OLINK DATA PROCESSING ADDENDUM

THIS OLINK DATA PROCESSING ADDENDUM ("DPA"), including all exhibits and attachments hereto, is dated as of the effective date as identified on the initial agreement by and between (i) the customer agreeing to these terms (the "Customer") and (ii) **Olink Proteomics AB**, a Swedish corporation with a main office at Salagatan 16F, SE-753 30, Sweden, acting on its own and as an agent for **Olink Proteomics Inc**., with its registered address at 130 Turner St., Building 2, Suite 230, Waltham, MA 02453 (the "Company", "Olink", "Processor" or "Service Provider").

Customer and Olink are herein collectively referred to as the "Parties" or each individually as the "Party".

WHEREAS, the Customer and Olink have entered into a primary written services agreement and/or any other relevant written agreement such as a Statement of Work ("SOW"), and any applicable documents incorporated by reference therein (the "Agreement") which involves the Processing of Personal Data of individuals subject to Applicable Data Protection Legislation.

WHEREAS, The Parties have agreed to enter into the Agreement and have the power to alter, amend, revoke, or terminate the Agreement as provided in the Agreement and this DPA is incorporated by reference into the Agreement.

NOW, THEREFORE, the Parties agree as follows:

1. BACKGROUND

1.1 This DPA governs the Processing of Personal Data subject to Applicable Data Protection Legislation including but not limited to the regulation 2016/679 General Data Protection Regulation ("GDPR"), the UK GDPR and Data Protection Act 2018; the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"), each as applicable, for the services provided in the Agreement.

1.2 Where Olink Processes Personal Data of individuals subject to Applicable Data Protection Legislation, Olink has agreed to the jurisdiction specific terms set forth in Attachment 4.

1.3 The Parties agree that the terms of this DPA supersede and replace any existing privacy and data protection terms previously concluded between the Parties.

1.4 The terms used in this DPA have the meaning set forth in this DPA. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement. Attachments 1 through 4 form an integral part of this DPA.

1.5 In the event of any conflict between the Agreement and this DPA, the provisions of this DPA shall prevail. This is without prejudice to the order of precedence between the Jurisdiction Specific Terms referenced in Attachment 4, the Standard Contractual Clauses in Section 13, and any other provision in this DPA.

2. DEFINITIONS. The following terms have the meanings set out below for this DPA:

2.1 "**Affiliate**" means (a) with respect to a Party, any corporation, company, partnership, joint venture and/or firm which controls, is controlled by or is under common control with such Party; and (b)

"Control" means (i) in the case of corporate entities, direct or indirect ownership of more than percent (50%) of the stock or shares having the right to vote for the election of directors (or such lesser percentage that is the maximum allowed under Applicable Law to be owned by a foreign corporation in a particular jurisdiction); and (ii) in the case of non-corporate entities, the direct or indirect power to manage, direct or cause the direction of the management and policies of the non-corporate entity or the power to elect more than fifty percent (50%) of the members of the governing body of such non-corporate entity. Affiliates of Olink specifically include, but are not limited to, as applicable, Olink Proteomics AB and Olink Proteomics Inc.

2.2 "**Applicable Data Protection Legislation**" means all laws and regulations related to the protection of individuals with regards to the Parties' processing of personal data under the Agreement including, but not limited to, the regulation 2016/679 General Data Protection Regulation ("GDPR"), the UK GDPR and Data Protection Act 2018; the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA"); each as applicable.

2.3 "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

2.4 "**Data Subject Rights**" means all rights available to individuals under Applicable Data Protection Legislation, which may include the right to know, to access, to request rectification or erasure, the rights relating to portability, restrictions on Processing, and objection to the Processing including the right to withdraw consent, among others.

2.5 "**Personal Data**" (or "**Personal Information**") means any information relating to an identified or identifiable natural person ("**Data Subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.6 "**Processor**" means the entity which processes personal data on behalf of the controller.

2.7 "**Processing of Personal Data**" (or "**Processing/Process**") mean any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

2.8 "**Security Incident**" means a confirmed or reasonably suspected security incident involving accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, or other unauthorized Processing of Personal Data

2.9 "**Sensitive Data**" means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, as well as any other information or combinations of information that falls within the definition of "special categories of data" under GDPR (as defined above) or any other Applicable Data Protection Legislation.

2.10 "**Sub-Processor**" means any natural person, legal entity or any other organization engaged by Olink to Process Personal Data on behalf of the Customer pursuant to the instructions of the Customer as set forth in the Agreement.

2.11 "**UK GDPR**" means the GDPR as incorporated into United Kingdom law pursuant to the European Union (Withdrawal) Act 2018 and as amended by the United Kingdom Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and any successor laws, as applicable.

3 SCOPE

3.1 This DPA applies to the Processing of Personal Data under the Agreement, regardless of country of origin, place of Processing, location of Data Subjects, or any other factor to the extent that such Processing falls under the material and territorial scope of the Applicable Data Protection Legislation.

4 REPRESENTATIONS, WARRANTIES AND COVENANTS.

4.1 Compliance with Applicable Data Protection Legislation. Each Party represents, warrants and agrees to comply with Applicable Data Protection Legislation when Processing Personal Data in the context of the Agreement, and that they will perform their obligations under this DPA in compliance with Applicable Data Protection Legislation. Customer is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Legislation in its own Processing of Personal Data and (b) it has, and will continue to have, the right to transfer, or provide access to, Personal Data to Olink for processing in accordance with the terms of the Agreement and this DPA.

4.2 Relationship: Customer and Olink agree that with regard to the Processing of Personal Data, Customer acts as a Controller and Olink is a Processor, except when Customer acts as a Processor of Personal Data, in which case Olink is a Sub-Processor. Olink will Process Personal Data on Customer's behalf to provide the services as specified in the Agreement and this DPA. Olink is prohibited from Processing Personal Data for any other purpose, in particular from selling any Personal Data, and does not share Personal Data with third parties for compensation or for those third parties' own business interests.

5 PROCESSING OF PERSONAL DATA

5.1 Olink, as Processor or Sub-Processor, undertakes to Process Personal Data only in accordance with documented instructions from Customer to provide the services as stated in the Agreement and this DPA, Attachment 3, which further sets forth the subject-matter and duration of the processing, the nature and purpose of the processing, the types of Personal Data and categories of data subjects.

5.2 Customer confirms that the Agreement and this DPA, including its attachments, constitute the complete instructions to be followed by Olink for the processing of Personal Data. Customer will ensure that its instructions comply with Applicable Data Protection Legislation. Additional instructions outside the scope of the Agreement or this DPA, shall, in order to be valid, be documented in writing and signed by both Parties, including any additional fees that may be payable by Customer to Olink for carrying out such additional instructions. The Customer is required to not, without such written agreement, allow Processor to Process other categories of Personal Data, or to Process Personal Data about other categories of Data Subjects than specified in Attachment 3.

5.3 Customer is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Legislation in its use of the services and its own Processing of Personal Data and (b) it has, and will continue to have, the right to transfer, or provide access to,

Personal Data to Olink for processing in accordance with the terms of the Agreement and this DPA.

5.4 Olink shall without undue delay inform Customer if Processor believes that Customer's instructions regarding the Processing of Personal Data are in violation of Applicable Data Protection Legislation, and Processor shall suspend the Processing until the Customer confirms the lawfulness of the instruction in writing.

5.5 Olink shall, to the extent required by Applicable Data Protection Legislation and in accordance with Customer's written instructions in each case, assist Customer in fulfilling its obligations under Applicable Data Protection Legislation.

6 SECURITY OF PROCESSING AND CONFIDENTIALITY

6.1 Olink shall take reasonable technical and organizational measures to ensure the confidentiality, integrity, availability and resilience of Olink systems used for Processing Personal Data and protect against the unlawful destruction, loss, encryption, alteration, unauthorized disclosure of or access to Personal Data transmitted, stored or otherwise Processed. Without limiting the generality of the foregoing, such measures shall include the security measures set out in Attachment 1.

6.2 Olink shall take steps to ensure that any person acting under its authority, including its Sub-Processor, who has access to Personal Data is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only Processes Personal Data in accordance with this DPA and Applicable Data Protection Legislation.

6.3 If a competent court or other legal authority requests information from Olink regarding the Processing of Personal Data, Olink shall inform the Customer thereof without undue delay. Olink may not act in any way on behalf of the Customer or as its agent and may not transfer or otherwise disclose Personal Data to third parties without the prior consent of Customer, unless otherwise required by applicable law or pursuant to a non-appealable decision by a competent court or other legal authority.

6.4 If, in accordance with applicable law, Olink is requested to disclose Personal Data Processed by Processor on behalf of Customer, Olink shall promptly notify Customer thereof, unless otherwise provided by applicable law or pursuant to a decision by a competent court or other legal authority, and in connection with the disclosure request that the Personal Data be given confidential treatment.

7 SECURITY BREACH AND INCIDENT RESPONSE

7.1 Olink shall notify Customer without undue delay after having become reasonably aware of a Security Incident under Olink's direct control or upon Olink being notified of a Security Incident under the direct control of a Sub-Processor, providing Customer with the requisite known information as per the Applicable Data Protection Legislation.

7.2 Taking into account the nature of processing and the information available to the Processor, Olink shall cooperate with the Customer and take all reasonable steps to assist Customer with complying with its own obligations under Applicable Data Protection Legislation relating to information security and personal data breaches, including information reasonably required to fulfil Customer's obligation to report or notify a relevant data protection authority of other governmental authority.

7.3 Olink shall take all reasonable measures to prevent, mitigate, investigate, and/or remediate the potential adverse effects of the Security Incident.

8 USE OF SUB PROCESSORS

8.1 Customer provides general authorization to Olink to appoint (and permit each Sub-Processor appointed in accordance with this section to appoint) Sub-Processors in accordance with this Section 8 and as otherwise set out in the Agreement, as the case may be.

8.2 Olink may continue to use those Sub-Processors already engaged by Olink as of the effective date of this DPA, subject to Processor meeting the obligations set out in this Section 8. Olink's existing Sub-Processors are set forth in Attachment 2.

8.3 If Olink intends to hire a new Sub-Processor or replace an existing Sub-Processor to Process Personal Data covered by this DPA, Olink shall provide timely written notice of the appointment or replacement of any Sub-Processor to the Customer by email not less than thirty (30) days in advance. Customer may object to such changes provided such objections are made in writing without undue delay from receipt of the notification and based on reasonable grounds relating to data protection. The Customer's written objection to any Sub-Processor must specify the grounds on which the objection is based.

8.4 If Customer objects on reasonable grounds relating to data protection to the use of a proposed Sub-Processor and Processor, despite Controllers objection, wants to hire the proposed Sub-Processor, Processor shall notify Customer no later than fourteen (14) days after receipt of Customer's written objection. Upon receipt of such notice, Customer is entitled to suspend or terminate the Agreement in accordance with the termination provisions in the Agreement. If the Customer's objection to the use of a Sub-Processor is not justified on reasonable grounds related to data protection, the Customer is not entitled to terminate the Agreement.

8.5 With respect to each Sub-Processor, Olink shall ensure that Sub-Processors are bound by written agreements which impose the same level of data protection and security as the obligations under the Agreement, the DPA, and Applicable Data Protection Legislation.

8.6 Where a Sub-Processor fails to fulfil its data protection obligations, Olink remains fully liable to the Customer for the performance of that Sub-Processor's obligations.

9 AUDIT RIGHTS

9.1 Upon Customer's reasonable request, Olink allows Customer to audit and review Processor's Processing of Personal Data in compliance with this DPA and Applicable Data Protection Legislation.

9.2 The Parties will mutually agree upon the scope, timing, and duration of any audits related to the Processing of Personal Data.

9.3 Olink undertakes to provide Customer with all information required to demonstrate Processor's compliance with its obligations under this DPA and Applicable Data Protection Legislation, and to enable and participate in such audit, including on-site inspections, carried out by Customer or other examiner appointed by Customer, provided that the persons performing the audit enter into customary confidentiality agreements.

9.4 Customer shall not conduct such audit more than once per year, unless required by applicable law or specific instruction of a competent data protection authority. Customer shall be solely responsible for any and all costs incurred by Customer with respect to this section.

10 RIGHTS OF DATA SUBJECTS

10.1 It is the responsibility of Customer to respond to requests related to the rights of their Data Subjects. Taking into account the nature of the Processing, Olink shall assist Customer by establishing and maintaining commercially reasonable appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise rights of the Data Subjects under Applicable Data Protection Legislation. In the event a Customer's Data Subject request is received by Olink, Olink will promptly inform the Customer. Olink will not respond to any Customer's Data Subject request without Customer's prior written consent.

11 DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

11.1 Olink shall provide Customer with relevant information and documentation of the Processing of Personal Data (upon a written request and subject to obligations of confidentiality) with regard to any data protection impact assessments, and prior consultations with supervisory authorities when the Customer reasonably determines that such data protection impact assessments or prior consultations are required pursuant to Applicable Data Protection Legislation.

12 DELETION OR RETURN OF PERSONAL DATA

12.1 Upon termination of this DPA, Olink shall return all Personal Data Processed under the Agreement and delete any remaining copies within thirty (30) days after the termination of the Agreement, unless continued storage of Personal Data is expressly agreed to or required under any applicable laws. Notwithstanding the foregoing, Olink may retain backups and archival copies of documents and files containing Personal Data to the extent required to comply with applicable laws, industry standards and Olink's data retention and archiving policies. Such copies shall remain subject to the terms of this DPA for so long as such data is retained. Upon Customer's request, Olink will delete any documents or files containing Personal Data. In case the Agreement contains specific provisions for this situation, the provisions of the Agreement shall prevail provided they comply with Applicable Data Protection Legislation.

13 INTERNATIONAL DATA TRANSFERS

13.1 Customer acknowledges and agrees that Personal Data may be Processed by Olink in a country outside the UK and/or EU/EEA, including but not limited to the United States of America. For the avoidance of doubt, Processor may conduct international data transfers between Olink Affiliates and/or to Sub-Processors within and outside the UK and/or EU/EEA and may transfer Personal Data outside the UK and/or EU/EEA for the purpose of data storage, and for providing, delivering, supporting, maintaining and/or improving the services stated in the Agreement, or for any other purpose authorized by the Agreement or this DPA.

13.2 Transfer Mechanisms: To enable the transfer of Personal Data from Customer ("Data Exporter") to Processor ("Data Importer") with regard to any data subject to the UK GDPR or GDPR within the scope of the Agreement, one of the following transfer mechanisms shall apply, in the following order of precedence:

(a) a valid adequacy decision pursuant to the requirements under the UK GDPR or GDPR that provides that the Third Country, a territory or one or more specified

sectors within that Third Country, or the international organization in question to which Customer Personal Data is to be transferred ensures an adequate level of data protection;

(b) (if applicable) Processor certification under the EU-US Data Privacy Framework, UK Extension to the EU-US Data Privacy Framework, or any successor to such framework, (only to the extent that such self-certification constitutes an "appropriate safeguard" or is subject to a valid "adequacy decision" pursuant to the UK GDPR or GDPR, as the case may be), provided that the services are covered by the self-certification;

(c) the Standard Contractual Clauses (as defined below) (insofar as their use constitutes an "appropriate safeguard" under the GDPR or UK GDPR, as the case may be); or

(d) any other lawful basis, as laid down in the GDPR or UK GDPR, as the case may be.

13.3 Standard Contractual Clauses and UK Addendum:

(a) The Parties agree that the Standard Contractual Clauses of Commission Implementing Decision (EU) 2021/914 of 4 June 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, including such optional sections as described below in this section 13(g) ("Standard Contractual Clauses"), and, as further amended by the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, in force as of 21 March 2022) ("UK Addendum") are incorporated into this DPA by reference and shall apply for any third country transfers of Personal Data from the Data Exporter to the Data Importer.

(b) References in this DPA to "GDPR" will be deemed references to the corresponding laws and regulations of the United Kingdom, including, without limitation, the UK GDPR and Data Protection Act 2018.

(c) In cases where the Standard Contractual Clauses (and including where amended by the UK Addendum) apply, and there is a conflict between the terms of the DPA and the terms of the Standard Contractual Clauses, the terms of the Standard Contractual Clauses (and including where amended by the UK Addendum) shall prevail.

(d) When Customer is a Controller located within the UK or EU/EEA and transfers Personal Data to Olink Proteomics Inc. in the United States, the Standard Contractual Clauses referenced as "Module Two: Transfer Controller to Processor" or "Module Three: Transfer Processor to Processor" shall apply between the Parties.

(e) When Customer is a Controller located outside of the UK or EU/EEA and engages Olink Proteomics AB in Sweden to either collect Personal Data in the UK or EU/EEA, as applicable, on behalf of the Controller or to process Personal Data received from the Controller in the UK or EU/EEA, as applicable, the Clauses referenced as "Module Four: Transfer controller to processor" shall apply between the Parties.

(f) When Customer is a Processor located within the UK or EU/EEA and transfers Personal Data to Olink Proteomics Inc. in the United States, the Clauses referenced as "Module Three: Transfer Processor to Processor" shall apply between the Parties.

(g) Olink Proteomics AB have implemented the Clauses referenced as "Module Three: Transfer Processor to Processor" as the transfer mechanism to govern any transfers of Personal Data to its Affiliates established outside EU/EEA.

(h) For each Module, where applicable, the Parties agree:

- Customer will take on the obligations of "Data Exporter" for the purposes of the Standard Contractual Clauses and Olink will take on the obligations of "Data Importer" for the purposes of the Standard Contractual Clauses;
- Clause 7, the optional docking Clause will not apply;
- Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes is set forth in Section 8.3 of this DPA;
- Clause 11, the optional language will not apply;
- Clause 17, Option 1 will apply, with the laws of Sweden governing the Clauses;
- Clause 18(b), disputes shall be resolved in the courts of Sweden;
- Annexes required by the Standard Contractual Clauses and UK Addendum are attached to this DPA as Attachment 3;
- Tables 1, 2 and 3 of Part 1 of the UK Transfer Addendum are deemed completed with the corresponding details set out in Attachment 3;
- Table 4 of Part 1 of the UK Transfer Addendum is completed by the box labelled 'Data Exporter' being deemed to have been ticked.
- Part 2 of the UK Transfer Addendum. The Parties agree (i) to be bound by the Mandatory Clauses of the UK Transfer Addendum and (ii) In relation to any UK Restricted Transfer to which the UK Transfer Addendum applies, where the context permits and requires, any reference in the Addendum to the SCCs shall be read as a reference to those SCCs as varied in the manner set out in this section 13.3.

14 ATTACHMENTS TO THE DPA

14.1 Jurisdiction Specific Terms. To the extent the Parties Process Personal Data originating from, or protected by, Applicable Data Protections Legislation in one of the jurisdictions listed in Attachment 4 ("Jurisdiction Specific Terms"), then the terms specified in Attachment 4 with respect to the applicable jurisdiction(s) shall apply in addition to the terms of this DPA and its attachments. In case of any conflict or ambiguity between the Jurisdiction Specific Terms and any other terms of this DPA, the applicable Jurisdiction Specific Terms will prevail.

15 GENERAL TERMS

15.1 Term of Agreement. The provisions of this DPA shall apply for the entire term of the Agreement and it shall terminate automatically upon expiry or termination of the Agreement, except for those provisions that, by their nature, must survive termination of the DPA.

15.2 Changes to this DPA. This DPA may be changed only in writing and signed by authorized representatives of each Party unless the Agreement specifies that Customer has agreed to Olink's Online Data Processing Addendum, the current version of which is available at https://olink.com/gtcs/ in which case Olink may update the terms of this DPA from time to time; provided, however, Olink will provide at least thirty (30) days prior written notice to Customer when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Services. The then-current terms of this DPA are available at https://olink.com/gtcs/

15.3 Applicable Law and Disputes. This DPA shall be interpreted and applied in accordance with the Agreement. Any disputes between Customer and Olink as a result of the creation, fulfillment, and/ or interpretation of the DPA shall be resolved in accordance with the Agreement.

15.4 Remuneration. Unless reasonably requested by Customer to comply with Applicable Data Protection Legislation, Processor is entitled to compensation in accordance with Processor's prevailing price list for work performed or assistance provided pursuant to the obligations in Section 8 of this DPA.

15.5 Limitations of liability. The limitation of liability set out in the Agreement shall apply to Processor's liability under this DPA as if set out herein. Processor shall only process Personal Data in accordance with Customer's instructions. Therefore, Processor is not liable in circumstances where Processor's actions result from instructions received from Customer, unless Processor should have reasonably been aware of the unlawfulness of its actions.

ATTACHMENT 1: Security Measures

Description of the technical and organisational measures implemented by the Processor / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Olink shall implement and maintain the measures listed in this Attachment 1 to reasonably protect Personal Data during Processing. Where applicable, this Attachment 1 will serve as Annex II to the EU Standard Contractual Clauses.

Measures of pseudonymisation and encryption of personal data

Industry standard encryption technologies for personal data that is: (i) transmitted over public networks (i.e., the Internet) or when transmitted wirelessly; or (ii) at rest.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Organisational management and dedicated staff responsible for the development, implementation and maintenance of Olink's information security program.

Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g., role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for personal data, as described above.

Network security controls that provide for the use of stateful firewalls and layered DMZ architectures and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Incident response procedures designed to allow Olink to investigate, respond to, mitigate and notify of events related to Olink's technology and information assets.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing.

Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Olink's organisation, monitoring and maintaining compliance with Olink's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

Measures for user identification and authorisation

Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Olink's passwords that are assigned to its employees: (i) be at least ten (10) characters in length, (ii) not be stored in readable format on Olink's computer systems, (iii) must have defined complexity, and (iv) must have a history threshold to prevent reuse of recent passwords. Multi-factor authentication, where available, must always be used.

Measures for the protection of data during transmission

Industry standard encryption technologies for personal data that is transmitted over public networks (i.e., the Internet) or when transmitted wirelessly.

Measures for the protection of data during storage

Industry standard encryption technologies for personal data that is at rest.

Measures for ensuring physical security of locations at which personal data are processed

Physical and environmental security of data center, server room facilities and other areas containing personal data designed to: (i) protect information assets from unauthorised physical access, (ii) manage, monitor and log movement of persons into and out of Olink facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

Measures for ensuring events logging

System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

Measures for ensuring system configuration, including default configuration

Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Olink's possession.

Measures for internal IT and IT security governance and management

Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to Olink's technology and information assets.

Measures for certification / assurance of processes and products

Organisational management and dedicated staff responsible for the development, implementation and maintenance of Olink's information security program.

Measures for ensuring data minimisation

Not applicable to Olink. Olink is processing the personal data on behalf of the Controller for the sole purpose of providing services to the Controller for the duration of the services agreement entered into between Olink and the Controller. The Controller has complete control over the collection, modification, and deletion of personal data (subject to the data retention section, below).

Measures for ensuring data quality

Not applicable to Olink. Olink is processing the personal data on behalf of Controller for the sole purpose of providing services to Controller for the duration of the services agreement entered into between Olink and Controller. Olink does not have the ability to monitor the quality of the personal data.

Measures for ensuring limited data retention

Controller is permitted to set its own retention rules in the Agreement.

Measures for ensuring accountability

Olink in place appropriate technical and organisational measures, such as: (i) adopting and implementing data protection policies (where proportionate), (ii) putting written contracts in place with organisations that process personal data on its behalf, (iii) maintaining documentation of its processing activities, (iv) implementing appropriate security measures, (v) recording and, where necessary, reporting personal data breaches, and (vi) carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.

Measures for allowing data portability and ensuring erasure

When a customer requests that Olink delete data, Olink responds promptly and in compliance with applicable laws.

ATTACHMENT 2: Sub-Processors

Where applicable, this Attachment 2 will serve as Annex III to the Standard Contractual Clauses. The Controller has authorised the use of the following sub-processors:

Sub-Processor	Location of processing (country)
Olink Proteomics Inc. (When acting as a sub-processor for Olink Proteomics AB) Olink Proteomics Inc., a fully owned subsidiary of Olink Proteomics AB, provides IT services, product support and other services on Olink Proteomics AB's behalf that are necessary for the provision of services under the Agreement. There is a DPA and SCC's in place between the companies.	130 Turner St., Building 2, Suite 230, Waltham, MA 02453, USA
Olink Proteomics AB (When acting as sub-processor for Olink Proteomics Inc.) Olink Proteomics AB is the sole owner of Olink Proteomics Inc. Where Olink Proteomics Inc is processing information as a Processor Olink Proteomics AB may perform processing activities as sub-processor on behalf of Olink Proteomics Inc.	Salagatan 16F, SE-753 30 Uppsala, Sweden
Amazon Web Services (AWS) AWS provides infrastructure and cloud services for Olink Proteomics AB and Olink Proteomics Inc.	Servers are located in Frankfurt, Germany, Stockholm, Sweden and Virginia, USA.
Microsoft Corporation Corporate Location: One Microsoft Way, Redmond, WA 98052-6399, U.S.A. Azure Hosting for back-up of server content and data held by our systems in the Olink Boston, MA location.	Azure Hosting Services in Virginia, USA.
FirstLight Fiber Corporate Location: 41 State Street, Floor 10, Albany, NY 12207 Hosting to support back-up of Olink Boston, MA server content and data.	Location is Somerville, MA, USA.
Standard BioTools Inc., previously known as Fluidigm Corp. Corporate Location: 2 Tower Place, Suite 2000, South San Francisco, CA 94080, U.S.A. Subprocessing limited to purchases of Kits and Instruments only and includes installation, relocations, repairs, instrument qualifications, troubleshooting and support, among others.	*Customer selects the location (country) of services.*

ATTACHMENT 3: Details of Processing

Where applicable, this Attachment 3 will serve as Annexes I - III to the Standard Contractual Clauses. (MODULE II and/or IV: Transfer Controller to Processor; or MODULE III: Transfer Processor to Processor)

Annex I

A. LIST OF PARTIES

Data exporter(s):

Name: The Customer entity identified in the Agreement and DPA with an address as set forth in the Agreement except in the case of Module 4 of the SCCs, where the "data exporter" is Olink Proteomics AB.

Contact person's name, position and contact details: see heading section of the Agreement for additional details

Activities relevant to the data transferred under these Clauses: See the Agreement, the applicable Statement of Work, and the DPA for a description of the services that the Processor is performing on behalf of Customer.

Signature and date: See signature to the Agreement to which this DPA, Attachment 3 is attached.

Role: The Customer is the Controller or Processor and the Olink entity identified in the Agreement and DPA with an address set forth in the Agreement is the Processor or Sub-Processor.

Data importer(s):

Name: The Olink entity identified in the Agreement and DPA with an address as set forth in the Agreement except in the case of Module 4 of the SCCs in which the Customer entity identified in the Agreement and DPA with an address as set forth in the Agreement is the "data importer".

Contact person's name, position and contact details: see heading section of the Agreement for additional details

Activities relevant to the data transferred under these Clauses: See the Agreement, the applicable Statement of Work, and the DPA for a description of the services that the Processor is performing on behalf of Customer.

Signature and date: See signature to the Agreement to which this DPA, Attachment 3 is attached.

Role: The Customer is the Controller or Processor and the Olink entity identified in the Agreement and DPA with an address set forth in the Agreement is the Processer or Sub-Processor.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See the Agreement and the applicable Statement of Work for Data Exporter's data subjects; e.g. Sample providers/patients, third party customer employees/contact persons.

Categories of personal data transferred

See the Agreement and the applicable Statement of Work; e.g. pseudonymized identifiers, related analysis results, health data, and clinical data.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See the Agreement, the applicable Statement of Work. Regarding safeguards, subject or sample ID's are pseudonymized and the key to re-identifying such data is held by the Controller, not the Processor.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

See the Agreement, the applicable Statement of Work.

Nature of the processing

See the Agreement, the applicable Statement of Work for details regarding statistical and/or laboratory data analyses and any related data storage and transfer of results.

Purpose(s) of the data transfer and further processing

See the Agreement, the applicable Statement of Work, and the DPA for processing of personal data for proteomic analysis and/or biostatistical services and related sample data storage.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Agreement between Customer and Olink and in accordance with this DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Sub-Processor list referenced in Section 8 and Attachment 2 of the DPA. Where the Data Importer, Olink, engages Sub-Processors it will do so in compliance with the terms of the Standard Contractual Clauses. The subject matter, nature and duration of the processing activities carried out by the Sub-Processor will not exceed the processing activities as described in the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority in accordance with Clause 17/18

Integritetsskyddsmyndigheten (IMY), Swedish identification number 202100-0050

P.O. Box 8114, 104 20 Stockholm, Sweden +46 (0)8 657 61 00 | imy@imy.se

Annex II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Attachment 1 to the DPA to which this Annex II is attached.

Annex III

LIST OF SUB-PROCESSORS

See Attachment 2 to the DPA to which this Annex III is attached.

ATTACHMENT 4: Jurisdiction Specific Terms

1. Australia:

1.1 The definition of "Applicable Data Protection Legislation" includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2 The definition of "personal data" includes "Personal Information" as defined under Applicable Data Protection Legislation.

1.3 The definition of "Sensitive Data" includes "Sensitive Information" as defined under Applicable Data Protection Legislation.

2. Brazil:

2.1 The definition of "Applicable Data Protection Legislation" includes the Lei Geral de Proteção de Dados (General Personal Data Protection Act).

2.2 The definition of "Security Incident" includes a security incident that may result in any relevant risk or damage to data subjects.

2.3 The definition of "processor" includes "operator" as defined under Applicable Data Protection Legislation.

3. Canada:

3.1 The definition of "Applicable Data Protection Legislation" includes the Federal Personal Information Protection and Electronic Documents Act.

3.2 Olink's Sub-Processors, as set forth in Section 8 and Attachment 2 of this DPA, are third parties under Applicable Data Protection Legislation, with whom Olink has entered into a written contract that includes terms substantially similar to this DPA. Olink has conducted appropriate due diligence on its sub-processors.

3.3 Olink will implement technical and organizational measures as set forth in Attachment 1 of this DPA.

4. European Economic Area (EEA):

4.1 The definition of "Applicable Data Protection Legislation" includes the General Data Protection Regulation (EU 2016/679) ("*GDPR*").

4.2 When Olink engages a Sub-Processor under Section 8 of this DPA, it will:

> (a) require any appointed Sub-Processor to protect the Personal Data to the standard required by Applicable Data Protection Legislation, such as including at least the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and
>
> (b) require any appointed Sub-Processor to (i) agree in writing to only process personal data in a country that the European Union has declared to have an "adequate" level of protection or (ii) only process personal data on terms equivalent to the Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

4.3 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party's indemnification obligations), neither party will be responsible for any GDPR fines issued or levied

under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

5. Israel:

5.1 The definition of "Applicable Data Protection Legislation" includes the Protection of Privacy Law.

5.2 The definition of "controller" includes "Database Owner" as defined under Applicable Data Protection Law.

5.3 The definition of "processor" includes "Possessor" as defined under Applicable Data Protection Law.

5.4 Olink will require that any personnel authorized to process Personal Data comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Legislation. Such personnel sign confidentiality agreements with Olink in accordance with Section 6 (Security of Processing and Confidentiality) of this DPA.

5.5 Olink must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Attachment 1 of this DPA and complying with the terms of the Agreement.

5.6 Olink must ensure that the personal data will not be transferred to a Sub-Processor unless such Sub-Processor has executed an agreement with Olink pursuant to Section 8 of this DPA.

6. Japan:

6.1 The definition of "Applicable Data Protection Legislation" includes the Act on the Protection of Personal Information ("***APPI***").

6.2 The definition of "Personal Data" includes information about a specific individual applicable under Section 2(1) of the APPI, which Customer entrusts to Olink during Olink's provision of the services to Customer.

6.3 Olink agrees it has and will maintain a privacy program conforming to the standards prescribed by rules of the Personal Information Protection Commission concerning the handling of personal data pursuant to the provisions of Chapter 4 of the APPI. Accordingly:

(a) Olink will (i) process personal data as necessary to provide the services to Customer in accordance with the Agreement, including the purpose of processing and processing activities set forth in this DPA (the "Purpose") and (ii) not process personal data for any purpose other than the Purpose without Customer's consent;

(b) Olink will implement and maintain measures appropriate and necessary to prevent unauthorized disclosure and loss of personal data and for the secure management of personal data in accordance with the APPI as set forth in Attachment 1 (Security Measures) of this DPA;

(c) Olink will notify Customer for (i) a failure to comply with Attachment 1 (Security Measures) or (ii) Olink's discovery of a Security Incident impacting Personal Data, in either case, in accordance with Section 7 (Security Breach and Incident Response). Olink will provide reasonable assistance to Customer in the event that Customer is required to notify a regulatory authority or any data subjects impacted by a Security Incident;

(d) Olink will ensure that any of its employees who have access to personal data (i) have executed employee agreements requiring them to keep such personal data confidential and (ii) who violate confidentiality will be subject to disciplinary action and possible termination; (iii) carry out appropriate employee supervision and training for the secure management of personal data; and (iv) limit the

number of authorized personnel, including Olink's employees, who have access to personal data and control such access such that it is only permitted for the time period necessary for the Purpose;

(e) Olink will not disclose personal data to any third party, except as Customer has authorized Olink to do so in the Agreement. When engaging Sub-Processors, Olink will comply with the obligations in Section 8 of this DPA to ensure that procedures are in place to maintain the confidentiality and security of personal data;

(f) Olink will keep records of the handling of personal data entrusted to it by, and performed for, Customer;

(g) Olink will promptly notify Customer of any Third Party Request and not respond to such Third Party Request without Customer's prior consent, except as legally required to do so or to confirm that such Third Party Request relates to Customer. To the extent Customer does not have the ability to resolve a Third Party Request from a data subject through the self-service features made available via the Services, then, upon Customer's request, Olink will provide reasonable cooperation and support to assist Customer in resolving such Third Party Request from a data subject in accordance with Section 10 (Rights of Data Subjects) of this DPA;

(h) Unless prohibited by applicable law or regulation, Olink will promptly notify Customer of any Third Party Request that requires Olink to disclose personal data on order or disposition of any governmental authority or court of law. Olink will limit any personal data provided to the minimum extent required and strictly for the required purpose;

(i) Customer may assess Olink's compliance with its obligations under Applicable Data Protection Legislation and as set forth in Section 9 (Audit Rights) of this DPA. In addition, Olink will respond to any Customer inquiries or questionnaires relating to Olink's processing of personal data under the Agreement in good faith and within a reasonable period of time;

(j) Olink will provide reasonable cooperation to Customer upon written request, where Customer is reporting to the Personal Information Protection Commission or other regulatory authorities; and

(k) Olink's primary processing facilities are located in Sweden and the United States of America, and, depending on Customer's use of the services, from the locations set forth in Attachment 2 (collectively, "*Processing Locations*"). Olink will notify customer of any Processing Location change and provide Customer the opportunity to object in accordance with, respectively, Section 8 of this DPA. Where Olink processes personal data in a country other than Japan, Olink will ensure it complies with this DPA. Olink will promptly notify Customer of any changes in applicable law and regulation that may materially affect Olink's obligations with respect to the processing of personal data, and in such case, Customer may, at its discretion, suspend the transfer of personal data.

6.4 The following data subject consent terms apply:

(a) Customer entrusts Olink with personal data for the Purpose of Use. Customer agrees that Olink is not a "third party" as the term is used in the APPI provisions that restrict the provision of personal data to third parties. As such, the requirement to obtain data subject consent in advance for domestic transfers within Japan do not apply; and

(b) Customer acknowledges that data subject consent may be required under Article 4 of the Telecommunications Business Act in the event Customer instructs Olink's support personnel to access the content of communications. Customer will comply with any consent requirements specific to its use of the services and instructions as required by Section 5 (Processing of Personal Data) of this DPA.

7. Mexico:

7.1 The definition of "Applicable Data Protection Legislation" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations.

7.2 When acting as a processor, Olink will:

(a) treat personal data in accordance with Customer's instructions set forth in Section 5 (Processing of Personal Data) of this DPA;

(b) process personal data only to the extent necessary to provide the services;

(c) implement security measures in accordance with Applicable Data Protection Legislation and Attachment 1 (Security Measures) of this DPA;

(d) keep confidentiality regarding the personal data processed in accordance with the Agreement;

(e) delete all personal data upon termination of the Agreement in accordance with Section 12 (Return or Deletion of Personal Data) of this DPA; and

(f) only transfer personal data to sub-processors in accordance with Section 8 (Sub-Processors) of this DPA.

8. Singapore:

8.1 The definition of "Applicable Data Protection Legislation" includes the Personal Data Protection Act 2012 ("*PDPA*").

8.2 Olink will process personal data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Attachment 1 (Security Measures) of this DPA and complying with the terms of the Agreement.

9. Switzerland:

9.1 The definition of "Applicable Data Protection Legislation" includes the Swiss Federal Act on Data Protection, as revised ("***FADP***").

9.2 When Olink engages a sub-processor under Section 8 of this DPA, it will:

(a) require any appointed sub-processor to protect the Personal Data to the standard required by Applicable Data Protection Legislation, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular, providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

(b) require any appointed sub-processor to (i) agree in writing to only process personal data in a country that Switzerland has declared to have an "adequate" level of protection or (ii) only process personal data on terms equivalent to the Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

9.3 To the extent that personal data transfers from Switzerland are subject to the Standard Contractual Clauses in accordance with Section 13.3 the following amendments will apply to the Standard Contractual Clauses:

(a) references to “EU Member State” and “Member State” will be interpreted to include Switzerland, and

(b) insofar as the transfer or onward transfers are subject to the FADP:

(i) references to "Regulation (EU) 2016/679" are to be interpreted as references to the FADP;

(ii) the “competent supervisory authority” in Attachment I, Part C will be the Swiss Federal Data Protection and Information Commissioner;

(iii) in Clause 17 (Option 1), the Standard Contractual Clauses will be governed by the laws of Switzerland; and

(iv) in Clause 18(b) of the Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland.

10. United Kingdom (UK):

10.1 References in this DPA to “GDPR” will be deemed references to the corresponding laws and regulations of the United Kingdom, including, without limitation, the UK GDPR and Data Protection Act 2018.

10.2 When Olink engages a Sub-Processor under Section 8 of this DPA, it will:

(a) require any appointed sub-processor to protect the Personal Data to the standard required by Applicable Data Protection Legislation, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

(b) require any appointed sub-processor to (i) agree in writing to only process personal data in a country that the United Kingdom has declared to have an “adequate” level of protection or (ii) only process personal data on terms equivalent to the UK International Data Transfer Agreement or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

10.3 Notwithstanding anything to the contrary in this DPA or in the Agreement (including, without limitation, either party’s indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party’s violation of the GDPR.

11. United States of America:

11.1 “***US State Privacy Laws***” mean all state laws relating to the protection and processing of personal data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“***CCPA***”), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act, and including other similar state privacy laws as they become effective.

11.2 The definition of “Applicable Data Protection Legislation” includes US State Privacy Laws.

11.3 The following terms apply where Olink processes personal data subject to the CCPA:

(a) The term "***personal information***", as used in this section, will have the meaning provided in the CCPA;

(b) Olink is a service provider when processing Personal Data. Olink will process any personal information only for the business purposes set forth in the Agreement, including the purpose of processing and processing activities set forth in this DPA (the "Purpose"). As a service provider, Olink will not sell or share Personal Data or retain, use, or disclose Personal Data (i) for any purpose other than the Purpose, including retaining, using, or disclosing Personal Data for a commercial purpose other than the Purpose, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and Olink;

(c) Olink will (i) comply with obligations applicable to it as a service provider under the CCPA and (ii) provide personal information with the same level of privacy protection as is required by the CCPA. Customer is responsible for ensuring that it has complied, and will continue to comply, with the requirements of the CCPA in its use of the Services and its own processing of personal information;

(d) Customer will have the right to take reasonable and appropriate steps to help ensure that Olink uses personal information in a manner consistent with Customer's obligations under the CCPA;

(e) Olink will notify Customer if it makes a determination that it can no longer meet its obligations as a service provider under the CCPA;

(f) Upon notice, Customer will have the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of personal information;

(g) Olink will provide reasonable additional and timely assistance to assist Customer in complying with its obligations with respect to consumer requests as set forth in the Agreement;

(h) For any Sub-Processor used by Olink to process personal information subject to the CCPA, Olink will ensure that Olink's agreement with such Sub-Processor complies with the CCPA, including, without limitation, the contractual requirements for service providers and contractors;

(i) Olink will not combine Personal Data that it receives from, or on behalf of, Customer, with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, unless such combination is required to perform any business purpose as permitted by the CCPA, including any regulations thereto, or by regulations adopted by the California Privacy Protection Agency; and

(j) Olink certifies that it understands and will comply with its obligations under the CCPA.

11.4 Olink acknowledges and confirms that it does not receive Personal Data as consideration for any services provided to Customer.

11.5 For avoidance of doubt, US State Privacy Laws do not apply to (i) personal information that qualifies as Protected Health Information subject to the Health Insurance Portability and Accountability Act of 1996 and (ii) personal information collected as part of a clinical trial or other biomedical research study subject to government regulations and guidance.