Sapio Sciences, LLC – Data Processing Agreement Addendum

This Data Processing Agreement Addendum (DPA) serves as the DPA for the Services (as defined in the Master Services Agreement [MSA]) performed by Sapio Sciences, LLC ("Sapio") for the Client defined in the applicable MSA. The current version of this DPA may be located at: sapiosciences.com/privacy/dpa.

In rendering the Services, Sapio may be provided with, or have access to, information of the Client which may qualify as Personal Data within the meaning of the 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, and repealing Directive 95/46/EC ("GDPR"), or the UK-GDPR. Parties agree that when Sapio receives these types of data, the terms of this DPA apply.

All definitions herein will be applied as defined by GDPR.

1. **Processing Details**

   Sapio will process Client Personal Data for the services described in the Master Services Agreement. For Processing services described in the MSA, Client serves as the Data Controller ("Controller") and Sapio serves as the Data Processor ("Processor").

   When Sapio processes business-to-business (B2B) data in order to provide services, it serves as the Controller of the data.

   When there are differences in this DPA Addendum due to Sapio's role of Controller or Processor, they will be noted.

1.1. **Retention Period**

   Sapio as Processor: The retention period of Processing when Sapio serves as Processor, will be for the period of time described in the MSA. Sapio will securely delete any Client Personal Data after and consistent with the duration of Processing defined in the MSA.

   Sapio as Controller: The retention period of Processing when Sapio serves as Controller (i.e., of B2B data), is defined in its Retention Policy, and as per applicable laws.

1.2 Nature of Processing

   Sapio as Processor: Sapio processes data on the Client's instruction. Processing includes collection, use, analysis, storage, and deletion, as required in order to perform the Services set out in the MSA.

   Sapio as Controller: Processing includes collection, use, analysis, and deletion.

1.3 Data Subjects

Sapio as Processor: Client defines its data subjects when it serves as Controller.

Sapio as Controller: Client's employees and representatives are the data subjects.

1.4 Types of Personal Data

Sapio as Processor: Sapio's software is intended to collect the data necessary to accomplish a Client's LIMS and ELN goals. Personal data may include name, title, email, and Protected Health Information (PHI) in some clinical instances. Given the nature of the services, Client acknowledges that Sapio is not able to review data provided by Client to determine whether it contains additional special categories of Personal Data, as defined by Article 9, of GDPR.

Sapio as Controller: Sapio processes Client's B2B Personal Data in order to provide its services. Examples include name and professional contact information.

2. Processor Obligations

2.1. Sapio is required to process the Personal Data on behalf of the Controller only and in accordance with the documented instructions given by the Controller, unless otherwise required by applicable data protection law to which Sapio is subject; in such a case, Sapio shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.2. Sapio must ensure that persons authorized to process the Personal Data on behalf of the Controller, in particular Sapio 's employees, as well as employees of any Subprocessors, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that such persons who have access to the Personal Data, process such Personal Data in compliance with the Controller's instructions.

2.3. Sapio must implement the technical and organizational measures as described in Section 6 before processing the Personal Data on behalf of the Controller.

2.4. Sapio is required to make available to the Controller any information necessary to demonstrate compliance with the obligations of Sapio relating to information security as required by applicable data protection law and by this DPA. Sapio is required to allow for and contribute to audits (e.g., providing audit reports to Controller upon Controller's request) or on-site inspections, conducted by the Controller or another auditor appointed by the Controller. Such audits are limited to once per year, unless for-cause, with reasonable notice.

2.5. Sapio is required to notify the Controller without undue delay about a Data Breach at Sapio or its Subprocessors after it becomes aware of such a Data Breach, and in such case Sapio will assist the Controller with the Controller's obligations under applicable data protection law to inform the data subjects and the supervisory authorities, as applicable, by providing the necessary information taking into account the nature of the processing and the information available to Sapio.

2.6. Sapio shall cooperate with the Controller and take reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Data Breach.

2.7. Sapio shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with supervising authorities or other competent data privacy authorities, which Controller reasonably considers to be required 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 Controller Personal Data by, and taking into account the nature of the processing and information available to Sapio.

2.8. Sapio is required - at the choice of the Controller - to delete or return to the Controller all Personal Data which are processed by Sapio on behalf of the Controller under this DPA after the end of the provision of the Services, and delete any existing copies unless applicable data protection law requires Sapio to retain such Personal Data.

2.9. Sapio is required to provide to the Controller the respective information on records of processing activities relating to the Services under this DPA, to the extent necessary for Sapio to comply with its obligation to maintain records of processing or to meet any other Controller obligation under GDPR or applicable data protection laws.

2.10. Sapio shall designate a data protection officer and/or representatives, to the extent required by applicable data protection law. Sapio must provide contact details of the data protection officer and/or representatives, if any, to the Controller.

2.11. Sapio shall immediately inform the Controller if, in its opinion, an instruction infringes any applicable data protection provisions.

3. Data Subject Rights – *Sapio as Processor*

3.1. Sapio shall assist the Controller, especially through appropriate technical and organizational measures, insofar as this is possible, with the fulfilment of the Controller's obligation to comply with the rights of the data subjects and respond to data subjects' requests relating to their rights of (i) access, (ii) rectification, (iii) erasure, (iv) restriction of processing, (v) data portability, and (vi) objection to processing.

3.2. The Controller maintains the responsibility to determine whether or not a data subject has a right to exercise any such data subject rights and to give instructions to Sapio and to what extent the assistance is required.

3.3. Sapio shall not respond to any request (excluding acknowledgement of request receipt, which is permitted) except on the documented instructions of Controller or as required by applicable laws to which Sapio is subject, in which case Sapio shall, to the extent permitted by applicable laws, inform Controller of that legal requirement before responding to the request.

4. Subprocessing

4.1. Sapio, when acting as Processor, uses a limited number of third-party providers (subprocessors) to assist in providing consulting and hosting services.

4.2. Sapio's subprocessors are as follows:

- AWS Hosting: AWS Privacy
- Google Analytics: Google Privacy
- Stripe: Stripe Privacy
- Netsuite (by Oracle): Netsuite Privacy

4.3 Sapio shall not engage any subprocessor without previously informing the Controller and obtaining the Controller's prior written consent. This includes informing the Controller of any intended changes or replacements of subprocessors.

4.4 Sapio shall enter into a written contract with any subprocessor and such agreement shall impose upon the subprocessor the same obligations as imposed by this DPA upon Sapio, to the extent applicable to the subcontracted Services.

4.5 Where the subprocessor fails to fulfil its data protection obligations, Sapio shall remain fully liable to the Controller for the performance of the subprocessor's obligations.

5. Data Transfers

5.1. Sapio may not transfer or authorize the transfer of Personal Data to countries not covered by GDPR or provided with an adequacy decision, without the prior written consent of Controller. If Personal Data processed under this DPA is transferred from a GDPR-covered country to a country that is not a GDPR-covered country or a country with an adequacy decision, the Parties shall ensure that the Personal Data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on Sapio's participation in the EU-US Data Privacy Framework (including the UK-US Extension).

6. Security

6.1. 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, Sapio shall, in relation to the Controller 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.

6.2. In assessing the appropriate level of security, Sapio shall take account in particular of the risks that are presented by processing, in particular the risk from a Personal Data breach.

6.3. Client Personal Data is encrypted when Sapio provides the hosting. This data is in the control of the Controller when it installs Sapio on premises within their own administrator-controlled environments.

6.4. For Technical and Organizational Measures when Sapio serves as the Controller or Processor of the data, see Annex II of the Standard Contractual Clauses.

7. Data Protection Officer

7.1. Client is responsible for providing complete, accurate, and updated information about its Data Protection Officer, if applicable, by contacting privacy@sapio.com.

7.2. Sapio's Data Protection Officer, Sean Blake, can be contacted at privacy@sapio.com.

8. Other Provisions

8.1. The Parties are required to comply with those obligations under the GDPR and under any other applicable data protection laws that apply, as applicable, to the Client in its role as Controller or to Sapio in its role as Processor, or Controller, depending on the type of data processed. Nothing in this DPA relieves the either party of its own direct responsibilities under GDPR or any other applicable data protection laws.

8.2. Notwithstanding anything contrary in the MSA, Sapio will indemnify and hold harmless Client, its affiliates, and its and their clients, officers, directors, employee, agents, and representatives (each an "Indemnified Party") from and against all third-party loss, harm, cost (including reasonable legal fees and expenses), expense, fines, and liability that an Indemnified Party may suffer or incur as a result of Sapio's non-compliance with the requirements of this DPA.

8.3. This DPA shall be governed by the same law as the MSA except as otherwise stipulated by applicable data protection law. The place of jurisdiction for all disputes regarding this DPA shall be as determined by the MSA except as otherwise stipulated by applicable data protection law.

8.4. In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in other such agreements related to the Parties' data protection obligations, this DPA shall prevail.

8.5. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or – should this not be possible – (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omission.