ATTACHMENT A: Terms and Conditions for Processing European Personal Data

If Vendor is processing European Personal Data on behalf of Cold Spring Harbor Laboratory ("CSHL"), Vendor agrees to be bound by the provisions of this Attachment A.

1. General

1.1 "European Personal Data" means any information that relates to a specific natural person who resides in the European Economic Area ("EEA") and who can be identified, directly or indirectly, such as by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.2 The processing of European Personal Data is subject to various data protection and privacy legal, regulatory, and contractual requirements (collectively "Applicable Data Protection Requirements"), including without limitation under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009; the Standard Contractual Clauses set out by the EU Commission Decision of 5 February 2010 (2010/87/EU) and the EU Commission Decision of 27 December 2004 (2004/915/EC) (collectively, the "EU Standard Contractual Clauses"); and any applicable European Union or Member State law relating to data protection or the privacy of individuals.

2. Data Protection

2.1 For purposes of this Attachment A, the following is set forth in Schedule 1: (i) the duration of the processing; (ii) the subject matter, nature, and purpose of the processing; (iii) the types of European Personal Data processed; and (iv) the categories of data subjects.

2.2 Each Party undertakes to comply with all Applicable Data Protection Requirements applicable to it and will not knowingly cause the other to breach Applicable Data Protection Requirements.

2.3 CSHL will be the controller and Vendor will be the processor regarding the European Personal Data processed by Vendor on CSHL's behalf under the Purchase Order.

2.4 Vendor will, and will ensure that any of its employees or agents will, only process European Personal Data in accordance with the Purchase Order, this Attachment A, and CSHL's instructions. If Vendor is legally required by European Union or European Member State law to process European Personal Data otherwise than as instructed by CSHL, it will notify CSHL before such processing occurs, unless the law requiring such processing prohibits Vendor from notifying CSHL on an important ground of public interest, in which case it will notify CSHL as soon as that law permits it to do so.

2.5 Vendor will: (i) implement and document appropriate physical, technical and organizational measures that are no less rigorous than accepted industry practices to protect European Personal Data against accidental or unlawful destruction, alteration, and unauthorized disclosure or access; and (ii) maintain and materially comply with a comprehensive written privacy and information security program designed to protect European Personal Data against reasonably foreseeable risks of unauthorized processing, including policies and procedures demonstrating that European Personal Data will be used and disclosed only as provided in this Purchase Order.

2.6 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 risks to the rights and freedoms of individual data subjects, Vendor agrees that the technical, organizational, and physical controls to protect European Personal Data will include, where appropriate: (i) the pseudonymization and encryption of European Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to European Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. In assessing the appropriate level of security, Vendor will take account of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to European Personal Data transmitted, stored or otherwise processed.

2.7 Vendor agrees to take reasonable steps to ensure that its personnel who have access to European Personal Data are both (i) informed of the confidential nature of the European Personal Data and required to keep such European Personal Data confidential; and (ii) aware of and in compliance with Vendor's duties and their personal duties and obligations under this Purchase Order.

2.8 Vendor will use commercially reasonable efforts to (i) assist CSHL with the fulfillment of CSHL's obligation to respond to requests for exercising the data subject's rights as set out in Applicable Data Protection Requirements; (ii) assist CSHL in ensuring compliance with Applicable Data Protection Requirements, including obligations to investigate, remediate, and provide information to regulators or data subjects about Security Incidents without undue delay, to carry out privacy impact assessments and to consult with regulators regarding processing that is the subject of a privacy impact assessment; (iii) make available all information necessary to demonstrate compliance with Applicable Data Protection Requirements; and (iv) allow for and contribute to audits, including inspections and information requests conducted by CSHL or an auditor mandated by CSHL. Vendor will promptly notify CSHL about any instruction from CSHL that, in Vendor's opinion, infringes Applicable Data Protection Requirements.

2.9 Upon termination, cancellation, expiration or other conclusion of the Purchase Order, Vendor shall return to CSHL or, if return is not feasible, destroy all European Personal Data in whatever form or medium that Vendor received from or created on behalf of CSHL, unless Applicable Data Protection Requirements prevent Vendor from returning or destroying all or part of the European Personal Data. This provision also applies to all European Personal Data that is in the possession of subcontractors or agents of Vendor.

2.10 Vendor will not subcontract any of its processing operations under this Purchase Order unless: (i) it has obtained the prior written consent of CSHL to do so; and (ii) the subcontractor is subject to a written agreement that imposes the same obligations on that subcontractor as are imposed on Vendor under this Attachment A of the Purchase Order. Vendor will remain fully liable to CSHL for any subcontractors' processing of European Personal Data under the Purchase Order.

2.11 Vendor will not transfer or permit the transfer of any of the European Personal Data across international borders without explicit written consent of CSHL and, where the recipient of the data is located outside the EEA, a legally compliant transfer mechanism. To the extent that the provision of goods or services under the Purchase Order, including by Vendor, involves the transfer of European Personal Data outside the EEA (either directly or via onward transfer) to any country or recipient that has not been recognized by the European Commission as offering an adequate level of protection for personal data transferred to it from the EEA, Vendor provides either (i) to comply with the EU Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries approved by European Commission Decision of February 5, 2010 ("EU Standard Contractual Clauses"), as included in Schedule 2, or any applicable successor clauses approved by the European Commission, where for the purposes of the EU Standard Contractual Clauses CSHL is the "data exporter" and Vendor is the "data importer," and for the purposes of Clauses 9 and 11(3) the law of the data exporter is the law of the Member State in which CSHL's representative is established; or (ii) that where Vendor has provided CSHL with a current and valid Privacy Shield certification, it warrants that it will maintain an active and valid certification with the EU-U.S. Privacy Shield Framework ("Privacy Shield"), and will process the European Personal Data in accordance with both that certification and the Privacy Shield Principles.

Schedule 1

Details of the processing activities

This Schedule forms part of the Processing Agreement and must be completed and signed by the parties.

Data subjects

The Personal Data concerns the following categories of data subjects (please specify):

[To be completed based on the specific agreement.]

Categories of data

The Personal Data concerns the following categories of data (please specify):

[To be completed based on the specific agreement.]

Special categories of data (if appropriate)

The Personal Data concerns the following special categories of data (please specify):

[To be completed based on the specific agreement.]

Processing operations

The Personal Data will be subject to the following basic processing activities (please specify):

[To be completed based on the specific agreement.]

Duration

The Personal Data will be processed by Vendor for the duration of the Services.

Schedule 2

Standard Contractual Clauses (processors)

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 and must be completed and signed by the parties.

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

The contents of Schedule 1 to the Agreement shall also form Appendix 1 to these Clauses

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

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

[Vendor/Data Processor to Provide details of the level of security applied to Personal Data.]