DATA PROCESSING AGREEMENT

To the extent Personal Data (as defined in the applicable data protection laws) from the European Economic Area (EEA), the United Kingdom and Switzerland is uploaded by customer and processed by QIAGEN as part of the Principle Agreement (as defined below), the EU-US and/or Swiss-US Privacy Shield, and/or the Standard Contractual Clauses shall apply. For the purposes of the Standard Contractual Clauses, customer and its applicable affiliates are each the data exporter, and customer's acceptance of this Agreement shall be treated as its execution of the Standard Contractual Clauses and Appendices. Herein after QIAGEN and customer shall be collectively referred to as the "Parties" or each individually as a "Party".

WHEREAS:

(A) The Parties entered into a written services agreement or any other relevant agreement (the "**Principle Agreement**") which involves Processing of Personal Data of Data Subjects subject to Data Protection Laws by Processor on behalf of Controller in the context of Services provided under the Principal Agreement (the "**Services**").

(B) This data processing agreement (this "**Agreement**") is hereby attached to and incorporated into the Principal Agreement between the Parties.

NOW, THEREFORE, the Parties agree as follows:

1. Definitions

In this Agreement, save where the context requires otherwise, the following words and expressions have the following meaning:

"**Affiliate**" shall mean any company or undertaking which directly or indirectly through one or more entities, controls or is controlled by or is under common control with either Party. Control shall mean the power to directly or indirectly direct the management and policies of the company or undertaking through for example the ownership of voting rights or by contract.

"**Applicable Law**" shall mean all regional, national and international applicable laws, orders, statutes, codes, regulations, ordinances, decrees, rules, subordinate legislation, treaties, directives, bylaws, standards or other requirements with similar effect of any governmental or regulatory authority, each as updated from time to time which apply to each of the Parties in the circumstances governed by the Agreement, including Data Protection Laws.

"**Controller**" shall have the meaning given to this term in Article 4 of the GDPR.

"**Data Breach**" shall mean any: (a) breach of security, confidentiality or integrity leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of or access to Personal Data transmitted, stored or otherwise Processed; (b) unauthorized intrusion into, control of, access to, modification of or use of any system that is used by Processor to secure, defend, protect or Process Personal Data; and (c) event which led Processor to suspect or would lead a reasonable person exercising a reasonable level of diligence and investigation to suspect that either (a) or (b) has occurred.

"**Data Protection Laws**" means all federal, state, regional, territorial, national and local laws, regulations and rules by any government, agency or authority that relate to the Processing or the security of Personal Data and which are applicable to Processor or the Processing of Personal Data by Controller. For the avoidance of doubt this includes, where applicable, the EU Data Protection Directive 95/46/EC and its national implementations in each case as amended, replaced or superseded from time to time, including without limitation the GDPR.

"**Data Subject**" shall have the meaning given to this term in Article 4 of the GDPR.

"**Employee**" shall mean any employee, staff member, agency worker or other full-time or temporary, paid or unpaid person working for Processor.

"**GDPR**" shall mean the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council.

"**Personal Data**" shall have the meaning given to this term in Article 4 of the GDPR.

"**Processing**" (or "**Processed**" or "**Process**") shall have the meaning given to this term in Article 4 of the GDPR.

"**Processor**" shall have the meaning given to this term in Article 4 of the GDPR.

"**Standard Contractual Clauses**" shall mean Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (or the -current European Commission approved version of such clauses) permitting transfers of Personal Data to Processors established outside the EU.

"**Sub-processor**" shall mean any third party engaged by Processor or by any other Sub-processor of Processor, with whom Processor enters into a contract, agreement or arrangement whereby it agrees to receive from Processor or from any other Sub-processor Personal Data exclusively with the intention for Processing to be carried out on behalf of Controller in accordance with its instructions, the terms of the Agreement, the Principal Agreement and the terms of the written subcontract.

"**Supervisory Authority**" shall have the meaning given to this term in Article 4 of the GDPR and which has jurisdiction over Processor's Processing of Personal Data.

2. Introduction

2.1. This Agreement governs the manner in which Personal Data shall be Processed. The data processing operation are described in **Schedule 1**.

2.2. Controller provides its own data and agrees and understands that Processor will not verify Personal Data's validity and it is therefore the sole liability of Controller to ensure that Personal Data are collected and transmitted to Processor in compliance with applicable Data Protection Laws. Controller shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Controller acquired Personal Data and shall establish the legal basis for Processing including by providing all notices and obtaining all consents as may be required under Data Protection Laws in order for Processor to Process Personal Data on behalf of Controller in order to provide the Services pursuant to the instructions.

2.3 In addition to any other obligations Controller may have pursuant to the Principal Agreement, Controller shall comply with the terms of this Agreement in connection with the Services.

2.4 Notwithstanding anything to the contrary in the Principal Agreement, if there is any ambiguity or inconsistency in or between the Principal Agreement and this Agreement, the terms and conditions of this Agreement shall take priority.

3. General Personal Data Obligations

3.1. The Parties shall comply with the terms of this Agreement and all applicable Data Protection Laws relating to the collection or Processing of Personal Data.

3.2. Processor shall Process Personal Data on behalf of Controller only in accordance with the Agreement and documented instructions received from Controller. If Processor is legally required to Process Personal Data other than as instructed by Controller, it shall inform Controller before

such Processing occurs, unless the law requiring such Processing prohibits Processor from informing Controller on an important ground of public interest, in which case it shall notify Controller as soon as that law permits it to do so. Processor shall not assume any responsibility for determining the purposes for which and the manner in which Protected Information is Processed.

3.3. Additional instructions outside the scope of this Agreement (if any) require prior written agreement between the Parties, including agreement on any additional fees payable by Controller to Processor for carrying out such instructions. Controller shall ensure that its instructions comply with laws, rules and regulations applicable in relation to Personal Data, and that the Processing of Personal Data in accordance with Controller's instructions will not cause Processor to be in breach of Data Protection Laws and, in particular, of the GDPR.

3.4. Processor shall not publish, disclose, divulge or otherwise permit third parties to access Personal Data except in accordance with this Agreement or with Controller prior written consent.

3.5. Processor shall notify Controller without undue delay about any complaint, communication or request received directly by Processor from a Data Subject and pertaining to their Personal Data, without responding to that request unless it has been otherwise authorized to do so by Controller. Processor shall provide Controller with reasonable assistance in relation to any complaint, communication or request received from a Data Subject.

3.6. Where applicable by virtue of Article 28(3) of the GDPR, Processor will provide reasonable cooperation and assistance to Controller with any data protection impact assessments which are referred to in Article 35 of the GDPR or with any regulatory consultations that Controller is legally required to make or to assist with in respect of Personal Data, taking into account the nature of the Processing and the information available to Processor.

3.7. Upon Controller's request, Processor will assist Controller in the event of an investigation by or a request from any regulator, including a data protection regulator or similar authority, if and to the extent that such investigation or request relates to Personal Data. Processor will take steps reasonably requested by Controller to assist Controller in complying with any obligations in connection with such an investigation or request.

3.8. Processor may charge Controller for its cooperation and assistance set forth in this Agreement that goes beyond the reasonable standards and that will require more than reasonable efforts to comply with.

3.9. Processor will not Process Personal Data for any other purposes than the Services and the purposes indicated by Controller.

4. Compliance

4.1. Processor shall notify Controller about any instruction from Controller which, in its opinion, obviously infringes Data Privacy Laws.

5. Data Transfers

5.1. Where there are transfers of Personal Data from a Member State of the EU or from a Member State of the EEA to a third country outside the EU and outside the EEA, such as to the United States (US), the Parties acknowledge that steps must be taken to ensure that such data transfers comply with Data Protection Laws. The Parties acknowledge that the same or similar obligations

can apply for international transfers of Personal Data from a non-EU country and shall in good faith take the steps required where necessary under applicable Data Protection Laws.

5.2. By this Agreement, Controller grants permission to transfer Personal Data from a Member State of the European Union ("EU")EU or from a Member State of the EEA to a third country outside the EU and outside the EEA, and, in order to ensure that adequate safeguards are in place for Processing and transfer of Personal Data, Processor and Controller accept by this Agreement to enter into the 2021 C-to-P Standard Contractual Clauses adopted by the European Commission in **Schedule 2**.

5.3. Controller will be regarded as the Data Exporter and Processor will be regarded as the Data Importer. The C-to-P Standard Contractual Clauses may be varied or terminated only as specifically set out in the C-to-P Standard Contractual Clauses. In the event of inconsistencies between the provisions of the C-to-P Standard Contractual Clauses and this Agreement or other agreements between the Parties, the C-to-P Standard Contractual Clauses shall take precedence. The terms of this Agreement shall not vary the C-to-P Standard Contractual Clauses in any way. In the event that the C-to-P Standard Contractual Clauses are amended, replaced or repealed by the European Commission or under applicable privacy and data security laws, the Parties shall work together in good faith to enter into any updated version of the C-to-P Standard Contractual Clauses or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with applicable law.

6. Notification of Access Requests and Complaints

6.1. To the extent Controller, in its use of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws, Processor shall comply with any commercially reasonable request by Controller to facilitate such actions to the extent Processor is legally permitted to do so.

6.2. Processor shall promptly notify Controller of: (i) any request to access or have copies of Personal Data; or (ii) any complaint or allegation made to it relating to Personal Data from individuals identified by Personal Data, a Supervisory Authority or other third party (each a "**Data Protection Communication**").

6.3. Processor shall not respond to a Data Protection Communication unless Processor is authorized to do so by Controller or Processor is legally compelled to respond.

6.4. Where Processor is compelled to respond to a Data Protection Communication, unless prohibited by law, it shall permit Controller to make representations and/or participate in the response process to ensure compliance with applicable laws including Data Protection Laws.

6.5. Processor shall provide Controller with commercially reasonable cooperation and assistance in relation to handling of a Data Protection Communication for access to that person's Personal Data, to the extent legally permitted and to the extent Controller does not have access to such Personal Data through its use of the Services.

7. Data Security Requirements

7.1. Processor shall, with regard to the state of the art and costs of implementation as well as taking into account the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, implement, maintain and comply with comprehensive information and network security programs, practices and procedures that govern the Services to ensure a level of security appropriate to the risk.

7.2. In assessing the appropriate level of security, Processor shall take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7.3. Processor implements appropriate technical and organizational measures (including, where applicable by virtue of Article 28(3)(c) of the GDPR, and, as appropriate, the measures referred to in Article 32(1) of the GDPR) to ensure (i) the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (ii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iii) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing; (iv) if possible whether pseudonymization or encryption of Personal Data is appropriate; (v) maintain all appropriate technical and organizational security and confidentiality measures to ensure a level of security appropriate to the risk to Personal Data and protect it from threats or hazards to its security and integrity, as well as accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Personal Data transmitted, stored or otherwise Processed and all other unlawful forms of Processing. The technical and organizational measures detailed in **Appendix 2 of Schedule 2** are accepted and deemed appropriate by Controller.

8. Data Breach

8.1. Processor shall notify Controller in writing within 36 hours after it is notified of or discovers or would have discovered had it exercised reasonable diligence a Data Breach. Processor shall provide Controller with all reasonable assistance in investigating and mitigating the impact of any such Data Breach. Processor will also provide all reasonable assistance to Controller in relation to its obligations to provide adequate notifications to the relevant Supervisory Authorities and affected Data Subjects.

8.2. Unless legally required by Data Protection Laws, Processor will not disclose the Data Breach to any third party without first obtaining Controller's prior written consent.

9. Certification and Audits

9.1 Processor shall create, protect and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate information system activity and to ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

9.2 At Controller's written request to Processor, Controller can conduct a security audit of Processor's facilities, systems, policies, controls and practices by Controller or representatives of Controller, including without limitation an independent third-party auditor ("**Controller Audit**").

9.3 Controller Audit shall (i) occur at a mutually agreeable time not more than once during any given calendar year and once following each Data Breach; (ii) not unreasonably interfere with Processor's operations. Any third party performing such Controller Audit on behalf of Controller shall execute a standard nondisclosure agreement with Processor with respect to the confidential treatment and restricted use of information gathered in conducting the audit, and access to Processor's facilities shall be subject to Processor'' reasonable access requirements and security policies. Notwithstanding the foregoing, Processor's access requirements, security policies and the nondisclosure agreement, if applicable, shall in no way materially impede Controller, or a third

party auditor selected by Controller, from conducting a Controller Audit. The specific situations where Controller can conduct a Controller audit are detailed below.

9.4 Where a Controller Audit discloses a material breach in Processor security system, Processor will reimburse Controller of the cost of Controller Audit. In any other case, Controller Audit will entirely remain at Controller's expenses.

10. Sub-processing

10.1 Controller acknowledges and specifically authorizes Processor's use of its Sub-processors existing as of the effective date, and Processor's Affiliates. A current list of Sub-processors as may be used for Processing Data is available to Controller without charge.

10.2 Controller hereby gives a general authorization to further Sub-processors, for any Processing of Personal Data performed on behalf of Controller under this Agreement, provided Processor gives a prior written notification of the identity of the Sub-processor to Controller and Controller does not reasonably object to the appointment. Where such a Sub-processor is engaged, Processor will :

10.2.1. Ensure that it has a written contract, agreement or arrangement in place with the relevant Sub-processor which imposes on the Sub-processor the same obligations in respect of Processing of Personal Data as are imposed on Processor under this Agreement; and

10.2.2. Provide a copy of the Processing Subcontract to Controller upon request, subject to reasonable confidentiality restrictions that may be applicable. Processor shall ensure that any confidentiality restrictions in the sub-contract do not prevent it from showing to Controller those provisions which demonstrate Processor's compliance with its obligations under Data Protection Laws.

11. Indemnity

11.1 The liability of each Party under this agreement shall not be subject to the exclusions and limitations of liability set out in the Principal Agreement. Notwithstanding any provisions elsewhere in the Agreement to the contrary, including but not limited to any indemnity set forth elsewhere in the Principal Agreement, each Party shall indemnify, defend and hold harmless the other Party and its Affiliates and their respective shareholders, directors, officers, Employees and agents from and against any and all liabilities, damages, losses, penalties, fines, costs and expenses, including reasonable attorneys' fees (each, an "**Indemnifiable Loss**"), paid or incurred by them in connection with any claim, suit, proceeding, action or demand (a "**Claim**") based upon or arising from: (i) the breach of the terms of this Agreement by such Party; or (ii) any third party claim including Supervisory Authorities or other national authority's Claim in relation to Personal Data that arise as a result of or in connection with such Party's failure to comply with its obligations under this Agreement or the Data Protection Laws.

12. Allocation of Costs

12.1. Each Party shall perform its obligations under this Agreement at its own cost, unless otherwise stated in the Agreement.

13. Miscellaneous

13.1 Any disputes or claims howsoever between the Parties arising under this Agreement, including disputes regarding its existence, validity, infringement, termination or the consequences of its nullity, will be subject to the exclusive jurisdiction of the courts set forth in the Principal Agreement.

13.2. In the event of inconsistencies between the provisions of this Agreement and other agreements between the Parties, the provisions of this Agreement shall prevail with regard to the Parties' data protection obligations relating to Personal Data. In cases of doubt, this Agreement shall prevail, in particular, where it cannot be clearly established whether a clause relates to a Party's data protection obligations.

13.3. This Agreement may only be modified by a written amendment signed by authorized representatives of each of the Parties.

13.4. The Parties agree that this Agreement is terminated upon the termination of the Principal Agreement.

13.5. If any provision of this Agreement is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this Agreement and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

SCHEDULE 1

DETAILS OF PROCESSING

a. The Personal Data is subject to the following processing activities: collecting, sorting, saving, transferring, analyzing, restricting and deleting data in the IT system.

b. The duration of the data Processing to be carried out by Processor shall be for the period stated in the Principal Agreement.

c. The nature and purpose of the data Processing to be carried out by Processor is performing the Services under the Principal Agreement.

d. The Personal Data transferred concern the following categories of Personal Data (***please select all that apply***) :

- ☐ Employee master data (such as name, address, date of birth, employee number, job title)
- ■ Communication information (such as phone and fax number, email)
- ☐ Employment history
- ☐ Contract master data (such as contractual relationship, name, address of personnel of contractual partner, etc.)
- ☐ Bank account and/or credit card information
- ☐ Employee salary
- ☐ Information on contract billing and payment details
- ☐ Credit reports, credit scores and fraud alerts
- ■ Internet protocol address (IP address)
- ☐ URLs (Web universal resource locator)
- ■ Any other identifier that permits the physical or online contacting of a specific individual
- ☐ Photographic images of data subjects
- ☐ Human clinical samples
- ■ Other: Genomic variant coordinates and data, gene expression data and minimal set of sample metadata needed for analysis
- ■ Other: Account and system information required to obtain and login to an account on relevant system

e. The Personal Data transferred concern the following categories of Data Subjects (***please select all that apply***):

- ☐ Employee
- ☐ Freelancer, consultants
- ■ Patient
- ■ Customer
- ■ Healthcare professional (HCP)
- ■ Employee of healthcare organizations (HCOs), such as doctor or nurse
- ■ Study staff in clinical trials
- ☐ Pharmacist
- ☐ Employee of pharmacies

- ■ Contractual partners (such as personnel of customers, suppliers, service providers, investors)
- ☐ Potential contacts/contractual partner or potential business contacts such as CEO of a potential business partner)
- ☐ Complainant
- ■ Contacts (persons approaching Controller with questions about products, such as consumers)
- ☐ Healthy volunteers
- ☐ Other: _____

f. The Personal Data transferred concern the following special categories of Data (***if applicable***):

- ■ Information about physical or psychical health
- ■ Medical care information (e.g., results of tests, medications)
- ■ Biometric identifiers (DNA, finger, iris and voice prints)
- ☐ Criminal charges and convictions and court records
- ☐ Information regarding sex life or sexual orientation
- ■ Racial or ethnic origin
- ☐ Religious or philosophical beliefs
- ☐ Trade-union memberships

SCHEDULE 2

C-to-P Standard Contractual Clauses

1. Purpose and Scope

1.1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

1.2. The Parties:

1.2.1. The natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A (hereinafter each "data exporter"), and

1.2.2. The entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

1.3. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

1.4. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

2. Effect and Invariability of the Clauses

2.1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

3. Third-party Beneficiaries

3.1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

3.1.1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

3.1.2. Clause 8.1(b), 8.9(a), (c), (d) and (e);

3.1.3. Clause 9(a), (c), (d) and (e);

3.1.4. Clause 12(a), (d) and (f);

3.1.5. Clause 13;

3.1.6. Clause 15.1(c), (d) and (e);

3.1.7. Clause 16(e);

3.1.8. Clause 18(a) and (b)

3.2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

4. Interpretation

4.1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

4.2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

4.3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

5. Hierarchy

5.1. In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

6. Description of the Transfer(s)

6.1. The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

7. Docking Clause

7.1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

7.2. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

7.3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

8. Data Protection Safeguards

8.1. The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.2. Instructions

8.2.1. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

8.2.2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.3. Purpose limitation

8.3.1. The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.4. Transparency

8.4.1. On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.5. Accuracy

8.5.1. If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.6. Duration of processing and erasure or return of data

8.6.1. Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.7. Security of processing

8.7.1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects.

The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.7.2. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.7.3. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

8.7.4. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.8. Sensitive data

8.8.1. Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8.2. Onward transfers

8.8.3. The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

8.9. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.10. Documentation and compliance

8.10.1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

8.10.2. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

8.10.3. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

8.10.4. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

8.10.5. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

9. Use of Sub-processors

9.1. The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

9.2. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

9.3. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

9.4. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

9.5. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become

insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

10. Data Subject Rights

10.1. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

10.2. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

10.3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

11. Redress

11.1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

11.2. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

11.3. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

11.3.1. Lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

11.3.2. Refer the dispute to the competent courts within the meaning of Clause 18.

11.4. The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

11.5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

11.6. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

12. Liability

12.1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

12.2. The data importer shall be liable to the data subject and the data subject shall be entitled to receive compensation for any material or non-material damages the data importer or its sub-

processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

12.3. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject and the data subject shall be entitled to receive compensation for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

12.4. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

12.5. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

12.6. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

12.7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

13. Supervision

13.1. The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

13.2. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

14. Local Laws and Practices Affecting Compliance with the Clauses

14.1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679 are not in contradiction with these Clauses.

14.2. The Parties declare that, in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

14.2.1. The specific circumstances of the transfer, including the length of the processing chain; the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

14.2.2. The laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer and the applicable limitations and safeguards;

14.2.3. Any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

14.3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

14.4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

14.5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

Following a notification pursuant to paragraph (e) or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

15. Obligations of the Data Importer in Case of Access by Public Authorities

15.1. Notification

15.1.1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

15.1.2. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

15.1.3. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

15.1.4. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

15.1.5. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2. Review of legality and data minimization

15.2.1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

15.2.2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

15.2.3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

16. Non-compliance with the Clauses and Termination

16.1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses for whatever reason.

16.2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

16.3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

16.4. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

16.5. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

17. Governing Law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

18. Choice of Forum and Jurisdiction

18.1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

18.2. The Parties agree that the jurisdiction and venue shall be the courts of Germany.

18.3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

18.4. The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX 1 OF SCHEDULE 2

DESCRIPTION OF THE TRANSFERS (CONTROLLER TO PROCESSOR)

This Appendix forms part of the Standard Contractual Clauses and must be completed and signed by the Parties.

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

Data exporter

The Data Exporter is Controller. Controller is transferring de-identified personal data to perform genetic variant interpretation services for the purpose of clinical decision support**.**

Data importer

The Data Importer is Processor. Processor is receiving de-identified personal data to perform genetic variant interpretation services for the purpose of clinical decision support.

Data subjects

The personal data transferred concern the following categories of data subjects (***please select all that apply***):

- ☐ Employee
- ☐ Freelancer, consultants
- ■ Patient
- ■ Customers
- ■ Healthcare professional (HCP)
- ■ Employee of healthcare organizations (HCOs), such as doctor or nurse
- ■ Study staff in clinical trials
- ☐ Pharmacist
- ☐ Employee of pharmacies
- ■ Contractual partners (such as personnel of customers, suppliers, service providers, investors)
- ☐ Potential contacts/contractual partner or potential business contacts such as CEO of a potential business partner)
- ☐ Complainant
- ■ Contacts (persons approaching Controller with questions about products, such as consumers)
- ☐ Healthy volunteers, as specified in the Principal Agreement
- ☐ Other: _____

Categories of data

The personal data transferred concern the following categories of data (***please select all that apply***) :

- ☐ Employee master data (such as name, address, date of birth, employee number, job title)
- ■ Communication information (such as phone and fax numbers, email)
- ☐ Employment history
- ☐ Contract master data (such as contractual relationship, name, address of personnel of contractual partner, etc.)

☐ Bank account and/or credit card information

☐ Employee salary

■ Information on contract billing and payment details

☐ Credit reports, credit scores and fraud alerts

■ Internet protocol address (IP address)

☐ URLs (Web universal resource locator)

☐ Any other identifier that permits the physical or online contacting of a specific individual

☐ Photographic images of data subjects

■ Human clinical samples

■ Other: Genomic variant coordinates and data, gene expression data and minimal set of sample metadata needed for analysis.

■ Other: Account and system information required to obtain and login to an account on relevant system

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (***if applicable***):

■ Information about physical or psychical health

■ Medical care information (e.g., results of tests, medications)

■ Biometric identifiers (DNA, finger, iris and voice prints)

☐ Criminal charges and convictions and court records

☐ Information regarding sexual life or sexual orientation

■ Racial or ethnic origin

☐ Religious or philosophical beliefs

☐ Trade-union memberships

Processing operations

The personal data transferred will be subject to the following basic processing activities: collecting, sorting, analyzing, saving, transferring, restricting and deleting data in the IT system.

Frequency of the transfer (please select one that apply)

■ Data are transferred on a one-off basis

☐ Data are transferred on a continuous basis

Period retention
According to applicable laws, to comply with the statutory limitation periods

APPENDIX 2 OF SCHEDULE 2

QIAGEN technical and organizational security measures

Requirements of the technical and organizational measures for implementing and complying with the requirements of Article 32 of the GDPR

The processor is to implement the measures described in this Annex provided that the measure in question contributes or is likely to contribute, directly or indirectly, to the protection of personal data under the agreement concluded between the parties concerning the processing order.

The technical and organizational measures are subject to technical progress and further development. The processor is therefore permitted to implement alternative adequate measures. The measures defined here must be of an appropriate security level. Significant changes must be coordinated with the controller and documented. In cases of doubt, the processor must prove that the alternative measure ensures the same protection objective and a comparable level of protection.

1. Data Protection Organization and Control Procedures

a) Data protection organization/management

The processor is to ensure that all data protection requirements are observed within the company.

(1) As well as training and sensitizing employees, this also includes the mandatory implementation of guidelines, processes, forms, etc.
(2) The general principles of data protection (cf. Article 5 (1) GDPR) are to be fully observed and appropriate evidence is to be provided (Article 5 (2) GDPR).
(3) The principle of data protection by default is to be observed (Article 25 GDPR).
(4) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing has been implemented.
(5) An overview of the data processing carried out as part of the order is available and can be provided to the controller upon request (Article 30 (2) GDPR).
(6) It is to be ensured that instructions from the controller are immediately forwarded to the appropriate persons for further compliance and that the processing of order data is carried out only in accordance with the order or instruction.
(7) An incident-response management organization is to be established and to be responsible for defining the reporting channels, so that relevant incidents are immediately reported to the controller.

b) Pseudonymization and encryption of personal data

(1) In principle, the processor is to process the personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person (pseudonymization).

(2) In principle, the processor is to ensure that the personal data is converted into a character sequence (ciphertext) that is not easily interpretable. The encryption procedure is to correspond to the technical state of the art.

2. Confidentiality

a) Unauthorized persons are to be denied access to data processing equipment that processes or uses personal data (access control).

<u>The processor is to take the following measures for access control if order data is processed on the processor's premises, or if the possibility of access to such data from the premises is not ruled out:</u>

(1) Restriction of access authorization to office buildings, computer centers and server rooms to a strict minimum.

(2) Effective control of access authorization through an adequate locking system (e.g., security keys with documented key management, electronic locking systems with documented management of authorizations).

(3) Documented and verifiable processes for obtaining, altering and revoking access authorizations.

(4) Regular and documented review of the assigned access authorizations for up-to-dateness.

(5) Appropriate measures for prevention and detection of unauthorized access and attempted access (e.g., regularly testing the anti-burglar security of doors, gates and windows, burglar alarm system, video surveillance, guard duty, security patrol).

(6) Written regulations for employees and visitors concerning the handling of technical access control measures.

b) Unauthorized persons are to be prevented from using data processing systems (access control).

The processor is to take the following measures for access control to systems and networks that process data or that may be used to access or to order data:

(1) Restriction of access authorization to IT systems and non-public networks to a strict minimum.

(2) Effective control of access authorization by means of personalized and unique user IDs and a secure authentication process.

(3) When passwords are used for authentication

a. there are guidelines that ensure consistent password quality of at least eight characters (upper-case letters, lower-case letters, numbers, special characters) and a change interval of ninety (90) days at most, or blocking after ninety (90) days in cases of inactivity

b. technical testing procedures are used to ensure password quality

(4) Documented and verifiable processes for obtaining, altering and revoking access authorizations.

(5) Regular and documented review of the assigned access authorizations for up-to-dateness.

(6) Appropriate measures for securing the network infrastructure (e.g., network port security in accordance with IEEE 802.1X, intrusion detection systems, use of two-factor authentication for remote access, separation of networks, content filters, encrypted network protocols, etc.).

(7) Written regulations for employees for the handling of the above security measures and the secure use of passwords.

(8) Updates/patches according to the following matrix:

Category	**Implementation time for assets connected to the internet**	**Implementation time for assets not connected to the internet**
Emergency	12 hours	24 hours
Critical	1 week	1 month
Important/high	2 weeks	2 months
Moderate/medium/low	To the best of Processor's ability, after six weeks at the latest	To the best of Processor's ability, after ten weeks at the latest

Network:

- The firmware version for firewalls is updated once a year.
- The Unified Threat Management (UTM) package for firewalls is updated daily.
- Emergency patches/fixes will be applied as soon as possible, followed by an emergency change.

Windows/workstations

- Windows servers/clients (third-party patches) are patched monthly.
- Security patching includes all types of patches (critical, high, medium and low).
- Emergency patches/fixes will be applied as soon as possible, followed by an emergency change.

Linux:

- Red Hat/Linux servers are patched quarterly.
- Emergency patches/fixes will be applied as soon as possible, followed by an emergency change.

3. Integrity

a) It is to be ensured that persons authorized to use a data processing system have access only to data subject to their access authorization and that personal data cannot be read, copied, altered or removed by unauthorized persons during processing or use or after storage (access control).

The processor is to take the following measures for access control if he or she is responsible for order-data access authorizations:

(1) Restriction of access authorization to order data to a strict minimum

(2) Effective control of access authorization by means of an appropriate privilege and role strategy

(3) Documented and verifiable processes for obtaining, altering and revoking access authorizations

(4) Regular and documented review of the assigned access authorizations for up-to-dateness

(5) Appropriate measures to protect end devices, servers and other infrastructure elements against unauthorized access (e.g., multi-level anti-virus strategy, content filters, application firewalls, intrusion detection systems, desktop firewalls, system hardening, content encryption)

(6) Data carrier encryption with algorithms that are in accordance with the current state of the art to gbe classified as secure for the protection of mobile devices (laptops, tablet PCs, smartphones, etc.) and, to some extent, of data carriers (external hard drives, USB sticks, memory cards, etc.). QIAGEN offers its employees USB sticks that are already encrypted

(7) Access logging, including by administrators

(8) Technical security measures for export and import interfaces (hardware- and application-related)

The processor has the following cooperation obligations for access control, unless it is the processor who manages the order data access rights:

(1) Documented and verifiable processes for requesting, altering and revoking access authorizations within his or her area of responsibility

(2) Regular and documented review of the assigned access authorizations for up-to-dateness where possible

(3) Immediate notification of the controller if existing access authorizations are no longer required

b) It is to be ensured that it is subsequently possible to verify and establish whether and by whom personal data has been entered into, altered in or removed from data processing systems (input control).

The processor is to use the following input control measures for his or her systems that are used for processing order data or that enable or mediate access to such systems:

(1) Creation and audit-proof storage of processing logs

(2) Protection of log files against manipulation

(3) Logging and evaluation of incorrect logon attempts

(4) Ensuring that no group accounts (including administrators or root) are used

Items 1) – 4) are supported by the QIAGEN Active Directory

c) The controller is to make the data to be processed available by a transmission procedure as defined in the contract/order. The results of the processing are also to be transmitted to the controller by a defined transmission procedure. The method of transmission and the security measures for the transmission (transmission control) are to be determined in accordance with the requirements. In particular, the use of state-of-the-art encryption technology is to be provided for.

It is to be ensured that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or during transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data is to be transmitted using data transmission equipment.

The processor is to take the following measures for transmission control if order data is received, transmitted or transported by the processor:

(1) Appropriate measures for securing the network infrastructure (e.g., network port security in accordance with IEEE 802.1X, intrusion detection systems, use of two-factor authentication for remote access, separation of networks, content filters, encrypted network protocols, etc.)
(2) Data carrier encryption with algorithms that are in accordance with the current state of the art to be classified as secure for the protection of mobile devices (laptops, tablet PCs, smartphones, etc.) and, to some extent, of data carriers (external hard drives, USB sticks, memory cards, etc.). QIAGEN offers its employees USB sticks that are already encrypted
(3) Use of secure encrypted transmission protocols (e.g., TLS-based protocols) in accordance with the current state of the art
(4) Testing mechanisms for identifying the remote station during transmissions
(5) Checksum comparison for received data
(6) Written regulations for employees for the handling and security of mobile devices and data carriers

4. Availability and Resilience

a) It is to be ensured that personal data is protected against accidental destruction or loss.

The processor is to implement the following availability control measures if the processing in the order is required for maintaining operational service:

(1) Operating and regularly maintaining fire alarm systems and power supply equipment (e.g., UPS, emergency power, etc.) in server rooms, data centers and important infrastructure rooms
(2) Creating daily backups
(3) Securing backup storage in a separate fire compartment
(4) Regularly checking backups for integrity
(5) Processes and documentation for restoring systems and data

5. Erasure of Data

Personal data processed for specific purposes is to be erased when it is no longer necessary for the fulfillment of the storage purpose. Erasure is the obliteration of stored personal data.

The processor is to take the following measures to ensure erasure of data, insofar as these are within his or her area of responsibility:

(1) Ensuring that the order data can be permanently erased at the request of the controller
(2) Using processes, tools and documentation to securely erase in such a way that it is not possible to restore the data according to today's state of the art (e.g., by overwriting)
(3) Ensuring the verifiability of erasures performed (logging)

(4) Specifications for employees as to how and when what data is to be erased

APPENDIX 3 OF SCHEDULE 2

LIST OF SUB-PROCESSORS

The controller has authorized the use of the following sub-processors:

Name: …not applicable

Address: …

Contact person's name, position and contact details: …

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized):