Karolinska Institutet

DATA PROCESSING AGREEMENT

This data processing agreement (the "**DPA**") has been entered into by

(1) **KAROLINSKA INSTITUTET**, Universitetsförvaltningen, org.nr 202100-2973, Nobels väg 5, 17177 Stockholm, Sweden, ("**KI**"); and

(2) **Agilent Technologies**, org.nr 556573-6773, Kronborgsgränd 1, 16446, Stockholm, Sweden, (the "**Processor**")

hereinafter jointly referred to as "**Parties**" and separately as "**Party**".

These persons shall be the Parties' contacts in regard to this DPA.

For KI
Name: Marith Wiedersheim-Paul
Address: Nobels Väg 5, 17177 Stockholm
Telephone: +46 8 52486173
E-mail: Marith.Wiedersheim-Paul@ki.se

For Processor
Name: Jesper Hoejlund
Address: Kronoborgsgränd 1
Telephone: +46 24632665
E-mail: Jesper.Hojlund

1. PURPOSE OF THE AGREEMENT

KI is the Controller of Personal Data originating from KI´s Core facilities containing information on personal data.

The Parties have agreed that the Processor shall perform particular duties involving Web based IT solution for providing Core facilities (the "**Assignment**") for and on behalf of KI.

In execution of the Assignment, KI shall furnish the Processor with Personal Data. In signing this DPA, the Processor becomes Personal Data Processor charged to process Personal Data for and on behalf of KI. This DPA forms part of the principal agreement between the Parties dated 2019-06-24 , Core facility management system 2-5229/2017 the "**Principal Agreement**"), that governs the Assignment and further details the purpose of the Processing.

This DPA applies where the Processor is processing Personal Data on behalf of KI.

This DPA further defines the technical and organizational measures that the Processor implements and maintains to protect Personal Data, as set out in **Schedule 1**.

2. DEFINITIONS

The following terms shall have the following meanings in this Agreement.

"**Data Controller**", shall mean an entity that alone or jointly with others determines the purposes and means of the Processing of Personal Data.

"**Data Processor**", shall mean an entity that Processes Personal Data on behalf of the Data Controller.

"**Data Protection Laws**", shall mean the relevant data protection and privacy laws to which the Parties are subject, in particular (but not limited to) 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, (and repealing Directive 95/46/EC) (General Data Protection Regulation), and any applicable laws and regulations relating to the processing of Personal Data in the field of research and development.

"**Model Clauses**", shall mean the model clauses for the transfer of Personal Data to Data Processors established in third countries as approved by the European Commission from time to time, at present the model clauses set out in the European Commission's Decision 2010/87/EU of 5 February 2010.

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

"**Processing**", shall mean any operation which is performed on Personal Data, whether or not by automated means, such as collection, organisation, structuring, storage, use, dissemination or otherwise making available, erasure or destruction.

"**Subprocessor**", shall mean any processor which the Data Processor engages to carry out specific Processing activities on behalf of the Data Controller, such as a subcontractor.

3. PROCESSING OF PERSONAL DATA

3.1 The Parties acknowledge and agree that with regard to the Processing of Personal Data, KI is the Data Controller and the Processor is the Data Processor.

3.2 All Processing of Personal Data under this DPA shall be carried out in accordance with all applicable Data Protection Laws.

3.3 The Processor shall:

a) comply with all Data Protection Laws and other laws generally applicable to the Assignment.

b) process the Personal Data only in accordance with the written instructions from KI, as may be further set out in the Principal Agreement, and this DPA. The Processor will not use or disclose the Personal Data for any other purposes.

c) notify KI if it considers an instruction from KI to be in violation of Data Protection Laws. Processor shall follow and comply with any additional instructions received from KI provided that they are legally required, technically feasible and do not require any material modifications of the Assignment. If the Processor is unable to comply with an additional instruction, it shall promptly notify KI hereof.

d) process the Personal Data only to the extent, and in such manner, as is necessary for the Assignment.

e) implement and maintain appropriate technical and organisational measures as set out in **Schedule 1**. KI understands and agrees that these measures are subject to technical progress and development and the Processor is therefore expressly allowed to implement alternative measures provided that they maintain or exceed the general security level described in **Schedule 1**.

f) ensure that confidentiality applies to Personal Data and that access is strictly limited to the personnel who require access for the Assignment.

g) ensure that all of its personnel engaged in the Processing of Personal Data (i) are informed of the confidential nature of the Personal Data, (ii) have received appropriate training of their responsibilities and (iii) have executed written confidentiality agreements or are under an appropriate statutory obligation of confidentiality. The Processor shall ensure that such confidentiality obligations survive the termination of their personnel arrangement.

h) assist KI in meeting the obligations KI is made subject to by Data Protection Laws, in particular to facilitate the exercise of the data subjects' rights under such laws. That includes but is not limited to an obligation for the Processor to (i) block, erase or anonymize Personal Data, (ii) provide information about the Processing activities, (iii) furnish Data Subjects with information about and access to their Personal Data, (iv) rectify incorrect Personal Data and (v) provide KI with Personal Data in a structured, commonly used and machine-readable format. The Processor undertakes to perform such actions when required and as instructed by KI.

i) without undue delay and in accordance with Data Protection Laws notify KI of any incident concerning unauthorised disclosure of Personal Data ("**Incident**"). Such notification shall in any event be given KI within forty-eight (48) hours of first discovering an Incident.

3.4 The Processor shall indemnify and hold harmless KI from and against any and all losses, damages, and expenses (including without limitation legal fees) awarded against KI and arising from a claim brought as a result of the Processor's breach of its obligations under this DPA or Data Protection Laws ("**Claim**"); *provided, however*, that the indemnity shall not extend to any Claim arising from (i) a negligent act or omission of KI and/or its personnel, (ii) any misconduct by KI and/or its personnel and/or (iii) any breach of this DPA by KI.

3.5 The Processor shall not be entitled to any additional payment for performing the obligations set out in this DPA.

4. THIRD PARTY REQUESTS FOR PERSONAL DATA

All third party requests regarding Personal Data or information about the Processing activities under the Principal Agreement shall be redirected to KI, whether the request is made by a data subject, the data protection authority or any other third party, unless such requests cannot legally be redirected to KI. The Processor shall promptly notify KI of all third party requests for information related to this DPA. The Processor further undertakes to assist KI to make Personal Data and information about the Processing activities under the Principal Agreement available to any third party making a request for such information.

5. USE OF SUBCONTRACTORS

5.1 Always subject to all applicable laws and regulations (including but not limited to Data Protection Laws) and provided that KI has given prior written approval, the Processor may use one or more Subprocessors to Process Personal Data during the course of carrying out the Assignment. In such case, the Processor must enter into a written agreement with each Subprocessor which requires the Subprocessor to comply with terms no less protective than the terms that the Processor is made subject to under this DPA.

5.2 The Subprocessor(s) may only Process Personal Data in order to carry out the Assignment. The Subprocessors are bound by KI's written instructions and may under no circumstances Process Personal Data for any other purpose. The Processor remains responsible for all Subprocessors it uses to carry out the Assignment. The Processor's responsibility for its Subprocessor(s) includes ensuring Subprocessors' compliance with the obligations of this DPA.

5.3 KI shall receive a list of all Subprocessors used by the Processor. Such list shall include particulars such as the name, corporate form, contact information, address and role of each Subprocessor. The information shall be communicated to KI by e-mail. The Processor must obtain prior written approval from KI before exchanging or adding any Subprocessor(s) to the list.

5.4 The Processor may not transfer Personal Data to a Subprocessor in a country outside of the EU/EEA (**"Third Country"**) unless KI has approved such transfer in writing, and the Processor has entered into the Model Clauses with the Subprocessor. The Processor may also transfer

Personal Data to the US, with KI's prior written consent, if the recipient is registered under the Data Privacy Shield according to the decision of the EU Commission 2016/1250.

6. AUDIT

6.1 KI shall be entitled, through follow-up, to verify the Processor's compliance of this DPA and the measures in **Schedule 1**. In conjunction with such follow-up, the Processor shall provide KI, or the third-party examiner engaged by KI, such access to premises or systems as are necessary. The Processor will on a regular basis audit the security of the computers and computing environment that it uses in Processing Personal Data when carrying out the Assignment.

6.2 Upon written request by KI, the Processor will, without undue delay, provide KI with a summary of the results of any audit so that KI can reasonably verify the Processor's compliance with the obligations under this DPA.

6.3 The Processor shall ensure that a data inspection authority may perform audits as provided for according to Data Protection Laws. In the event Personal Data is requested from any data inspection authority, the Processor must without undue delay refer such requests to KI.

7. MISCELLANEOUS

7.1 No Party may assign, subcontract or otherwise transfer this DPA without the prior written consent of the other Party.

7.2 At the request of KI and/or upon termination of this DPA, the Processor shall either return or delete the Personal Data in such a way that it cannot be recovered, as instructed by KI. In case the Processor is unable to return or delete the Personal Data as instructed, the storage media where the Personal Data concerned is stored is to be destroyed. In the event KI directs that Personal Data is returned, it shall be returned within thirty (30) days of completion of the Assignment or termination of this DPA.

7.3 This DPA shall continue to apply for the duration of the Processing activities under the Principal Agreement, notwithstanding any termination or expiration of the same. The Processor's obligation to ensure that confidentiality applies to Personal Data continues to apply even after the termination of this DPA.

7.4 If there is any conflict between any provision of this DPA and any provision of the Principal Agreement, the provisions of this DPA shall prevail.

7.5 Except for changes made by this DPA, the Principal Agreement remains unchanged and in full force and effect.

7.6 KI shall always have a one-sided right to change any terms and conditions in this DPA to ensure that Data Protection Laws are complied with. Such changes shall enter into force within thirty (30) days after the Processor has received a notification from KI unless the Processor promptly notifies KI that it is unable to comply with the changes. In case the Processor is unable to comply with such changes, KI shall have a one-sided right to terminate all agreements with the Processor that include Processing of KI's Personal Data, with immediate effect. Any other changes to the terms and conditions in this DPA shall be made in writing and duly signed by the Parties to come into effect.

7.7 KI reserves the right to terminate all agreements with the Processor that include Processing of KI's Personal Data upon written notification with immediate effect in the event of a serious breach by the Processor and/or any Subprocessor.

7.8 This DPA is governed by the laws of Sweden. Any dispute arising out of or in connection with this DPA shall be settled by the courts of Sweden with the district court of Stockholm as first instance.

8. SIGNATURES

This DPA has been drawn up in two originals of which the parties have taken one each.

Bayer Karolinska Institutet 2021002973	**Seller** Agilent Technologies 556573-6773
City/date	City date
Solna 2019-07-03	Kista 20190624
Signature	Signature
Printed name	Printed name
Nils Emlund	Martin Steen
Position	Position
Head of procurement	Service Business Manager

TECHNICAL AND ORGANIZATIONAL MEASURES

This schedule provides instructions to the processor. The controller has a right to verify compliance in accordance with the terms of the data processing agreement.

1. Any computer equipment and portable storage media that is not supervised must be securely locked up in order to protect against unauthorized access, manipulation and theft. Premises containing such equipment shall always be protected with such physical security measures deemed necessary to ensure that only authorized personnel is granted access.

2. Personal data shall regularly be backed up. Backup copies shall be kept separate and protected as to allow restoration in case of a disruption. The processor shall implement routine testing of readback capability.

3. Access to personal data shall be controlled with a technical solution for authentication. Authorization shall be limited to only those in need of the data for their work. User identity and passwords shall be personal and may not be transferred to someone else. The processor shall implement routines for the granting and revoking of rights.

4. Access to personal data shall be traceable through the use of logs or similar solutions that allows the processor to verify access and report back to the controller.

5. Any external connection for communication of data must be protected by a technical solution that ensures that the connection is authorized.

6. The transfer of personal data by technical means outside of the processor's control and supervision shall employ encryption.

7. Systems and components shall carry active security measures configured in such a way that they provide adequate levels of protection for the personal data.

8. Whenever mounted or portable storage media containing personal data are taken out of use, all personal data shall be deleted in such a way that it cannot be recovered. This may necessitate the destruction of hardware.

9. Written agreements ensuring security and confidentiality must be executed between the processor and any third party carrying out repairs or service of equipment used for the storage of personal data.

10. On-site visits by third parties for repairs and service must be supervised by the processor. If that is not possible, any storage media containing personal data must be removed prior to any such

visit.

11. Service by remote communication is only allowed provided it can be done through a secure connection and a reliable electronic identification of the person performing the service. Access shall only be given for the time required to perform the service. Any separate access way for service shall be closed whenever service is not actively being performed.

12. The controller, or any third party hired by the controller for the purpose, has a right to investigate unauthorized access at the processor.