DATA PROCESSING ADDENDUM

Technical Support and Maintenance Services

1. APPLICATION

1.1 This Data Processing Addendum and its Schedules ("**DPA**") are incorporated into and form part of the applicable terms of use, terms of service, end user license agreement or other agreement between Illumina and Customer under which Illumina provides Customer the Services (the "**Agreement**"). The use of the Services shall be deemed as an acceptance of the terms of this DPA.

1.2 The provisions of this DPA shall apply only to the extent required by Data Protection Laws in respect of Illumina's Processing of Personal Data on behalf of the Customer in providing the Services.

1.3 In the event and to the extent of a conflict between this DPA and the Agreement, this DPA shall prevail to the extent of such conflict.

2. DEFINITIONS

2.1 Unless otherwise defined in the Agreement:

"**Affiliate**" means, with respect to Illumina, an entity that, directly or indirectly, controls, is controlled by or is under common control with such party.

"**Customer**" means the customer or recipient of the Services under the Agreement.

"**Data Exporter**" means a Customer which is transferring Personal Data directly or via onward transfer to Illumina, where Illumina is located in a country that triggers additional requirements for the protection of Personal Data being transferred in accordance with Data Protection Laws.

"**Data Importer**" means Illumina where it is located in a country that triggers additional requirements for the protection of Personal Data being transferred in accordance with the applicable Data Protection Laws.

"**Data Protection Laws**" means privacy laws and regulations applicable to the Processing of Personal Data under the Agreement.

"**Illumina**" means the Affiliate within the Illumina Group that provides the Services under the Agreement.

"**Illumina Group**" means Illumina and its Affiliates.

"**Restricted Transfer**" means a transfer of Personal Data from a Data Exporter to a Data Importer.

"**Services**" means the provision by Illumina of support and maintenance work for the Illumina products and/or services provided, in each case provided by Illumina directly pursuant to the Agreement (hereinafter "**Technical Support and Maintenance Services**").

"**Your Customer**" means any or all individuals or entities that directly or indirectly access or use the Services under Customer's registered Illumina account.

2.2 In this DPA the terms "**Business**", "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Process/Processing**", "**Processor**", "**Sell**", "**Service Provider**", "**Share**", and "**Supervisory Authority**" shall have the meaning given in Data Protection Laws, or where not specifically defined under Data Protection Laws, the same meaning as analogous terms in those Data Protection Laws. For the avoidance of doubt, "Controller" shall include an entity that meets the definition of a "Business", and "Processor" shall include an entity that meets the definition of "Service Provider", as both are defined by the California Consumer Privacy Act, as amended and as applicable to this DPA.

2.3 A reference to a law, regulation or other document is a reference to such law, regulation or document as amended, superseded or repealed from time to time.

3. ROLE OF THE PARTIES

3.1 Illumina and Customer acknowledge that depending on the circumstances, and to the extent such concepts are recognized under Data Protection Laws:

(a) Customer is the Controller of Personal Data and Illumina its Processor; or

(b) Your Customer is the Controller of Personal Data, Customer its Processor, and Illumina is Customer's sub-processor.

4. DETAILS OF PERSONAL DATA PROCESSING

4.1 The Processing description is set out at **Schedule 1** of this DPA.

5. COMPLIANCE WITH LAWS

5.1 Customer shall ensure that its Processing of Personal Data and instructions to Illumina comply with Data Protection Laws.

5.2 Illumina shall only Process Personal Data in accordance with Customer's documented instructions, including the performance of the Services as set out in this DPA unless required otherwise by applicable law, in which case Illumina shall inform Customer of the legal requirement where legally permitted to do so. In particular, and without limitation to the foregoing, Illumina shall not: (i) retain, use, disclose, combine, or otherwise Process Personal Data except in the context of the direct business relationship between Illumina and Customer as set out in this DPA and the Agreement and as otherwise necessary for the business purposes and the performance of the Services specified in the Agreement or this DPA; or (ii) Sell or Share Personal Data.

5.3 Illumina agrees that Customer has the right to take reasonable and appropriate steps to stop and remediate any breach of this section 5, including any unauthorized Processing of Personal Data.

6. ILLUMINA PERSONNEL

6.1 Illumina shall ensure that its personnel engaged in providing the Services are subject to appropriate obligations of confidentiality.

7. SUB-PROCESSORS

7.1 Customer provides general authorization to Illumina to appoint sub-processors in performing the Services, including Illumina's Affiliates and third-party service providers. As of the date of this DPA, a list of sub-processors is set out in **Schedule 2** of this DPA. Where Your Customer is the Controller, Customer has Your Customer's general authorization for Illumina to engage the sub-processors listed in **Schedule 2** of this DPA.

7.2 Illumina shall ensure that any sub-processor is subject to obligations which are substantially similar to those set out in this DPA.

7.3 Illumina sub-processor portal (available at https://www.illumina.com/destination/dpa-sub-processor.html) contains a mechanism to subscribe to notifications of new sub-processors, and if Customer subscribes, Illumina shall provide notifications of any new sub-processors engaged in connection with the provision of the applicable Services. Customer may raise any objections to such changes by contacting privacy@illumina.com.

7.4 Illumina shall be liable for the acts and omissions of its sub-processors.

8. SECURITY

8.1 Illumina shall maintain the technical and organisational measures, as set out in **Schedule 3** of this DPA.

9. DATA SUBJECT REQUESTS

9.1 Customer shall be responsible for responding to requests from Data Subjects exercising their rights under Data Protection Laws ("**Data Subject Requests**").

9.2 Illumina shall notify Customer if Illumina receives a Data Subject Request concerning Personal Data Illumina Processes in the provision of Services to Customer.

9.3 To the extent Customer in its use of the Services does not have the ability to address a Data Subject Request, upon Customer's request, Illumina shall provide commercially reasonable efforts to assist Customer in

responding to such Data Subject Request, to the extent Illumina is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws.

10. ASSISTANCE

10.1 Upon Customer's request and at Customer's expense, Illumina shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligations as a Controller, as required under Data Protection Laws, including to carry out a data protection impact assessment related to Customer's use of the Services and any related consultation with a competent Supervisory Authority, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Illumina.

11. PERSONAL DATA BREACH

11.1 Upon becoming aware of a Personal Data Breach, Illumina shall notify Customer without undue delay, and take steps to investigate and remediate the Personal Data Breach.

12. DELETION

12.1 Illumina shall delete Personal Data as set out in **Schedule 1** of this DPA.

12.2 Customer acknowledges, agrees, and authorizes Illumina to retain aggregated data generated in the performance of the Services (which is not considered Personal Data) for internal record keeping, quality and audit requirements.

13. INTERNATIONAL DATA TRANSFERS

13.1 Where Illumina provides Technical Support and Maintenance Services as contemplated by section 7 and **Schedule 2** of this DPA, Customer authorizes Illumina to transfer Personal Data to its authorized sub-processors, provided that Illumina shall comply with section 7 of this DPA at all times and ensure that any Restricted Transfers are made in accordance with Data Protection Laws, including the use of an applicable transfer mechanism such as standard contractual clauses.

13.2 Where Illumina and Customer are located in different jurisdictions and there is a Restricted Transfer of Personal Data from Customer to Illumina, the Data Exporter (Customer) and the Data Importer (Illumina) shall transfer and Process Personal Data in accordance with **Schedule 4**. In respect of any jurisdiction not listed in **Schedule 4**, where required by Data Protection Laws, upon either party's request, the parties shall discuss any further steps that may be required to ensure any international transfers are lawful (including the entry into any additional transfer agreement or terms).

14. INFORMATION AND AUDIT

14.1 Illumina shall, at Customer's cost, provide such information as Customer may reasonably request to demonstrate compliance with this DPA.

14.2 Upon Customer's reasonable and prior written request, and no more frequently than once every twelve (12) months, Illumina shall make available to Customer evidence of the most recent third-party audit or certifications setting out Illumina's conformity in relation to Personal Data Processing activities pursuant to this DPA.

14.3 Any information provided under this section is Illumina's confidential information, and shall be subject to the confidentiality terms of the Agreement or such other terms as Illumina may require. Customer may not provide such information to any third-party or use such information for any purpose other than to verify Illumina's compliance with this DPA without Illumina's prior written consent.

14.4 If Customer can reasonably demonstrate that the information provided is not sufficient to demonstrate compliance with this DPA, Illumina shall reasonably consider any further requests for information from Customer to demonstrate compliance with this DPA.

14.5 Illumina will notify Customer if, in its opinion, any instruction from Customer infringes Data Protection Laws.

15. CHANGES

15.1 Customer acknowledges and agrees that the Services are provided on a one-to-many basis, and Illumina may from time to time update this DPA, including to ensure compliance with Data Protection Laws.

15.2 Where Illumina makes such changes:

(a) Illumina shall use reasonable endeavors to notify Customer of such changes, which may include publishing such changes on Illumina's website; and

(b) if Customer, acting reasonably, considers that such changes would have a material adverse effect on Customer's ability to comply with Data Protection Laws, Customer may, within thirty (30) days of the date of such change, terminate this DPA by providing written notice to privacy@illumina.com. Customer acknowledges that Illumina will not have to provide the Services if such termination occurs.

SCHEDULE 1: Description of the Processing

Technical Support and Maintenance Services

Contact details

Illumina can be contacted at privacy@illumina.com. Illumina's Global Data Protection Officer can be contacted at DPO@illumina.com.

Purpose of the Processing

The purpose of the Processing of Personal Data by Illumina is to provide the Services pursuant to the Agreement.

Nature of the Processing.

Personal Data may be subject to Processing activities including: (i) receiving Personal Data, including collection, accessing, retrieval, recording and data entry, (ii) holding Personal Data, including storage, organization and structuring, (iii) using Personal Data, including analyzing, consultation and testing, (iv) protecting Personal Data, including restricting, encrypting, and security testing, (v) returning data to Customer and (vi) erasing Personal Data, including destruction and deletion.

Categories of Personal Data.

Illumina will attempt to provide Technical Support and Maintenance Services by using run metric data (which is not considered Personal Data). Depending on the issue, Illumina may need to access genomic data and/or pseudonymized information contained in, for example, BAM files, FastQ files and VCF files including run sequencing data (such as WGS or WXS data) in order to properly troubleshoot and suitably investigate an issue which may arise with respect to Customer's purchased products/services. The transfer of Personal Data to Illumina takes place on a continuous or a on an as-needed basis (e.g., to troubleshoot the reported issue), as applicable.

Illumina also Processes data localization requirements, i.e., whether data is determined to be sensitive within a region and required to remain within that region or be scrubbed of the sensitive information before transiting outside the region.

Data Subjects.

The categories of Data Subjects whose Personal Data will be Processed by Illumina include patients, research cohorts, and other individuals who have consented to Customer's use of the Services, or for whom Customer has another lawful basis to Process their Personal Data.

Duration of the Processing.

Where Customer shares genomic data files containing run sequencing data with Illumina to perform troubleshooting, such files shall be deleted within thirty (30) working days from the date the technical issue which was being attempted to solve is reported as closed by Illumina.

SCHEDULE 2: List of Sub-processors

Technical Support and Maintenance Services

List of sub-processors for Technical Support and Maintenance Services only (where no Cloud Services are provided to Customer) can be found here.

SCHEDULE 3: Technical and Organizational Measures

Illumina has established and maintains technical and organizational measures ("**TOMS**") designed to maintain the confidentiality, integrity, and availability of Customer Data within the Products, and to prevent access, intrusion, alteration or other interference by any unauthorized third parties of the same, that are compliant with (i) the requirements of this TOMS; (ii) applicable laws and regulations; and (iii) industry best practices.

Except as otherwise allowed in the Agreement, Illumina shall use Customer Data on behalf of, or to provide Services to, Customer solely and exclusively for the purposes authorized by Customer in order to perform pursuant to the Agreement and only for Customer's benefit. Illumina shall not de-identify (pursuant to all applicable legal requirements) Customer Data unless required to do so as part of the Services or as otherwise permitted by Customer.

1. **Definitions.**

(a) "**Customer Data**" means all proprietary or other non-public information related to the business of Customer, including but not limited to all Personal Data received by Illumina in any tangible or intangible form that relates to or personally identifies any Customer employee, patient, agent, consumer, end user, or representative.

(b) "**Products**" means any and all tangible items provided by Illumina to Customer under the Agreement. In addition, and where applicable, "Products" shall include all hosted, platform, or cloud services furnished by Illumina to Customer.

(c) "**Security Incident**" means the successful unauthorized access, use, disclosure, modification, or destruction of information within Illumina's system involving Customer Data; provided, however, Illumina shall not be required to report pings and other broadcast attacks on Illumina's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in the defeat or circumvention of any security control, or in the unauthorized access, use or disclosure of Customer Data.

(d) "**Services**" means any services for or on behalf of Customer performed by Illumina in connection with the Agreement, including, but not limited to professional services, training, development, support, maintenance, and any other services.

2. **Information Security.**

(a) **Information Security Policy.** Illumina has enacted, implemented, and adheres to a written internal information security policy ("**ISP**") that addresses the roles and responsibilities of its personnel and agents (the "**Workforce**") who have access to Customer Data or the Products. Illumina's ISP accurately reflects the laws, regulations, operational procedures, industry standards, and systems security configurations implemented, and is appropriate for Illumina's size and type of business, the Services, the types of Products produced or sold by Illumina, and the cumulative volume and nature of the data that Illumina may store, access, or transmit.

(b) The ISP shall address the following:

i. administrative, technical, and physical safeguards to protect the confidentiality and integrity of all Customer Data within the Products;

ii. controls used with regard to identification, authorization, availability, assurance, and audit;

iii. maintaining and updating the ISP in accordance with industry standard practices; and

iv. roles and responsibilities of Workforce members

v. education and awareness

vi. Security Incident responses

vii. auditing and reporting

viii. infrastructure information security

ix. access controls based on the principle of least privilege

x. authorization controls based on the principle of need to know

xi. encryption of information in transit and at rest

xii. physical access

xiii. asset classification and related controls.

(c) **Risk Assessment.** Illumina's ISP identifies and assesses reasonably foreseeable internal and external risks to the confidentiality, integrity and availability of Customer Data within the Products. Identification of material threats and vulnerabilities shall be addressed with effective security controls within a reasonable period of time after the completion of the assessment.

(d) **Access by Individuals.** Illumina shall limit access to Customer Data to Illumina's Workforce who need access to Customer Data for purposes of performing the Services. Illumina shall implement role-based access controls designed to permit user access to Customer Data which are necessary to accomplish assigned tasks on behalf of Customer.

i. Each user who has access to Customer Data and systems and equipment that host Customer Data ("**User**") shall have a unique identifier.

ii. Users shall be authenticated by one of the following methods: unique token, card key, biometric reader, or individual password. Users shall be advised that their unique identifier and authentication tool (e.g. password) shall not be shared with others.

iii. Where password authentication is employed to authenticate Users, Illumina shall:

1. prohibit guest accounts;

2. instruct Users not to write down passwords or store them on hard copy or locally on devices;

3. periodically review User accounts and inactivate them when access is no longer required;

4. implement inactivity time-outs, where technically feasible, for User devices that access Customer Data; and

5. implement automatic logoffs for Illumina systems and equipment that process Customer Data.

iv. Illumina shall implement policies and procedures that state that Users are only permitted access to Customer Data they have a business need to access.

(e) **Computing and Network Infrastructure Controls.**

i. **Network Isolation.** If Illumina hosts applications which store or process Customer Data:

1. Network segments containing Internet-accessible services shall be isolated from internal networks.

2. Network segments where Customer Data resides shall be physically or logically isolated from segments containing other data.

3. Network segments shall be protected by a firewall. A change control system shall be in place for changes made to firewall rule sets or other network infrastructure such as routers and switches.

ii. **Intrusion Detection and Prevention.** Illumina shall employ risk-appropriate security measures, such as network intrusion detection systems and intrusion prevention systems, to protect telecommunications systems and any networked computer systems or devices that store, process, transmit Customer Data. Illumina shall actively monitor network intrusion detection and intrusion prevention systems.

(f) **Disposal of Files, Media, or Products Containing Customer Data.** Illumina shall destroy files, media, or Products containing Customer Data in accordance with its ISP and industry standards.

(g) **External Access.**

i. **Internet.** Illumina shall protect its network architecture in accordance with industry standard architecture, tools, and **practices**. This includes industry standard security for any DMZ, proxy server, and internet connections. Internet access and communication to or from the internet shall occur through an actively managed internet firewall service.

ii. **Remote Access.** If any member of Illumina's Workforce has or shall have remote access to Customer Data, Illumina shall adopt and maintain systems and procedures to secure such connections and transmissions prior to granting remote access, including the use of secure technologies employing multi-factor authentication, authorization and encryption, as applicable.

iii. **Devices.** Illumina shall limit access to Customer Data solely to Illumina owned and/or managed devices. The access, transmission, use, storage and processing of Customer Data in not permitted on any device other than Illumina owned and/or managed devices.

iv. **Wireless Devices.** Illumina will encrypt wireless network data transmission and authentication of wireless devices containing Customer Data to Illumina's network. Illumina shall employ industry standard wireless encryption protocols in accordance with its ISP.

(h) **Software Controls on Illumina's Equipment, Systems and Media.**

i. Illumina shall employ up-to-date and commercially available virus, anti-malware, and other commercially reasonable system security agents (i.e. whitelisting) protection on its equipment and systems, and such protection systems shall include real-time or periodic scans for viruses.

ii. Illumina shall apply security patches to any Illumina equipment and systems that address the confidentiality, integrity, or availability of Customer Data as soon as practicable after they are released, taking into account the criticality of the security patches.

(i) **Security Training and Enforcement.**

i. Workforce who shall have access to the Customer Data or the Products shall receive regular training and instruction regarding security policy and proper security practices in accordance with industry standard practices.

ii. Illumina shall have a process in place for Workforce to report instances of noncompliance with the ISP.

iii. Illumina shall implement technical features or controls to record Security Incidents. Illumina shall investigate and resolve incidents where unauthorized access and attempts are verified.

(j) **Monitoring and Logging.** Illumina network and systems that process Customer Data have the capability to produce system and security logs in accordance with industry standards.

(k) **Data at Rest.** Illumina shall encrypt all Customer Data at rest using methods and algorithms consistent with current National Institute of Science and Technology (NIST) standards.

(l) **Limited Data Collection.** Illumina shall limit the amount of Customer Data collected (or that may be accessed) to that reasonably necessary to accomplish the legitimate purpose for which it is accessed or collected. Illumina shall limit the time Customer Data is retained to that reasonably necessary to accomplish such purpose and comply with applicable laws.

(m) **Return or Destruction.** Upon completion of the functions performed on behalf of Customer and upon written request by Customer, Illumina agrees to, and shall, immediately destroy, or upon Customer's written request, return all Customer Data to Customer, except to the extent it is commercially unreasonable to return and/or destroy such Customer Data. Such return or destruction of Customer Data shall include all originals; however, Illumina may retain copies stored on disaster recovery or other archival systems in accordance with its retention requirements or as otherwise required by applicable laws. If requested by Customer to destroy Customer Data, Illumina shall provide a written attestation to Customer that such Customer Data has been destroyed. If the return or destruction of some or all such Customer Data is commercially unreasonable, Illumina shall (i) retain only that Customer Data which is commercially unreasonable to destroy (ii) return to Customer or destroy the remaining Customer Data that Illumina still maintains in any form; (iii) continue to extend the protections of this Security Agreement and the Data Privacy Agreements to the Customer Data for as long as Illumina retains the Customer Data; and (iv) limit further uses and disclosures of such Customer Data to only those purposes that make return or destruction of the Customer Data commercially unreasonable which applied prior to termination.

(n) **Business Continuity Management.** Illumina shall conduct a business impact analysis for the Products to prioritize their criticality and recovery in order that critical services and data are recoverable in a timely fashion following any business interruption.

(o) Illumina shall document and maintain technical recovery and business resumption plans for the continuity of critical services in the event of an interruption.

(p) **Security Incident Procedures.**

i. Illumina will notify Customer, in writing, of any verified Security Incident of which Illumina becomes aware as soon as practicable.

ii. If a Security Incident caused by Illumina or its agents or subcontractors requires notification to an individual under any law or regulation, Customer will have sole control over the timing, content, and method of notification with respect to the Customer Data, and Illumina will promptly reimburse Customer for reasonable costs and expenses incurred as a result of the breach, subject

to the limitations on liability in the Agreement. Illumina will mitigate, to the extent practicable, any harmful effect that is known to Illumina of an unauthorized use or disclosure of Customer Data by Illumina or its subcontractors in violation of the requirements of this TOMS, the Agreement, or applicable law.

3. **Communication Systems and Access to Information.** During the term of the applicable Agreement, Illumina may receive access to Customer's systems. Such systems are intended for legitimate business use related to Customer's business. Illumina acknowledges that Illumina does not have any expectation of privacy as between Illumina and Customer in the use of or access to Customer's Systems and that access by Illumina to Customer's systems is subject to Customer's scrutiny, use and disclosure, in Customer's discretion. Customer reserves the right, for business purposes, to monitor, review, audit, intercept, access, archive and/or disclose materials received by or from, or stored in any of the Customer Systems. This includes, without limitation, email communications sent by users across the internet and intranet from and to any domain name owned or operated by Customer. Illumina further agrees that it will use appropriate security, such as, for example, encryption and passwords, to protect Customer Data from unauthorized disclosure (internally or externally) when accessing Customer's systems.

SCHEDULE 4: **International Data Transfers**

1. **Definitions**. For the purposes of this **Schedule 4**, the following definitions shall apply:

   (a) "**FADP**" means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1).

   (b) "**FDPIC**" means the Swiss Federal Data Protection and Information Commissioner.

   (c) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

   (d) "**SCCs**" means the Controller-Processor (Module 2) or the Processor-Processor (Module 3) of Standard Contractual Clauses published by the European Commission, as applicable.

   (e) "**UK Addendum**" means template Addendum B.1.0 issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

2. **European Economic Area**. Where Customer transfers Personal Data that is subject to the GDPR to Illumina, and Illumina is located in a country that does not ensure an adequate level of protection within the meaning of the GDPR, the SCCs shall apply as follows:

   (a) The SCCs shall be incorporated into this DPA by reference and be considered duly executed between Customer and Illumina upon entering into force of this DPA.

   (b) Clause 7 (*docking clause* – optional) shall not apply.

   (c) Option 2 (*general authorization*) under Clause 9(a) (*use of sub-processors*) of the SCCs shall apply and "[Specify time period]" shall be replaced with "ten (10) days".

   (d) The option under Clause 11 (redress) shall not apply.

   (e) For the purposes of Clause 13(a) (supervision) of the SCCs, the Data Exporter shall be considered as established in an EU Member State.

   (f) Option 1 under Clause 17 (governing law) of the SCCs shall apply, and the governing law shall be the law of the Netherlands.

   (g) Any disputes arising from the SCCs shall be resolved by courts of the Netherlands (Clause 18 (choice of forum and jurisdiction)).

   (h) For the purposes of Annex I.A, Customer and Illumina can be contacted as set out in **Schedule 1** of this DPA. The activities relevant to the transfer under the SCCs relate to the reception and provision of the Services under the Agreement, as applicable.

   (i) Annex I.B to the SCCs shall be interpreted in accordance with the descriptions in this DPA, including in **Schedules 1 and 2** of this DPA.

   (j) The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) shall be the competent Supervisory Authority for the purposes of Annex I.C to the SCCs.

   (k) Annex II to the SCCs shall be interpreted in accordance with **Schedule 3** of this DPA.

3. **Switzerland**. Where Customer transfers Personal Data that is subject to the GDPR and the FADP to Illumina, and Illumina is located in a country that does not ensure an adequate level of protection within the meaning of those Data Protection Laws, the following additional provisions to the SCCs shall apply in order for the SCCs to be suitable for ensuring an adequate level of protection for such transfer in accordance with Article 16 paragraph 2 letter a FADP:

(a) The FDPIC shall be the competent Supervisory Authority insofar as the data transfer is governed by the FADP.

(b) The law of the Netherlands shall be the governing law.

(c) The courts of the Netherlands shall be the choice of forum (Clause 18), but this shall not exclude individuals in Switzerland from the possibility of bringing a claim in their place of habitual residence in Switzerland, in accordance with Clause 18(c) of the SCCs.

(d) The SCCs protect the data of legal entities in Switzerland until the entry into force of the revised FADP.

4. **United Kingdom**. Where Customer transfers Personal Data that is subject to the Data Protection Laws of the United Kingdom to Illumina, and Illumina is located in a country that does not ensure an adequate level of protection within the meaning of those Data Protection Laws, Customer and Illumina agree to the terms of Part 2: Mandatory Clauses of the UK Addendum. The information included in Part 1 of the UK Addendum is as set out in the Schedules of this DPA. Either Customer or Illumina may end the UK Addendum as set out in Section 19 of the UK Addendum.