Data Processing Addendum
Version Date: April 2026

This Data Processing Addendum (this "**DPA**") is subject to and hereby incorporates by reference the terms and conditions of the Agreement. Capitalized terms used, but not defined, herein shall have the meaning given to them in the Agreement.

To the extent the Offerings (as defined in the Agreement) are subject to the GDPR (defined below), the terms of this DPA shall apply to such Offerings. In the event of a conflict between the terms in this DPA and any other terms in the Agreement, the following order of precedence shall apply: (i) the Standard Contractual Clauses and/or the UK Addendum (as applicable) shall prevail over this DPA and the Agreement solely with respect to the subject matter of such clauses; (ii) this DPA shall prevail over the Agreement solely with respect to the Parties' data processing obligations outlined herein; and (iii) the Agreement shall prevail in all other respects.

1. Definitions

"**Client Instance**" means any version of the data processing equipment or system owned or under the control of Instem used to Process Personal Data that the Client has access to and that has been configured according to the Client's requirements.

"**Client System**" means any information technology system or systems owned or operated by the Client from which Personal Data is received in accordance with this DPA.

"**Controller**" means the natural or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("**GDPR**") and any implementing laws or regulations, the UK Data Protection Act of 2018 or any other applicable privacy and data protection legislation or regulations applicable to Instem's Processing of Personal Data under the Agreement. Any capitalized terms relating data protection herein, if not defined in this DPA or in the Agreement, take the definitions provided in the Data Protection Laws.

"**Data Subject**" means an identified or identifiable (whether directly or indirectly) natural person to whom the Personal Data relates.

"**Personal Data**" means the information described in Attachment 1 to this DPA or which otherwise identifies or may be used to identify a Data Subject that Instem Processes in providing the Offerings.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or the unauthorized disclosure of or access to, Personal Data transmitted, stored or otherwise Processed.

"**Processing**", "**Process**", "**Processed**" and "**Processes**" means any operation or set of operations performed upon Personal Data, whether or not by automatic means, including, but not limited to, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction.

"**Processor**" means a natural or legal person which Processes Personal Data on behalf of a Controller.

"**Specific Instructions**" means instructions for the Processing of Personal Data given by or on behalf of the Client to Instem, including configuration of the Client Instance and any support services that Instem provides to the Client.

"**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses annexed to the European Commission's decision 2021/914 of June 4, 2021, on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

"**Subprocessor**" means (a) an Instem Affiliate, when Instem is Processing Personal Data, (b) Instem, when Instem is Processing Personal Data and where Client is itself a Processor of such Personal Data, (c) any third-party Processor engaged by Instem to Process Personal Data in order to provide the Offerings to Client.

"**UK Addendum**" means the International Data Transfer Addendum to the Standard Contractual Clauses issued by the United Kingdom's Information Commissioner Office and effective as of March 21, 2022.

2. Background

2.1 Client and Instem have entered into the Agreement for the provision of the Offerings to Client. In providing the Offerings, Instem may from time to time engage on behalf of Client, in the Processing of Personal Data submitted to and stored within the Offerings by Client or third parties with whom Client transacts using the Offerings.

2.2 To the extent that any Personal Data is being Processed on any Client Instance, it is the Client, and not Instem, who determines the purposes for which it is Processed, and the Client, and not Instem, which determines the configuration of the Client Instance.

2.3 The Client, as Controller or Processor of its customer's Personal Data, acknowledges that it is the Client's responsibility to ensure that the configuration of its Client Instance(s) including, but not limited to, non-transient storage, deletion, amendment, blocking, erasure, unauthorized transmission, and transfer to third countries is such that it remains compliant with Data Protection Laws.

2.4 Client (a) acknowledges and agrees that it is the Controller of all Personal Data or Processor of its customers' Personal Data provided by Client to Instem (in the course of Client's use of the Offerings or otherwise) and (b) hereby appoints Instem as a Processor of such Personal Data, or as Subprocessor of such Personal Data when Client is the Processor of its customers' Personal Data.

3. Client Data and Processing of Personal Data

3.1 Instem shall:

3.1.1 only Process Personal Data in accordance with Client's or its Affiliates relevant Specific Instructions unless Processing is required by Data Protection Laws to which Instem is subject, in which case Instem shall, to the extent permitted by applicable law, inform the Client of that legal requirement before the relevant Processing of that Personal Data;

3.1.2 inform the Client without undue delay upon becoming aware of any instructions given by the Client that infringe applicable Data Protection Laws; provided, however, that Instem is under no duty to investigate the completeness, accuracy or sufficiency of any Specific Instructions or Client Data; and

3.1.3 implement appropriate technical and organizational measures in a manner such that Processing will meet the requirements of the GDPR and ensure the protection of the rights and freedoms of the Data Subject.

3.2 The subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data, and the categories of Data Subjects are set forth in this DPA and Attachment 1.

3.3 Processing by Instem and its Affiliates shall be governed by this DPA and any applicable Data Protection Laws.

3.4 Client acknowledges that Instem is under no duty to investigate the completeness, accuracy or sufficiency of any Specific Instructions or Client Data.

3.5 Client warrants and represents that it is and will at all relevant times have the authority and lawful basis to provide Personal Data and to give the Specific Instructions set out in Section 3.1.1. Client shall have obtained all necessary consents, or shall have established an alternative lawful basis or bases, for the Processing of Personal Data by Instem in accordance with the Agreement.

4. Security

4.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Instem shall, in relation to Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR and Attachment 2.

4.2 Instem shall notify Client without undue delay after becoming aware of a Personal Data Breach, and upon Client's written request, provide Client with all cooperation and assistance reasonably requested by Client to enable Client or if applicable its customer (as the Controller) to notify the relevant supervisory authority and relevant Data Subject(s) of the Personal Data Breach (as applicable).

4.3 Client agrees that, as Controller (or, if applicable, as its customer's Processor) it is itself (or with its customer) responsible for ensuring compliance with Data Protection Laws, and that it will design, implement and operate the Client Systems accordingly and, as Processor (including as Processor for Instem's Personal Data shared with the Client), protect and Process such Personal Data in compliance with the applicable Data Protection Laws.

5. Data Subject Rights

5.1 Taking into account the nature of the Processing, Instem and its Affiliates shall assist Client by implementing appropriate technical and organizational measures for the fulfilment of Client's and Client Affiliates' (or, if applicable, their clients') obligations to respond to requests by Data Subjects to exercise their rights of access, rectification or erasure, to restrict or object to Processing of Personal Data, or to data portability.

5.2 In the event a Data Subject makes a request to Instem to exercise any of the rights referred to in Section 5.1, Instem shall refer the requestor to Client promptly and, upon Client's (or if applicable its customer's) written request, provide Client (or if applicable its customer) with cooperation and assistance requested by Client in relation to that request to enable Client (or if applicable its customer) to respond to that request in compliance with applicable deadlines.

6. Subprocessing

6.1 Subprocessing for the purpose of this DPA is to be understood as a service which relates directly to the provision of the principal obligation related to the Processing of Personal Data pursuant to the Agreement. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services, or the disposal of data carriers, or other measures to ensure the confidentiality, availability, integrity, and resilience of Instem's hardware or software.

6.2 Client authorizes Instem to engage any Affiliate, and any third-party subcontractors as Subprocessors in connection with the provision of the Offerings to Client. The parties agree that (a) Instem shall maintain and make available to Client an up-to-date list of its Subprocessors, giving Client notice of any change in Subprocessors prior to any new Subprocessor being authorized to Process any Personal Data by updating the list accordingly; (b) Instem shall impose written data protection terms on any Subprocessor it appoints requiring such Subprocessor to Process any Personal Data to the extent necessary to provide the Offerings and to protect Personal Data to at least the standard required by this DPA and Data Protection Laws. Instem shall remain liable for any breach of this DPA that is caused by an act, error or omission of its Subprocessor.

6.3 If Client (acting reasonably) objects to a new Subprocessor on grounds related to the protection of Personal Data only, then without prejudice to any right to terminate the Agreement, Client may request that Instem move the Personal Data to another Subprocessor and Instem shall, if possible, within a reasonable time following receipt of such request, use reasonable measures to accommodate such request. If it is not reasonably possible to use another Subprocessor, and Client continues to object for a legitimate reason, either party may terminate the Agreement without additional liability upon thirty (30) days advance written notice. If Client does not object within thirty (30) days of Instem's notice, Client will be deemed to have accepted the new Subprocessor.

6.4 Client agrees that any Subprocessors may access Client Instance so that Instem can deliver the Offerings under the Agreement. Client further agrees that those Subprocessors may be based outside of the location in which Client has chosen to store Personal Data, subject to Instem taking steps to ensure transfer protections, to the extent required by applicable Data Protection Laws.

7. **International Transfers**

7.1 Client acknowledges that Instem and its Sub-processors may Process Personal Data in countries that are outside of the European Economic Area ("**EEA**"), United Kingdom, and Switzerland ("**European Countries**"). This will apply even if Client has agreed with Instem to host Personal Data in the EEA, if Processing in such non-European Countries is necessary to provide support-related or other services requested by Client. If Personal Data is transferred to a country or territory outside of European Countries, then such transfer will only take place if: (a) the country ensures an adequate level of data protection; or (b) one of the conditions listed in Article 46 GDPR (or its equivalent under any successor legislation) is satisfied.

7.2 To the extent Client's use of the Offerings requires an onward transfer mechanism to lawfully transfer Personal Data from a jurisdiction (i.e., the EEA, the United Kingdom, Switzerland) to Instem or any of its Affiliates located outside of that jurisdiction ("**Transfer Mechanisms**"), the following terms will apply:

7.2.1 In the event the Offerings are covered by more than one Transfer Mechanism, the transfer of Personal Data will be subject to a single Transfer Mechanism in accordance with the UK Addendum and/or the Standard Contractual Clauses as set forth in Section 7.2.2 (UK Addendum), Section 7.2.3 (SCCs), or Section 7.2.4 (Switzerland Data Transfers) of this DPA; and, if neither is applicable, then other applicable data Transfer Mechanisms permitted under Data Protection Laws.

7.2.2 **UK Addendum**. If UK Data Protection Laws (including the UK GDPR and Data Protection Act 2018) govern the export or Processing of Personal Data outside the UK, and reliance on the UK Addendum is lawfully permitted for transfers to Processors, the UK Addendum applies between Client and Instem as follows:

(a) when and as applicable, Client and any applicable Affiliates are each the data exporter, then Client's signing of an Order and/or SOW, or a Client's Affiliate signing an Order and/or SOW, shall be treated as signing of the UK Addendum; Instem's signature of an Order and/or SOW shall be treated as Instem's and any applicable Instem's Affiliates signing of the UK Addendum; the parties shall comply with the UK Addendum, and the UK Addendum shall be deemed incorporated into this DPA; and in the event of a conflict between the UK Addendum and the SCCs, the UK Addendum shall control;

(b) the completed SCCs, as set out below in Section 7.2.3, shall apply to transfers of such Personal Data, as amended in accordance with the UK Addendum in respect of the transfer of such Personal Data;

(c) Table 1 of the UK Addendum shall be deemed completed with the information set out in Attachment 1 to this DPA;

(d) Table 2 of the UK Addendum shall be deemed completed as follows: the SCCs with only the following modules, clauses or optional provisions of the SCCs brought into effect for the purposes of the UK Addendum; Module Two (Controller to Processor) of the SCCs will apply where Client is a Controller of Personal Data and Instem is Processing Personal Data; Module Three (Processor to Processor) of the SCCs will apply where Client is a Processor of Personal Data and Instem is Processing Personal Data; Clause 7 of the SCCs, the optional docking clause will not apply; Clause 9 of the SCCs, Option 2 will apply and the time period for prior notice of Subprocessor changes will be as set forth in Section 6.3; Clause 11 of the SCCs, the optional language will not apply; and no Personal Data is collected by Processor on behalf of Controller;

(e) Table 3 of the UK Addendum shall be deemed completed as follows: Annex 1A and Annex 1B shall be deemed completed as set forth in Attachment 1 to this DPA; Annex II shall be deemed completed as set forth in Attachment 2 to DPA; Annex III shall be deemed completed as set forth in Section 6.2; and

(f) in Table 4 of the UK Addendum, approval of both parties is required to end the UK Addendum as set out in Section 19 of the UK Addendum.

7.2.3 **Standard Contractual Clauses**. When and as applicable, Client and any applicable Affiliates are each the data exporter, then Client's signing of an Order and/or SOW, or a Client's Affiliate signing of an Order and/or SOW, shall be treated as the signing of the SCCs and their Annexes. Instem's signature of an Order and/or SOW shall be treated as the signing of the SCCs and their Annexes. The parties shall comply with the SCCs and the SCCs shall be deemed incorporated into this DPA. The parties agree that the SCCs will apply to Personal Data that is transferred via the Offerings from the European Economic Area or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA that are subject to the SCCs, the SCCs will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

(a) Module Two (Controller to Processor) of the SCCs will apply where Client is a Controller of Personal Data and Instem is Processing Personal Data.

(b) Module Three (Processor to Processor) of the SCCs will apply where Client is a Processor of Personal Data and Instem is Processing Personal Data.

(c) For each Module, where applicable:

(i) in Clause 7 of the SCCs, the optional docking clause will not apply;

(ii) in Clause 8.3 of the SCCs, on request by a Data Subject, the Client may make a copy of the SCCs, available to the Data Subject in accordance with Clause 8.3. Client shall not make the entirety of this DPA available but a copy of the SCCs (including the relevant Schedules of this DPA) only. Client shall make commercially reasonable efforts to consult Instem in order to redact the SCCs and/or the relevant Schedules of this DPA to the extent necessary to protect Instem's business secrets or other Confidential Information, prior to sharing them with the Data Subject. The parties shall make good faith efforts to coordinate the response to the Data Subject regarding the reasons for the redactions, to the extent possible without revealing the redacted information;

(iii) in Clause 8.4 of the SCCs, Instem will provide assistance to Client to erase or rectify inaccurate Personal Data in accordance with Clause 8.4, by providing appropriate technical and organizational measures, where possible through the Instem Offerings and/or as outlined in the Documentation;

(iv) in Clause 8.6 of the SCCs, Instem shall comply with its obligations under Clause 8.6(c) and 8.6(d) by providing reasonable commercial assistance to the Client in relation to a Personal Data Breach, taking into account the nature of the Processing and the information available to Instem. Instem conducts regular checks of the technical and organisational measures required by Clause 8.6 in the form of an annual audit;

(v) in Clause 8.9 of the SCCs, audits pursuant to Clause 8.9 shall be carried out in accordance with Section 8;

(vi) in Clause 9 of the SCCs (Option 2) the time period for prior notice of Subprocessor changes will be as set forth in Section 6.3;

(vii) in Clause 11 of the SCCs, the optional language will not apply;

(viii) in Clause 12, any claims brought under the SCCs shall be subject to the terms and conditions set forth in the Agreement, including the limitations of liability in Section 13 thereof. In no event shall any party limit its liability with respect to any Data Subject rights under the SCCs where such limitation is prohibited by Data Protection Laws;

(ix) in Clause 17 (Option 1), the SCCs will be governed by Irish law;

(x) in Clause 18(b) of the SCCs, disputes will be resolved before the courts of Dublin, Ireland;

(xi) in Annex I of the SCCs shall be deemed completed with the information set out in Attachment 1 to this DPA; and

(xii) in Annex II of the SCCs shall be deemed completed with the information set out in Attachment 2 to this DPA.

7.2.4 **Switzerland Data Transfers**. To the extent an adequate transfer safeguard is required for the transfer of customer Personal Data subject to the Swiss data protection laws, the parties agree to be bound by the SCCs, which are amended to reflect corresponding Swiss legislation and Swiss competent authorities as appropriate, including the following amendments (such 2021 EU SCCs being hereinafter described as the "**Swiss SCCs**"):

(a) The following definitions are included in the SCCs prior to their Section 1: "**Swiss FADP**": the Swiss Federal Act of 19 June 1992 on Data Protection, the Ordinance to the Swiss Federal Act on Data Protection and the revised Swiss Federal Act of 25 September 2020 on Data Protection which comes into force on 1 January 2023; and "**the Switzerland 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 Switzerland, including the Swiss FADP;

(b) References to "Regulation (EU) 2016/679" OR "That Regulation" are replaced by "Switzerland Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of Swiss data protection laws;

(c) References to Regulation (EU) 2018/1725 are removed;

(d) References to the "Union", "EU" and "EU Member State" are all replaced with "Switzerland";

(e) The Supervisory Authority selected for the purposes of Clause 13 (Supervision) of the Swiss SCCs is the Swiss Federal Data Protection and Information Commissioner (FDPIC); and

(f) Clause 17 (Governing law) of the Swiss SCCs shall refer to the laws of Switzerland as the governing law of the Swiss SCCs and Clause 18 (Choice of forum and jurisdiction) shall refer to the Swiss courts as the proper forum and jurisdiction for disputes and legal proceedings arising under the Swiss SCCs.

7.3 Where any mechanism for cross-border transfers of Personal Data is found by a supervisory authority, court of competent jurisdiction or other governmental authority to be an invalid means of complying with the restrictions on transferring Personal Data to a third country or territory as set out in Data Protection Laws, the parties shall act in good faith to agree to the implementation of an alternative solution to enable Client to comply with the provisions of Data Protection Laws in respect of any such transfer.

8. **Assessments**

8.1 Subject to the terms of the Agreement and upon Client's request with not less than 30 days' notice, and not more than once in a 12-month period, Client may provide Instem with an information security questionnaire for Instem to complete (at Client's expense) so that Client may perform an assessment to determine Instem's compliance with its security obligations set forth under this DPA. Such questionnaire shall be limited to the security aspects of those data centers where the server(s) on which Personal Data is located reside and those **Offerings** that the Client is using under the Agreement. Such scope does not include any documentation, data or other information related to other customers of the data center or Instem, or that could otherwise pose a risk to the **Offerings**, as determined by Instem or the data center in their sole discretion.

9. **Termination/Expiry**

9.1 Instem shall:

9.1.1 unless expressly stated otherwise in the Agreement, upon termination or expiration of the Agreement, promptly cease to use the Personal Data and shall, subject to Section 14.4.1 of the Agreement (Client Data Retrieval), at Client's option, return the Personal Data to Client or delete the Personal Data and all copies and extracts of the Personal Data (and shall procure same from its Affiliates).

9.1.2 retain Personal Data only to the extent and for such period as required by applicable law, provided that Instem, Instem's Affiliates, and its and their employees shall ensure the confidentiality of all such Personal Data, and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable law requiring its storage, and for no other purpose.

9.1.3 on expiry or termination of the Agreement (however arising) the provisions of this Section 9 shall survive and continue in full force and effect.

9.2 This DPA, the UK Addendum, and the SCCs will terminate with the termination or expiration of the applicable Order and/or SOW, or as set forth in Section 9.1.

9.3 Instem may terminate the UK Addendum and/or SCCs if Instem offers alternative mechanisms to Client that comply with Data Protection Laws to transfer of Personal Data outside the EEA, UK or Switzerland.

10. **Indemnification and Liability**

10.1 Each party shall indemnify and hold harmless the other party and its Affiliates, employees, and agents, for all costs, damages, or losses incurred in connection with claims, demands, or proceedings by a Data Subject or any other third party, and/or any associated financial penalties imposed by supervisory or regulatory authorities, arising from any breach by the indemnifying party of its obligations under Sections 3, 4 and 5, the UK Addendum, and the SCCs. The indemnification procedures set forth in Section 12.3 of the Agreement shall apply to indemnification claims under this Section 10.

10.2 The indemnification obligations set forth in this Section 10 shall be the parties' sole and exclusive indemnification obligations relating to or arising from any breach of this DPA.

10.3 This DPA, the UK Addendum, and the SCCs, and any liability arising hereunder, are subject to the limitations of liability set forth in Section 13 of the Agreement (including, without limitation, the disclaimers of indirect damages in Section 13.1 and the limitations on direct damages in Section 13.2). For the avoidance of doubt, (a) Client acknowledges and agrees that Instem's total aggregate liability for all claims from Client or its Affiliates arising out of or related to the Agreement and this DPA shall apply in aggregate for all claims under both the Agreement and this DPA and shall not exceed the limits specified in Section 13 of the Agreement, and (b) this Section shall not be construed as limiting the liability of either party with respect to claims brought by Data Subjects where such limitations are prohibited by applicable Data Protection Laws or conflict with the exclusions set forth in Section 13.3 of the Agreement.

10.4 Neither Instem nor its Affiliates shall be liable for any claim brought by Client or any third party (including without limitation any Data Subject, or regulatory or supervisory authority) arising from its or their compliance with Client's instructions.

10.5 The indemnifying party shall not enter into any settlement without the indemnified party's express prior written consent that (a) assigns, imparts or imputes fault or responsibility to the indemnified party or its Affiliates, (b) includes a consent to an injunction or similar relief or otherwise imposes any obligation binding upon the indemnified party or its Affiliates, or (c) provides for relief other than monetary damages covered by the indemnity.

11. **Governing Law**

11.1 This DPA shall be governed by and construed in accordance with Section 16.5 of the Agreement, except where the Standard Contractual Clauses or UK Addendum mandate a different governing law solely for the specific data transfers they cover.

ATTACHMENT 1: DETAILS OF PROCESSING OF PERSONAL DATA

List of Parties

Data Exporter:

- **Name:** Client (or any applicable Client Affiliate) is the Controller and the exporter under the Standard Contractual Clauses
- **Address:** As specified in the Agreement
- **Contact person's name, position and contact details:** As specified in the Agreement or relevant Transaction Document
- **Signature and date:** Execution of the relevant Transaction Document incorporating the Agreement and this DPA constitutes signature.
- **Role (controller/processor):** Controller (or Processor, where Client acts as Processor for its customers)

Data Importer:

- **Name:** Instem LSS Limited (or the Instem Affiliate signatory to the relevant Transaction Document)
- **Address:** Diamond Way, Stone Business Park, Stone, Staffordshire, ST15 0SD, England (or as specified for the relevant Instem Affiliate)
- **Contact person's name, position and contact details:** Nathan Rowley, CIPP/E, QA Manager, Global Data Protection Compliance Manager, nathan.rowley@instem.com
- **Signature and date:** Execution of the relevant Transaction Document incorporating the Agreement and this DPA constitutes signature.
- **Role (controller/processor):** Processor (or Subprocessor, where Client acts as Processor)

Personal Data

- **Data Subjects:** Client, business partners, employees, consultants, vendors, clinical trial participants, patients, healthcare professionals, or other individuals whose Personal Data Client inputs into the Offerings.
- **Data Categories:** Name, title, contact information (address, email, telephone number, etc.), username, password, professional details, system usage data, study/trial related data, health information (if input by Client into relevant Offerings), other categories as determined and controlled by Client.
- **Special Categories:** May include health data, genetic data, biometric data, racial or ethnic origin, etc., if processed by Client using the Offerings. Client is responsible for ensuring a lawful basis for processing any special category data.

Additional Information Regarding Data Transfers (where the Standard Contractual Clauses apply)

- **Activities relevant to the data transferred under SCCs:** Instem Processes Personal Data as necessary to provide the Offerings subscribed to by Client under the Agreement and applicable Transaction Documents. The specific activities are determined by the functionality of the subscribed Offerings and Client's configuration and use thereof.
- **Frequency of the Transfer:** Continuous, based on Client's use of the Offerings.
- **Duration of Processing:** Instem is authorized to Process Personal Data for the duration of the applicable subscription term(s) under the Agreement and any post-termination retrieval period specified in the Agreement (Section 14.4.1).
- **Nature of Processing:** Personal Data will be subject to Processing activities necessary for Instem to provide, maintain, secure, and support the Offerings pursuant to the Agreement, including hosting, storage, retrieval, analysis (as directed by Client via the Offerings), backup, technical support, and troubleshooting.
- **Purpose of Processing:** Personal Data will be Processed by Processor for the purposes of providing the Offerings as set out in the Agreement and enabling Client's use of such Offerings for its internal business operations.
- **Criteria for determining how long the Personal Data will be retained:** For the duration specified above, subject to Section 9 of this DPA and Section 14.4.1 of the Agreement.
- **For transfers to Subprocessors:** subject matter, nature and duration of the Processing: As necessary for the Subprocessor to provide its specific service contributing to the overall Offerings, for the duration required to provide such service, as described in Section 6 of this DPA.
- **Competent Supervisory Authority:** The competent supervisory authority will be the applicable data protection authority determined in accordance with the SCCs or UK Addendum (e.g., typically where the Data Exporter is established, or as specified in the SCCs/UK Addendum).

ATTACHMENT 2: SECURITY STANDARDS

Instem has developed and implemented a broad range of security measures included within their Quality Management System (QMS), which are regularly reviewed and tested. The following summary sets out broad categories of those measures.

- **Personnel**
  - application to employees and contractors, and privacy awareness training
  - ongoing monitoring and training; record keeping
  - accessibility of Client Data by employees and contractors based on role and need-to-know
- **Data Handling**
  - replication of stored data for availability
  - Client Data archiving procedures
  - encryption for data in transit and at rest: as considered appropriate by Instem based on risk
  - policy for handling Client Data in physical form (minimization)
- **Vulnerabilities**
  - communication channels monitoring for security vulnerabilities
- **Change Management**
  - change management review process
  - prioritized patch management policy
  - installation of security patches
- **Access Control**
  - limits on physical and logical access to systems processing Client Data
- **User Roles**
  - user roles control access privileges
- **Password Policy**
  - internal password complexity and lifecycle policy
  - guidance on client password policy configuration within Offerings
  - connectivity requirements (e.g., secure protocols)
  - multiple security layers and services (e.g., firewalls, intrusion detection/prevention where applicable)
  - audit logging capabilities within Offerings
- **Data Center Environment and Physical Security**
  - review and evaluation of third-party data center security procedures and premises (for hosted services)
  - security measures for internal premises where applicable
- **Continuity Management**
  - business continuity and disaster recovery internal practices and procedures
- **Development and Testing**
  - test and development activities policy (e.g., separation from production)
  - minimization of security risks in software development practices (e.g., secure coding guidelines)
  - security review of the source code
  - annual security vulnerability training for developers