DATA ACCESS AGREEMENT
for EGA Study

This Data Access Agreement ("Agreement" or "DAA"), including its appendices, is to allow a researcher's institution ("User Institution") to seek approval from the Board of Trustees of the Leland Stanford Junior University, on behalf of its School of Medicine, Biochemistry Division (collectively, "Stanford" or "Data Producer") to allow Approved Personnel at User Institution to access certain data and information available in a cloud-based data environment for the purpose of conducting _____ research. Prior to Stanford giving final approval for access to said data, an application must be reviewed and approved by the Data Access Committee (DAC).

These terms and conditions govern access to the managed access datasets (details of which are set out in Appendix I) to which the User Institution has requested access. The User Institution agrees to be bound by these terms and conditions.

Definitions

Applicable Law: All U.S. Federal, state and local laws and regulations to the extent applicable to the terms of this Agreement, including without limitation the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5), and the General Data Protection Regulation (EU) 2016/679 (GDPR), in each case as the same may be amended or supplemented from time to time.

Authorized Personnel*:* The individual(s) at the User Institution to whom the DAC grants access to the Data. This includes the User, and may include additional individuals as listed in Appendix II, and any other individuals for whom the User Institution subsequently requests access to the Data and for whom DAC has issued written approval. Details of the initial Authorized Personnel are set out in Appendix II.

Data*:* The managed access datasets to which the User Institution has requested access.

DAC: The data access committee for Stanford University related to the research in Appendix 1 and Appendix 2 attached to this Agreement. The DAC includes the Stanford Principal Investigator for such research, and any other personnel that Stanford may deem appropriate in its sole discretion (e.g., experts in research, ethics, privacy and/or legal matters).

Data Producers*:* The DAC and any other Stanford personnel responsible for the development, organization, and oversight of access to these Data.

External Collaborator*:* A collaborator of the User, working for an institution other than the User Institution.

Institutional Review Board (IRB): The independent ethics committee (IEC), ethical review board (ERB), or research ethics board (REB), which is/are committee(s) designated to safeguard ethical conduct of studies using human subjects by monitoring and reviewing biomedical and behavioral research under certain national and international laws, regulations, codes and/or norms.

Joint Controller Arrangement (Arrangement): The arrangement by and between Stanford and the User Institution as detailed in Appendix IV providing additional party obligations to ensure each party complies with data protection laws applicable to the Data under local, state, national and/or foreign laws, treaties, and/or regulations, laws of the European Union, and the European Economic Area, including the GDPR.

Protected Health Information (PHI): Individually Identifiable Health Information that is transmitted by electronic media; maintained in any medium described in the definition of the term electronic media in the HIPAA regulations; or transmitted or maintained in any other form or medium as defined in 45 C.F.R. § 164.501. Protected Health Information excludes Individually Identifiable Health Information in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g, and records described at 20 U.S.C. § 1232g(a)(4)(B)(iv).

Personally Identifiable Information (PII): Information or data that (i) identifies an individual, including by name, signature, address, telephone number or other unique identifier, (ii) can be used to identify or authenticate an individual, including passwords, PINs, biometric data, unique identification numbers (e.g., social security numbers), answers to security questions or other personal identifiers, (iii) PHI under HIPAA and the HITECH Act and/or (iv) can be used in combination with other information or data to identify an individual, including but not limited to the individual's gender, race, income, date of birth, geographic location, school or workplace name, group affiliations, mental, emotional or physical characteristics, or other indirect identifiers.

Project*:* The project for which the User Institution has requested access to these Data. A description of the Project is set out in Appendix II.

Publications*:* Includes, without limitation, articles published in print journals, electronic journals, reviews, books, posters and other written and verbal presentations of research.

Research Participant*:* An individual whose data form part of these Data.

Research Purposes: The purpose for which these Data are being sought and where such research seeks to advance the understanding of _____, including the treatment of disorders, and work on statistical methods that may be applied to such research.

User*:* The principal investigator for the Project at User Institution.

User Institution(s)*:* The Institution that has requested access to the Data. Please include your Institution legal name and address here:

[NAME]
[LEGAL ADDRESS 1]
[LEGAL ADDRESS 2]
[PHONE]
[FAX]
[ATTN:]

Terms and Conditions

1. The User Institution agrees to only use these Data for the purpose of the Project (described in Appendix II) and only for non-commercial research purposes. The User Institution further agrees that it will only use these Data for research purposes which are within the limitations (if any) set out in Appendix I and the Joint Controller Arrangement (Arrangement), attached hereto at Appendix IV and hereby incorporated by reference.

2. The process for accessing these Data in accordance with this DAA is as set forth below:

- The process of the application review by the Data Access Committee (DAC) is being managed by the Stanford Principal Investigator, in coordination with the Stanford University Privacy Office where appropriate; but the authority for final approval to grant access and to oversee data usage is under the responsibility and control of the Stanford. The organization entering into this Agreement with Stanford is referred to as the "User Institution." User Institution's agreement with Stanford through the DAA is to obtain access to the Stanford Data stored in The European Genome-phenome Archive at the European Bioinformatics Institute Database for the stated purpose of conducting the Research Purposes as detailed in the Project and this DAA.

- User Institution will apply for EGA Database access via _____, which will see that applications are reviewed by the DAC. Final responsibility for access to Data will be governed by Stanford; however, oversight of its usage and compliance with applicable laws will be the responsibility of User Institution.

- In order to access the Data, the User and User Institution must apply for and receive approval from both the DAC and the Data Producer for access to the Data in the EGA Database in accordance with the terms and conditions hereunder.

- Once the application and DAA are received, the DAC will review the application to confirm the following: the application is complete and the DAA has been properly completed and signed; the User or User Institution is not on any type of debarment list; the User is from a recognized institution that has the appropriate research, legal and financial means to support the project; the Project is feasible given the resources in the EGA Database; and the Project aims to advance scientific exploration and principles of openness in research.

- The DAC will have the discretion to approve or decline an application or DAA based on ethical, scientific, programmatic or other relevant considerations. Among other things, the DAC may consider the following criteria: the User is qualified to conduct the Project and undertake the proposed analysis; the User Institution has confirmed that the minimum data security safeguards described at Section 6, below, have been implemented; the User has confirmed that IRB approval has been obtained, or, if no confirmation of IRB approval is provided, documentation explaining why the Institutional Review Board is not requiring approval.

- The DAC will submit to the User Institution its decision as to whether a User's application and/or DAA is approved, declined or conditionally approved. If the DAC has approved the User application, the DAC will then determine if access is appropriate and sign the DAA. An Access Authorization Letter with directions for accessing the EGA database and Data will be emailed to the address provided by the User in the application. Even though the Data is provided by the Data Producer at no cost to the User Institution, access to the Data will require the Institution to establish an account on the EGA Website and cover all costs associated with access, storage, egress charges, compute costs, and/or maintenance to service the User's account. This account will be owned by _____ and all costs associated with work undertaken in that account will be the responsibility of the Institution.

- The Access Authorization Letter will also be accompanied with a copy of the DAA executed by the Data Producer and User Institution. This DAA will govern the User's and User Institution's access to the EGA Database and Data. The terms of this DAA will prevail over any inconsistent terms of the EGA Website or elsewhere, and over any oral or written statement made by the staff of the DAC.

- If the DAC has conditionally approved an Institution's application, the Access Authorization Letter will set forth the additional information required to be submitted to the DAC, which may include additional data access and use terms to which User and User Institution must assent. Upon receipt of such additional information, the DAC will review User Institution's revised application, should one be submitted, together with the additional required information in accordance with the above steps and a notification of the decision of the DAC will be provided in accordance with this step.

- Each DAA will have a term of one (1) year from the date of last signature ("Effective Date") of the DAA. To renew a DAA and continue access to the EGA Database after expiration of the then-existing DAA, the User will be required to submit a renewal request. The Renewal Request will require User to provide: an updated User application or confirmation that the content of the User application originally submitted remains correct and complete; an updated list of and contact information for the Authorized Personnel, or confirmation that the list of and contact information for the original Authorized Personnel remains correct and complete; and all Publications prepared using the results of the Project in accordance with the Publication Policy at Appendix III.

3. Data may be used only for an IRB-approved Project as mutually agreed upon by both the DAC and the User Institution and only for the purposes of advancing science, deriving outcomes, and generating research results. The User Institution acknowledges and understands that the Data is/are valuable and that except as expressly permitted only User, Authorized Personnel, and External Collaborators agreeing to abide by the protections set forth herein are the only persons permitted to use the Data under this

Agreement. Confirmation that an Institutional Review Board (IRB) and ethics committee has approved the User's use of these Data, including the name of the approved protocol, the date of approval and the name, address and email address of the IRB, and a letter from the IRB approving the Project subject to annual oversite and approval or stating that approval is not required due to the type of data being accessed, must be received by the DAC prior to approval.

4. The User Institution will notify the DAC prior to any significant changes to the protocol for the Project or the Project itself.

5. The User Institution will notify the DAC within thirty (30) days of any changes or departures of Authorized Personnel. The User Institution agrees to distribute a copy of these terms to the Authorized Personnel. The User Institution shall ensure that the Authorized Personnel comply with the terms of this agreement.

6. User Institution agrees to use the Data only in connection with this Agreement and to hold the Data in strict confidence. The User Institution agrees not to disclose, share, sell or allow access to any of the Data except as expressly permitted by this Agreement. Furthermore, with regard to PII/PHI received in connection with the Data, the User represents and warrants that it shall comply with all Applicable Law and ensure that all computer systems and devices used to access or process these Data meet Data Producers' minimum security standards for high risk data, found at https://uit.stanford.edu/guide/securitystandards in order to protect these Data.

7. If requested, the User Institution will allow data security and management documentation to be inspected to verify that it is complying with the terms of this agreement.

8. The User Institution agrees only to transfer or disclose these Data, in whole or part, or any material derived from these Data, only to the Authorized Personnel. Should the User Institution wish to share these Data with an External Collaborator, the External Collaborator must complete a separate Data Access Agreement for access to these Data.

9. The User Institution agrees not to link, attempt to link, combine, or attempt to combine these Data to any other information or archived data available in a way that could reasonably be used to re-identify the Research Participants, even if access to that data has been formally granted to the User Institution or is freely available without restriction. Should User Institution inadvertently receive identifiable information or otherwise identify a subject, Recipient shall immediately notify the Data Producers and follow Data Producers' reasonable written instructions, which may include return or destruction of the identifiable information.

10. The User Institution agrees to protect the confidentiality of Research Participants in any research papers or Publications that they prepare by taking all reasonable care to limit the possibility of identification.

11. The User Institution will notify the DAC immediately upon becoming aware a breach of the terms or conditions of this agreement or upon User Institution's discovery of any unauthorized use or disclosure of these Data.

12. The parties will promptly confer and agree on legally required steps the User Institution shall take to minimize the harm (if any) resulting from such breach. The User Institution will cooperate with the Data Producer in complying with such steps. In the event of actual or suspected unauthorized disclosure of, access to, or other breach of these Data, the User Institution will comply with all Applicable Law and regulations related to such breach, and will cooperate with the Data Producer in assisting it to fulfill its legal obligations.

13. The User Institution agrees that the Data Producers, and all other parties involved in the creation, funding or protection of these Data: a) make no warranty or representation, express or implied, of any kind as to the accuracy, quality, or comprehensiveness of these Data; b) exclude to the fullest extent permitted by law all liability for actions, claims, proceedings, demands, losses (including but not limited to loss of profit), costs, awards damages and payments made by the User Institution that may arise (whether directly or indirectly) in any way whatsoever from the User Institution's use of these Data or from the unavailability of, or break in access to, these Data for whatever reason and; c) bear no responsibility for the further analysis or interpretation of these Data.

14. The User Institution shall defend, indemnify and hold the Data Producer and its directors, officers, employees, students, agents, successors and assigns harmless, to the full extent permitted in law or equity, from and against any and all losses, claims, actions, damages, regulatory actions or investigations, liabilities, costs and expenses (including reasonable attorneys' fees and expenses), fines, penalties, judgments, and costs (including but not limited to the costs of providing appropriate notice to all parties and credit monitoring, credit rehabilitation, or other credit support services to individuals with information impacted by the actual or suspected breech, to the extent procured by the User Institution (each a "Claim" or, collectively, "Claims") to the extent that a Claim or Claims: (i) arise out of a breach of the User Institution's obligations hereunder; (ii) arise out of the User Institution's use, handling or storage of these Data in a manner not permitted by this Agreement or Protocol; or (iii) relate to User Institution's gross negligence or intentional acts under this Agreement, except to the extent a Claim or Claims is/are caused by the Data Producer's own gross negligence or intentional misconduct.

15. THE DATA PRODUCER WILL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES OF THE OTHER ARISING OUT OF OR IN CONNECTION TO ANY PERFORMANCE OF THIS AGREEMENT OR IN FURTHERANCE OF THE PROVISIONS OR OBJECTIVES OF THIS AGREEMENT, REGARDLESS OF WHETHER SUCH DAMAGES ARE BASED ON TORT, WARRANTY, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

16. The User Institution agrees to follow the *Publication Policy* in Appendix III. This includes respecting the moratorium period for the Data Producers to publish the first peer-reviewed report describing and analyzing these Data.

17. The User Institution agrees that all Data shall be owned exclusively by the Data Producer. To the extent the User Institution has or acquires any rights in or to the Data, the User and User Institution each hereby irrevocably assigns, transfers and conveys to the Data Producer all of its right, title and interest in and to the Data, excluding any modifications, enhancements or derivative works developed by the User Institution using the Data. For clarity, summaries, analyses and interpretations of the Data generated by the User pursuant to this Agreement shall not be considered "Data" and rights with respect to such summaries, analyses and interpretations shall be the property of the User or User Institution, as the case may be. Furthermore, and notwithstanding anything to the contrary herein, to

the extent Data cannot be segregated from the User's research results generated under the Project, the User and User Institution hereby grants to the Data Producer perpetual unrestricted right and license in and to that subset of Data necessary to fully exploit its rights in the Data and research results generated therefrom.

18. The User Institution can elect to perform further research that would add intellectual and resource capital to these Data and decide to obtain intellectual property rights on these downstream discoveries. In this case, the User Institution agrees to implement licensing policies that will not obstruct further research and to follow the U.S. National Institutes of Health *Best Practices for the Licensing of Genomic Inventions (2005)* (*https://www.icgc.org/files/daco/NIH_BestPracticesLicensingGenomicInventions_2005_en.pdf*) in conformity with the Organisation for Economic Co-operation and Development *Guidelines for the Licensing of the Genetic Inventions (2006)* (*http://www.oecd.org/science/biotech/36198812.pdf*). The User Institution hereby grants to the Data Producer a perpetual unrestricted right and license use these intellectual property rights on these downstream discoveries.

19. The User Institution agrees to certify the destruction or, if destruction is not feasible, the return of the Data held once it is no longer used for the Project, unless obliged to retain the Data for archival purposes in conformity with audit or legal requirements.

20. The Data Producer may terminate this agreement at any time and at its sole discretion by written notice to the User Institution. If this agreement terminates for any reason, the User Institution will be required to destroy any Data held, including copies and backup copies. This clause does not prevent the User Institution from retaining these data for archival purpose in conformity with audit or legal requirements.

21. The User Institution accepts that it may be necessary for the Data Producers to alter the terms of this agreement from time to time. As an example, this may include specific provisions relating to the Data required by Data Producers other than the DAC. In the event that changes are required, the Data Producers or their appointed agent will contact the User Institution to inform it of the changes and the User Institution may elect to accept the changes by written amendment to this Agreement, or terminate the agreement.

22. The validity, construction and performance of this Agreement and the legal relations among the parties hereto shall be governed by and construed in accordance with the laws of the State of California, excluding that body of law applicable to choice of law and the parties consent to the jurisdiction of the courts of California State in connection with the resolution of any dispute among them arising from the validity, construction or performance hereof. If any provision of this Agreement or the application of any such provision shall be held by a tribunal of competent jurisdiction to be unenforceable or contrary to law, the remaining provisions of this Agreement shall continue in full force and effect.

23. In the event of a dispute arising out of or relating to this Agreement, the parties shall first attempt in good faith to resolve such dispute by negotiation and consultation between themselves. Either party may, by written notice to the other party, refer the dispute to the other party for attempted resolution by formal good faith negotiation within thirty (30) days after such notice is received. If the dispute remains unresolved after the good faith negotiation period provided in the previous sentence, either party by written notice to the other party may have such issue referred for resolution to the parties'

respective executive officers or senior legal counsel. The executive officers or senior legal counsel shall meet promptly to discuss the matter submitted and to determine a resolution. If the executive officers or senior legal counsel fail to resolve the dispute within thirty (30) days after it is referred to them, each party shall have the right to pursue any other remedies legally available to resolve the dispute and the matter may be brought by a party as a suit in a court of competent jurisdiction in accordance with Section 22, above.

24. The User Institution shall not use the name, symbol, logo, likeness, service mark or trademark of the Data Producer without the prior written consent of the Data Producer.

25. All Notices. All notices under this Agreement are deemed fully given when written, addressed, and sent as follows:

All notices to User Institution:

[NAME]
[ADDRESS 1]
[ADDRESS 2]
[Attention:]
[Phone:]
[Fax:]
[Email:]

All notices to Data Producer:

Office of Sponsored Research
Stanford University
485 Broadway, Floor 3
Redwood City, California USA
94063-3136
Attention: OSR Intake (AGR799947, PI: Krasnow)
Phone: (650) 725-2525
Email: osr_intake@stanford.edu
cc: murphyjd@stanford.edu
cc: krasnow@stanford.edu

[*intentionally left blank*]

[*signatures continue on next page*]

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed below by their duly authorized signatories.

Agreed for User Institution

Signature:	
Name:	
Title:	
Date:	

I confirm that I have read and understood this Agreement.

User

Signature:	
Name:	
Title:	
Date:	

Agreed for the Data Producer

Signature:	
Name:	
Title:	
Date:	

As reviewed by the Data Access Committee

Signature:	
Name:	
Title:	
Date:	

APPENDIX I
DATASET DETAILS

Dataset reference (EGA Study ID and Dataset Details)

EGA study accession: _____.

Description: _____.

EGA dataset for study: _____.

Description: _____.

Name of project that created the dataset

EGA study accession: _____.

Description: _____.

Names of other data producers/collaborators

Specific limitations on areas of research

The User Institution agrees that it will only use these Data for Research Purposes.

APPENDIX II
PROJECT DETAILS

[to be completed by the User Institution]

Details of dataset requested (i.e., EGA Study and Dataset Accession Number):

Title of the Research Project:

Research question proposed to be answered by the Project (500 words max):

Summary of Project suitable for a lay audience (200 words max):

Country(ies) where the Project will be conducted and downloaded copies of Data will be held:

All Individuals who the User Institution to be named as registered users:

Name of Registered User	***Email***	***Job Title***	***Supervisor****

All Individuals that should have an account created at the EGA:

Name of Registered User	**Email**	**Job Title**

APPENDIX III
PUBLICATION POLICY

The DAC and/or Data Producer intend to publish the results of their analysis of this dataset(s) and do not consider its deposition into the European Genome-phenome Archive or any public databases to be the equivalent of such publications. The DAC and/or Data Producer anticipates that the Data could be useful to other qualified researchers for a variety of purposes. However, some areas of work are subject to a publication moratorium. The publication moratorium covers any publications (including oral communications) that describe the use of the Data.

For research papers or Publications, submission for publication should not occur until one (1) year after these Data were first made available on the relevant hosting database, unless the DAC has provided written consent to earlier submission. Without limiting the foregoing, the User Institution shall inform the Data Producers at least thirty (30) days prior to its intent to publish the results of their analysis of this Data. A shorter review time is permissible by mutual agreement. The User Institution agrees that if the Data Producers reasonably determine that the proposed publication contains confidential, proprietary, or sensitive information belonging to the Data Producers or Research Participant(s), then the User Institution shall remove any such confidential, proprietary or sensitive Information if requested to do so before publishing. If the Data Producers determine that the proposed publication contains patentable subject matter and desires to have such subject matter protected by a patent application, the User Institution agrees to delay publication for up to an additional ninety (90) days after the one-year publication moratorium in order for a patent application to be filed. For the avoidance of doubt, no right of manuscript approval is implied by this section.

In Publications based on these Data, please describe how the Data can be accessed, including the name of the hosting database (e.g., The European Genome-phenome Archive at the European Bioinformatics Institute) and its accession numbers (e.g., EGAS000000000XX), and acknowledge Stanford and the Stanford Principal Investigator in each use of the Data or analysis or research results derived therefrom in a form agreed by the User Institution with the approval of the DAC.

The User Institution agrees to follow the *Fort Lauderdale Guidelines* (*http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtd003207.pdf*) and the *Toronto Statement* (*http://www.nature.com/nature/journal/v461/n7261/full/461168a.html*). This includes but is not limited to recognizing the contribution of the Data Producers and including a proper acknowledgement in all reports or Publications resulting from the use of these Data.

Nothing herein shall authorize the User Institution to use or further disclose the Data in a manner that would violate the requirements of Data Producers under any Applicable Law.

APPENDIX IV
JOINT CONTROLLER ARRANGEMENT

This Joint Controller Arrangement (this "**Arrangement**") forms part of the Data Access Agreement by and between Stanford and User Institution dated _____ __, 20__ (the "**Agreement**"). Stanford and User Institution are each referred to as a "**Party**" and collectively, the "**Parties**."

1. Definitions

Unless otherwise defined below, all capitalized terms have the same meaning given to them in the Agreement and/or exhibits thereto.

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

"**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller.

"**Data Protection Laws**" means all data protection laws applicable to the Processing of Personal Data under this Arrangement, including local, state, national and/or foreign laws, treaties, and/or regulations, laws of the European Union, and the European Economic Area, including the GDPR.

"**EEA**" means the European Economic Area.

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679.

"**Joint Controllers**" means two Data Controllers that jointly determine the purposes and means of processing.

"**Personal Data**" means Research Participant Data that is related to an identified or identifiable person.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"**Processing**" or "**Process**" means any operation or set of operations concerning Personal Data, including the collection, recording, organization, storage, updating, modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure, or destruction of Personal Data.

"**Subprocessor**" means any person or entity working on behalf of the Processor to process Personal Data.

"**Valid Transfer Mechanism**" means a data transfer mechanism recognized by the European Commission as a legitimate basis for the transfer of Personal Data outside the EEA.

2. Processing Personal Data

2.1. Scope and Role of the Parties. This Arrangement applies to the Processing of Personal Data by the Parties wherein the Parties are Joint Controllers with respect to the Personal Data collected or Processed under the Agreement.

2.2. Responsibilities for Processing, Notice and Legal Basis.

- **a.** Stanford shall Process the Personal Data in the following ways: approving access to Stanford Data deposited in the European Genome-phenome Archive at the European Bioinfomatics Institute Database for the stated purpose of conducting the Research Purposes as detailed in the Project attached to the Agreement. Personal Data will be processed by Stanford and its Data Processors in the United States and the European Union, unless the Parties otherwise expressly agree in writing.
- **b.** User Institution shall Process the Personal Data in the following ways [insert description of Processing activities by Sponsor]. Personal Data will be processed by User Institution and its Data Processors in [insert country jurisdictions where data will be processed] unless the Parties otherwise expressly agree in writing.
- **c.** Stanford shall make available a privacy notice which shall describe and allocate the respective responsibilities of compliance of Stanford and User Institution as set out in this Arrangement. Such notice must be in a concise, transparent, intelligible, and easily accessible form that uses clear and plain language. Stanford shall provide notice in writing, or by other means, as required by Data Protection Laws. Prior to providing the notice to Research Participants, and prior to any subsequent modifications of such notice, Stanford and User Institution shall agree on method, form and content of the notice.
- **d.** The data protection notice shall contain contact points for Research Participants to contact each Party. Where a Party receives a request, query, complaint or other communication in relation to the Processing of Personal Data in accordance with the notice, that Party shall notify the other Party of such request, query, complaint or other communication.
- **e.** Each Party is responsible for ensuring that there is a legal basis for its Processing of Personal Data, including any special categories of Personal Data, under the Agreement and pursuant to this Arrangement.
- **f.** If a Party intends to modify its processing activities, such Party shall provide prior notice to the other Party.

2.3. Compliance with Laws. The Parties shall comply with the obligations under Data Protection Laws as set forth and assigned to them in this Arrangement or the Agreement. For the avoidance of doubt, the Parties are not responsible for complying with obligations not assigned to them in this Arrangement or otherwise not applicable to them. In the event that there is an obligation under Data Protection Laws that is not specifically assigned to either Party, then both Parties are responsible for complying with that obligation.

2.4. Data Processing Compliance. Without prejudice to the foregoing, The Parties agree Personal Data Processing shall be:

- **a.** Lawful, fair, and transparent in relation to the Research Participants;
- **b.** Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. Accurate and, where necessary, kept up to date;
e. Kept in a form which permits identification of Research Participants for no longer than is necessary for the purposes for which the Personal Data are processed, unless otherwise permitted or provided by Data Protection Laws; and
f. Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

3. Data Processors

The Parties may engage Data Processors to Process the Personal Data. Each Party shall ensure that it has entered into written agreements with its own Data Processors that require the Data Processors to abide by terms no less protective than those provided in this Arrangement. Such written agreements must comply with Data Protection Laws, including Article 28 of the GDPR. Each Party shall be liable for the acts and omissions of its Data Processors to the same extent as if the acts and omissions were performed by that Party.

4. Data Transfers.

Notwithstanding Section 2.2(a) and (b), the Parties agree that they will only access Personal Data from (i) countries in the EEA; (ii) countries formally recognized by the European Commission as providing an adequate level of data protection ("**Adequate Countries**"); and, (iii) the United States and other non-Adequate Countries, provided that the Parties put in place a Valid Transfer Mechanism and that, with respect to access by Data Processors, the requirements of Section 3 are met. For example, the Parties may implement the Standard Contractual Clauses attached as Attachment A as the Valid Transfer Mechanism under this Arrangement.

5. Rights of Research Subjects

5.1. Research Subject Requests. Stanford is responsible for responding to Research Participant requests for access, correction, deletion, or restriction of that person's Personal Data or any objection to processing or withdrawal of any consent ("**Research Participant Request**"). If User Institution receives a Research Participant Request, User Institution shall promptly redirect the Research Participant to Stanford. User Institution will cooperate with and provide reasonably assistance to Stanford to enable Stanford to meet its obligations to respond to and fulfill Research Participant Requests. For the avoidance of doubt, Stanford is responsible for responding to Research Participant's data portability requests. To the extent a Research Participant's Personal Data is not accessible to Stanford, User Institution will, as necessary to enable Stanford to meet its obligations under applicable Data Protection Laws, provide such Personal Data extract in a structured, commonly used and machine-readable format.

6. Government Access Requests and Litigation

Unless prohibited by applicable law or a legally-binding request of law enforcement, Parties shall promptly notify the other Party of (i) any request by government agency or law enforcement authority for access,

investigation, audit or seizure of Personal Data; and, (ii) any request for a copy of any Personal Data pursuant to any third party claim, litigation, legal action, arbitration, or mediation.

7. Personnel

Parties shall take reasonable steps require screening of its personnel who may have access to Personal Data, and shall require such personnel to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data.

8. Security

8.1. Security Program. Without limiting Section 6 of the Agreement, the Parties shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and, (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing. In addition such measures shall be designed to protect Personal Data against unauthorized access or disclosure or accidental or unlawful destruction, loss, or alteration and shall be appropriate to (i) the size, scope, and type of their business; (ii) the type of information that the Parties will Process; and, (iii) the need for security and confidentiality of such information.

8.2. Breach Notification. A Party impacted by a Data Breach affecting the Personal Data that is under joint control of the Parties (the "**Impacted Party**") shall promptly (and in any case not more than 24 hours of becoming aware of a Personal Data Breach) notify the other Party of any Personal Data Breach. The notice will include: (i) the date or date range of the incident; (ii) date of discovery; (iii) description of Personal Data involved; (iv) number of EU Research Participants affected; (v) likely consequences of the breach; and, (vi) investigative and mitigation actions taken. The Impacted Party shall also take all reasonable steps to ensure that such information is covered by client attorney or litigation privilege where possible. The Impacted Party will promptly submit updates to the other Party as appropriate; including regarding any legal actions required due to the breach. The Parties shall cooperate in any investigation and provide sufficient information to allow the Parties to meet legal and contractual obligations. To the extent any applicable law requires that the affected Research Subjects or governmental authority be notified of a Personal Data Breach, the Impacted Party will be responsible for, at its own cost and expense, and indemnify the other Party for:

- **a.** Upon mutual agreement by the Parties, providing notices to Research Participants or governmental authorities containing the information required by applicable law;
- **b.** Conducting any forensic and security review, investigation and audit in connection with such Personal Data Breach; and
- **c.** Providing remediation services and other reasonable assistance to such Research Subjects as (a) required under law, (b) requested by governmental authorities and (c) are consistent with customary industry practice in the applicable jurisdiction.

To the extent that any Party is subject to or involved in an investigation by a governmental authority or litigation arising out of or related to a Personal Data Breach, the other Party will provide reasonable cooperation to the Impacted Party in responding to such event.

9. Audit

The Parties agree that each shall make available, upon reasonable request, information necessary to demonstrate compliance with this Arrangement and shall, upon reasonable prior written consent no more than once annually, allow for audits or inspection by the other Party in relation to the Processing of Personal Data under the Agreement.

10. Accountability

The Parties shall be responsible for, and be able to demonstrate compliance with, this Arrangement and applicable Data Protection Laws.

10.1 Record of Processing Activities. Each Party shall maintain a record of its Processing activities under the Agreement that includes the following information:

- **a.** The name and contact details of the Controller and, where applicable, the joint controller, the Controller's representative and the data protection officer;
- **b.** The purposes of the Processing;
- **c.** A description of the categories of Research Participants and of the categories of Personal Data;
- **d.** The categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organizations;
- **e.** Where applicable, transfers of Personal Data to a third country or an international organization, including the identification of that third country or international organization and, when applicable, the documentation of suitable safeguards;
- **f.** Where possible, the envisaged time limits for erasure of the different categories of Personal Data; and
- **g.** Where possible, a general description of the technical and organizational security measures implemented to protect the Personal Data.

11. Indemnification; Limitations on Liability; Remedies.

11.1. The User Institution shall defend, indemnify and hold Stanford and its directors, officers, employees, students, agents, successors and assigns harmless, to the full extent permitted in law or equity, from and against any and all losses, claims, actions, damages, regulatory actions or investigations, liabilities, costs and expenses (including reasonable attorneys' fees and expenses), fines, penalties, judgments, and costs (including but not limited to the costs of providing appropriate notice to all parties and credit monitoring, credit rehabilitation, or other credit support services to individuals with information impacted by the actual or suspected breech, to the extent procured by the User Institution (collectively, "Losses") to the extent that Losses: (i) arise out of a breach of the User Institution's obligations hereunder, (ii) arise out of the User Institution's use, handling or storage of these Personal Data in a manner not permitted by this Arrangement, or (iii) relate to User Institution's gross negligence or intentional acts under this Arrangement.

11.2. STANFORD WILL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES OF THE OTHER ARISING OUT OF OR IN CONNECTION TO ANY PERFORMANCE OF THIS ARRANGEMENT OR IN FURTHERANCE OF THE PROVISIONS OR

OBJECTIVES OF THIS ARRANGEMENT, REGARDLESS OF WHETHER SUCH DAMAGES ARE BASED ON TORT, WARRANTY, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11.3. In the event of a dispute arising out of or relating to this Arrangement, the Parties shall first attempt in good faith to resolve such dispute by negotiation and consultation between themselves. Either Party may, by written notice to the other party, refer the dispute to the other Party for attempted resolution by formal good faith negotiation within thirty (30) days after such notice is received. If the dispute remains unresolved after the good faith negotiation period provided in the previous sentence, either Party by written notice to the other Party may have such issue referred for resolution to the Parties' respective executive officers or senior legal counsel. The executive officers or senior legal counsel shall meet promptly to discuss the matter submitted and to determine a resolution. If the executive officers or senior legal counsel fail to resolve the dispute within thirty (30) days after it is referred to them, each Party shall have the right to pursue any other remedies legally available to resolve the dispute and the matter may be brought by a Party as a suit in a court of competent jurisdiction in accordance with Section 22 of the Agreement.

ATTACHMENT A
STANDARD CONTRACTUAL CLAUSES

Commission Decision C (2004)5721

INTER-COMPANY DATA TRANSFER AGREEMENT
(CONTROLLER TO CONTROLLER – SET II)

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

Between

……. (name)

……. (address and country of establishment)

(hereinafter, each the "Data Exporter" and collectively, the "Data Exporters")

And

……. (name)

……. (address and country of establishment)

hereinafter "data importer" each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

b) "the data exporter" shall mean the controller who transfers the personal data;

c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data

processor shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

   i. the data protection laws of the country in which the data exporter is established, or

   ii. the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

   iii. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: ……

Initials of data importer: ……

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

   i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

   ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

   iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

   iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each

other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated:

Signed for and on behalf of the data exporter/Controller:	**Signed for and on behalf of the data importer/Controller:**
……	……
Signatory Name (written out in full)	Signatory Name (written out in full)
……	……
Position	Position
……	……
Address	Address
……	……
Signature	Signature

ANNEX A
DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   (a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   (ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   (b) where otherwise provided by the law of the data exporter.

ANNEX B
DESCRIPTION OF THE TRANSFER

Data subjects
The personal data transferred concern the following categories of data subjects:
……
……
……

Purposes of the transfer(s)
The transfer is made for the following purposes:
……
……
……

Categories of data
The personal data transferred concern the following categories of data:
……
……
……

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients:
……
……
……

Sensitive data (if appropriate)
The personal data transferred concern the following categories of sensitive data:
……
……
……

Data protection registration information of data exporter (where applicable)
……
……
……

Additional useful information (storage limits and other relevant information)
……
……
……

Contact points for data protection enquiries

Data importer/Controller
……

Data exporter/Controller
……