DIGITAL SCIENCE DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") shall form part of any agreement pursuant to which Digital Science (as defined below) agrees to provide products, services and / or data ("**Services**") that expressly incorporates this DPA (the "**Agreement**"). Capitalized terms used herein and not otherwise defined shall have the respective meanings given in the Agreement.

1. APPLICABILITY OF THIS DPA

1.1 The parties acknowledge and agree that the provision of the Services pursuant to the Agreement may involve the Processing of Personal Information. To ensure the continued protection of such Personal Information, the parties have agreed to supplement the Agreement as set out herein. If a provision in this DPA conflicts with another provision in the Agreement that specifically governs the Processing of Personal Information, then the provision of this DPA will prevail.

2. PROCESSING OF CUSTOMER PERSONAL INFORMATION

2.1 To the extent Digital Science Processes Customer Personal Information, it shall do so in accordance with its obligations under Data Protection Laws and shall:

2.1.1 only Process Customer Personal Information: (i) to perform its obligations under the Agreement and to meet your other documented and reasonable instructions; and (ii) to comply with any applicable law to which Digital Science is subject, in which case Digital Science shall (if legally permissible) inform you of that legal requirement before such Processing;

2.1.2 inform you if it receives an instruction that, in Digital Science's opinion, conflicts with Data Protection Laws, provided Digital Science shall have no liability arising from any failure to notify you of such conflict or reliance placed on any notice given;

2.1.3 implement appropriate technical and organisational measures in relation to its Processing of Customer Personal Information to ensure a level of security appropriate to the risks presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Information transmitted, stored or otherwise Processed, having regard to the state of technological development and the cost of implementing any measures, including as described in Schedule 1. Notwithstanding, you shall be responsible for evaluating the adequacy of such measures for your needs;

2.1.4 inform you of any request from a Data Subject to exercise its data protection rights under Data Protection Laws, and provide reasonable assistance to you in responding to any such request and otherwise in complying with your obligations, under the Data Protection Laws, including those obligations relating to: (i) security of Processing; (ii) notifications by you of Security Incidents to supervisory authorities or Data Subjects; and (iii) data protection impact assessments; in each case at your reasonable cost and only to the extent that you do not have access to the information required and are otherwise unable to respond/comply without Digital Science's assistance, including through functionality that may be included as part of the Services;

2.1.5 inform you of any legally binding request for disclosure of Customer Personal Information by a law enforcement authority, unless otherwise prohibited, such as in order to preserve the confidentiality of an investigation by the requesting authority, and you acknowledge that Digital Science may disclose Customer Personal Information to comply with such a legally binding disclosure request;

2.1.6 upon becoming aware of a Security Incident, inform you without undue delay and within any time-limits required by Data Protection Laws, and provide details of the breach;

2.1.7 ensure that all Digital Science personnel authorised to Process Customer Personal Information are subject to a duty of confidentiality (contractual or statutory); and

2.1.8 either delete or return to you Customer Personal Information within a reasonable period of the later of the expiry or termination of the Agreement and any post-termination obligations and/or rights relating to such Customer Personal Information (unless retention is required by applicable law), and in accordance with the Documentation.

2.2 The details of the Processing of Customer Personal Information by Digital Science are set out in Schedule 2 to this DPA.

2.3 You acknowledge and agree that Digital Science may engage its Affiliates, hosting providers and other entities in connection with the provision of the Services that may involve processing of Customer Personal Information ("**Sub-Processors**"), which you hereby authorise. Digital Science will only permit access to Customer Personal Information by the Sub-Processors as is required for the purpose of their respective involvement in the provision of the Services and will enter into a written agreement with each Sub-Processor that complies with the requirements of Data Protection Laws. Digital Science shall make a current list of Sub-Processors available to you on the website relevant to the Services and shall remain liable for their acts or omissions as if they were its own. You may object to the appointment of any new Sub-Processor in writing within thirty (30) days of being informed of the same and Digital Science will act reasonably to consider such objection and seek to propose an alternative solution, together with any additional cost required for their implementation.

2.4 As part of the Agreement, Digital Science may have agreed to store your content in a particular region. Without prejudice to any such obligation, you authorise the transfer of Customer Personal Information as required to perform the Services, including to any countries in which Digital Science's Sub-Processors operate, or as necessary to comply with applicable law. For the purposes of European Data Protection Laws, the European Cross-Border Transfer Provisions (as applicable) in Schedule 3 shall apply to any relevant transfers.

2.5 This DPA incorporates the provisions of the "Jurisdiction-Specific Addendum", to the extent applicable.

2.6 Digital Science shall provide you with such reasonable information as is necessary to verify its compliance with this DPA and allow for and contribute to reasonable audits at mutually convenient dates and times, including inspections, by you (or an independent auditor you reasonably appoint) for that purpose on reasonable notice during working hours, but no more than once in any twelve (12) month period, subject to you ensuring that any such audit or inspection is undertaken to the least invasive degree practicable, without causing disruption and in accordance with any relevant policies and procedures. All information obtained or generated in connection with this clause shall be treated as Confidential Information of Digital Science.

3. GENERAL

3.1 You shall comply with your obligations under Data Protection Laws. Without prejudice to the generality of the foregoing, you shall: (i) ensure data subjects are provided with all information required under Data Protection Laws in respect of Personal Information; (ii) ensure that the processing of Personal Information in accordance with your instructions will not cause Digital Science to breach Data Protection Laws or any other applicable law; and (iii) not provide or make available to Digital Science any Sensitive Personal Data.

3.2 You acknowledge that Digital Science may derive and collect aggregate or other non-personal data from the use of the Services for product improvement, analytical, reporting and research purposes, which may involve the processing of Personal Information. Digital Science will ensure that the results of this processing do not identify you or any of your data subjects and that all such processing is subject to appropriate technical and organisational measures. Where you use multiple Services that interoperate, Personal Information may be combined across those Services, to deliver an improved and more integrated overall solution, provided this does not involve information stored on your behalf that is intended to be segregated.

3.3 To the extent Digital Science, in its capacity as a controller, provides Data as part of the Services to you that comprises Personal Information for you to use for your own purposes ("**Digital Science Controlled Data**"), you shall: use (the most up-to-date version, where appropriate of) that Personal Information solely and exclusively in accordance with the Agreement, maintain a lawful basis for such use and notify Digital Science without undue delay of any security issue, complaint or request relating to the Digital Science Controlled Data; provide promptly all information and reasonable assistance as may be required to mitigate such security issue or respond to such complaint or request; and implement technical and organisational measures to ensure an appropriate level of security; and, for the purposes of European Data Protection Laws, the European Cross-Border Transfer Provisions (as applicable) in Schedule 3 shall apply. For clarity, each party shall be an independent controller of such Personal Information and nothing in this clause shall modify your rights to use any Data (or restrictions thereon) under the Agreement.

3.4 Notices or other information to be provided to you in connection with the subject matter of this DPA may be given by posting the information on a support, status or other webpage related to the relevant Services. Notwithstanding that this DPA may be updated by Digital Science from time to time, such change will only take effect upon the commencement of the Renewal Period (or other agreed renewal or extension period) following the update; or such earlier date as it may be accepted by you, including as part of an amendment or via the acceptance of an Order Form, proposal or quote that references the updated DPA; except where the update is required to comply with Data Protection Laws, in which case the change will take effect immediately without further action.

3.5 This DPA shall form part of, and terminate automatically upon termination or expiry of, the Agreement. This DPA and any disputes or claims arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by the same laws and subject to the same jurisdiction as the Agreement save as expressly specified.

3.6 If there is any conflict between the Schedules and/or any Annexes to the Schedules and/or the remaining terms of this DPA, then conflict shall be resolved in accordance with the following order of precedence:

3.6.1 The Jurisdiction-Specific Addendum;

3.6.2 Schedule 3, and then Schedule 4 and 5; and

3.6.3 The remaining provisions of this DPA.

DEFINITIONS

Customer Personal Information means Personal Information that is Processed by Digital Science on your behalf, including as a "service provider" as defined under CCPA.

Data Protection Laws means as applicable the European Data Protection Laws, CCPA and PIPEDA, and/or such other data protection or privacy laws that may require a party to grant and/or impose on the other party some or all of the rights and/or obligations set out in this DPA.

European Data Protection Laws means EU General Data Protection Regulation 2016/679 ("**GDPR**"), the UK Data Protection Laws and the Swiss Data Protection Laws.

Digital Science means the Digital Science entity that is party to the Agreement, being either Digital Science & Research Solutions Inc. (a Delaware corporation), Digital Science UK Ltd (a limited liability company incorporated in England) or Fairview LLC (a Connecticut limited liability company).

EEA shall mean the members of the European Economic Area from time to time plus Switzerland.

Personal Information means information about living individuals that is subject to the Data Protection Laws to the extent such information is Processed under the Agreement in a way which is also subject to those laws, including personal data (as applicable).

Security Incident means any security breach or incident (or analogous concept) affecting Customer Personal Information that is reportable to you under Data Protection Laws, including a personal data breach under GDPR (as applicable).

Sensitive Personal Data means categories of Personal Information that are sensitive or otherwise require higher levels of protection under Data Protection Laws, including "special categories of personal data" as defined under GDPR (as applicable).

Swiss Data Protection Laws means all laws relating to personal data in force from time to time in Switzerland, including the Swiss Federal Data Protection Act ("**SFDPA**") as amended or replaced from time-to-time.

UK Data Protection Laws means all laws relating to personal data in force from time to time in the United Kingdom ("**UK**"), including the Data Protection Act 2018 and the UK General Data Protection Regulation, 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 ("**UK GDPR**").

personal data, **process/processing**, **controller**, **processor**, **personal data breach**, **data subject**, and **supervisory authority** shall have the same meaning as in the GDPR, UK GDPR or SFDPA (as applicable).

Last update: January 2023

SCHEDULE 1

TECHNICAL AND ORGANISATIONAL INFORMATION SECURITY MEASURES

Digital Science will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to ensure a level of security appropriate to the risk, which will include the following technical and physical safeguards, in each case as appropriate:

Access Control

Access control measures, including by restricting access to confidential information only to those with a need to know and at the least level of privilege necessary to perform their assigned functions, and restricting access to active users and active user accounts only and removing system access rights for terminated employees or contractors; and user authentication protocols, including by controlling user identification and authentication through the use of strong passwords (with policies requiring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as token devices.

Transmission Security and Data Integrity

Technical security mechanisms to guard against unauthorised access to confidential information that is transmitted over unsecure networks or stored on mobile devices, such as encryption, and measures to prevent information from being altered or destroyed in an unauthorised manner.

Computer and Network Security

System monitoring for preventing, detecting, and responding to unauthorised use of or access to confidential information or other attacks or system failures, which may include:

- Protecting Information Assets: Installing and configuring systems and devices according to current technical standards and procedures, including: through the use of anti-virus software; and by configuring user accounts to require strong passwords; other standard security controls, in each case as appropriate.

- Perimeter Controls: Implementing and configuring perimeter controls to secure networks against external attacks, including through the use of: firewalls, configured according to current technical standards and procedures, to separate trusted networks from the internet or internet-facing environments; intrusion detection and prevention services; and network monitoring, in each case as appropriate.

- Log Management and Retention: Regularly review logs, using automated means where feasible, to identify unusual activities that may indicate a security incident. Secure log data and files to prevent tampering and retain them for a reasonable period.

- Remote Access: Require authentication against existing authentication sources and, where technically feasible, two-factor authentication, to access networks remotely. Configure remote access capabilities to limit access to reasonable business needs.

Physical Security

Measures to protect the security of premises wherever confidential information is stored, including through the use of physical barriers, such as gates, locked doors and barriers, human security guards and patrols, and mechanical security such as entry and exit controls and monitoring.

SCHEDULE 2

Data Processing Details

1 **Subject matter of the Processing**

Digital Science's provision of the Services to you pursuant to the Agreement.

2 **Nature and purpose of the Processing**

Digital Science will process Personal Information in the course of providing the Services.

3 **Duration of the Processing**

During the term of the Agreement and the period of any post-termination obligations and/or rights relating to such Personal Information.

4 **Categories of Data Subjects**

End users of the Services and any other person whose details you may provide to be integrated into the Services.

5 **Type of Personal Information**

Any of: name; contact information; supplementary identifiers (e.g. ORCID ID, institutional identifiers, photos); basic professional information (e.g. job title, place of work/research/department); research-biography information (e.g. publication and affiliation history), in each case as may be relevant to the Services.

Digital Science does not knowingly process (and you shall not submit to Digital Science for processing) any Sensitive Personal Data.

SCHEDULE 3

EUROPEAN CROSS-BORDER TRANSFER PROVISIONS

1. APPLICABILITY OF THE SCHEDULES

1.1 For the purposes of European Data Protection Laws, it is agreed that the Standard Contractual Clauses are incorporated into, and form part of, this DPA and will apply to any cross-border transfer of personal data made to any Third Country. If you subsequently determine (acting reasonably) such transfers are not subject to appropriate safeguards, you shall notify us immediately with details and Digital Science shall act reasonably to consider such determination and seek to propose an alternative solution, together with any additional cost required for its implementation.

2. INTERPRETATION

2.1 While it is acknowledged that, in the event of a contradiction between the clauses of the Standard Contractual Clauses and this DPA, those clauses are required to prevail in accordance with their terms, it is agreed that together they are intended to form part of a single, wider agreement, a fundamental part of which is to establish a commercially reasonable and appropriate allocation of liability (taking into account the fees to be paid and the other terms of the Agreement). Accordingly, it is agreed that the Standard Contractual Clauses should be construed in such a way so as to give effect to that intent to the fullest extent possible without impacting the validity of the Standard Contractual Clauses, notwithstanding that they may be subject to different governing laws and jurisdiction. For the avoidance of doubt, neither party's liability to a data subject exercising his / her / their third party beneficiary rights as provided for by the Standard Contractual Clauses shall be limited by any provision of this DPA.

2.2 To the extent any provision of this DPA would impact the validity of the Standard Contractual Clauses, such provision shall apply with such modifications as may be necessary to preserve the validity of the Standard Contractual Clauses.

3. ADDITIONAL DEFINITIONS

Third Country means: (i) where the European Data Protection Laws apply, a country not recognised by the European Commission (or other relevant authority, as the case may be) as providing an adequate level of protection where such processing is subject to the European Data Protection Laws and an alternative recognised compliance standard for the lawful transfer of Personal Information does not apply; (ii) where the UK Data Protection Laws apply, a country not recognised by the UK Government (or other relevant authority, as the case may be) as providing an adequate level of protection where such processing is subject to the UK Data Protection Laws and an alternative recognised compliance standard for the lawful transfer of Personal Information does not apply; and (iii) where the Swiss Data Protection Laws apply, a country not recognised by the competent Swiss authority as providing an adequate level of protection where such processing is subject to the Swiss Data Protection Laws and an alternative recognised compliance standard for the lawful transfer of Personal Information does not apply.

Standard Contractual Clauses means:

1. where the personal data being transferred is Customer Personal Information, which is subject to:

(a) EU GDPR, Module 2 (Transfer from controller to processor) of the standard contractual clauses for the transfer of personal data, approved by the European Commission Decision of 4 June 2021, as may be updated or superseded, incorporating Schedule 4 and the parties' relevant contact information and signatures (the "**2021 C2P SCCs**"). The Parties acknowledge that for the purposes of the 2021 C2P SCCs: (i) Digital Science will be the data importer and you will be the data exporter; (ii) the optional clause set out at Clause 7 of the 2021 C2P SCCs ('Docking clause') shall not apply; (iii) Clause 9(a) of the 2021 C2P SCCs ('Use of sub-processors') shall be amended as follows: "The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object"; (iv) the optional clause set out at Clause 11(a) of the 2021 C2P SCCs ('Redress') shall not apply; (v) Clause 13(a) of the 2021 C2P SCCs ('Supervision') shall be amended as follows: "The supervisory authority with responsibility for ensuring compliance by the data exporter with

Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority."; (vi) Clause 17 of the 2021 C2P SCCs ('Governing law') shall be amended as follows: "These Clauses shall be governed by the law of one of the EU Member States, provided that such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland."; (vii) Clause 18(b) of the 2021 C2P SCCs ('Choice of forum and jurisdiction') shall be amended as follows: "The Parties agree that those shall be the courts with jurisdiction over the Agreement or the courts of Ireland.";

(b) UK GDPR, the 2021 C2P SCCs as amended by the UK Terms of the Jurisdiction Specific Addendum; and / or

(c) Swiss DP Laws, the 2021 C2P SCCs as amended by the Swiss Terms of the Jurisdiction Specific Addendum.

2. where the personal data being transferred is Digital Science Controlled Data, which is subject to:

(a) EU GDPR, Module 1 of the standard contractual clauses for the transfer of personal data, approved by the European Commission Decision of 4 June 2021, as may be updated or superseded, incorporating Schedule 5 and the parties' relevant contact information and signatures (the "**2021 C2C SCCs**"). The Parties acknowledge that for the purposes of the 2021 C2C SCCs: (i) Digital Science will be the data exporter and you will be the data importer; (ii) the optional clause set out at Clause 7 of the 2021 C2C SCCs ('Docking clause') shall not apply; (iii) the optional clause set out at Clause 11(a) of the 2021 C2C SCCs ('Redress') shall not apply; (v) Clause 13(a) of the 2021 C2C SCCs ('Supervision') shall be amended as follows: "The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority."; (vi) Clause 17 of the 2021 C2C SCCs ('Governing law') shall be amended as follows: "These Clauses shall be governed by the law of one of the EU Member States, provided that such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland."; (vii) Clause 18(b) of the 2021 C2C SCCs ('Choice of forum and jurisdiction') shall be amended as follows: "The Parties agree that those shall be the courts with jurisdiction over the Agreement or the courts of Ireland.";

(b) UK GDPR, the 2021 C2C SCCs as amended by the UK Terms of the Jurisdiction Specific Addendum; and / or

(c) Swiss DP Laws, the 2021 C2C SCCs as amended by the Swiss Terms of the Jurisdiction Specific Addendum.

SCHEDULE 4

DETAILS REQUIRED FOR 2021 C2P SCCS

Annex I to Appendix of standard contractual clauses (schedule 4)

A. LIST OF PARTIES

Data exporter(s):

Name: The data exporter is the entity identified as "Customer" in the Agreement.

Address: The address for the Customer associated with the Services as specified in the Agreement.

Contact person's name, position and contact details: The contact details for the Customer, for notice purposes, associated with the Services as specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in part B of this Annex.

Signature and date: By agreeing to the terms of the DPA, the data exporter will be deemed to have signed this Annex.

Role (controller / processor): Controller

Data importer(s):

Name: The data importer is Digital Science.

Address: The address for Digital Science as specified in the Agreement.

Contact person's name, position and contact details: The contact details for Digital Science, for notice purposes, as specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in part B of this Annex.

Signature and date: By agreeing to the terms of the DPA, the data importer will be deemed to have signed this Annex.

Role (controller / processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data subjects are defined in Schedule 2 to the DPA.

Categories of personal data transferred

The personal data is defined in Schedule 2 to the DPA.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Digital Science does not knowingly process (and the Data Exporter has agreed not to submit to Digital Science for processing) any special categories of personal data (as defined under EU Data Protection Laws).

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

Personal data is transferred as and when required to provide the Services as may be initiated by the data exporter.

Nature of the processing

The nature of the processing is defined in Schedule 2 to the DPA.

Purpose(s) of the data transfer and further processing

The purpose of the transfer and processing is defined in Schedule 2 to the DPA.

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

During the term of the Agreement and the period of any post-termination obligations and/or rights relating to such personal data, or such shorter period as may be determined by the data exporter within the Services.

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

The involvement of sub-processors is described in clause 2.3 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

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

The Data Exporter's competent supervisory authority will be the authority that has competence (within the meaning of Article 55 and 56 of GDPR) over the data exporter.

Annex II to Appendix of standard contractual clauses (schedule 4)

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The technical and organisational security measures implemented by the data importer are as described in Schedule 2 of the DPA and other parts of the Agreement.

Additional Annex to Appendix of standard contractual clauses (schedule 4)

ADDITIONAL CLAUSES

The exclusions and limitations of liability provision of the Agreement are an additional clause pursuant to Clause 2 of these Clauses.

SCHEDULE 5

DETAILS REQUIRED FOR 2021 C2C SCCS

Annex I to Appendix of standard contractual clauses (schedule 5)

A. LIST OF PARTIES

Data exporter(s):

Name: The data exporter is Digital Science.

Address: The address for Digital Science as specified in the Agreement.

Contact person's name, position and contact details: The contact details for Digital Science, for notice purposes, as specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in part B of this Annex.

Signature and date: By agreeing to the terms of the DPA, the data importer will be deemed to have signed this Annex.

Role (controller / processor): Controller

Data importer(s):

Name: The data importer is the entity identified as "Customer" in the Agreement.

Address: The address for the Customer associated with the Services as specified in the Agreement.

Contact person's name, position and contact details: The contact details for the Customer, for notice purposes, associated with the Services as specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in part B of this Annex.

Signature and date: By agreeing to the terms of the DPA, the data exporter will be deemed to have signed this Annex.

Role (controller / processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The data subjects whose personal data may be included in the Data that is provided by Digital Science as part of the Services.

Categories of personal data transferred

Any of: name; contact information; supplementary identifiers (e.g. ORCID ID, institutional identifiers); basic professional information (e.g. job title, place of work/research/department); research-biography information (e.g. publication and affiliation history), in each case as is publicly available.

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None.

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

Continuous.

Nature of the processing

Digital Science will make Digital Science Controlled Data available to the Customer as part of providing the Services.

Purpose(s) of the data transfer and further processing

The purpose of the transfer is for the Customer to receive the Services and the purpose of any further processing is for the internal purposes of the Customer in accordance with 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

The period determined by the Agreement.

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

N/A

C. COMPETENT SUPERVISORY AUTHORITY

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

Ireland

Annex II to Appendix of standard contractual clauses (schedule 5)

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Contractual commitments as per the Agreement to keep the Data secure and confidential and to report any incidents of unauthorised use or other security breach.

Additional Annex to Appendix of standard contractual clauses (schedule 5)

ADDITIONAL CLAUSES

The exclusions and limitations of liability provisions of the Agreement are an additional clause pursuant to Clause 2 of these Clauses.