aptum

THIS DATA PROCESSOR ADDENDUM ("**Addendum**"), to the extent applicable, automatically forms part of the Agreement between you ("**Customer**") and the Aptum entity ("**Aptum**") providing you with the Services set forth in an Order.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them elsewhere in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

The terms and conditions set out below shall be added as an addendum to Agreement from the date that Aptum publishes this Addendum on its website. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Master Services Agreement, including documents referenced therein, such as the applicable Product Terms and the Order as amended by, and including, this Addendum.

PART A

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below:

1.1.1 "**Applicable Law**" means any laws or regulations, regulatory policies, guidelines or industry codes (whether national or international) which apply to Aptum (or any of its Sub-Processors) and/or the provision of or the subject matter of the Services in each case as in force from time to time;

1.1.2 "**Customer Group Member**" means Customer or any entity that owns or controls, is owned or controlled by or is or under common control or ownership with Customer, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Customer Personal Data**" means any Personal Data Processed by Aptum on behalf of a Customer Group Member pursuant to or in connection with the Agreement;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means the laws implementing or supplementing GDPR (or to the extent applicable EU Directive 95/46/EC, as transposed into domestic legislation of each Member State or the United Kingdom and as amended, replaced or superseded from time to time);

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Personal Data**" means any data that relates to an identified or identifiable natural person and where such data is protected under applicable Data Protection Laws;

1.1.9 "**Service/s**" means the services and other activities set forth in an Order to be supplied to or carried out by or on behalf of Aptum for Customer Group Members pursuant to the Agreement;

1.1.10 "**Standard Contractual Clause/s**" means the contractual clauses set out in Schedule B (incorporating the UK Addendum to the contractual clauses set out in Annex IV);

1.1.11 "**Subprocessor/s**" means any person (including any third party and any Aptum Affiliate) appointed by or on behalf of Aptum or any Aptum Affiliate and that Processes Customer Personal Data on behalf of any Customer Group Member in connection with the Agreement; and

1.1.12 "**Aptum Affiliate/s**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Aptum, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "**Commission**", "**Controller**", "**Processor**", "**Data Subject/s**", "**Member State**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Authority

Aptum warrants and represents that, before any Aptum Affiliate Processes any Customer Personal Data on behalf of any Customer Group Member, Aptum's entry into this Addendum as agent for and on behalf of that Aptum Affiliate will have been duly and effectively authorized (or subsequently ratified) by that Aptum Affiliate. References to 'Aptum' shall be deemed to include a reference to each Aptum Affiliate as applicable.

3. Processing of Customer Personal Data

3.1 Scope of this Addendum and Role of Parties. This Addendum applies to the Processing of Personal Data by Aptum in the course of providing the Services. For the Purposes of the Services and this Addendum, Customer and each Customer Group Member are the Controller(s) and Aptum is the Processor and shall be Processing Personal Data on the Customer's behalf, the Customer receiving the Services as principal and as agent of each Customer Group Member.

3.2 Instructions for Processing Personal Data. Aptum shall Process Personal Data as reasonably necessary for the provision of the Services arising from the Agreement (inclusive of this Addendum) and in accordance with Customer's documented instructions which, unless expressly agreed otherwise, shall at all times be consistent and in accordance with the nature of the Agreement. Aptum may terminate the Agreement if Customer provides instructions to Process Personal Data which are inconsistent with the Agreement, or which Aptum could not comply with without (i) incurring material additional costs or (ii) undertaking material variations to the manner in which the Services are provided which variations Aptum does not propose to introduce in respect of the majority of its other customers. Aptum may Process Personal Data otherwise than in accordance with Customer's instructions if required to do so by Applicable Law. In such case Aptum shall inform Customer of that legal requirement, unless prohibited from doing so by Applicable Law.

3.3 Compliance with Laws. Aptum, in Processing the Customer Personal Data in accordance with Clause 3.2 above, shall reasonably comply with all applicable Data Protection Laws. Aptum shall not be responsible for complying with Data Protection Laws applicable to Customer or its industry that are not otherwise consistent with the provision of the Services or if, and to the extent that, the relevant provision of Data Protection Law would not also apply to Aptum's provision of services equivalent to the Services to other customers. Customer shall comply with all Data Protection Laws applicable to Customer as Controller.

4. Aptum Personnel

4.1 Personnel Reliability. Aptum shall take reasonable steps to (i) require background screening and to ensure the reliability of any personnel who may have access to the Customer Personal Data or

the Customer environments in which the Personal Data is processed, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Customer Personal Data, as strictly necessary for the purposes of the Agreement; and (ii) ensuring that any personnel are informed of the confidential nature of Personal Data, have received training, and are subject to confidentiality obligations or professional or statutory obligations of confidentiality.

4.2 Data Protection Officer. Aptum have appointed a data protection officer. The appointed person may be reached at privacy@aptum.com or contracts@aptum.com

5. Sub-processors

5.1 Appointment of Subprocessors. Subject always to section 3.2 above, each Customer authorizes Aptum to appoint Subprocessors in accordance with this section 5 to Process Customer Personal Data. Aptum shall be responsible for ensuring that each Subprocessor has entered into a written agreement requiring the Subprocessor to comply with terms no less protective than those provided in this Addendum (a summary of such terms will be made available to Customer on request). Aptum shall be liable for the acts and omissions of any Subprocessor to the same extent as if the acts and omissions were performed by Aptum.

5.2 Notification of New Subprocessors. Aptum may continue to use those Subprocessors already engaged by Aptum or any Aptum Affiliate as at the date of this Addendum. Aptum shall notify Customer of any updates to the approved Subprocessors ("**Subprocessor Notice**") at least thirty (30) days prior to authorising any new Subprocessor to Process Personal Data.

5.3 Subprocessor Objection Right. This section 5.3 shall apply only where and to the extent that Customer is established within the EEA, United Kingdom, or where otherwise required by Data Protection Laws applicable to the Customer. In such an event, If Customer notifies Aptum in writing of any objections (on reasonable grounds) to a new Subprocessor within fourteen (14) days after the date of the applicable Subprocessor Notice:

5.3.1 Aptum shall work with Customer in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that Proposed Subprocessor; and

5.3.2 where such a change cannot be made and Aptum choose to retain the Subprocessor, Aptum shall notify Customer at least fourteen (14) days prior to the authorisation of the Subprocessor to Process Personal Data and the Customer may discontinue using the relevant Services and terminate the relevant portion of the Services which require the use of the Proposed Subprocessor immediately upon written notice to Aptum, such notice to be given by Customer within thirty (30) days of having been so notified by Aptum.

6. Support in Complying with Data Subject Rights

6.1 Requests from Data Subjects. Customer acknowledges, as part of the Services, it is responsible for responding to any Data Subjects' request under any Data Protection Law to exercise the Data Subject's right of access, right of rectification, restriction of Processing, right to be forgotten, data portability, object to processing, or its right not to be subjected to an automated decision making process ("**Data Subject Request**"). Aptum shall:

6.1.1 to the extent permitted by Applicable Law, promptly notify Customer if it receives a Data Subject Request from a Data Subject; and

6.1.2 taking into account the nature of the Processing, reasonably assist Customer to access Customer Personal Data to the extent that Customer Personal Data is not accessible to Customer (as part of the Services) to fulfill the Customer's obligations, as reasonably

understood by Customer, to respond to Data Subject Requests and to comply with Data Protection Laws.

6.2 Government and Law Enforcement Authority Requests. Unless prohibited by Applicable Law or a legally-binding request of law enforcement, Aptum shall promptly notify Customer of any request by government agency or law enforcement authority for access to or seizure of Personal Data.

7. **Breach Incident Notification.**

7.1 Breach notice. Aptum shall notify Customer within 24 hours upon Aptum becoming aware of a confirmed Personal Data Breach affecting Customer Personal Data. To the extent able within the scope of the Services, Aptum will provide Customer with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Investigatory Cooperation. Aptum shall co-operate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. **Security**

8.1 Technical and organisational measures. Aptum shall implement and maintain appropriate technical and organisational measures designed to protect the security, confidentiality and integrity of Customer Personal Data, including to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, such Personal Data as set forth in Schedule A. Aptum regularly monitors compliance with these measures. Aptum reserves the right to update its technical and organisational measures and will not materially decrease the overall security of the Services pursuant to the Agreement.

8.2 Audit. Customer agrees that Aptum's then-current attestation of compliance ("**AOC**") for SOC2 TYPE 2, ISO 27001 and/or PCI DSS (or comparable industry-standard successor reports), as applicable to the Services, will be used to satisfy any audit or inspection requests by or on behalf of the Customer, including any Customer Group Member arising from this Addendum, and at the Customer's written request, a copy of such AOC shall be provided to the Customer by Aptum. In the event that Customer, any Customer Group Member, a regulator, or Supervisory Authority requires additional information, including information necessary to demonstrate compliance with this Addendum, Aptum will provide commercially reasonable cooperation to make such information available.

8.3 Customer Applications. Customer acknowledges that if at any time it installs, uses or enables products or applications that operate using the Services, but are not part of the Service itself, then by such action Customer is instructing Aptum to cause the Service to allow such products or applications to operate and potentially access Personal Data. Accordingly, this Addendum does not apply to the processing of Personal Data by such products or applications.

8.4 Return and Deletion of Personal Data. Upon termination of the Services, Aptum shall at Customer's option, return and/or delete any Personal Data retained on the Services in accordance with the terms of the Agreement and not retain any copies unless Aptum is required to do so by Applicable Law.

9. Location and Storage of Personal Data. Personal Data will be stored at the data centre premises selected by Customer as part of the Services (the "**Designated Data Centre Location**").

10. **General Terms**

10.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 17 (Governing Law) of the Standard Contractual Clauses, or the applicability of any Data Protection Laws:

10.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

10.1.2 the obligations of Aptum and Aptum Affiliates arising hereunder are subject to and governed by the laws of the country or territory expressly set forth in the Agreement.

10.2 With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

10.3 Customer is responsible for coordinating all communication with Aptum on behalf of its Customer Group Members with regard to this Addendum. Customer represents that, in relation to this Addendum, it, as agent for its Customer Group Members, is authorized to issue instructions; make and receive any communications or notifications; and enter into any agreement expressly contemplated herein for and on behalf of any of its Customer Group Members.

10.4 Customer and/or its Customer Group Members may only disclose the terms of this Addendum to a Supervisory Authority to the extent required by law or such Supervisory Authority. Customer shall reasonably ensure that the Supervisory Authority does not disclose the terms of this Addendum to the public or any third party, including: (i) marking copies of this Addendum as "Confidential and Commercially Sensitive"; (ii) requesting return of copies of this Addendum once the governmental regulatory notification has been completed or approval granted; and (iii) requesting prior notice and consultation before any disclosure of this Addendum by the Supervisory Authority.

10.5 Aptum and/or Aptum Affiliates' aggregate liability to the Customer and/or any Customer Group Member, and to any relevant Controller on whose behalf the Customer enters into the Standard Contractual Clauses, arising from a breach of this Addendum (including the Standard Contractual Clauses) shall be subject to the terms of the Agreement and for this purpose references to the Customer in the Agreement shall be deemed to include a reference to the relevant Controller. Subject to the foregoing, no third party shall have any rights under this Addendum.

PART B

In addition to the terms set out in Part A above, the terms set out in this Part B shall apply to the Processing of Personal Data by Aptum on behalf of a Customer established in the European Union or otherwise subject to the requirements of the GDPR.

11. Additional European Terms.

11.1 General Data Protection Regulation. With effect from 25 May 2018, Aptum will Process any Personal Data in accordance with the requirements of GDPR as directly applicable to Aptum's provision of the Services.

11.2 Subject Matter, Nature, Purpose and Duration of Data Processing. Aptum will Process Customer Personal Data to provide the Services. The subject matter, nature and purpose of the Processing shall be as required to perform the Services and shall be determined by the nature of Customer Personal Data submitted for Processing by the Customer. The duration of the Processing of Personal Data shall be for the term of the Agreement.

11.3 Types of Personal Data and Categories of Data Subjects. The types of Personal Data and categories of Personal Data, and the categories of Data Subjects, shall be those determined by the Customer being the Customer Personal Data. The obligations and rights of the Customer in relation to the Processing of Personal Data shall be as set out in this Addendum and the Agreement and in the Data Protection Laws.

11.4 Data Protection Impact Assessment and Prior Consultation. Customer for itself and on behalf of each Customer Group Member agrees that Aptum's then-current SOC 2 TYPE 2, ISO 27001 and/or PCI DSS AOC (or comparable industry-standard successor AOC), together with Aptum's standard documented information about the Services, will be used to carry out Customer's data protection impact assessments and prior consultations, and Aptum shall make such AOC available to Customer. Aptum and each Aptum Affiliate shall provide reasonable assistance to each Customer Group Member with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of any Customer Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, Aptum. Customer shall ensure, to the extent that such data protection impact assessments and, where necessary, prior consultations with Supervisory Authorities, are required by Data Protection Laws, that Customer and relevant Customer Group Members take such steps as are required to implement such assessments and consultations. If, following the implementation of a data protection impact assessment or a consultation, Customer reasonably determines that it would be a breach of Data Protection Laws to continue with the Services, Customer shall notify Aptum, and the parties shall attempt to reach a solution. If the parties fail to agree a solution within thirty (30) days of commencing discussions, Customer shall be entitled to terminate the Services, subject to the payment of an early termination fee determined in accordance with the Agreement.

11.5 Access to Personal Data. Unless otherwise agreed and notwithstanding Section 9 above, in order to provide the Services Aptum and its Subprocessors will only access Personal Data from (i) countries in the EEA or (ii) countries or territories formally recognized by the European Commission as providing an adequate level of data protection ("**Adequate Countries**") unless Aptum makes available to Customer a Valid Transfer Mechanism in accordance with Section 11.6 below. When Aptum or its Subprocessors access Personal Data from outside the Designated Data Centre Location for the purposes of providing the Services, Customer agrees that such Personal Data may be transferred accordingly.

11.6 Valid Transfer Mechanisms. Aptum makes available the transfer mechanisms listed below, which shall apply, in order of precedence in the order set out below, to any transfers of Personal Data under this Addendum from countries within the European Economic Area (as constituted from time to time) or from Switzerland or the UK to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws of the foregoing territories (each known as a "third country"), to the extent such transfers are subject to such Data Protection Laws:

11.6.1 Country-specific arrangement. In the event that, after the date that this Addendum becomes effective, an alternative mechanism is approved under Data Protection Laws for the transfer of Personal Data to a specific third country, Aptum shall be entitled to rely upon this mechanism, subject to being able to demonstrate compliance with its requirements.

11.6.2 Standard Contractual Clauses. The Standard Contractual Clauses attached as Schedule B (inclusive of Annexes I, II, III & IV) to this Addendum, shall apply to the Services to the extent that any country-specific arrangement, cannot be relied upon.

11.6.3 Where formal recognition of an adequate level of data protection for a country or territory ends (e.g. due to temporary adequacy decisions or declaration of invalidity), the Standard

Contractual Clauses, as noted in clause 1.6.2 shall automatically apply to such data transfers.

12. Additional Terms

12.1 For the purposes of the Standard Contractual Clauses the parties agree that:

12.1.1 the descriptions in Annex I(B) and Annex III of the processing in respect of the Services are determined pursuant to clause 11 of this Addendum;

12.1.2 in respect of Annex II, Aptum shall implement and maintain the technical and organizational security measures set out in this Addendum;

12.1.3 in respect of Section II, Module Two and Module Three, Clause 9(a) (Use of sub-processors), Option 2 (General Written Authorisation) shall apply in respect of the appointment of any sub-processors to process any personal data; an Order placed by the Customer for Services provided by such sub-contractor shall be considered such General Written Authorisation and in all other cases the relevant timeframe for such General written Authorisation shall be 30 days;

12.1.4 in respect of Annex I(C), the competent supervisory authority shall be CNIL; and, for the purposes of Section IV, Clauses 17 and 18 of the SCCs, Option 1 shall apply and the Member State shall be France;

12.2 Without prejudice to the supplementary provisions set out in clause 12.1 of this Section, nothing in the Agreement (including this Addendum), is intended to vary or modify the Standard Contractual Clauses.

12.3 In the event that the Standard Contractual Clauses: (i) are deemed invalid by the European Commission, Supervisory Authorities or other competent data privacy authorities for whatever reason; or (ii) are superseded by other standard contractual clauses issued or approved by the European Commission, Supervisory Authorities or other competent data privacy authorities, the parties shall promptly comply with such other standard contractual clauses or any other valid mechanism under Data Protection Laws for transferring and processing Personal Data outside the EEA Area or the United Kingdom.

SCHEDULE A: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Aptum will maintain administrative, physical, and Technical Safeguards for the Protection of the security, confidentiality and integrity of Personal Data processed using the Services as described in the technical documentation made available with the Services. Specifically, Aptum's responsibility for technical and organisational measures shall extend to those controls outlined in its then-current SOC 2 TYPE 2, ISO 27001 and/or PCI DSS compliance documentation.

SCHEDULE B: STANDARD CONTRACTUAL CLAUSES

These Clauses are deemed to be amended from time to time to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with EU Data Protection Laws by the Commission to or of the equivalent contractual clauses approved by the Commission under the GDPR (or the EU Directive 95/46/EC to the extent applicable).

CONTROLLER TO PROCESSOR

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) 'The Appendix to these clauses containing the Annexes referred to therein forms an integral part of the Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms hall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the

data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive

data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (1) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall

submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION 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 [*Specify time period*] 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.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (2) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([3]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph I for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] 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.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic

society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (4);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of (*specify Member State*).]

[OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of (*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

aptum

ANNEX I: DETAILS

(A) LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: _____

Address: _____

Contact person's name, position and contact details: _____

Activities relevant to the data transferred under these Clauses:

Signature and date: _____

Role (controller/processor):

2. …

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: _____

Address: _____

Contact person's name, position and contact details: _____

Activities relevant to the data transferred under these Clauses:

Signature and date: _____

Role (controller/processor):

2. …

By entering into these Clauses we also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses set out in Annex IV.

(B) DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

…

Categories of personal data transferred

…

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

...

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

...

Nature of the processing

...

Purpose(s) of the data transfer and further processing

...

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

...

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

...

(C) COMPETENT SUPERVISORY AUTHORITY

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

...

ANNEX II: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organizational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organizational 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.

[Examples of possible measures:

Measures of organizational and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data organization

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

.....

ANNEX III: LIST OF SUB- PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. …

ANNEX IV: UK ADDENDUM TO THE STANDARD CONTRACTUAL CLAUSES

Date of this Addendum:

1. The Clauses are dated [INSERT DATE.] This Addendum is effective from:

   ~~Choose one option and delete the other:~~

   The same date as the Clauses.

   ~~[DATE]~~

Background:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

Interpretation of this Addendum

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

This Addendum	This Addendum to the Clauses.
The Annex	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
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	The United Kingdom 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	The United Kingdom of Great Britain and Northern Ireland.

4. This Addendum shall be read and interpreted in the light of the provisions of UK Data Protection Laws, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.

5. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws.

6. 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

7. In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

8. This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary, so they operate:

    (a) for 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 transfer; and

    (b) to provide appropriate safeguards for the transfers in accordance with Articles 46 of the UK GDPR Laws.

9. The amendments required by Section 7 above, include (without limitation):

    (a) References to the "Clauses" means this Addendum as it incorporates the Clauses

    (b) 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."

    (c) References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws. In particular:

        (i) i. [Deliberately left blank]

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

    (e) References to the "Union", "EU" and "EU Member State" are all replaced with the "UK"

    (f) Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Information Commissioner;

    (g) Clause 17 is replaced to state "These Clauses are governed by the laws of England and Wales".

    (h) Clause 18 is replaced to state:

"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."

        (i) The footnotes to the Clauses do not form part of the Addendum.

Amendments to this Addendum

10. The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.

11. The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Art 46 UK GDPR for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 7 above.

Executing this Addendum

12. The Parties may enter into the Addendum (incorporating the Clauses) in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in the Clauses. This includes (but is not limited to):

    (a) By adding this Addendum to the Clauses and including in the following above the signatures in Annex 1A:

    "By signing we agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated:" and add the date (where all transfers are under the Addendum)

    "By signing we also agree to be bound by the UK Addendum to the EU Commission Standard Contractual Clauses dated" and add the date (where there are transfers both under the Clauses and under the Addendum)

    (or words to the same effect) and executing the Clauses; or

    (b) By amending the Clauses in accordance with this Addendum and executing those amended Clauses.