Sapio Sciences, LLC – Data Processing Agreement Addendum

This Data Processing Agreement Addendum ("DPA") serves as the DPA to the written agreement (the "MSA") between Sapio Sciences, LLC ("Sapio") and the Customer defined in the applicable MSA (the "Customer") that references this DPA, including for the Services (as defined in the MSA) provided under the 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 Customer which may qualify as Personal Data within the meaning of applicable Data Protection Law, meaning all laws, rules, regulations, and orders that apply to the performance of the Services under the MSA and relating in any way to data protection, privacy, security, and breach notification, which may include, but are not limited to, those enacted within the United States of America and any state therein, as well as the EU General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council including implementing or supplementing laws ("GDPR"), or the UK-GDPR. The Parties agree that when Sapio receives Personal Data, to the extent required by applicable Data Protection Law, the terms of this DPA apply.

For purposes of this DPA, all capitalized terms defined herein shall have the meaning ascribed to them. Capitalized terms not defined herein shall have the meaning given them in applicable Data Protection Law.

1. Processing Details

Sapio will Process Customer Personal Data for the Services described in the MSA. The specific business purpose for which Sapio Processes Personal Data on the Controller's behalf is Sapio's performance of the Services described in the MSA. For Processing Services described in the MSA, Customer serves as the Data Controller ("Controller") and Sapio serves as the Data Processor or Service Provider ("Processor").

When Sapio Processes business-to-business (B2B) Personal Data in order to provide Services, it serves as the Controller of the data.

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

1.1 Retention Period

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

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

1.2 Nature of Processing

Sapio as Processor: Sapio Processes Personal Data on the Customer'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: When Sapio Processes Personal Data as Controller, Processing includes collection, use, analysis, and deletion as set forth in Sapio's Privacy Notice (https://www.sapiosciences.com/privacy/).

1.3 **Data Subjects**

Sapio as Processor: Customer defines its data subjects when it serves as Controller.
Sapio as Controller: Customer'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 Customer's LIMS and ELN goals. Personal Data may include name, title, email, and Protected Health Information (PHI) in some clinical instances. When Personal Data includes PHI, and Sapio acts as a business associate in connection with Processing the Personal Data, Customer shall not provide PHI without Sapio's prior written consent and the parties will enter into a separate Business Associate Agreement as and to the extent required under HIPAA. Given the nature of the Services, Customer acknowledges that Sapio is not able to review data provided by Customer to determine whether it contains additional special categories of Personal Data, as defined by applicable Data Protection Law, including Article 9 of GDPR.

Sapio as Controller: Sapio processes Customer's B2B Personal Data in order to provide its Services. Examples of such Personal Data include name and professional contact information.

Aggregated Statistics: Notwithstanding anything contrary in the MSA or this DPA, Sapio shall have the right to collect and analyze information relating to the provision, use and performance of various aspects of the Services and related systems and technologies; provided that any information concerning Personal Data shall be used on an aggregated and de-identified basis ("Aggregated Statistics"). Notwithstanding anything to the contrary in the MSA or this DPA, Sapio will be free during and after the term of this DPA to (i) use such Aggregated Statistics internally to improve and enhance the Services and for other development, operational, diagnostic and corrective purposes in connection with the Services and other Sapio offerings, and for such other purposes as permitted by law; and (ii) disclose such Aggregated Statistics and data solely in aggregate and de-identified form unless otherwise required by law. No rights or licenses are granted except as expressly set forth herein. For clarity, the Aggregated Statistics do not constitute Personal Data.

2. Processor Obligations

2.1 Sapio, as Processor, will Process the Personal Data on behalf of the Controller only on 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 Without limiting any terms set forth in the MSA or this DPA, Sapio shall not:

i. Sell or share the Personal Data (as such terms are defined in applicable Data Protection Law, including California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. Seq., including as modified by the California Privacy Rights Act ("CPRA"), together with any implementing regulations);
ii. Retain, use, or disclose the Personal Data outside of the direct relationship between Sapio and the Controller;
iii. Retain, use, or disclose the Personal Data for any other purpose than the specified business purpose in the MSA or this DPA; or
iv. Combine the Personal Data that Sapio receives from the Controller with Personal Data Sapio receives or collects through other means.

2.3 Sapio will 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.

2.4 Sapio agrees to implement appropriate and reasonable technical and organizational measures as described in Section 6 before Processing the Personal Data on behalf of the Controller.

2.5 Upon receipt of reasonable written notice, Sapio will make available to the Controller sufficient information necessary to demonstrate compliance with the obligations of Sapio relating to information security as required by applicable Data Protection Law. Sapio will cooperate in all reasonable respects with audits or on-site inspections, conducted by the Controller or another auditor appointed by the Controller during normal business hours and pertaining to Sapio's performance under and compliance with the MSA and DPA. Such audits are limited to once every twelve (12) months, unless otherwise required by applicable Data Protection Law.

2.6 Sapio will notify the Controller without undue delay of a Data Breach at Sapio or its Subprocessors after it discovers such a Data Breach, and in such case Sapio will assist the Controller in all reasonable respects with the Controller's obligations under applicable Data Protection Law by providing the necessary information taking into account the nature of the processing and the information available to Sapio.

2.7 Sapio agrees to cooperate with the Controller and take commercially reasonable steps to assist in the investigation, mitigation and remediation of each such Data Breach.

2.8 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.

2.9 Upon notice and subject to the requirements of the MSA and this DPA, the Controller may take reasonable and appropriate steps to help ensure that Sapio processes the Personal Data received from the Controller in a manner consistent with Sapio's obligations under applicable Data Protection Law, and may also take reasonable and appropriate steps to stop and remediate any unauthorized use of the Personal Data by Sapio.

2.10 Sapio will destroy 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 destroy any existing copies unless applicable Data Protection Law requires Sapio to retain such Personal Data.

2.11 Sapio will provide to the Controller information on Sapio's records of processing activities relating to the Services, to the extent necessary for Sapio to comply with its obligation to maintain records of processing.

2.12 Sapio will designate a data protection officer and/or representatives, to the extent required by applicable Data Protection Law. Sapio will provide contact details of the data protection officer and/or representatives, if any, to the Controller.

2.13 Sapio will immediately inform the Controller if, in its opinion, an instruction infringes any applicable data protection provisions, or if it makes a determination that it can no longer meet its obligations under applicable Data Protection Law.

3. Data Subject Rights – *Sapio as Processor*

3.1 Sapio will assist the Controller, 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 as set forth under applicable Data Protection Law 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 will 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 Data Protection Law to which Sapio is subject, in which case Sapio will, to the extent permitted by applicable Data Protection Law, inform Controller of that legal requirement before responding to the request.

4. Subprocessing

4.1 Sapio, when acting as Processor, and pursuant to Controller's express general written authorization by entering into the MSA and this DPA, uses a limited number of third-party providers ("Subprocessors") to assist in providing 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 will inform the Controller of any intended changes concerning the addition or replacement of other Subprocessors, giving the Controller the opportunity to object to such changes.

4.4 Sapio will enter into a written contract with any Subprocessor which will 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 fulfill 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 from a GDPR-covered country to a country not covered by GDPR and which has not been provided with an adequacy decision, without the prior written consent of Controller unless Sapio implements appropriate cross-border transfer mechanisms between the parties, including, but not limited to standard contractual clauses or participation in the EU-US Data Privacy Framework. If Personal Data Processed under this DPA is transferred from a GDPR-covered country to a country that is not a GDPR-covered country and which has not been provided 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) or through the use of standard contractual clauses.

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 will, in relation to the Controller Personal Data, implement appropriate technical and organizational measures designed to ensure a level of security appropriate to that risk, including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR.

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

6.3 Customer 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 Customer 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 Law that apply, as applicable, to the Customer in its role as Controller or to Sapio in its role as Processor, or Controller, depending on the type of Personal Data processed. Nothing in this DPA relieves the either party of its own direct responsibilities under GDPR or any other applicable Data Protection Law.

8.2 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.

8.3 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.

8.4 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.