request to do so.

Nothing herein shall be interpreted to cause Operative or any Personal Data to be subject to the provisions of any law or regulation that would not otherwise be applicable, or subject Operative or such Personal Data to any requirements hereunder not required by relevant Applicable Data Protect Laws and Regulations, as , information obtained from residents of a particular jurisdiction shall only be subject to any provisions herein required by or relating to Applicable Data Protection Laws and Regulations of such jurisdiction.

The terms used in this DPA shall have the meanings set forth in this DPA, unless Applicable Data Protection Laws and Regulations provides a more stringent definition, in which case such definition shall apply. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement and Applicable Data Protection Laws and Regulations. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties agree that the terms and conditions set out below shall be added as an addendum to the Agreement. Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by, and including, this DPA.

1. DEFINITIONS

Affiliate means any person, organization, or entity controlling, controlled by or under common control with a party.

Applicable Data Protection Laws and Regulations means personal data protection laws and regulations applicable to the Processing of Personal Data under the Agreement, including where applicable: (i) European Data Protection Laws, including the GDPR, (iii) the LGPD and (iv) the laws, statutes and regulations of the United States (federal and state), including but not limited to the CCPA; (v) PIPEDA and (vi) privacy laws of the Republic of India.

CCPA means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations, as amended by the California Privacy Rights Act.

Contractor has the meaning set forth in the CCPA, as and where the CCPA applies.

Controller means the entity which determines the purposes and means of the Processing of Personal Data and, for purposes of this DPA, shall mean Customer.

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

EEA means the European Economic Area.

European Data Protection Laws mean (i) the GDPR; (ii) the UK General Data Protection Regulation and (iii) the laws and regulations of the Swiss Confederation, including the Swiss FDPA.

GDPR means the General Data Protection Regulation (Regulation (EU) 2016/679), including as implemented under the UK Data Protection Regulation.

LGPD means the Brazilian General Data Protection Law (LGPD), Federal Law no. 13,709/2018.

Member State means any member state of the EEA.

Personal Data means information that identifies or is identifiable to a natural person or is otherwise subject to Applicable Data Protection Laws and Regulations.. By way of example, information relating to, describing, capable of being associated with, or that could reasonably be linked with an identified or identifiable California resident or household consisting of California residents protected by the CCPA, and considered Personal Information under the CCPA, shall be considered Personal Data for the purposes of this DPA.

Personal Data Breach means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Customer's Personal Data in breach of this DPA.

Personal Information has the meaning set forth in the CCPA, as and where the CCPA applies.

PIPEDA means the Personal Information Protection and Electronic Documents Act (S.C. 2000, C.5).

Process means an operation performed by such party upon Personal Data in connection with the performance of the Agreement, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor means the entity which Processes Personal Data on behalf of the Controller and, for purposes of this DPA, means Operative.

Sale has the meaning set forth in the CCPA, as and where the CCPA applies.

Service Provider has the meaning set forth in the CCPA, as and where the CCPA applies.

Services describes the services provided to Customer (and/or, as applicable, Customer's Affiliates) by Operative under the Agreement.

Sharing has the meaning set forth in the CCPA, as and where the CCPA applies.

Standard Contractual Clauses and SCCs means Module 2 (Controller to Processor) of the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, incorporated by reference into this DPA with the options set forth in Schedule 1, and as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. With respect to transfers of personal data subject to the Swiss FADP or the UK General Data Protection Regulations, Standard Contractual Clauses and SCCs also include the Swiss and UK addenda modifying the EU Standard Contractual Clauses set forth in Annexes 4 and 5 to Schedule 1.

Sub-processor means any Processor engaged by Operative in relation to the provision of the Services.

Swiss FADP means the Swiss Federal Act on Protection 1992, as amended.

UK General Data Protection Regulation means the UK General Data Protection Regulation (based on the General Data Protection Regulation (EU) 2016/679). May also be referred to as the UK GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 With regard to the Processing of the Personal Data under the Agreement, Operative is the Processor and Customer is the Controller.

3. PROCESSOR OBLIGATIONS

3.1 Operative understands the following requirements and shall:

3.1.1 make commercially reasonable efforts to ensure that any natural person or entity acting under its authority shall

only Process the Personal Data as required for the provision of the Services and on the documented instructions from Customer. For the avoidance of doubt, Operative shall not engage in the Sale of Personal Data. Notwithstanding the foregoing, Operative may Process the Personal Data as required to do so by any law applicable to it. In such cases, Operative shall inform Customer of that legal requirement, unless the applicable law prohibits such notification on important grounds of public interest. Operative shall then comply with all reasonable directions of Customer with respect to such Processing and shall limit the extent and nature of such Processing of Personal Data to that which is strictly required to comply with applicable law. If it cannot provide such compliance for whatever reasons, Operative agrees to inform Customer of its inability to comply, in which case Customer is entitled to suspend the transfer of the Personal Data;

3.1.2 not retain, use, or disclose any Personal Data provided by Customer except as necessary for the specific business purpose of performing the services for Customer pursuant to the Agreement or otherwise as permitted by Applicable Data Protection Laws and Regulations, including the CCPA. For the avoidance of doubt, Operative is a Service Provider for the purposes of the CCPA;

3.1.3 deal with and provide all reasonable assistance with all enquiries by Customer regarding Processing of Personal Data and, if required, make available to Customer all information necessary for Operative to demonstrate its compliance with the Applicable Data Protection Laws and Regulations as it relates to Operative in its capacity as a Processor;

3.1.4 notify Customer in the event that it believes that any instructions given by Customer regarding Processing infringe any applicable law;

3.1.5 to the extent permitted by law, notify Customer of any request for disclosure of the Personal Data from a third party (including a governmental entity) which Operative receives directly. If permitted by law, Operative shall comply with all reasonable directions of Customer with respect to such request for disclosure and shall limit the extent and nature of such disclosure to that which is strictly required;

3.1.6 notify Customer as soon as practicable of any actual or reasonably suspected Personal Data Breach;

3.1.7 notify Customer as soon as practicable in the event that it becomes aware that it (or any Sub-processor) is Processing, or has Processed Personal Data in contravention of terms of this DPA;

3.1.8 abide by the advice of any relevant supervisory authority with regard to Processing of the Personal Data;

3.1.9 provide reasonable assistance , at Customer's expense, with the conduct of any data protection impact assessments and necessary prior consultations with relevant supervisory authorities, and otherwise assist Customer in meeting its obligations under Applicable Data Protection Laws and Regulations, including under Articles 35 and 36 of the GDPR; and

3.1.10 provide reasonable assistance at Customer's expense, to Customer in connection with its record-keeping obligations under Applicable Data Protection Laws and Regulations, including Article 30 of the GDPR.

3.2 A description of the processing activities to be undertaken as part of the Agreement and this DPA is set out in Annex 1 to Schedule 1 attached hereto.

3.3 Operative shall, and shall ensure that all its relevant Affiliates, perform intercompany international transfers of Personal Data subject to applicable European Data Protection Laws.

4. RIGHTS OF DATA SUBJECTS

4.1 Operative shall

4.1.1 provide commercially reasonable and necessary assistance to Customer in complying with any request

received by Customer from any Data Subject to exercise their rights of access, to know, rectification, restriction of Processing, erasure or deletion ("right to be forgotten"), data portability, or not to be subject to an automated individual decision making. (Each such request hereafter is referred to as a "**Data Subject Request**".)

4.1.2 assist Customer by appropriate technical and organization measures, taking into account the nature of the Processing at issue (including any required analysis, such as under Chapter III of GDPR), insofar as possible for the fulfilment of Customer's obligations to respond to a Data Subject Request under Applicable Data Protection Laws and Regulations. To the extent legally permitted, notify Customer if it directly receives a Data Subject Request from any Data Subject and seek to obtain Customer's instructions prior to responding to any such Data Subject request and provide reasonable assistance to Customer for the fulfilment of Customer's obligation to respond to a Data Subject Request.

4.1.3 make commercially reasonable efforts to ensure that each of its Sub-processors that process Personal Data provide commercially reasonable and necessary assistance to fulfil Customer's obligations to respond to Data Subject Requests.

5. OPERATIVE PERSONNEL

5.1 Operative shall

5.1.1 make commercially reasonable efforts to ensure that its personnel engaged in the Processing of the Personal Data are informed of the confidential nature of the Personal Data and are subject to contractual or appropriate statutory obligations of confidentiality;

5.1.2 take all commercially reasonable steps to ensure the reliability of its personnel who have access to the Personal Data and train all personnel responsible for Processing Personal Data regarding the obligations set forth in this DPA and the Agreement; and

5.1.3 make commercially reasonable efforts to ensure that access to the Personal Data is limited to such authorized personnel who require access to it for the purpose of providing the Services.

6. OBLIGATIONS OF CUSTOMER

6.1 Customer shall

6.1.1 in its use of the Services, process Personal Data in accordance with the requirements of Applicable Data Protection Laws and Regulations, including any requirements to provide notice to Data Subjects of the use of Operative as Processor.

6.1.2 obtain any and all necessary consents with respect to the use of Operative as a Processor.

6.1.3 comply with Applicable Data Protection Laws and Regulations in its use of the Services, and its own collection and processing of Personal Data, including its instructions to Operative, taking sole responsibility for the accuracy, quality and legality of the Personal Data and the means by which Customer acquired the Personal Data.

7. SUB-PROCESSORS

7.1 Customer acknowledges and agrees that with respect to Processing under the Agreement and this DPA (a) Operative's Affiliates may be retained as Sub-processors; and (b) Operative and its Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services; (c) the third parties listed in Annex 3 to Schedule 1 hereof are providing services to Operative or its Affiliates as Sub-processors related to the provision of Services to Customer and Customer authorizes these engagements; and (d) Operative or its Affiliates have made commercially reasonable efforts to enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data with regard to Applicable Data Protection Laws and Regulations applicable to such Sub-processor and to the extent applicable to the nature of the Services provided by such Sub-processor. For the avoidance of doubt, Customer consents to the Sub-processing activities mentioned in this section for purposes of Clause 9 of the Standard Contractual Clauses.

7.2 If Operative intends to engage with Sub-processors other than the companies listed in Annex 3 to Schedule 1 to the extent required by Applicable Data Processing Laws and Regulations, Operative will notify Customer thereof in writing (email sufficient), and Customer shall have the opportunity to object to the engagement of the new Sub-processors within ten (10) days after being notified. The objection must be based on reasonable grounds (e.g. if the Customer proves that significant risks for the protection of its Personal Data exist at the Sub-processor), in which case Operative and Customer will make a bona fide, good faith effort to resolve the dispute. In the event that the Parties are unable to resolve the dispute, Operative may terminate Services, in whole or in part, in its sole discretion.

7.3 Operative shall be liable for the acts and omissions of its Sub-processors for failure to comply with Applicable Data Protection Laws and Regulations to the same extent Operative would be liable if performing the Services of each Sub-processor directly under the terms of this DPA.

8. THIRD PARTY BENEFICIARIES

8.1 The parties agree that Customer may make available a copy of this DPA to any Data Subject on his/her request.

8.2 Data Subjects whose Personal Data is subject to GDPR and Processed hereunder are entitled to directly enforce the applicable sections of this DPA against Operative (and shall be entitled to receive compensation from Operative in respect of such breach) in the event that both Customer and, where relevant, Customer's customer (from which the relevant Personal Data was received) have factually disappeared or ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of Customer by contract or by operation of law. The liability of Operative shall be limited to its own processing operations under the Agreement.

8.3 In respect of any claim by a Data Subject against Operative pursuant to Section 8.2, Operative agrees it will accept the decision of the Data Subject to (i) refer the dispute to mediation, by an independent person or, where applicable, by a supervisory authority; or (ii) refer the dispute to the courts in the Member State in which the relevant Customer from which the data originated is established.

8.4 Operative agrees that any choice made by a Data Subject pursuant to Section 8.2 above will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8.5 Except for the foregoing and Customer Affiliates with regard to Operative, no third party may enforce this DPA's terms against Customer or Operative.

9. SECURITY

9.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, Operative and each of its Affiliates shall in relation to Customer's Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as applicable, the measures referred to in Article 32(1) of the GDPR.

9.2 Operative maintains and follows incident management policies and procedures. Operative will notify Customer as soon as practicable (email sufficient) of any actual or reasonably suspected Personal Data Breach which directly affects Customer's Personal Data and provide necessary assistance necessary for Customer to comply with its obligations under Applicable Data Protection Laws and Regulations to notify the relevant supervisory authorities and affected Data Subjects of such Personal Data Breach.

10. RETURN AND DELETION OF DATA

10.1 Subject to thirty days' prior written notice by Customer to Operative, Operative shall delete or return all Customer Personal Data to Customer on termination of the Agreement. If Customer does not provide such a request, Operative will hold Personal Data in archive for support usage and test environments in accordance with Operative's practices.

11. AUDITS AND CERTIFICATIONS

11.1 Upon request and reasonable notice from Customer, for the purpose of demonstrating Operative's compliance with its obligations under Applicable Data Protection Laws and Customer may:

11.1.1 make requests from Operative to provide commercially reasonable information in volume and scope.

11.1.2 request Operative to provide to Customer an existing attestation or certificate by an independent professional expert, including an ISO 27001 certificate or the successor or equivalent thereto within 60 days following Operative's receipt of such a signed certificate.

11.1.3 request that Operative complete a questionnaire regarding its and/or its Affiliates data privacy and security practices.

11.2 The parties agree that certain relevant supervisory authorities may have the right to conduct an audit of Operative, which has the same scope and is subject to the same conditions as would apply to an audit of Customer under Applicable Data Protection Laws and Regulations.

12. DATA TRANSFER

12.1 Customer acknowledges and agrees that, in connection with the performance of the Services under the Agreement, Personal Data may be transferred out of the EEA, the United Kingdom and the Swiss Confederation, including to the United States. Accordingly, if Customer is established within the EEA, then the Parties shall, unless agreed otherwise, execute the Standard Contractual Clauses (EU), and follow the provisions set forth in Schedule 1 attached hereto.

13. CALIFORNIA CONSUMER PRIVACY ACT

13.1 To the extent Operative acts as a Service Provider or Contractor for purposes of the CCPA, the terms set forth in this section 13 shall apply.

13.1.1 Operative may not Sell or Share Personal Information it collects pursuant to the Agreement.

13.1.2 Operative may process Personal Information for the provision of the Services as reasonably necessary for the following business purposes:

a. helping to ensure security and integrity to the extent the use of Customer's Personal Information is reasonably necessary and proportionate for these purposes.

b. debugging to identify and repair errors that impair existing intended functionality.

c. performing services on behalf of Customer, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of Customer.

d. providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a Service Provider or Contractor shall not combine the Personal Information of opted-out consumers that the Service Provider or Contractor receives from, or on behalf of, Customer with Personal Information that the Service Provider or Contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

e. undertaking internal research for technological development and demonstration.

Customer is disclosing the Personal Information to Operative only for the limited and specified business purposes set forth above and for the performance of the Services referenced in the Agreement.

13.1.3 Operative may not retain, use, or disclose the Personal Information collected pursuant to the Agreement for any purposes other than those set forth in section 13.1.2 above, as specified in the Agreement, or as otherwise permitted by the CCPA.

13.1.4 Operative may not retain, use, or disclose the Personal Information collected pursuant to the Agreement for any commercial purpose other than the business purposes specified in the Agreement, unless expressly permitted by the CCPA.

13.1.5 Operative may not retain, use, or disclose Personal Information collected pursuant to the Agreement outside the direct business relationship between Operative and Customer, unless expressly permitted by the CCPA.

13.1.6 Operative shall comply with all applicable sections of the CCPA, including providing the same level of privacy protection to the Personal Information collected pursuant to the Agreement as required of businesses by the CCPA.

13.1.7 Customer shall have the right to take reasonable and appropriate steps to ensure that Operative uses the Personal Information collected pursuant to the Agreement, in a manner consistent with the Customer's obligations under the CCPA.

13.1.8 In the event Operative determines that it can no longer meet its obligations under the CCPA, Operative shall

notify Customer.

13.1.9 Customer shall have the right, upon written notice to Operative, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information by Operative.

13.1.10 Operative shall enable Customer to comply with consumer requests made pursuant to the CCPA.

13.1.11 Operative may subcontract with any other person for the provision of the services under this Agreement provided that Operative notifies Customer of the engagement and enters into a contract with such subcontractor(s) that complies with the CCPA including the requirements set forth in this Section 13.

14. LIMITATION OF LIABILITY

14.1 Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, to the greatest extent permitted under law is subject to the limitations of liability provisions set forth in the Agreement.

*****

SCHEDULE 1

CROSS BORDER TRANSFERS

For the purposes of the Standard Contractual Clauses, including this Schedule 1 and Annexes attached hereto, Customer is the Data Exporter and Operative is the Data Importer. The relevant provisions contained in the Standard Contractual Clauses are incorporated by reference and form an integral part of the DPA. In the event of any conflict between the Standard Contractual Clauses and the DPA, the provisions of the Standard Contractual Clauses shall prevail. Capitalized terms not defined shall have the meaning ascribed in the DPA. The parties agree as follows:

1. Module 2 (Controller to Processor) of the Standard Contractual Clauses shall apply.

2. In Clause 7 of the SCCs (EU) the docking clause shall not apply.

3. With respect to the certificate of deletion as described in Clause 8.5 and 16(d) of the SCCs , the same will be provided in accordance Section 10 of the DPA.

4. Audit rights as described in Clause 8.9 of the SCCs (EU), as applicable, shall be carried out in accordance with Section 11 of the DPA.

5. In Clause 9, Option 2 shall apply, and Operative has Customer's authorization to engage sub-processors in accordance with Section 7 of the DPA. The time period for prior notice of sub-processor changes shall be as set out in Section 7.2 of the DPA.

6. In Clause 10(a), the optional language shall not apply.

7. In Clause 11(a) the optional language shall not apply.

8. With respect to Clause 12 of the SCCs (EU),to the greatest extend permitted under law, any claims brought under the SCCs (EU) will be subject to limitations of liability provisions in the aggregate as set forth in the Agreement.

9. Clause 13 shall apply as follows:

    a. Where the data exporter is established in the EEA, the supervisory authority shall be the supervisory authority applicable to the data exporter in its EEA country of establishment.

    b. Where the data exporter is not established in the EEA and has appointed a representative pursuant to Article 27(1) of the GDPR, the supervisory authority shall be the supervisory authority applicable in the EEA country where such representative of the data exporter is established.

    c. Where the data exporter is not established in an EU Member State, and not required to appoint a representative pursuant to Article 27(2) of the GDPR, the supervisory authority shall be the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located.

10. In Clause 17, Option 1 shall apply, and the EU SCCs shall be governed by the laws of Luxemburg.

11. In Clause 18(b), disputes shall be resolved before the courts of Luxemburg. The parties agree to submit themselves to the jurisdiction of such courts.

ANNEX 1 TO SCHEDULE 1
DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

A. LIST OF PARTIES

Data exporter:

Name of data exporting organization: The Customer identified in a mutually signed Schedule describing the Services.

Contact Information (Address/Telephone/E-mail)/: The Customer contact information identified in a mutually signed Schedule describing the Services

Role (controller/processor): Controller

Activities relevant to the data transferred under these Clauses:

1. Submitting requests for support with the Operative.One platform ("**Op.one**"), the AOS platform ("**AOS**") and the STAQ Reporting Platform ("**STAQ**").
2. Receiving support typically via the exchange of e-mails, screenshots and recordings and occasionally over calls and/or live screenshare.
3. Accessing the Op.one and AOS platforms via login pages.
4. Accessing the STAQ platform via a login page.
5. In connection with STAQ, collection of IP addresses in connection with logins.
6. Logging into Basecamp to participate in configuration and project activities.
7. Logging into training webinars regarding new releases.

Data importer(s):

Name: SintecMedia NYC, Inc. d/b/a Operative
Address: 530 Fifth Avenue, Suite 19A, New York, NY 10036
Contact:
Alyssa Greenspan
Senior Counsel & Chief Privacy Officer
Operative
530 Fifth Avenue, Suite 19A
New York, NY 10036
(212) 994-8931
agreenspan@operative.com

EU Contact
Mihai Oprea
Finance Controller Romania
D: +40 351 442 882 int.105
M: +40 723-887394
mihaio@operative.com
1st floor, Proiect Building, Ion Maiorescu Str., nb. 4,
Craiova, Dolj County, Romania

Activities relevant to the data transferred under these Clauses are as follows (please see Annex 3 to Schedule 1 for additional information regarding the sub-processors referenced herein):

1. Receiving and reviewing requests for support.
2. Providing support typically via the exchange of e-mails screenshots and recording and occasionally over calls and/or live screenshare
3. Storing Customer Personal Data in the AOS, Op.one and STAQ environments, as applicable, for the purposes of the Services
4. Providing professional services in connection with configuration and project activities.
5. Providing training webinars regarding new releases webinars.
6. Accessing Customer Personal Data for the purpose of billing, invoicing, and other finance-related activities.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

1. Employees of Customer
2. Independent Contractors of Customer
3. Customers of Customer

Categories of personal data transferred

Personal Data may include

1. Names
2. Surname
3. Email addresses
4. Physical addresses
5. Usernames associated with employees and authorized independent contractors of Customer.
6. Location data
7. Telephone contact details and (including country code)
8. In addition, in some instances contact information (e.g., names, email addresses, physical addresses, usernames) of customers of Customer.
9. IP addresses

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.

Not applicable

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

Data is transferred on a continuous basis (for example, at the time of each login into the Operative.one/AOS and STAQ Platforms; during the request for and provisioning of support and during the provisioning of professional services).

Nature of the processing

Operative collects, accesses and uses Customer's Personal Data for the purposes of providing the Services, including support services, configuration, and professional services. In addition, Operative stores and deletes Customer's Personal Data in accordance with the terms of the Agreement.

Purpose(s) of the data transfer and further processing

Personal Data is transferred for the purpose of providing the STAQ, Op.one and AOS Services in accordance with the terms of the Agreement.

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

Subject to thirty days' prior written notice by Customer to Operative, Operative shall delete or return all Customer Personal Data to Customer on termination of the Agreement. If Customer does not provide such a request, Operative will hold Personal Data in archive for support usage and test environments in accordance with Operative's practices (for STAQ purposes Personal Data that is held in archive for up to 6 months past date of termination).

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

The Controller has authorized the use of the sub-processors set forth in Annex 3 to Schedule 1 attached hereto for the term of the Agreement (except in connection with AWS and Google Cloud where Personal Data may be held in archive for support usage and test environments in accordance with Operative's practices).

ANNEX 2 TO SCHEDULE 1

TECHNICAL AND ORGANIZATIONAL MEASURES FOR THE SECURITY OF DATA APPLICABLE TO THE USE OF THE OPERATIVE.ONE ENTERPRISE STANDARD EDITION SERVICES, AOS PLATFORM AND STAQ PLATFORM

These Technical and Organization Measures for the Security of Data detail security measures applicable to the Operative.One, AOS and STAQ Services.

A. Security Program:

Operative maintains an information security program that includes the following:

1. Appropriate and reasonable technical and organizational security controls which include written, physical, electronic, and procedural safeguards designed to prevent Security Incidents and the unauthorized or unlawful Processing of Customer Data.

2. Policies and procedures to protect Customer Data including but not limited to a privacy policy, an acceptable use policy, a third-party risk management policy and an incident response policy. Operative shall review and update such policies annually at a minimum (as necessary) and following material changes in related business practices.

3. Ongoing security awareness training for its employees and contractors to address practices for the usage and protection of Customer Data.

4. Designation of one or more qualified employees to maintain the information security program, which will be endorsed and approved by the Operative organization's executive management.

B. Access Controls

Operative shall utilize logical and physical access controls for access to Customer Data, and shall:

1. Review and revalidate user access for least privilege and separation of duties with an annual and quarterly frequency that is commensurate with organizational risk tolerance.

2. Implement and evaluate processes, procedures and technical measures for authenticating access to systems, applications and data assets, including single sign on (SSO) multifactor authentication and least privileged user access to Customer Data.

3. Implement and evaluate processes, procedures and technical measures to verify access to Customer Data and system functions is authorized.

4. Process user accounts and other identifiers for uniqueness to maintain a policy of not sharing such accounts and identifiers.

5. Use password complexity configurations including selection and aging procedures.

6. Not use shared or elevated privileged accounts unless the usage can be reliably tracked back to a user.

7. Implement multi-factor authentication for access to critical applications and infrastructure.

8. Authenticate users authorized to access Customer Data by implementing strong authentication practices; verifying user identity; requiring first-time password resets; establishing minimum password length, expiration, account lockouts, password resets and timely termination.

9. Assign a unique identification number to Operative employees, agents and contractors with computer access to Customer Data.

10. Encrypt passwords during transmission and storage on all network and system components.

C. Asset Management

Operative shall upon request by Customer following termination or expiration of the Agreement, return to Customer, or securely destroy or render unreadable or undecipherable, Customer Data that is no longer required for the purpose of the Services.

D. Logging and Monitoring

With respect to monitoring and logging systems utilized to provide the Services or systems that hold Customer Data, Operative shall:

1. Identify and monitor security-related events within applications and related underlying infrastructure.

2. Communicate alerts of security-related events to responsible stakeholders.

3. Restrict audit log access to authorized personnel and maintain records that provide unique access accountability.

4. Monitor security audit logs to detect activity outside of typical or expected patterns.

5. Follow a defined review process and take appropriate and timely actions on detected anomalies.

E. Compliance and Audit

1. Operative shall produce annual independent third-party audit and/or assessment reports (such as SSAE 18, ISO 27001, or other similar industry standard report) from a reputable third-party auditing firm assessing Operative's technical and organizational security measures for environments in which any Customer Data is Processed. Such third-party reports shall assess the confidentiality, availability, integrity and privacy of Customer Data in those environments in which Customer Data is Processed.

2. If third-party audit and/or assessment reports do not address the confidentiality, availability, integrity and privacy of Customer Data in those environments in which Customer Data is Processed, Operative shall comply with reasonable requests by Customer to describe its technical and organizational security measures in writing upon prior written request of at least thirty (30) days.

3. In the event of a Data Security Incident, Operative shall cooperate in good faith with an audit or assessment of its data privacy and data security procedures and related documentation pertaining to Customer Data and the impacted environments in which Customer Data is Processed (to the extent permitted by applicable law). Customer assessments and audits shall include administrative, and technical measures involved with the Processing of Customer Data. Should any such assessment and/or audits reveal material vulnerabilities that impact the security

of Customer Data, Operative shall implement commercially reasonable efforts to make commercially reasonable changes to correct such vulnerabilities.

F. Cryptography

With respect to the Operative.One and AOS Platforms, Operative implements encryption in transit with respect to Customer Data that traverses networks outside of the Operative organization and encryption at rest for Customer Data that resides in Operative's hosted environments, and for the STAQ platform Operative implements encryption in transit[1]

G. Incident Management

1. Operative will include in its information security program a plan for security incident management and response ("**Incident Response Plan**") in the event of a security compromise with respect Customer Data; any operations providing Services to customers; or malware posing a significant threat to Customer Data or any operations providing Services to customers.

2. Operative will monitor incidents using both external Managed Detection Response (MDR) Services and internal 24/7 monitoring of critical environments.

3. Operative will maintain internal playbooks for management of Security Incidents

4. Operative will test periodically the technical and organizational aspects of its Incident Response Plan.

H. Operations

Operative will maintain operational controls to protect Customer Data, including systems hosting in-scope and/or Customer web applications by maintaining and/or by implementing:

1. Policies and standards for the secure build of desktops, laptops, servers, networks, and mobile devices.

2. Separation of the development, testing and operational environments.

3. Configurable file share permissions.

4. Anti-virus/malware software on Operative laptops and desktops.

5. Anti-virus libraries (updated daily).

6. Scans of all files on local drives on laptops and desktops on a monthly basis.

7. Scans of all systems and boot files, drives, registry and memory conducted weekly on servers.

8. Continuous vulnerability scanning both externally and internally on web application and critical assets.

9. Implement critical security patches as required to mitigate Security Incidents in Operative systems where

[1] Encryption in transit and at rest is employed with respect to the Operative.One and AOS platforms. For STAQ, Operative implements TLS encryption for incoming and outgoing communications including all connections to the STAQ database. Those encryption standards are tested on a periodic basis. Encryption of data at rest is implemented within the STAQ platform for all backups copied in Google Cloud Storage (GCS) and AWS S3 Buckets, as well as encryption of user access credentials. Data at rest in the database platform is not encrypted.

Customer Data is stored and processed. .

I. Physical and Environmental Controls

Operative has controls in place to restrict access to authorized individuals only with a reasonable business need for access into facilities and areas where systems and information are stored or are accessible. Confidential Information contained in paper form or unencrypted electronic media is stored in controlled or locked storage containers (locked drawer, cabinet, restricted access space).

J. Employee Security Awareness

Operative implements a staff awareness program for the information security and privacy program within the organization including:

1. Annual information security and privacy awareness sessions for all employees (frontal and remote sessions) that describe Operative's security program, and common attack vectors and how to safeguard against the same.

2. Training and awareness for staff dedicated to information security and incident response.

3. Implementation of cyber-attack simulation to continuously measure employee understanding.

K. Data and Operations Recovery

1. Operative maintains back-up and restoration capabilities relevant to the scope of the service provided.

2. Customer data is stored in multiple availability zones with third party cloud hosting providers (Amazon Web Services with respect to the AOS and Op.one Platforms, and Google Cloud with respect to the STAQ platform) to address recovery in the event of a disaster.

L. Application Security

Operative shall implement commercially reasonable application security procedures including:

1. The utilization of secure software development practices throughout the development lifecycle, security requirements definition, security architecture design, security code reviews, and penetration testing.

2. Design of appropriate audit trails and activity logs into application systems.

3. Security risk assessments via documentation or hands-on testing of scoped systems and data.

4. Testing of vulnerabilities on software and hosted environments including but not limited to, trojans, back-doors, key-loggers and malicious file execution.

5. Annual penetration tests by a reputable third-party vendor.

M. Infrastructure Security

Operative shall implement the following infrastructure security practices:

1. Network protection by utilizing, intrusion detection/prevention systems, firewalls, network segmentation,

encryption[2], and malware detection.

2. Configuration of servers, routers, switches and firewalls to, as necessary, to harden and disable unnecessary protocols and ports and to remove insecure protocols.

3. The deployment of digital certificates on web server components and the encryption of communications using 256-bit encryption level Advanced Encryption Standard (AES) algorithm or better.

4. The use of anti-virus software or programs, to detect, remove, and protect against malware, spyware and adware. Such anti-virus software or programs shall be regularly updated, and capable of generating audit logs, and deployed on all systems used to access Customer Data.

5. Maintain a vulnerability program that identifies vulnerabilities in the environment through scanning and vendor notifications.

6. A documented, formal asset and change management process to control changes to scoped infrastructure and production applications.

7. Document and log access to Customer Data, by tracking individual user access to Customer Data, user-identification, event-type, date and time, login success or failure indication, and invalid logical access attempts.

8. Intrusion prevention and detection systems are in place within networks and environments containing Customer Data.

9. Access to Customer Data from locations outside of Operative's facilities utilizing a virtual private network (VPN) connection including transport encryption.

10. Operative maintains data flows and network diagrams relevant to the Services.

11. Operative will monitor and make commercially reasonable efforts to detect security vulnerabilities in production environments.

12. Operative will monitor production environments 24/7 and utilize use of external MDR services to make commercially reasonable efforts to identify attacks including, but not limited to:

    a. Application attacks
    b. Brute-force attacks
    c. Denial of service attacks
    d. Information leaks
    e. Security misconfigurations
    f. Suspicious activity
    g. Malicious activity
    h. Reconnaissance attempts

13. Operative will implement, as applicable web application protection to production environments.

[2] Encryption in transit and at rest is employed with respect to the Operative.One and AOS platforms. For STAQ Operative implements TLS encryption for incoming and outgoing communications including all connections to the STAQ database. Those encryption standards are tested on a periodic basis. Encryption of data at rest is implemented within the STAQ platform for all backups copied in Google Cloud Storage (GCS) and AWS S3 Buckets, as well as encryption of user access credentials. Data at rest in the database platform is not encrypted.

14. Operative will implement as applicable, distributed denial of service protection mechanisms.

N. Back-Up Recovery

1. Operative will implement backups which are configured to run daily for data, application and infrastructure purposes.

2. Backup restoration is performed and tested monthly.

3. Multi-availability cloud hosting is implemented for recovery purposes in case of disaster

O. Definitions

1. **Customer Data** means as applicable data provided by Customer to Operative that is Processed or stored on computers or other electronic media on Customer's behalf, which Operative has access to, obtains, uses, maintains or otherwise handles in connection with the performance of Services. Customer Data includes Personal Data of Customer.

2. **Security Incident** means as a result of breaching the terms of the Agreement: (i) the loss or misuse of Customer Data in the care, custody and control of Operative; (ii) the unauthorized and/or unlawful Processing of Customer Data by Operative or (iii) to the extent caused by an act or omission of Operative, the compromise of the security, confidentiality or integrity of Customer Data. A Personal Data Breach qualifies as a Security Incident hereunder.

ANNEX 3 TO SCHEDULE 1

SUBPROCESSORS

Subprocessor	Description of the Processing	Location of the Processing	Corporate Location
Atlassian Pty, Inc.	Provider of Jira Software, used for provisioning customer support	Ireland	Australia
Amazon Web Services, Inc.	Data/System Hosting	United States	United States
Basecamp, LLC	Project Management tool for configuration projects	United States	United States
Epona USA, Inc.	Communication and Collaboration Tool	European Union	United States
Freshworks, Inc.	Support services (STAQ)	United States and European Economic Area	United States
Google Cloud Platform (STAQ only)	Hosting, storage, backup and cloud computing resources	United States	United States
Hubspot, Inc.	Marketing and communication tool	United States	United States
Makepositive Ltd.	Saleforce Services	Ireland	United Kingdom
Microsoft Corporation (Office 365)	Microsoft communication and document management Services	European Union	United States
Mongo DB, Inc.	Database technology and management	United States	United States
New Relic, Inc.	System Monitoring	United States	United States
Oracle America, Inc.	Corporate billing system and hosting provider	The Netherlands	United States
OwnBackup Inc.	Salesforce backup and recovery services	United Kingdom	United States
Salesforce.com, Inc.	Customer relations management	United States	United States
Smartsheet, Inc.	Online work collaboration services	United States	United States
Valiantys, Inc.	Managed services for Jira/customer support	United States	Ireland

Affiliates

1. SM Lux TopCo S.a, 6D, route de Treves, L-2633 Senningerberg, Luxembourg
2. SM LuxCo HoldCo S.à r.l., 6D, route de Treves, L-2633 Senningerberg, Luxembourg
3. M.M.S.G Management Ltd, 16 Abba Hillel Rd., Ramat Gan, Israel 5250608
4. SintecMedia Ltd, d/b/a Operative 21 Nahum Hafzadi St., Jerusalem, Israel 9548402
5. SintecMedia Software Ltd. d/b/a Operative, 21 Nahum Hafzadi St., Jerusalem, Israel 9548402
6. SintecMedia (RG) Ltd. d/b/a Operative, 21 Bar Kochva St., Bnei Brak, Israel 5126001
7. SintecMedia (LON) Ltd. d/b/a Operative, Artemus House Odyssey Business Park, West End Road, Ruislip, England, HA4 6QE
8. SintecMedia (WEM) Ltd. d/b/a Operative, Artemus House Odyssey Business Park, West End Road, Ruislip, England, HA4 6QE
9. SintecMedia Global Ltd. d/b/a Operative, Artemus House Odyssey Business Park, West End Road, Ruislip, England, HA4 6QE
10. SintecMedia Inc. d/b/a Operative, 530 Fifth Avenue, Suite 19A, New York, NY 10036
11. SintecMedia DV Inc. d/b/a Operative, 530 Fifth Avenue, Suite 19A, New York, NY 10036
12. SintecMedia SYD Pty Ltd., 233 Castlereagh St. Level 5, Suite 502, Sydney NSW 2000, Australia
13. SintecMedia SMR S.R.L Ltd. d/b/a Operative, 4th Ion Maiorescu St. Project Building, 1st Floor, Craiova, Doj 200760, Romania
14. Operative India Private Limited, 12 Floor, IBS Knowledge Park, Tower D, 4/1, Bannerghatta Main Road, Bhavani Nagar, Bengaluru Banglore KA 560029 IN
15. Operative (UK) Limited, Artemus House Odyssey Business Park, West End Road, Ruislip, England, HA4 6QE
16. SintecMedia São Paulo Ltda., Avenida Paulista, 726 – conj. 1604 16° Andar – Bela Vista São Paulo, BSP – 01310-100
17. STAQ, Inc., 530 Fifth Avenue, Suite 19ª, New York, NY 10036

ANNEX 4 to Schedule 1
UK GDPR SCC ADDENDUM

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Effective date of the Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details		
Key Contact		
Signature (if required for the purposes of Section 2)	Mutual execution of the applicable Schedule or Agreement governing the DPA is deemed execution of this UK Addendum	Mutual execution of the applicable Schedule or Agreement governing the DPA is deemed execution of this UK Addendum

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Effective date of the Agreement Reference (if any): None. Other identifier (if any): None.
	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:

Addendum EU SCCs	Date: Reference (if any): Other identifier (if any): Or the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisa tion or General Authorisa tion)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	No					
2	Yes	No	No	General	As set forth in DPA Section 7.2	No
3	No					
4	No					

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex 1 to Schedule 1
Annex 1B: Description of Transfer: See Annex 1 to Schedule 1
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex 2 to Schedule 1.
Annex III: List of Sub processors (Modules 2 and 3 only): See annex 3 to Schedule 1.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs.

    b. In Clause 2, delete the words:

    "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"

    c. Clause 6 (Description of the transfer(s)) is replaced with:

    "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer."

    d. Clause 8.7(i) of Module 1 is replaced with:

    "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer"

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

    "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer"

    f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced

by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws

g. References to Regulation (EU) 2018/1725 are removed.

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK".

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)".

j. Clause 13(a) and Part C of Annex I are not used.

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner".

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply".

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales."

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also 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."

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 1

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or

    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

ANNEX 5 to Schedule 1
FADP ADDENDUM

To the extent the Standard Contractual Clauses are used for the processing of personal data subject to the data protection laws of Switzerland, the Standard Contractual Clauses shall apply with the following revisions:

1. References to the GDPR in the Clauses shall be understood as references to the Swiss Federal Act on Data Protection ("FADP"), as it may be amended from time to time, insofar as the transfers of personal data are subject to the FADP.

2. For purposes of Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner insofar as the personal data is subject to the Swiss Federal Act on Data Protection. To the extent EU and Swiss supervisory authorities both have jurisdiction, the supervisory authority named in Clause 13 shall also retain jurisdiction.

3. For purposes of Clause 17, Swiss law shall apply.

4. For purposes of Clause 18, any dispute arising between the Parties from these Clauses shall be resolved by the courts of Luxemberg Further, the term "Member State" shall not be interpreted to exclude data subjects that reside in Switzerland from bringing suit in Switzerland pursuant to Clause 18(c).

5. The Clauses also protect the data of legal entities until the entry into force of the revised FADP.