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means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;**

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 indentifiable 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;**

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 make available to Customer through Aptum's customer website a list of Subprocessors authorized to Process Customer Personal Data ("Subprocessor List") and provide Customer with a mechanism to obtain notice of any updates to the Subprocessor List ("Subprocessor Notice"). At least thirty (30) days prior to authorising any new Subprocessor to Process Personal Data, Aptum shall provide notice by updating the Subprocessor List.***

5.3 ***Subprocessor Objection Right. This section 5.3 shall apply only where and to the extent that Customer is established within the EEA 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 Subprocessor added to the Subprocessor List 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 SOC1 TYPE 2 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 9 (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 1 TYPE 2 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, (ii) countries or territories formally recognized by the European Commission as providing an adequate level of data protection ("Adequate Countries") and (iii) the United States provided, in this case, that 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 Switzerland 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 ***Privacy Shield. Aptum (US) Inc. self-certifies with the EU – U.S. Privacy Shield Framework, as administered by the US Department of Commerce, and Aptum shall ensure that it maintains this self-certification to and compliance with the EU – U.S. Privacy Shield Framework with respect to the processing of Personal Data that is transferred from the European Economic Area to the United States. Aptum (US) Inc.'s self-certification applies to the Services to the extent that they are delivered by Aptum (US) Inc as a Aptum Affiliate.***

11.6.2 ***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.***

11.6.3 **Standard Contractual Clauses. The Standard Contractual Clauses attached as Schedule B (inclusive of Appendices 1 & 2) to this Addendum, together with the sections in PART C of this Addendum below, shall otherwise apply to the Services to the extent that Aptum (US) Inc.'s Privacy Shield Framework self-certification, or any subsequently approved country-specific arrangement, cannot be relied upon.**

11.7 ***Transfers Required by Applicable Law. Notwithstanding the foregoing, Aptum shall be entitled to access Personal Data from, or transfer Personal Data to, territories outside the EEA other than in the circumstances specified in clause 11.6 if required to do so by***

Applicable Law. Unless prohibited by Applicable Law, Aptum shall inform Customer of the requirement for such transfer or access before taking steps to implement the transfer or access.

12. Additional Terms for Standard Contractual Clauses.

12.1 **Entities. The Standard Contractual Clauses apply (i) to the entity that has executed the Standard Contractual Clauses as the Data Exporter and its Affiliates established within the European Economic Area and Switzerland that utilize the Services. For the purposes of the Standard Contractual Clauses such entities shall be deemed "Data Exporters". Where the Customer is itself a Processor of the Customer Personal Data, the Customer warrants that it is entering into the Standard Contractual Clauses with the authority of, and as agent for, the relevant Controller.**

12.2 **Audits. For the purposes of Clause 5 (f) of the Standard Contractual Clauses, Data Importer agrees to provide the audit information in accordance with Section 11.2 above.**

12.3 **Subprocessors. For the purposes of clause 11 of the Standard Contractual Clauses, Customer consents to Aptum appointing sub-processors in accordance with Section 5 above.**

12.4 **Return and Deletion of Personal Data. For the purposes of Clause 12 (1) of the Standard Contractual Clauses, Aptum shall return and delete Data Exporter's data in accordance with the Agreement.**

12.5 **Conflict. The parties agree nothing in this Addendum is intended to modify or amend the Standard Contractual Clauses. In the event of a conflict between the terms of this Addendum or the Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall apply in precedence.**

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 1 TYPE 2 and/or PCI DSS compliance documentation.

A high-level summary of controls provided by Aptum by service-type, is provided further below:

	Colocation	Connectivity	Dedicated Hosting	Managed hosting	Cloud
Organisational management and dedicated staff responsible for the development and implementation of Cogeco Peer 1's security program.	x	x	x	x	x
Internal/External audit and risk assessment procedures for the purposes of periodic assesment of risks to Cogeco Peer 1's organisation and delivery of services.	x	x	x	x	x
Physical and evironmental security of data centres, server room facilities and other areas containing Customer Personal Data are designed to protect from unauthorised access, monitor and log movement of persons in the data centre environment (e.g. biomteric security) and guard against enviromental hazards such as heat, fire or water damage.	x	x	x	x	x
Data Centres are designed with redundancy and controls to maintain continuity and availability of services during emergency situations.	x	x	x	x	x
Incident/problem management procedures designed to enable Cogeco Peer 1 to respond to and mitigate events impacting Cogeco Peer 1's technology, services and information assets.	x	x	x	x	x
Change Management procedures designed to test, approve and monitor all changes to Cogeco Peer 1's technology and information assets and Services.	x	x	x	x	x
Network Security Controls that provide for the use of enterprise firewalls and layered DMZ architechtures, intrusion detection systems and event correlation procedures designed to protect systems from intrusion and limit the scope of any attack.		x	x	x	x
System audit and event logging of internal systems used to deliver Services (excludes event logging for customer systems).	x		x	x	x
Operational procedures and controls to provide for monitoring and maintenance of customer environment technology and systems, and Cogeco Internal Systems, used to deliver Services according to prescribed internal and adopted industry standards, including secure disposal of media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal by Cogeco Peer 1.			x	x	x
Vunerability assessment and threat protection for Cogeco Peer 1's internal systems designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code and/or actors.	x	x	x	x	x
Password policies and controls designed to manage password complexity and security applicable to Cogeco Peer 1's internal systems used to deliver the Services.	x	x	x	x	x
Logical segregation of Cogeco Peer 1 data systems and records used to deliver the Services to ensure data can be restricted and controlled.	x	x	x	x	x
Logical access controls designed to manage electronic access to data and system functionality based on role and authority (need-to-know and least privilige basis).	x	x	x	x	x

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 EU Directive 95/46/EC or the GDPR.

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization: the Customer

……

(the data **exporter**)

And

Name of the data importing organization: Aptum (including the relevant Aptum Affiliate)

……

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in

which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations

of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is:

Customer or, where Customer is itself a Processor of the Customer Personal Data and has been given authority to enter into the Standard Contractual Clauses on behalf of the Controller for whom the Customer is acting as Processor, that Controller

Data importer

The data importer is:

Aptum (including the relevant Aptum Affiliate)

Data subjects

The personal data transferred concern the following categories of data subjects:

Determined pursuant to clause 11 of this Addendum

Categories of data

The personal data transferred concern the following categories of data:

Determined pursuant to clause 11 of this Addendum

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

Determined pursuant to clause 11 of this Addendum

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Determined pursuant to clause 11 of this Addendum

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The technical and organizational measures are outlined in Schedule A to this Addendum.