EEA/UK/SWISS DPA

If indicated as applicable in the SDPA between Customer and Supplier, and where Customer is acting as controller and Supplier is acting as processor, this EEA/UK/Swiss DPA ("DPA") supplements the SDPA with respect to Supplier's obligations relating to its processing of EEA/UK/Swiss Personal Data under the SDPA and/or the Agreement. To the extent that any of the terms of this DPA conflict with any of the terms of the SDPA, this DPA shall take precedence and supersede the SDPA (other than to the extent the SDPA affords a higher level of protection to EEA/UK/Swiss Personal Data).

1. DEFINITIONS. As used in this DPA, the following capitalized terms shall have the meanings provided below. All other terms shall be as defined in the SDPA.

"Controller", "processor", "data subject", "personal data breach" and "processing" shall have the meaning given to them in the EEA/UK/Swiss Rules. For the purposes of this DPA, a "personal data breach" shall be included in the definition of "Information Security Incident" in the SDPA.

"EEA/UK/Swiss Personal Data" means, as applicable, (i) Personal Data to which data protection laws of the European Union ("EU") or a Member State of the EU or EEA, were applicable prior to its processing by Supplier ("EEA Personal Data"); (ii) Personal Data to which data protection laws of the UK were applicable prior to its processing by Supplier ("UK Personal Data") and (iii) Personal Data to which the FADP was applicable prior to its processing by Supplier ("Swiss Personal Data").

"EEA/UK/Swiss Rules" means the GDPR, Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Directive on security of network and information systems (the NIS Directive), the Swiss Federal Act on Data Protection and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them, and all other applicable laws relating to processing of personal data and privacy in any relevant jurisdiction, including, where applicable, guidance and codes of practice issued by supervisory authorities.

"GDPR" means, in each case to the extent applicable to processing activities: (i) Regulation (EU) 2016/679 (the "EU GDPR"); and (ii) the GDPR as applicable as part of UK domestic law 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 (as amended) (the "UK GDPR").

"Protected Area" means (a) in respect of EEA Personal Data, the member states of the EU and EEA and any country, territory, sector or international organization in respect of which an adequacy decision under Art 45 EU GDPR is in force; (b) in respect of UK Personal Data, the UK and any country, territory, sector or international organization in respect of which an adequacy decision under UK adequacy regulations is in force; and (c) in the case of Swiss Personal Data, any country, territory, sector or international organization which is recognized as adequate under the laws of Switzerland.

"Relevant Law" means: (a) in respect of EEA Personal Data, any legislation of the EU or a Member State of the EU or EEA; (b) in respect of UK Personal Data, any legislation of any part of the UK; and (c) in respect of Swiss Personal Data, any legislation of Switzerland.

"Standard Contractual Clauses" or "SCCs" means:

(a) in respect of EEA Personal Data, the standard contractual clauses for the transfer of personal data to third countries pursuant to the EU GDPR, adopted by the European Commission under Commission

Implementing Decision (EU) 2021/914, including the text from module two of such clauses to the extent the Customer is acting as controller and Supplier is acting as processor, and not including any clauses marked as optional ("EU SCCs");

(b) in respect of UK Personal Data, the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 but, as permitted by clause 17 of such Addendum, the parties agree to change the format of the information set out in Part 1 of the Addendum so that:

1. the details of the parties in table 1 shall be as set out in Appendix 1, Annex I of this DPA (with no requirement for signature);
2. for the purposes of table 2, the Addendum shall be appended to the EU SCCs (including the selection of modules and disapplication of optional clauses as noted above) and the section of the SDPA titled "Subcontractors" selects the option and timescales for clause 9; and
3. the appendix information listed in table 3 is set out in Appendix 1, Annex II of this DPA and the EVSRs.

(c) in respect of any Swiss Personal Data, the EU SCCs, provided that any references in the clauses to the GDPR shall refer to the FADP; the term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses; and the clauses shall also protect the data of legal persons until the entry into force of the revised FADP.

2. CONTROL OF EEA/UK/SWISS PERSONAL DATA. Customer has the exclusive authority to instruct the processing of all EEA/UK/Swiss Personal Data by Supplier. Supplier will process EEA/UK/Swiss Personal Data only in accordance with the written instructions of Customer (which may be specific instructions or instructions of a general nature) as set out in this DPA, the SDPA and the Agreement, or as otherwise notified by Customer to Supplier from time to time. Supplier will not use EEA/UK/Swiss Personal Data for any other purpose. Supplier acknowledges that all EEA/UK/Swiss Personal Data remains the exclusive property of Customer or ultimate data controller who instructs Customer. The subject matter of the data processing is the performance of the Services and the processing will be carried out for the duration of the Agreement. Schedule 1 to the SDPA sets out the nature and purpose of the processing by Supplier, the types of Personal Data processed by Supplier and the categories of data subjects in relation to such Personal Data.

3. ADDITIONAL DATA PROTECTION REQUIREMENTS. In respect of EEA/UK/Swiss Personal Data processed by Supplier in providing the Services, Supplier will, at no additional cost to Customer:

(a) Process the EEA/UK/Swiss Personal Data only to the extent, and in such manner, as is necessary for the provision of the Services and inform Customer if Supplier is required by Relevant Law to process the EEA/UK/Swiss Personal Data other than pursuant to the written instructions of Customer prior to the processing unless that law prohibits it on important grounds of public interest.

(b) Upon Customer's request, provide a copy of the EEA/UK/Swiss Personal Data or correct, delete, archive, anonymize, port or block the EEA/UK/Swiss Personal Data, and promptly notify Customer upon becoming aware that any EEA/UK/Swiss Personal Data is or has become inaccurate.

(c) Appoint a data protection officer if required by the EEA/UK/Swiss Rules and maintain written records of all categories of EEA/UK/Swiss Personal Data processing activities carried out on behalf of Customer containing the information prescribed in the EEA/UK/Swiss Rules.

(d) Immediately refer to Customer any requests, notices, complaints or other communication relating to the EEA/UK/Swiss Personal Data processed by Supplier from data subjects, supervisory authorities, law enforcement or any other third parties, to the extent permitted by applicable law, for Customer to resolve.

(e) Provide Customer with reasonable cooperation and assistance in relation to any request, notice, complaint or other communication made under paragraph (d) above, including by providing Customer with: (i) details of the request, notice, complaint or other communication; (ii) any EEA/UK/Swiss Personal Data it holds in relation to a data subject on Customer's request (and within the reasonable timescales required by Customer); and (iii) upon reasonable request, any information relating to the Services and/or the associated processing of EEA/UK/Swiss Personal Data that may assist Customer in complying with its obligations under the EEA/UK/Swiss Rules.

(f) Comply with its obligations as a data processor under the EEA/UK/Swiss Rules.

(g) Reasonably assist Customer in complying with its obligations under the EEA/UK/Swiss Rules and not perform its obligations under the Agreement, the SDPA and this DPA in such a way as to cause Customer to breach any such obligations.

(g) Provide Customer with reasonable cooperation and assistance in relation to its security and breach notification obligations, any requirements to conduct data protection impact assessments or transfer impact assessments, accountability documentation or similar requirements and to consult with supervisory authorities in relation to data processing pursuant to EEA/UK/Swiss Rules.

(h) If the European Commission or the UK Information Commissioner (as applicable) lays down, or any other applicable supervisory authority adopts, standard contractual clauses for the matters referred to in Article 28(3) and Article 28(4) of EU GDPR or UK GDPR pursuant to Article 28(7) or Article 28(8) of the EU GDPR or Article 28(8) of the UK GDPR (as appropriate) and Customer notifies Supplier that it wishes to incorporate any element of any such clauses into the SDPA, this DPA and the Agreement, it shall work with Customer to do so.

(i) Provide any other any information reasonably requested by Customer to demonstrate Supplier's compliance with this DPA.

4. USE OF SUBCONTRACTORS. Supplier will impose and enforce on all Subcontractors obligations equivalent to the terms of this DPA by way of a written agreement. For the avoidance of doubt, if a Subcontractor which is instructed by Supplier to process EEA/UK/Swiss Personal Data fails to fulfil its obligations under any sub-processing agreement or any applicable EEA/UK/Swiss Rules Supplier will remain fully responsible for its Subcontractors' compliance with this DPA.

5. INTERNATIONAL TRANSFER MECHANISMS.

(a) Supplier will not, and will ensure that none of its affiliates or Subcontractors, transfer, access or use EEA/UK/Swiss Personal Data outside of the Protected Area without Customer's prior authorization. Customer agrees to authorize the transfers set out at Appendix 1 to this EEA/UK/Swiss DPA on the basis that the Supplier and Customer agree to comply with the obligations set out in the SCCs as though they

were set out in full in this DPA, with Customer as the 'data exporter' and Supplier as the 'data importer', with the parties' signature and dating of the SDPA being deemed to be the signature and dating of the SCCs and with the Annexes to the SCCs being as set out in Appendix 1 to this Addendum. The Enterprise Supplementary Measures, which are set forth below, shall provide additional appropriate safeguards of EEA/UK/Swiss Personal Data in connection with any transfers or access outside the Protected Area authorized pursuant to Appendix 1 of this DPA.

(b) For the purposes of the EU SCCs, the following shall apply:

1. Clause 9 option 2: general written authorization and the parties agree that the time period for informing Customer of any changes to the list of sub-processors shall be 30 days in advance;
2. Clause 17 (Governing law): the clauses shall be governed by the laws of Ireland; and
3. Clause 18 (Choice of forum and jurisdiction): the courts of Ireland shall have jurisdiction.

(c) In the event that Customer gives its consent to Supplier transferring EEA/UK/Swiss Personal Data outside the Protected Area and a relevant European Commission decision or other valid adequacy method under applicable EEA/UK/Swiss Rules on which Customer has relied in authorizing the data transfer is held to be invalid, or that any supervisory authority requires transfers of EEA/UK/Swiss Personal Data made pursuant to such decision to be suspended, then Customer may, at its discretion, require Supplier to cease processing the EEA/UK/Swiss Personal Data to which this paragraph applies, or cooperate with Customer to facilitate use of an alternative transfer mechanism.

(d) Supplier shall promptly notify Customer if Supplier is no longer able to provide the level of protection to EEA/UK/Swiss Personal Data required under any data transfer mechanism.

(e) Supplier agrees that Customer may at any time novate all of its rights and obligations under the SCCs to its affiliates and/or in connection with any merger, reorganization, outsourcing, divestments, sale of all or substantially all its assets or similar transaction.

APPENDIX 1 TO THE EEA/UK/SWISS DPA

INFORMATION REQUIRED FOR THE STANDARD CONTRACTUAL CLAUSES

Annex I

A. LIST OF PARTIES

Data exporter(s): The data exporter shall be the Customer at the address given in the SDPA. Its contact person's name, position and contact details are set forth in the SDPA. For the activities relevant to the data transferred under these Clauses, please see Part 2 of Schedule 1 of the SPDA. The data exporter's signature and date to these Clauses shall be deemed to be the signature and date by Customer to the SDPA. The data exporter's role is that of a controller.

Data importer(s): The data importer shall be the Supplier at the address given in the SDPA. Its contact person's name, position and contact details are set forth in the SDPA. For the activities relevant to the data transferred under these Clauses, please see Part 2 of Schedule 1 of the SPDA. The data importer's signature and date to these Clauses shall be deemed to be the signature and date by Supplier to the SDPA. The data importer's role is that of a processor.

B. DESCRIPTION OF TRANSFER

MODULE TWO: CONTROLLER TO PROCESSOR

Categories of personal data transferred and categories of data subjects whose personal data is transferred: See Part 1 of Schedule 1 of the SPDA.

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 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: See Part 1 of Schedule 1 and the EVSRs.

Frequency of transfer: See Part 1 of Schedule 1 of the SPDA

Nature and purpose of the processing/processing operations: See Part 2 of Schedule 1 of the SPDA.

The period for which EEA/UK/Swiss Personal Data will be retained, or the criteria used to determine that period: See the section of the SPDA titled "Destruction and Return of Customer Information."

For transfers to (sub-) processors, the subject matter, nature and duration of the processing: See the section of the SPDA titled "Destruction and Return of Customer Information."

C. **COMPETENT SUPERVISORY AUTHORITES (EU Standard Contractual Clauses only)**: As determined by GDPR

Annex II: Technical and Organizational measures: See the EVSRs.

SUPPLEMENTARY MEASURES

Unless otherwise herein defined, any terms used in these Supplementary Measures shall have the meaning given to them the SDPA (including its Addendums).

1. PERSONNEL. The data importer's personnel will not process Personal Data without authorization. Personnel are obligated to maintain the confidentiality of any such Personal Data and this obligation continues even after their engagement by or employment with the data importer ends.

2. TECHNICAL AND ORGANIZATIONAL MEASURES. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Personal Data against accidental loss, destruction, or alteration, unauthorized disclosure or access or unlawful destruction as follows: the EVSRs, which are incorporated into these Supplementary Measures by this reference and are binding on the data importer as if they were set forth in these Supplementary Measures in their entirety.

3. THIRD PARTY REQUESTS.

3.1 A "Third Party Request" means any legally binding request from a public authority, including judicial authorities or law enforcement agencies ("Relevant Third Party") to the data importer to access, disclose, or otherwise process Personal Data.

3.2 Unless prohibited by law (and without prejudice to Clause 15 of the EU Standard Contractual Clauses), the data importer shall:

3.2.1 Notify Customer promptly, and in any event within twenty-four (24) hours, upon receipt of a Third Party Request (and prior to any response to or any disclosure of EEA/UK/Swiss Personal Data to the Relevant Third Party);

3.2.2 Provide Customer with the information, reasonable cooperation and/or tools required for it to evaluate, quash, limit, and/or respond to the Third Party Request (including a copy of the Third Party Request);

3.2.3 Subject to below, not respond to any Third Party Request without the explicit written authorization of Customer. Where the data importer has a mandatory obligation under applicable law to respond directly, the data importer shall notify Customer at the same time as making the initial notification as required above and shall only disclose the minimum amount of Personal Data necessary to comply with law or judicial process and comply with Customer's reasonable requests in responding to, and dealing with, any such Third Party Request.

3.2.4 The data importer will:

3.2.4.1 immediately inform in writing the Relevant Third Party that some or all the material covered by the Third Party Request is the subject of a non-disclosure agreement;

3.2.4.2 use every reasonable effort to redirect the Relevant Third Party to request the Personal Data directly from Customer;

3.2.4.3 use all lawful efforts to challenge the Third Party Request on the basis of any legal deficiencies under the laws of the Relevant Third Party or any relevant conflicts with Relevant Law;

3.2.4.4 not provide any Relevant Third Party: (a) direct, indirect, blanket or unfettered access to Personal Data; (b) any encryption keys used to secure the Personal Data or the ability to break such encryption; or (c) with access to Personal Data if the data importer is aware (or should reasonably be aware) that the Personal Data is to be used for purposes other than those stated in the Third Party Request; and

3.2.4.5 within twenty four (24) hours of a written request by Customer, provide Customer with access to the Personal Data (and other information) requested in the Third Party Request in the format in which it is maintained in the ordinary course of business (or, on Customer's request, with copies).

3.2.5 The data importer agrees that (i) it has not purposefully created back doors or similar programming that could be used to access the Personal Data; (ii) it has not purposefully created or changed its business processes in a manner that facilitates access to such Personal Data; and (iii) law or government policy to which the data importer is subject does not require it to create or maintain back doors or to facilitate access to such Personal Data.

3.2.6 The data importer agrees to monitor any legal or policy developments that might lead to its inability to comply with its obligations under these Supplementary Measures and promptly inform Customer of any such changes and developments, if possible, ahead of their implementation.

3.2.7 If the data importer discloses Personal Data in breach of these terms, it will compensate data subjects for any material and non-material damage suffered.

3.2.8 The data importer will notify Customer if, at any time it is unable to continue complying with the commitments outlined in these Supplementary Measures and agrees that Customer may terminate the Agreement or the impacted Services on such notice period as is stipulated by Customer in the event that the Supplier breaches these terms.