Revision Date: September 2, 2020

DNAnexus Data Processing Addendum

This Data Processing Addendum ("**DPA**") and its applicable DPA Exhibits apply to the Processing of Personal Data by DNAnexus on behalf of the Customer ("**Customer Personal Data**") in order to provide DNAnexus Platform Services and other professional services ("**Services**") described in the Master Subscription Agreement ("**Agreement**"), solely to the extent that the Processing of Customer Personal Data is subject to the GDPR (defined below). DPA Exhibits for each Service will be provided in the applicable License/Statement of Work, also known as the Transaction Document ("**TD**"). This DPA forms part of and is subject to the terms of the Agreement (capitalized terms used and not defined herein have the meaning given them in the General Data Protection Regulation 2016/679 ("**GDPR**")). In the event of conflict, the DPA Exhibit prevails over the DPA which prevails over the Agreement except where explicitly set out in the Agreement identifying the relevant Section of the DPA over which it prevails.

1. PROCESSING

1.1   The Customer (a) is the sole Controller of Customer Personal Data or (b) has been instructed by and obtained the authorization of the relevant Controller(s) to agree to the Processing of Customer Personal Data by DNAnexus as set out in this DPA. The Customer appoints DNAnexus as Processor to Process Customer Personal Data. If there are other Controllers, the Customer will identify and inform DNAnexus of any such other Controllers prior to providing their Personal Data, as set out in the DPA Exhibit.

1.2   A list of categories of Data Subjects, types of Customer Personal Data, Special Categories of Personal Data and the Processing activities is set out in the applicable DPA Exhibit for a Service. The duration of the Processing corresponds to the duration of the Service, unless otherwise stated in the respective DPA Exhibit. The nature, purpose and subject matter of the Processing is the provision of the Service as described in the applicable TD.

1.3   DNAnexus will Process Customer Personal Data according to the Customer's written instructions. The scope of the Customer's instructions for the Processing of Customer Personal Data is defined by the Agreement, this DPA – including the applicable DPA Exhibit – and, if applicable, Customer's and its authorized users' use and configuration of the features of the Service. The Customer may provide further instructions that are legally required ("**Additional Instructions**"). If DNAnexus believes an Additional Instruction violates the GDPR or other applicable data protection laws or regulations, DNAnexus will inform the Customer immediately and may suspend the performance of the Service until the Customer has modified or confirmed the lawfulness of the Additional Instructions in writing. If DNAnexus notifies the Customer that an Additional Instruction is not feasible or the Customer notifies DNAnexus that it does not accept the quote for the Additional Instruction prepared in accordance with Section 10.2 of this DPA, the Customer may terminate the affected Service by providing DNAnexus with a written notice within one month after notification. DNAnexus will refund a prorated portion of any prepaid charges for the period after the termination date.

1.4   If DNAnexus cannot process Customer Personal Data in accordance with Customer's instructions due to a legal requirement under any applicable European Union or Member State law, DNAnexus will (i) promptly notify the Customer of such inability, providing a reasonable level of detail as to the instructions with which it cannot comply and the reasons why it cannot comply, to the greatest extent permitted by applicable law; and (ii) cease all Processing of the affected Customer Personal Data (other than merely storing and maintaining the security of the affected Customer Personal Data) until such time as the Customer issues new instructions with which DNAnexus is able to comply. If this provision is invoked, DNAnexus will not be liable to the Customer under the Agreement for failure to perform the Services until such time as the Customer issues new instructions that comply with applicable legal requirements.

1.5   The Customer may serve as a single point of contact for DNAnexus. As other Controllers may have certain direct rights against DNAnexus, the Customer undertakes to exercise all such rights on their behalf and to obtain all necessary permissions for other Controllers. DNAnexus shall be discharged of its obligation to inform or notify another Controller when DNAnexus has provided such information or notice to the Customer. Similarly, DNAnexus will serve as a single point of contact for the Customer with respect to its obligations as a Processor under this DPA.

1.6   DNAnexus will comply with all EEA data protection laws and regulations ("**Data Protection Laws**") in respect to the Services applicable to Processors. DNAnexus is not responsible for determining the requirements of

laws applicable to the Customer's business or that DNAnexus' provision of Services meet the requirements of such laws. As between the parties, the Customer is responsible for the lawfulness of the Processing of the Customer Personal Data. The Customer will not use the Services in conjunction with Personal Data to the extent that doing so would violate applicable Data Protection Laws.

2. TECHNICAL AND ORGANIZATIONAL MEASURES

2.1 DNAnexus will implement and maintain technical and organizational measures set forth in the applicable DPA Exhibit ("TOMs") to ensure a level of security appropriate to the risk for DNAnexus' scope of responsibility. TOMs are subject to technical progress and further development. Accordingly, DNAnexus reserves the right to modify the TOMs provided the functionality and security of the Services are not degraded.

2.2 Customer is solely responsible for reviewing the TOMs and agreeing that they meet Customer's requirements and obligations The Customer confirms the TOMs provide an appropriate level of protection for the Customer Personal Data taking into account the risks associated with the Processing of Customer Personal Data.

3. DATA SUBJECT RIGHTS AND REQUESTS

3.1 To the extent permitted by law, DNAnexus will inform the Customer of requests from Data Subjects exercising their Data Subject rights (e.g. rectification, deletion and blocking of data) addressed directly to DNAnexus regarding Customer Personal Data. The Customer shall be responsible to respond to such requests of Data Subjects. DNAnexus will reasonably assist the Customer in responding to such Data Subject requests in accordance with Section 10.2 of this DPA.

3.2 If a Data Subject brings a claim directly against DNAnexus for a violation of their Data Subject rights, the Customer will indemnify DNAnexus for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that DNAnexus has notified the Customer about the claim and given the Customer the opportunity to cooperate with DNAnexus in the defense and settlement of the claim. Subject to the terms of the Agreement, the Customer may claim from DNAnexus amounts paid to a Data Subject for a violation of such Data Subject's rights caused by DNAnexus' breach of its obligations under GDPR.

4. THIRD PARTY REQUESTS AND CONFIDENTIALITY

4.1 DNAnexus will not disclose Customer Personal Data to any third party, unless authorized by the Customer or required by law. If a government or data protection authority demands access to the Customer Personal Data, DNAnexus will notify the Customer prior to disclosure, unless prohibited by law.

4.2 DNAnexus requires all of its personnel authorized to Process Customer Personal Data to commit themselves to confidentiality and not Process such Customer Personal Data for any other purposes, except on instructions from the Customer or unless required by applicable law.

5. AUDIT

5.1 DNAnexus shall allow for and assist the Customer in connection with audits, including inspections, of DNAnexus Processing of Customer Personal Data conducted by the Customer or an auditor mandated by the Customer to ascertain DNAnexus compliance with this DPA, in accordance with the following procedures:

(A). At Customer's written request, DNAnexus will provide the Customer or its mandated auditor with the most recent certifications and/or summary audit report(s), which DNAnexus has procured to regularly test, assess and evaluate the effectiveness of the TOMs.

(B). DNAnexus will reasonably cooperate with the Customer to comply with its own or other Controllers' audit obligations or a competent data protection authority's request as it relates to the Processing of Customer Personal Data. The Customer will inform DNAnexus in writing to enable DNAnexus to provide such information or to grant the Customer access to it.

(C). If further information is needed by the Customer to comply with its own or other Controller's audit obligations or a competent data protection authority's request as it relates to the Processing of Customer Personal Data, the Customer shall inform DNAnexus in writing to enable DNAnexus to provide such information or grant the Customer access to it.

(D).   To the extent it is not possible to otherwise satisfy an audit obligation mandated by applicable law, only legally mandated entities (such as a governmental regulatory agency having oversight of the Customer's operations), the Customer or its mandated auditor may conduct an onsite visit of the facilities used to Process Customer Personal Data, during normal business hours and only in a manner that causes minimal disruption to DNAnexus' business, subject to coordinating the timing of such visit and in accordance with any audit procedures in the DPA Exhibit in order to reduce any risk to DNAnexus' other customers.

5.2   Each party will bear its own costs in respect to paragraphs (A) and (B) of Section 5.1 of this DPA. Any further assistance will be provided in accordance with Section 10.2 of this DPA. The Customer will be responsible for any fees charged by any auditor appointed by the Customer to execute any such audit.

6.   RETURN OR DELETION OF CUSTOMER PERSONAL DATA

6.1   Upon termination or expiration of the Agreement, DNAnexus will either delete or return the Customer Personal data in its possession as set out in the respective DPA Exhibit within a reasonable timeframe, unless otherwise required by applicable law.

7.   SUBPROCESSORS

7.1   The Customer authorizes DNAnexus to engage subcontractors to Process Customer Personal Data ("**Subprocessors**"). A list of the current Subprocessors is set out in the respective DPA Exhibit. For the avoidance of doubt, the above authorization constitutes Customer's prior written consent to the sub-processing by DNAnexus for purposes of Clause 11 of the Standard Contractual Clauses (as defined under Section 8.1 of this DPA). DNAnexus will notify the Customer in advance of any changes to the Subprocessors as set out in the respective DPA Exhibit. Within 30 days after DNAnexus' notification of the intended change, the Customer can object to the addition of a Subprocessor on the basis that such addition would cause the Customer to violate applicable legal requirements. The Customer's objection shall be in writing and include the Customer's specific reasons for the objection and options to mitigate, if any. If the Customer does not object within such period, the respective Subprocessor may be commissioned to Process Customer Personal Data. DNAnexus shall impose the same data Processing obligations as set forth in this DPA on any approved Subprocessor prior to the Subprocessor Processing any Customer Personal Data.

7.2   If the Customer legitimately objects to the change of a Subprocessor and DNAnexus cannot reasonably accommodate the Customer's objection, DNAnexus will notify the Customer. The Customer or DNAnexus may terminate the affected Services by providing the other party with a written notice within one month of termination. DNAnexus will refund a prorated portion of any pre-paid charges for the period after such termination date. The Customer is responsible for removing its data prior to termination.

8.   TRANSBORDER DATA PROCESSING

8.1   In connection with the performance of the Agreement, Customer authorizes DNAnexus to transfer Personal Data from the European Economic Area ("**EEA**"), the United Kingdom and Switzerland to the United States. The parties agree to enter into the Standard Contractual Clauses pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection ("**Standard Contractual Clauses**") attached to this DPA as Schedule 1, in order to implement appropriate safeguards for such transfers of Customer Personal Data.

8.2   If the Customer notifies DNAnexus about another Controller and DNAnexus does not object within 30 days after the Customer's notification, the Customer agrees on behalf of such other Controller(s), or if unable to agree, will procure agreement of such Controller(s), to be additional data exporter(s) under the Standard Contractual Clauses concluded between DNAnexus and the Customer. The Customer agrees and, if applicable, procures the agreement of other Controllers that, as between the parties and without prejudice to Data Subjects' rights, the Standard Contractual Clauses, including any claims arising from them, are subject to the terms set forth in the Agreement, including the exclusions and limitations of liability. In case of conflict between the provisions of this DPA or the Agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

8.3   To the extent that DNAnexus or the Customer are relying on a specific statutory mechanism to legitimize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the parties agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer of Customer Personal Data.

9.   PERSONAL DATA BREACH

9.1   DNAnexus shall notify the Customer without undue delay after becoming aware of a Personal Data Breach with respect to the Customer Personal Data. DNAnexus will promptly investigate the Personal Data Breach if it occurred on the DNAnexus infrastructure. DNAnexus is responsible for and will assist the Customer as set out in Section 10 of this DPA.

10.   ASSISTANCE

10.1   DNAnexus will assist the Customer by technical and organizational measures, insofar as possible, for the fulfillment of the Customer's obligation to comply with the rights of Data Subjects and in ensuring compliance with the Customer's obligations relating to the security of Processing, the notification of a Personal Data Breach, data protection impact assessments and consultation with competent data protection authorities (if required by the Data Protection Law), taking into account the information available to DNAnexus.

10.2   The Customer will make a written request for any assistance referred to in this DPA. DNAnexus will charge the Customer no more than a reasonable charge to perform such assistance or Additional Instructions, such charges to be set forth in a quote and agreed in writing by the parties, or as set forth in an applicable change control provision of the Agreement.

<u>SCHEDULE 1</u>

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: ....

Address: ....

Tel.:...; fax:....................................; e-mail:....................................

Other information needed to identify the organisation:

………………………………………………………………

(the data **exporter**)

And

Name of the data importing organisation: **DNAnexus Inc., 1975 W El Camino Real, Suite 204**

Mountain View, CA 94040

Tel.: 1 (650) 617-3201; e-mail: privacy@dnanexus.com

Other information needed to identify the organisation:

………………………………………………………………………

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a)   *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b)   *'the data exporter'* means the controller who transfers the personal data;

(c)   *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d)   *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e)   *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f)   *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1.   The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2.   The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.   The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4.   The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a)   that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b)   that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c)   that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d)   that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e)   that it will ensure compliance with the security measures;

(f)   that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g)   to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h)   to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)   that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j)   that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a)   to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)   that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d)   that it will promptly notify the data exporter about:

         (i)   any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

         (ii)   any accidental or unauthorised access, and

         (iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)   at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g)   to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h)   that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i)   that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j)   to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1.   The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2.   If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data

exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3.   If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1.   The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a)   to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b)   to refer the dispute to the courts in the Member State in which the data exporter is established.

2.   The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1.   The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2.   The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

On behalf of the data importer: DNAnexus, Inc.
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Data exporter
The data exporter is the entity identified as "Customer" in the DPA.

Data importer
The data importer is DNAnexus, Inc.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
DNAnexus user's email address and related contact information, the latter voluntarily provided.
The data exporter may transfer identified or de-identified personal health information in the form of genomic sequence information as well as phenotypic information (e.g. sex, age, eye color, etc). This information is encrypted both in-transit and at-rest and is not available to DNAnexus without the data exporter's explicit permission.

The categories of data subjects set out in the applicable DPA Exhibit for a Service (as described in the DPA).

Categories of data
The personal data transferred concern the following categories of data (please specify):

The categories of personal data set out in the applicable DPA Exhibit for a Service (as described in the DPA).

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

As set out in the applicable DPA Exhibit for a Service (as described in the DPA).

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

The processing activities set out in the applicable DPA Exhibit for a Service (as described in the DPA).

DATA EXPORTER
Name:………………………………

Authorised Signature ……………………

DATA IMPORTER
Name:**DNAnexus, Inc.**

Authorised Signature ……………………

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):
DNAnexus uses security measures compliant with the "Moderate" configuration of the NIST 800-family of security standards, specifically: NIST SP 800-18, NIST 800-26, NIST SP 800-27, NIST SP 800-30, NIST SP 800-34, NIST SP 800-37, NIST SP 800-39, NIST 800-47, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-60, NIST SP 800-61, NIST SP 800-63-2, NIST SP 800-64, NIST SP 800-115, NIST SP 800-128, NIST SP 800-137, NIST SP 800-122, NIST SP 800-144, and NIST SP 800-145. DNAnexus uses security measures compliant with the privacy regulations from the U.S. Federal Trade Commission, U.S. Federal Deposit Insurance Corporation, and National Archives (NARA) Bulletin 2010-05. DNAnexus uses security measures compliant with respect to FIPS PUB 140-2, FIPS PUB 199, FIPS PUB 200, and FIPS PUB 201-2.

DNAnexus is compliant and certified on HITRUST around the following CSF areas: Information Protection Program, Endpoint Protection, Portable Media Security, Mobile Device Security, Configuration Management, Vulnerability Management, Network Protection, Transmission Protection, Password Management, Access Control, Audit Logging and Monitoring, Education, Training and Awareness, Third Party Assurance, Incident Management, Business Continuity & Disaster Recovery, Risk Management, Physical & Environmental Security and Data Protection & Privacy.

DNAnexus is compliant and certified by BSI in ISO/IEC 27001:2013, certificate # IS 594520

……
……
……
………………………………………………………………………………………………

DATA EXPORTER
Name:…………………………………

Authorised Signature ……………………

DATA IMPORTER
Name: **DNAnexus, Inc.**

Authorised Signature ……………………