Revision Date: March 30, 2023

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**") together with all Customer Affiliates 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 Data Protection Laws (defined below). This DPA forms part of and is subject to the terms of the Agreement. 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. In the event of any conflict between the terms of the SCCs and this DPA (including any exhibits), the Agreement, or any other document, the SCCs shall prevail to the extent that applicable Data Protection Laws so require.

1. DEFINITIONS

Unless otherwise defined in the applicable Data Protection Law, the following terms shall have the definitions set out below. If the following terms are defined in the applicable Data Protection Law (e.g. GDPR), the definition given to them under such Data Protection Law shall apply. Capitalized terms used and not defined herein shall have the meaning given them in the GDPR (as defined below).

"**Account"** means the Customer's account on the DNAnexus offering where the Customer stores and processes Customer data.

"**Affiliate**" has the meaning set forth in the Agreement.

"**Authorised Affiliate"** shall mean a Customer Affiliate who has not signed an Order Form pursuant to the Agreement but is either a Data Controller or Data Processor for the Customer Personal Data processed by DNAnexus pursuant to this Agreement, for so long as such entity remains a Customer Affiliate.

"**Business Associate**" or **"BA**", as defined by 45 CFR § 160.103, is a person or entity who assists a **covered entity** in a function or activity regulated by "**HIPAA**," involving the use or disclosure of individually identifiable health information, or that provides certain services to a covered entity that involve the use or disclosure of individually identifiable health information.

"California Consumer Privacy Act" or "**CCPA**" means the California Consumer Privacy Act of 2018, and effective on Jan 1, 2020, as may be amended from time to time.

"California Privacy Rights Act" or "**CPRA**" means the California Privacy Rights Act of 2020, effective on Jan 1, 2023, as may be amended from time to time.

"Colorado Privacy Act" or "**CPA**", means the Colorado Privacy Act effective July 1, 2024, as may be amended from time to time.

"Covered entities" are defined by 45 CFR § 160.103 refers to (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with direct or indirect transactions as defined by the US Health and Human Services.

"**Customer Data**" has the meaning set forth in this Agreement.

"**Customer Personal Data**" means any Customer Data that is Personal Data, including, but not exclusive, genomic, individually identifiable information and protected health information (PHI)

"**Data Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means an entity that Processes Personal Data on behalf of a Data Controller.

"Data Protection Laws" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Data under this Agreement, including, where applicable, EU & UK Data Protection Law, the CCPA, CPRA, CPA, VCDPA, and HIPAA.

"**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

"**Data Subject Request**" has the meaning given to it in Section 6.1.

"**EU & UK Data Protection Law**" means (i) Regulation 2016/679 of the European Parliament and the Council on

the protection of natural persons with regard to the Processing of Personal Data and the free movement of such data (General Data Protection Regulation) ("**GDPR**"); and (ii) the GDPR as it forms part of the United Kingdom law pursuant to Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the Data Protection Act of 2018.

"**Health Insurance Portability and Accountability Act of 1996**" or "**The Privacy Rule**" or **"HIPAA"** is a US federal law pertaining to Personal Health Information as defined by 45 CFR §164.102, 45 CFR §164.162 and 45 CFR §164.162.

"**Hosting Region**" is the geographic location of the physical infrastructure where DNAnexus operates the storage and processing.

"**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses effective March 21, 2022, available here: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

"**Personal Data**" means any information, including opinions, relating to an identified or identifiable natural person and includes similarly defined terms in Data Protection Laws, including, but not limited to, the definition of "**personal information**" or "**Customer Personal Data**" in CCPA, CPRA, CPA, UCPA, and VCDPA. Personal data extends to Personal Identifiable Information as defined by GDPR in *Article 4*.

"**Personal Identifiable Information**" or "**PII**" is any data that can be used to clearly identify an individual.

"**Protected Health Information**" or "**PHI**" or "ePHI" is paper or electronic health information that the US federal protections held by "**covered entities**" and gives patients an array of rights with respect to that information, while also permitting the disclosure of PHI needed for patient care and other important purposes.

"**Processing"** shall have the meaning given to it in the applicable Data Protection Law. If it is not defined by applicable Data Protection Law, it shall mean any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination and "**Process**," "**Processes**," and "**Processed"** will be interpreted accordingly. This definition does not amend the definition where GDPR applies.

"Purposes" shall mean (i) DNAnexus' provision of the Services as described in the Master Subscription Agreement, including Processing initiated by Users in their use of the Services; and (ii) further documented, reasonable instructions from the Customers agreed upon by the Parties.

"**Restricted Countries**" has the meaning given to it in Section 12.1.

"**Restricted Transfers**" has the meaning given to it in the GDPR.

"**Security Incident**" means a breach of security, leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data, Customer Personal Data, Protected Health Information, and Personal Identifiable Information.

"**Services**" has the meaning given to it under the applicable Data Protection Law. This term generally means the available DNAnexus Platform-as-a-Service offering described in the Documentation and procured by the Customer, and any other services provided by DNAnexus as described under the Master Subscription Agreement, including but not limited to support and technical services.

"**SCCs**" or "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to third countries approved pursuant to Commission Decision (EU) 2021/914 of 4 June 2021, found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

"**Third Party Controller**" has the meaning given to it in Section 4.1.

"**User**" is the individual operating under a commercial contract or End User Agreement with DNAnexus.

"**Utah Consumer Privacy Act"** or "**UCPA**", effective on December 31, 2023, as may be amended from time to time.

"Virginia Consumer Data Protection Act" or "**VCDPA**", effective January 1, 2023, as may be amended from time to time.

2. PROCESSING

2.1 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.

2.2 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.

2.3 DNAnexus shall 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 authorised 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 any applicable data protection laws or regulations, DNAnexus shall 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 shall refund a prorated portion of any prepaid charges for the period after the termination date.

2.4 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 shall (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 shall 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.

2.5 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 shall serve as a single point of contact for the Customer with respect to its obligations as a Processor under this DPA.

DNAnexus shall 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 meets 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.

3. TECHNICAL AND ORGANIZATIONAL MEASURES

3.1 DNAnexus shall implement and maintain technical and organizational measures set forth in Annex II ("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.

3.2 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.

4. ROLES AND SCOPE OF PROCESSING

4.1 Roles of the Parties: As between DNAnexus and the Customer, DNAnexus shall Process Customer Personal Data only as a Data Processor (or sub-processor) acting on behalf of Customer and, with respect to CCPA, as a "service provider" as defined herein, in each case regardless of whether Customer acts as a Data Controller or as a Data Processor on behalf of a third-party Data Controller ("**Third-Party Controller**") with respect to Customer Personal Data. To the extent any Usage Data (as defined in the Master Subscription Agreement) is considered Personal Data under applicable Data Protection Laws, DNAnexus is the Data Controller of such data and shall Process such data in accordance with the Master Subscription Agreement and applicable Data Protection Laws.

4.2 Customer Instructions: DNAnexus shall Process Customer Personal Data only for the purposes described in the Master Subscription Agreement. Customer shall ensure its Processing instructions are lawful and that the Processing of Customer Personal Data in accordance with such instructions will not violate applicable Data Protection Laws. The Parties agree that the Master Subscription Agreement (including this DPA) sets out exclusive and final instructions to DNAnexus for all Processing of Customer Personal Data, and (if applicable) include and are consistent with all instructions from Third-Party Controllers. Any additional requested instructions require the prior written agreement of DNAnexus. DNAnexus shall promptly notify Customer if, in DNAnexus' opinion, such an instruction violates EU & UK Data Protection Law. Where applicable, Customer shall be responsible for any communications, notifications, assistance and/or authorizations that may be required in connection with a Third-Party Controller.

4.3 Customer Affiliates: DNAnexus' obligations set forth in this DPA shall also extend to Authorised Affiliates, subject to the following conditions:

a) Customer must exclusively communicate any additional Processing Instructions requested pursuant to Section 4.2 directly to DNAnexus, including instructions from its Authorised Affiliates;

b) Customer shall be responsible for Authorised Affiliates' compliance with this DPA and all acts and/or omissions by an Authorised Affiliate with respect to Customer's obligations in this DPA shall be considered the acts and/or omissions of Customer; and

c) Authorised Affiliates shall not bring a claim directly against DNAnexus. If an Authorised Affiliate seeks to assert a legal demand, action, suit, claim, proceeding or otherwise against DNAnexus ("**Authorised Affiliate Claim**"): (i) Customer must bring such Authorised Affiliate Claim directly against DNAnexus on behalf of such Authorised Affiliate, unless Data Protection Laws require the Authorised Affiliate be a party to such claim; and (ii) all Authorised Affiliate Claims shall be considered claims made by Customer and shall be subject to any liability restrictions set forth in the Master Subscription Agreement, including any aggregate limitation of liability

4.4 Customer Processing of Personal Data: Customer agrees that it: (i) will comply with its obligations under Data Protection Laws with respect to its Processing of Customer Personal Data; (ii) will make appropriate use of the DNAnexus offerings to ensure a level of security appropriate to the particular content of the Customer Personal Data, such as backing up Customer Personal Data; and (iii) has obtained all consents, permissions and rights necessary under Data Protection Laws for DNAnexus to lawfully Process Customer personal Data in accordance with the Master Subscription Agreement, including, without limitation, Customer's sharing and/or receiving Customer Personal Data from third-party via the DNAnexus offerings.

5. DATA SUBJECT RIGHTS AND REQUESTS

5.1 To the extent permitted by law, DNAnexus shall 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 shall reasonably assist the Customer in responding to such Data Subject requests in accordance with Section 10.2 of this DPA.

5.2 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.

6. THIRD PARTY REQUESTS AND CONFIDENTIALITY

6.1 Data Subject Request. DNAnexus shall promptly notify Customer if DNAnexus receives a request from a Data Subject that identifies Customer Personal Data or otherwise identifies Customer, including where the Data Subject seeks to exercise any of its rights under the applicable Data Protection Laws (collectively, "**Data Subject Request**"). Unless otherwise required under applicable Data Protection Laws, Customer will be responsible for responding to any such Data Subject Requests. To the extent Customer is unable to access the relevant Customer Personal Data within the DNAnexus offerings, DNAnexus shall (upon Customer's written request and taking into account the nature of the Processing) provide commercially reasonable cooperation to assist Customer in responding to Data Subject Requests.

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

6.3 DNAnexus requires all of its personnel authorised 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.

7. AUDIT

7.1 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 shall 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 shall 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 or virtual visit of the DNAnexus 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.

e) Where the Customer's Auditor is a third-party, the Auditor may be required to execute a separate confidentiality agreement with DNAnexus prior to any review of Reports or an audit of DNAnexus, and DNAnexus may object in writing to such Auditor, if in DNAnexus' reasonable opinion, the Auditor is not suitably qualified or is a direct competitor of DNAnexus. Any such objection by DNAnexus shall require the Customer to either appoint another Auditor or conduct the audit itself. Any expenses incurred by an Auditor in connection with any review of Reports or an audit shall be borne exclusively by the Auditor. For clarity, the exercise of audit rights under the SCCs shall be as described in this Section (Audit) and Customer agrees these rights are carried out on behalf of Customer and all relevant Third-Party Controllers, subject to the confidentiality and non-use restrictions of the Agreement.

7.2 Each party will bear its own costs in respect to 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.

8. RETURN OR DELETION OF CUSTOMER PERSONAL DATA

8.1 Upon termination or expiration of the Agreement, DNAnexus shall 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.

9. SUBPROCESSORS

9.1 The Customer provides DNAnexus with a general authorization to engage Sub-processors, subject to Annex I (Changes to Sub-processors), as well as DNAnexus' current Sub-processors identified in Annex III of the SCCs as of the effective date of this DPA. 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.

9.2 Sub-Processor Obligations: DNAnexus shall (i) enter into a written agreement with each Sub-Processor imposing data protection obligations no less protective of Customer Personal Data as DNAnexus' obligations under this DPA to the extent applicable to the nature of the services provided by each Sub-processor; and (ii) remain liable for each Sub-processor's compliance with the obligations under this DPA. Upon written request, and subject to any confidentiality restrictions, DNAnexus shall provide the Customer all relevant information it reasonably can in connection with its applicable Sub-processor agreements where required to satisfy the Customer's obligations under Data Protection Laws.

9.3 The Customer authorizes DNAnexus to engage new subcontractors to Process Customer Personal Data ("**Sub-processors**"). A list of the current Sub-processors is set out in the respective DPA Exhibit. DNAnexus shall notify the Customer in advance of any changes to the Sub-processors as set out in the respective DPA Exhibit. Within thirty (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.

9.4 If the Customer legitimately objects to the change of a Subprocessor and DNAnexus cannot reasonably accommodate the Customer's objection, DNAnexus shall 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 shall 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.

10. SECURITY

10.1 Security Measures: DNAnexus shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from Security Incidents in accordance with the DNAnexus' security controls described in Annex II of the SCCs and attached to this DPA. DNAnexus may review and update this Annex II from time to time, provided these updates shall not materially diminish the overall security of the Services or Customer Personal Data.

10.2 Confidentiality of Processing: DNAnexus shall ensure that any person who is authorised by DNAnexus to Process Customer Personal Data (including its employees, contingent workers and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

10.3 No Assessment of Customer Personal Data by DNAnexus: DNAnexus shall have no obligation to assess the contents or accuracy of Customer Personal Data, including to identify information subject to any specific legal, regulatory, or other requirement. Customer is responsible for reviewing the information made available by DNAnexus relating to data security and making an independent determination as to whether the Services meet the Customer's requirements and legal obligations under the applicable Data Protection Laws.

11. SECURITY INCIDENT RESPONSE

11.1 Security Incident Reporting: If DNAnexus becomes aware of a Security Incident, DNAnexus will notify the

Customer without undue delay, and in any case, where feasible, notify the Customer within seventy-two (72) hours after becoming aware. DNAnexus' notification shall be sent to the email registered by the Customer within the Service for such purposes, and where no such email is registered, the Customer acknowledges that the means of notification shall be a DNAnexus' reasonable discretion and DNAnexus' ability to timely notify shall be negatively impacted. DNAnexus shall promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

11.2 Security Incident Communications: DNAnexus shall provide the Customer with timely information about the Security Incident, the status of DNAnexus' investigation, a contact point from which additional information may be obtained, and the categories and approximate number of data objects concerned. Notwithstanding the foregoing, the Customer acknowledges that because DNAnexus does not have visibility to the content of the Customer Personal Data, it will be unlikely that DNAnexus can provide information as to the particular nature of the Customer Personal Data, or where applicable, the identities, number of categories of the affected Data Subjects. Communications by or on behalf of DNAnexus with the Customer in connection with a Security Incident shall not be construed as an acknowledgement of any fault or liability with respect to the Security Incident.

12. TRANSBORDER DATA PROCESSING

12.1 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 (collectively, "**Restricted Countries**") to DNAnexus in a country that does not ensure an adequate level of protection (within the meaning and to the extent governed by the applicable Data Protection Laws of the Restricted Countries), such transfers shall be governed by a valid mechanism for the lawful transfer of Customer Personal Data recognized under applicable Data Protection Laws, such as those in the next paragraph. For clarity, for transfers from the United Kingdom and Switzerland, references in the SCCs shall be interpreted to include applicable terminology for those jurisdictions (e.g., "Member State" shall be interpreted to mean "United Kingdom" for transfers from the United Kingdom.) The Standard Contractual Clauses (SCCs) are attached to this DPA as Schedule 1, to implement appropriate safeguards for such transfers of Customer Personal Data.

SCCs: Each party agrees to abide by and transfer Customer Personal Data from the Restricted Countries in accordance with the SCCs set out in Schedule 1.

For the avoidance of doubt, and notwithstanding anything herein to the contrary, the SCCs will only apply to the extent the data being transferred relates to individuals from a Restricted Country.

12.2 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.

12.3 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.

12.4 DNAnexus shall only host Customer Personal Data in the region(s) offered by DNAnexus and selected by Customer on the DNAnexus Order Form (the "**Hosting Region**"). Customer is solely responsible for the regions from which its Users access the Customer Personal Data, for any transfer or sharing of Customer Personal Data by Customer or its Users and for any subsequent designation of other Hosting Regions (either for the same Account, a different Account or a separate Service). Once Customer has selected a Hosting Region(s), DNAnexus shall not process Customer Personal Data from outside the Hosting Region except as reasonably necessary to provide the Services procured by Customer, or as necessary to comply with the law or binding order of a governmental body.

12.5 In the event that any data transfers under the Agreement are subject to the UK GDPR, the UK Addendum, set out in Schedule 2, shall apply.

13. PERSONAL DATA BREACH

DNAnexus shall notify the Customer without undue delay after becoming aware of a Personal Data Breach with respect to the Customer Personal Data. DNAnexus shall 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 14 of this DPA.

14. ASSISTANCE

14.1 DNAnexus shall 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.

14.2 DSARs: The Customer will make a written request for any assistance referred to in this DPA. DNAnexus shall 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.

15. RELATIONSHIP WITH THE MASTER SERVICES AGREEMENT

15.1 The Parties agree that this DPA shall replace and supersede any existing data processing addendum, attachment, exhibit or standard contractual clauses that DNAnexus and Customer may have previous entered into in connection with the DNAnexus offerings.

15.2 Except as provided by this DPA, the Master Subscription Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Master Subscription Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Data. Notwithstanding the foregoing, and solely to the extent applicable to any Customer Personal Data comprised of patient, medical or other protected health information regulated by HIPAA or similar U.S. federal or state health care laws, rules or regulations ("**HIPAA**"), if there is any conflict between this DPA and a business associate agreement between Customer and DNAnexus ("**BAA**"), then the BAA shall prevail solely with respect to such HIPAA Data. Notwithstanding the foregoing, and solely to the extent that the SCCs apply to the Processing of Personal Data hereunder, if there is any conflict between this DPA and the SCCs, then the SCCs shall prevail solely with respect to such Personal Data.

15.3 Notwithstanding anything to the contrary in the Master Subscription Agreement or this DPA, except to the extent such liability cannot be limited by applicable law, including applicable Data Protection Laws, each party's and all of its Affiliates' liability, taken together in aggregate, arising out of or relating to this DPA, the SCCs, and any other data protection agreements in connection with the Master Subscription Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Master Subscription Agreement. Without limiting the Parties' obligations under the Master Subscription Agreement, each party agrees that any regulatory penalties incurred by one party (the "**Incurring Party**") in relation to the Customer Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Master Subscription Agreement as if it were liability to the other party under the Master Subscription Agreement.

15.4 In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a Third-Party Controller), but without prejudice to the rights or remedies available to Data Subjects under Data Protection Laws or this DPA (including the SCCs).

15.5 This DPA will be governed and construed in accordance with governing law and jurisdiction provisions of the Master Subscription Agreement, except as otherwise required by applicable Data Protection Law, including where the SCCs apply.

Schedule 1: STANDARD CONTRACTUAL CLAUSES

If, and to the extent, Applicable Data Protection Law requires the parties to enter into the SCCs in connection with the Processing of Personal Data, each party is deemed to have executed the SCCs by entering into this DPA. The below shall apply to the SCCs, including the election of specific terms and/or optional clauses as described in more detail in (i) through (x) below, and any optional clauses not expressly selected are not included:

(a) The Module 2 terms apply to the extent Customer is a Data Controller and the Module 3 terms apply to the extent Customer is a Data Processor of the Customer Personal Data;

(b) The optional Clause 7 (Docking Clause) in Section I of the SCCs is incorporated, and Authorised Affiliates may accede to this DPA and the SCCs under the same terms and conditions as Customer, subject to Section 3.3 of this DPA via mutual agreement of the Parties;

(c) For purpose of Clause 9 of the SCCs, Option 2 ("General written authorization") is selected and the process and time period for the addition or replacement of Sub-processors shall be as described in Section 9 (sub-processing) of this DPA and identified in Annex III of the SCCs;

(d) For purposes of Clause 13 and Annex I of the SCCs, the following shall apply [CUSTOMER TO SELECT APPLICABLE PROVISION]:

[Where the data exporter is established in an EU Member State:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(e) For purpose of Clause 17 and Clause 18 of the SCCs, the Member State for purpose of governing law and jurisdiction shall be the Republic of Ireland;

DATA EXPORTER
Name:……

Authorised Signature ……

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

Authorised Signature ……

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

Address: …

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

Activities relevant to the data transferred under these Clauses:

Use of the DNAnexus platform processing……

Signature and date: …

Role (controller/processor): …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: DNAnexus, Inc.

Address: 1975 W El Camino Real, Suite 204, Mountain View, CA 94040

Contact person's name, position and contact details: E. Loren Buhle, Jr. Ph.D, VP of Risk, Quality and Compliance, DNAnexus. Email: privacy@dnanexus.com

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

<examples might include DNAnexus and Customer's PII working on the platform (email address, contact information>

- DNAnexus and Customer's personnel working on the platform
- Patient sampels involved in research

Categories of personal data transferred (example below)

Data Category	DNAnexus & Customer Personnel	Patient Samples involved in Research
Civil status *(e.g. name, sex, age, etc.)*	Yes	No
Contact information (e.g. e-mail address, postal address, phone numbers, etc)	Yes	No
Data specifically related to the provision of electronic communication services (e.g. location data or connection, data on internet browsing histories, etc.)	Yes	No
Identification or access data *(e.g. login, passwords, API activity)*	Yes	No

Data Category	DNAnexus & Customer Personnel	Patient Samples involved in Research
Data relating to financial information *(e.g. credit card information, bank details, Purchase Order, etc.)*	Yes	No

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
Example below

Data Category	DNAnexus & Customer Personnel	Patient Samples involved in Research
Data revealing racioal or ethnic origin or ethnic origin	No	Yes (but pseudonymized information)
Data revealing political opinions	No	No
Sensitive data – philosophical or religious beliefs, political opinionms, trade union membership	No	No
Sensitive data – data related to a natural person's sex life or sexual orientation	No	No
Genetic data	No	Yes (but pseudonymized information)
Sensitive data – Health data	No	Yes (but pseudonymized information)
Data on criminal convictions or offenses	No	No
Unique national idenfifier Number	No	No

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfer between the Customer and the DNAnexus Platform wil be done as needed.

Nature of the processing

The Customer Personal data transferred will be subject to the following basic processing activities:

a) Frequency and duration: Notwithstanding expiry or termination of the Agreement, DNAnexus shall Process the Customer Personal Data continuously and until deletion of all Customer Personal Data as described in this DPA.

b) Purpose: DNAnexus shall Process the Customer Personal Data for the Purposes, as described in this DPA.

c) Nature of the Processing: DNAnexus shall perform Processing as needed for the Purposes, and to comply with the Customer's Processing instructions as provided in accordance with the Agreement and this DPA.

Retention of Data

The period for which Customer Personal Data will be retained and the criteria used to determine that period shall be determined by the Customer during the term of the Agreement via its used and configuration of the Service. Upon termination or expiration of the Agreement, Customer may retrieve or delete all Customer Personal Data as set forth in Section 8 of this Agreement. Any Customer Personal Data not deleted by the Customer shall be deleted by DNAnexus in accordance with DNAnexus' procedures as triggered by the later of (i) expiration or termination of the Agreement and (ii) expiration of any post-termination "grace period" set forth in the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

<Customer lists their subprocessors>

- DNAnexus' subprocessors are described in Annex III of this document.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

……

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

DNAnexus implies multiple security and privacy controls based on principles of "zero trust", "least privilege" and continuous monitoring. DNAnexus complies and is audited by third parties for ISO 27001 and has the "Moderate" category of an Authorization to Operate (ATO) under the U.S. FedRAMP program. DNAnexus' FedRAMP authorization is under the sponsorship of the U.S. Department of Health & Human Service ("HHS"), requiring annual audits, continuous monitoring and monthly reporting to HHS. FedRAMP is largely based around the U.S. NIST 800-family of controls.

With respect to Confidentiality, Integrity and Availability, the sensitivity categorization of information types is:

Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availability
Research and Development	D.20.1	Moderate (M)	Moderate (M)	Low (L)
Health Care Research and Practitioner Education	D.14.5	Moderate (M)	Moderate (M)	Low (L)

Based on these categories, DNAnexus' controls are set to the mitigate the risks aligned with the following Security Impact Level:

Security Objective	Low, Moderate or High
Confidentiality	Moderate (M)
Integrity	Moderate (M)
Availability	Low (L)

It is based on these risks, third party independent assessors and a monthly review by HHS that DNAnexus uses the Moderate (M) baseline security controls. These controls are monitored continuously by DNAnexus and are assessed annually by a FedRAMP certified 3rd party assessor.

For customers using DNAnexus for performing regulated operations, DNAnexus provides a 21 CFR § 11 compliant system supported by Quality Systems compliant with ISO/IEC 13485:2016 and 21 CFR § 820.

In addition to deploying the principles of zero trust and least privilege, all data is encrypted in transit (TLS v1.2+) and at rest (AES256+). DNAnexus inherits the physical and environments of our cloud service providers, namely Amazon's AWS and Microsoft Azure as indicated to be sub-processors of DNAnexus in the following Annex.

A sampling of the overall processes employed by DNAnexus to protect the data includes:

1	Encryption at rest and in transit
2	Zero trust compartmentalization
3	Logical access control
4	Separation of Data from meta-tags

12	Reduction in Attack surfaces
13	Employee management
14	Security Trianing
15	Web site protection

5	Physical Security
6	Continuous Monitoring
7	Logging
8	Least Access. Least Priviledge
9	Active sense & response to malicious software
10	Workstation management
11	Traceability

16	Subcontractor agreements
17	ISO/IEC 27001:2013 certification
18	FedRAMP Moderate “ATO”
19	21 CFR § 11 and Annex 11 compliance
20	Quality System Regulation Compliance
21	Alignment with applicable privacy standards
22	Resilience to changing workloads

ANNEX III – LIST OF SUB-PROCESSORS

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

1. Name: Amazon Web Services (AWS)
   Address: 410 Terry Avenue North, Seattle WA 98109
   Contact: https://aws.amazon.com/contact-us/compliance-support/
   Description of processing: infrastructure hosting services

2. Name: Microsoft Azure
   Address: One Microsoft Way, Redmond, WA 98052, USA
   Contact: https://azure.microsoft.com/en-gb/overview/trusted-cloud/privacy/
   Description of processing: infrastructure hosting services

3. Name: Salesforce.com
   Address: 55 2nd Street, 4th Floor, San Francisco, CA 94105, USA
   Contact: privacy@salesforce.com and (1) 844.287.7147
   Description of processing: ServiceCloud is used for support services

4. Name: SendGrid
   Address: 400 Spectrum Center Dr #400, Irvine, CA 92618, USA
   Contact: (1) 887.749.5740
   Description of processing: Email notification services (non-FedRAMP customers)

5. Name: RemoFirst
   Address: 415 Mission Street, San Francisco, CA 94105, USA
   Contact: help@remofirst.com
   Description of processing: Customer Support and software development, including billing

6. Name: Splunk
   Address: 270 Brannan Street, San Francisco, CA 94107, USA
   Contact: 1 855-775-8657
   Description of processing: Processing of log internal log information, including IP addresses and userIDs

7. Name: Okta
   Address: 100 First Street, San Francisco, CA 94105, USA
   Contact: Americas: 1 800-588-1656, Europe: +44 (800) 368-8930
   Description of processing: Processing of userIDs and IP addresses for Single Sign On (SSO)

Schedule 2: INTERNATIONAL DATA TRANSFER ADDENDUM

Also known as the "UK Addendum"

The full text of this document is here:
https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

The tables for completion are reproduced here. All mandatory clauses remain unaltered.

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: DNAnexus, Inc. Trading name (if different): Main address (if a company registered address): 1975 W El Camino Real, #204, Mountain View, CA 94040 USA. Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email: privacy@dnanexus.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or

	☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:

Annex 1B: Description of Transfer:

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Annex III: List of Sub processors (Modules 2 and 3 only):

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**: ☐ Importer ☐ Exporter ☐ neither Party