Data Processing Agreement (DPA)

pursuant to Article 28 General Data Protection Regulation (GDPR)

THIS DPA FORMS AN INTEGRAL PART AND IS INCORPORATED INTO THE ITA OR MSA CONCLUDED BETWEEN THE CUSTOMER OF SUCH ITA OR MDA AS THE CONTROLLER AND NOSTOS GENOMICS GMBH, A GERMAN ENTREPRENEURIAL COMPANY WITH LIMITED LIABILITY WITH ITS REGISTERED SET AT C/O STRESEMANNSTRASSE 123 TENANT GMBH, STRESEMANNSTRASSE 123, 10963 BERLIN GERMANY AS THE PROCESSOR CONCERNING THE PROCESSING OF PERSONAL DATA UNDER THE ITA OR MSA AND ANY ORDER CONCLUDED BETWEEN THE PARTIES IN RELATION THERETO. THE TERMS AND CONDITIONS OF THIS DPA WILL BE LEGALLY BINDING ON THE PARTIES UPON THE EFFECTIVE DATE. UNLESS STATED TO THE CONTRARY HEREINAFTER, THE DEFINITIONS OF THE ITA OR MSA SHALL APPLY. FOR THE AVOIDANCE OF DOUBT, IN CASE OF A CONFLICT BETWEEN THE PROVISIONS OF THE PRESENT DPA AND THE ITA OR MSA, THE FORMER SHALL PREVAIL.

1. Subject matter, term, categories of personal data and data subjects

(1) Providing and supporting the SaaS Solution requires the processing of certain personal data for which Controller is the controller in accordance with applicable data protection laws. Concerning the personal data set out hereinafter, Processor shall act as a processor in accordance with applicable data protection law. The subject matter of this DPA is to set forth the terms and conditions for such processing of personal data by Processor on behalf of Controller.

(2) For the avoidance of doubt, it is, therefore, the sole responsibility and liability of Controller to ensure that personal data is collected and transmitted to Processor in compliance with applicable data protection laws, in particular, to have a legal basis for its processing, and to properly inform data subjects of the collection and processing of their personal data.

(3) Processor shall carry out the following processing activities on behalf of Controller: Providing and supporting the SaaS Solution for the interpretation of genetic sequencing cases with machine learning technologies, including the creation of Aggregated Data, as set out in further detail in the ITA or MSA and the Order Form(s).

(4) This DPA will become effective as of the date the Parties have executed it and, notwithstanding expiry of the term of the ITA or MSA, will remain in effect until, and will automatically expire upon, deletion of all personal data by Processor and/or any applicable sub-processors.

(5) The categories of personal data processed by Processor and the categories of data subjects affected by such processing are set out (a) concerning the ITA, in the main body of the ITA itself, or (b) concerning the MSA, in Annex 1 to each Order Form.

2. Place of Processing; Data Transfers

(1) Controller's personal data will be processed by Processor at its own or its authorized sub-contractor's premises. Usually, any processing activities will, therefore, be carried out in the member states of the European Union or in another state that is party to the Agreement on the European Economic Area.

(2) Processor may not transfer or authorize the transfer of personal data to countries outside the EU and/or the European Economic Area without the prior written consent of Controller. If personal data processed under this DPA is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected (i.e. ensure that the conditions of Art 44 et seq. GDPR are met). To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of

personal data.

3. Technical and Organisational Measures

(1) Prior to the execution of this DPA, Processor undertakes to adopt all the necessary technical and organisational security measures, and to provide Controller with a document whereby all such measures are described in detail, also in specific reference to this DPA. Such measures are subject to Controller's scrutiny and prior approval. Upon Controller's approval, the measures documented above will become an integral and substantial part of this DPA and are hereby incorporated by reference. Insofar as an audit by Controller shows the necessity for amendments, such amendments shall be implemented by mutual agreement of the Parties.

(2) Processor warrants that it has taken all the security measures in accordance with Article 28(3)(c), and Article 32 GDPR in particular in conjunction with Article 5(1) and 5(2) GDPR. Such measures shall guarantee data security and a protection level adequate to the level of risk concerning confidentiality, integrity, availability, and resilience of the systems. According to Article 32(1) GDPR the following must be taken into account when assessing the appropriateness of the security measures adopted: whether or not the measures can be reasonably considered to be state-of-the-art, the implementation costs, the nature, scope and purposes of processing as well as the likelihood of data breaches and the severity of risks to the rights and freedoms of natural persons.

(3) The technical and organisational measures are subject to technical and technological progress and development. Hence, Processor may adopt alternative adequate measures which are up to date with the changed technological environment. When doing so, the processing security level may not be reduced. Substantial changes must be documented.

4. Data subjects’ rights

(1) Processor undertakes to provide full cooperation and assistance, as it may be reasonably possible, in order to assist Controller in responding to data subjects' requests for the exercising of their rights.

(2) In particular, Processor undertakes to (**i**) immediately communicate to Controller any request received by data subjects concerning the exercising of their rights and, if feasible and appropriate, to (**ii**) enable Controller to design and deploy all the technical and organisational measures necessary to answer the data subjects' requests.

(3) Notwithstanding the fact that Controller bears the responsibility to respond to the data subjects' requests, Processor can accept to be tasked with the fulfilment of some specific requests, provided that such tasks do not require disproportionate efforts from Processor and that Controller provides detailed instructions in writing.

5. Further Duties of Processor

In addition to complying with the provisions of this DPA, Processor commits to meet all applicable statutory requirements set forth at Articles 28 to 33 GDPR. To this end, Processor warrants compliance with the following:

a) Data Protection Officer

Processor has appointed a data protection officer whose contact data are as follows: dpo@nostos-genomics.com. Processor will inform Controller about any changes in these contact data without undue delay.

b) Confidentiality

Processing activities under this DPA shall only be performed by individuals (such as employees, agents, or staff members) that have been instructed by Processor on the appropriate way to process data and have been contractually subjected to confidentiality pursuant to Article 28(3)(b) and Article 32 GDPR. Processor, and any person acting under its authority who has access to the personal data, shall not process that data unless acting upon instructions given by Controller – incl. the powers granted under this DPA – unless they are required to do so by statutory law.

c) Technical and Organisational Measures

Implementation of, and compliance with, all appropriate technical and organisational measures in the framework of this DPA, in particular as set forth at art. 32 GDPR. Processor shall periodically monitor the internal processes and the technical and organisational measures to ensure that processing activities pertaining to it are carried out in accordance with the requirements of applicable data protection law and the protection of data subjects' rights. Processor shall grant verifiability of the technical and organisational measures to Controller as part of Controller's supervisory powers referred to in Section 7 of this contract.

d) Cooperation with Supervisory Authorities

The Parties shall cooperate, upon request, with the supervisory authority. Processor shall notify Controller without undue delay about any inspections and measures executed by the supervisory authority, insofar as they relate to the activities under this DPA. This also applies insofar as Processor is under investigation or is party to an investigation by a competent authority in connection with infringements to any provision regarding the processing of personal data in connection with the processing of this DPA. Insofar as Controller is subject to an inspection by the supervisory authority, an administrative fine, a preliminary injunction or criminal procedure, a liability claim by a data subject or by a third party or any other claim in connection with the processing of data by Processor as part of this DPA, Processor shall reasonably support Controller upon respective request.

6. Sub-processors

(1) Controller hereby authorizes Processor to outsource part of the processing activities pursuant to this DPA to sub-processors. The sub-processors shall be subject to contractual obligations that are equivalent to Processor's obligation under this DPA (Article 28(4) GDPR).

(2) At the date of signature of this DPA, the Parties acknowledge and agree that Processor currently commissions the following sub-processors on the condition of a contractual agreement in accordance with Article 28(4) GDPR:

	Sub-processor	**Address/country**	**Processing activity**
1	Amazon Web Services EMEA SARL.	38 Avenue John F. KennedyL-1855 Luxembourg	Cloud service provider

(3) It is understood between the Parties that the communication of personal data to any sub-processor shall only take place after all conditions set out in Paragraph (1) for the appointment of sub-processors have been met.

(4) Processor will maintain and keep updated a list of sub-processors. Controller shall be notified of any change to such list without undue delay, thereby giving Controller the option to object. If, within two (2) weeks of receipt of that notice, Controller notifies Processor in writing of any reasonable objection to the proposed appointment, the Parties shall negotiate in good faith a mutually acceptable alternative. If no such alternative is agreed within two (2) weeks of the objection, either Party shall have the right to terminate the MSA to the extent it relates to services which require use of the proposed sub-processor.

(5) Processor shall bear full responsibility and liability for the activities of its sub-processors *vis a vis* Controller.

(6) The Parties agree that ancillary service providers of Processor are no sub-processors within the meaning of data protection laws; this includes in particular transport services of postal or courier companies, cash transport services, telecommunication services, security services and cleaning services. However, Processor shall enter into customary confidentiality agreements with such service providers.

(7) Should a sub-processor provide its services outside the EU/EEA, the Processor shall ensure compliance with the rules regarding data transfer abroad, as described under Section 2 of this DPA. Conditional upon Controller's non-objection to the appointment of such sub-processor, Controller hereby authorizes Processor to enter into an agreement on behalf of Controller, including the EU standard contract clauses for the transfer of personal data to processors in third countries dated February 5, 2010 or, if applicable, standard data protection clauses issued later by the EU Commission or the competent supervisory authority, with such sub-processor located in a third country.

7. Audits

(1) During normal business hours (Monday to Friday from 9 a.m. to 5 p.m.), Controller has the right, at its own expense, without disrupting operations and with strict confidentiality of Processor's trade secrets, to carry out inspections or to have them carried out by an auditor appointed on a case-by-case basis. Such an auditor shall assess Processor's compliance with this DPA in its business operations by means of random checks, of which Processor will be notified in advance. Controller must oblige the auditor to secrecy and confidentiality, unless the auditor is subject to a professional obligation of secrecy. Controller must not appoint a competitor of Processor to carry out the inspection.

(2) Processor shall allow Controller to verify compliance with its obligations as provided by Article 28 GDPR**.** Processor undertakes to give Controller the necessary information on request and, in particular, to demonstrate the implementation of the technical and organisational measures as agreed hereunder.

(3) Evidence of the implementation of such measures, which may not only concern the activities under this DPA, may also be provided by:

a) compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
b) certification according to an approved certification procedure in accordance with Article 42 GDPR;
c) current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, data protection officer, IT security department, data protection auditor);
d) a suitable certification by IT security or data protection auditing.

(4) The Processor may charge a reasonable fee to the Controller for enabling inspections.

8. Assistance to the Controller

(1) Processor shall assist Controller in complying with the obligations concerning the security of personal data, reporting of data breaches, data protection impact assessments and prior consultations set forth at Articles 32 to 36 of the GDPR, including:

a) ensuring adequate protection standards through technical and organisational measures, taking into account the type, circumstances and purposes of processing, the likelihood of data breaches and the severity of the risk to natural persons possibly resulting thereof;
b) ensuring immediate detection of infringements;
c) reporting data breaches without undue delay to the Controller;
d) assisting Controller in answering to data subjects' requests for the exercising of their rights.

(2) Processor may charge Controller a reasonable fee for support services which are not included in the description of the services and which are not attributable to Processor's misconduct, mistakes or infringements. Processor is obligated to provide in written form all information necessary to carry out obligations under this DPA.

9. Directive powers of Controller

(1) Processor shall not process any personal data under this DPA except on Controller's documented instructions, unless required to do so by Union or Member State law, in which case Processor shall inform Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(2) Specific instructions from Controller shall in principle be issued in writing or at least in text form. Oral instructions must be confirmed immediately in writing or in text form by Controller in order to be effective. Controller shall be obligated to document all instructions given to Processor.

(3) In case the Controller should require any change in the processing of personal data set forth by the documented instructions mentioned at Section 2, the Processor shall immediately inform the Controller if it considers such changes likely to result in infringements to data protection provisions. The Processor may refrain from carrying out any activity that may result in any such infringement.

10. Deletion and return of personal data

(1) Processor shall not create copies or duplicates of the data without Controller's knowledge and consent, except for backup copies, insofar as they are necessary for ensuring that data is processed correctly, and where the retention of such data is required by law.

(2) After conclusion of the provision of services under the ITA or MSA, Processor shall, at Controller's choice, either delete in a data-protection compliant manner or return to Controller, all personal data collected and processed under this DPA, unless any applicable legal provision requires further storage of the personal data.

(3) In any case, Processor may retain beyond termination of the ITA or MSA and all Order Form(s) all the information necessary to demonstrate the compliance of the processing activities carried out.

11. General Terms

(1) All notices and communications given under this DPA must be in writing and will be sent by email.

(2) If any provision in this DPA is held by a court of competent jurisdiction to be invalid or unenforceable, all other provisions shall remain in full force and effect.

12. Governing Law and Jurisdiction

(1) This DPA will be governed by German law without regard to the choice or conflicts of law provisions of any jurisdiction.

(2) Any disputes, actions, claims or causes of action arising out of or in connection with this DPA will be subject to the exclusive jurisdiction of the courts located in Berlin, Germany.

ANNEX 1: Technical and organisational measures of Nostos Genomics GmbH

TECHNICAL AND ORGANISATIONAL MEASURES

pursuant to Article 32 General Data Protection Regulation (GDPR)

March 1, 2021

Organisations, which collect, process or use personal data themselves as a controller, or which collect, process or use personal data on behalf of others as a processor must take the technical and organisational measures necessary to ensure a level of security in accordance with the provisions of applicable data protection legislation. All measures shall be implemented following a risk-based approach, whereby the state of the art, the costs of implementation and the nature, scope, context and purposes of the intended processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, need to be considered. Thus, technical and organisational measures shall only be deemed required if, *inter alia*, the expenditures incurred by their implementation stands in reasonable proportion to the intended purpose and the risks of the processing.

Considering the sensitivity of the personal data, we at Nostos Genomics GmbH have implemented the following adequate security measures. The measures described herein come in addition to the measures set out in the main body of the DPA.

As a preliminary remark, please note that we have selected our sub-processors upon thoroughly assessing their data security standards. In particular, we have focused on certificates that ensure compliance with high-level standards in the fields of IT and data security, and which require regular re-certification procedures through independent auditors. Our sub-processor Amazon Web Services EMEA SARL has committed itself to IT and data security and holds various certificates verifying compliance with ISO 27001, ISO 27017, and ISO 27018 (or alternative standards that are substantially equivalent to these) as well as with SOC 1, SOC 2, and SOC 3 (or alternative reports or other documentation that replace or are essentially equivalent to these). Insofar as our service is sub-contracted to AWS, our customers may rely upon these standards which are hereby incorporated into this Annex by reference. We will verify AWS' adherence to these standards on a regular basis in accordance with the AWS Data

Processing Addendum.

Safe the above, please find below the technical and organisational measures implemented at Nostos Genomics GmbH :

1. Confidentiality (Article 32(1)(b) GDPR)

1.1. Admission control

Measures designed to prevent unauthorised persons from gaining access to data processing equipment that processes or otherwise uses personal data.

Technical measures	**Organisational measures**
Manual lock system	Key control / list
	Visitors accompanied by employees
	Diligence in the selection of support services

1.2. Access control

Measures designed to prevent data processing systems from being used by unauthorised people.

Technical measures	**Organisational measures**
Multi-Factor-Authentication on AWS	Creation & management of user profiles
Sensitive data stored in a separate virtual private cloud VPC on AWS with encryption	General guideline on data protection, privacy and security
Login with username & password locally	
Automatic desktop lock	
Newest anti-virus updates & firewall	

1.3. Permission control

Measures to ensure that persons authorised to use a data processing system have access only to data which are subject to their right of access and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after storage.

Technical measures	**Organisational measures**
Logging of access to applications, specifically when entering, changing and deleting data	Administration of granular user rights by a AWS administrator; only technically instructed employees have access to data

Data protection safe / password vault	One single administrator on AWS

1.4. Separation control

Measures to ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical measures	**Organisational measures**
Separation of productive and test environment	Definition of database rights
Physical separation (systems / databases / data storage)	Sensitive data include purpose-related attributes
Multi-client capability of relevant applications	Clinical data always stored separately from genetic data

1.5. Pseudonymisation (Article 32(1)(a) GDPR; Article 25(1) GDPR)

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without additional information, provided that such additional information is kept separately and is subject to appropriate technical and organisational measures;

Technical measures	**Organisational measures**
In case of pseudonymisation: separation of the allocation data and storage in a separate and secure system.	Internal instruction to anonymise / pseudonymise personal data in the event of transfer or after expiry of the statutory deletion period

2. Integrity (Article 32(1)(b) GDPR)

2.1. Transmission control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during their electronic transmission or during their transport or storage on data carriers and that it is possible to verify and establish the points to which personal data are to be transmitted by data transmission facilities.

Technical measures	**Organisational measures**
Fully encrypted (SSL) data transfers on https://app.nostos-genomics.com	Documentation of the data recipients as well as the duration of the planned transfer or the deletion periods
Recording of accesses and retrievals	In the case of personal handover: care in selecting transport staff and vehicles as well as use of a handover protocol

2.2. Input control

Measures to ensure that it can be subsequently verified and established whether and by whom personal data have been entered, modified or removed in data processing systems.

Technical measures	**Organisational measures**
Technical logging of the input, modification and deletion of data	Traceability of input, modification and deletion of data by individual user names (not user groups)
	Clear responsibilities for deletions

3. Availability und Resilience (Article 32(1)(b) GDPR)

3.1. Availability control

Measures to ensure that personal data are protected against accidental destruction or loss.

Technical measures	**Organisational measures**
Fire and smoke detection systems	Backup concept (detailed)
Data protection safe	Storage of the backup media at a safe place

3.2. Rapid recoverability

Technical measures	**Organisational measures**
Regular local backups	Documented recovery concept with regular backup and disaster-proof storage of data

4. Periodic Review, Evaluation and Assessment Procedures (Article 32(1)(d) GDPR; Article 25(1) GDPR)

4.1. Data protection management

Technical measures	Organisational measures
Central documentation of all procedures and regulations on data protection with access for employees as required / authorized (Wiki)	Cooperation with external data protection consulting firm **OpenReg GmbH**, Berlin, Germany (which also carries out the data protection impact assessment if required)
	Employees trained and under obligation of confidentiality/data secrecy
	Regular sensibilisation of employees; at least annually
	The organisation complies with the obligations to provide information pursuant to Articles 13 and 14 GDPR

4.2. Incident-Response-Management

Support in responding to security breaches

Technical measures	Organisational measures
Use of firewall with regular updates	Documentation and reporting of security incidents and data breaches
Use of spam filter with regular updates	
Use of anti-virus software with regular updates	

4.3. Data-protection-friendly default settings (Article 25(2) GDPR)

Privacy by design / Privacy by default

Technical measures	Organisational measures
Not more personal data is collected than is necessary for the purpose in question	The team highlights to the user what data is required for which purpose

4.4. Contract control

Measures to ensure that personal data processed as a sub-processor can only be processed in accordance with the instructions of Nostos Genomics GmbH .

Technical measures	**Organisational measures**
	Preliminary examination of the security measures taken by the contractor and their documentation
	Selection of the contractor under due diligence aspects (especially with regard to data protection and data security)
	Entering into the necessary agreement for data processing or EU standard contract clauses
	Ensuring the destruction of data after completion of the assignment
	In the case of prolonged cooperation: ongoing review of the contractor and its level of protection
	Written notification to Controller in case of use of an additionally vetted sub-processor