Exhibit E: Data Processing Agreement pursuant to Art. 28 GDPR (or a corresponding provision pursuant to national laws)

Data Processing Agreement (DPA)

Between the Customer (Controller as defined by the GDPR/national laws, hereinafter referred to as "the Customer") and Alphacruncher (Processor as defined by the GDPR/national laws)

1. Subject of this DPA

The Processor processes Personal Data within the meaning of Article 4 (1) GDPR/national law on behalf of the Customer according to Article 5 GDPR/national law. This includes activities specified in the Service Agreement, entered on Effective Date between the Parties (hereinafter referred to as the "Service Agreement") and specified in the terms of reference contained therein.

In particular, the following data are part of the data processing:

Type of data	Purpose of data processing	Circle of the affected data subjects
Customer Data	Storing of Data.	Any data or data files of any type that are uploaded by or on behalf of Customer to the Services for storage in a data repository.

2. Definitions

2.1 Pursuant to Article 4 (7) GDPR/national law, the Controller is that party which, on its own or together with other controllers, decides on the purposes and means of processing Personal Data.

2.2 According to Article 4 (8) GDPR/national law, the Processor is a natural or legal person, public authority, institution or other body that processes Personal Data on behalf of the Controller.

2.3 Personal Data, pursuant to Article 4 (1) GDPR/national law, is any information relating to an identified or identifiable natural person (hereinafter referred to as "Data Subject"). A natural person is considered to be identifiable if they can be directly or indirectly identified, in particular by means of an identifier such as a name, an identification number, location data, an online identifier or one or more special

characteristics expressing the physical, physiological, genetic, mental, economic, cultural or social identity of this natural person.

2.4 Processing, pursuant to Article 4 (2) GDPR/national law, means any operation or set of operations which 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 or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.5 A Supervisory Authority, within the meaning of Article 4 (21) GDPR/national law, is an independent public authority established by any one of the Member States, in accordance with Article 51 GDPR/national law.

3. Responsibility

3.1 The Customer is responsible for the data processing within the framework of this DPA as "Controller" within the meaning of Article 4 No. 7 GDPR/national law. The Processor is responsible for complying with the relevant data protection laws.

3.2 The Customer and the Processor ensure that the persons authorized to process the Personal Data have committed themselves to confidentiality or are subject to an appropriate statutory confidentiality obligation. For this purpose, all persons receiving access to Customer's Personal Data at the Processor for handling of the DPA must be obligated to maintain data confidentiality and be informed about their data protection obligations. Each Party is responsible for the obligation of its own personnel. Furthermore, the personal deployed by the Processor must be informed that the data confidentiality obligation shall continue even after the activity has been completed.

4. Duration of the Agreement

4.1 The DPA becomes effective upon signing. The term corresponds to the Term of the Service Agreement.

4.2 The Parties are always aware that no (further) data processing may be carried out without the existence of a valid data processing agreement, for example, when the present DPA has expired.

4.3 The right to terminate without notice for good cause remains unaffected.

4.4 Terminations must be in writing (E-Mail is sufficient) to be effective.

5. Authority of the Customer

5.1 The data shall exclusively be handled within the framework of the agreements made and the Processor will only process the data according to documented instructions of the Customer. This obligation excludes circumstances under which the Processor has to process the data based on mandatory legal provisions by Union or Member State law or applicable national law. In such situations, the Processor shall, as far as

possible, inform the Customer about the corresponding legal requirements prior to commencement of processing. In case the Processor is not permitted to inform the Customer on such processing, he will try to obtain a waiver from this obligation. The Customer reserves the right to give instructions regarding the type, scope and procedure of the data processing within the context of this DPA, and may specify these instruction further on by issuing individual instructions.

5.2 The instructions of the Customer are documented by the Processor and made available to the Customer as a signed copy immediately after the documentation has been completed.

6. Place of Performance

6.1 The Processor shall provide the contractual services in the European Union (EU) or in the European Economic Area (EEA). Any transfer to a third country requires the prior approval by the Customer and may only take place if the Processors ensures that the specific requirements of Art. 44 subsequent GDPR/national law and regulatory requirements are met.

6.2 If the change of service location and cross-border data transfer is permissible under this DPA (especially with 6.1 DPA) and the GDPR and/or the Swiss Federal Act on Data Protection of 25 September 2020 (FADP), as applicable, the Processor shall guarantee compliance with and implementation of all legal requirements to ensure an adequate level of data protection for such transfers. This includes, without limitation, ensuring that any transfer of Personal Data from the European Economic Area, the United Kingdom, or Switzerland to a country not recognized as providing an adequate level of data protection under the GDPR or the FADP, as applicable, is conducted pursuant to a valid data transfer mechanism, such as the Standard Contractual Clauses as adapted for Switzerland where required, Binding Corporate Rules, or a recognized adequacy framework like the Swiss-U.S. Data Privacy Framework.

7. Obligations of the Processor

7.1 The Processor may only collect, process or use data within the scope of this agreement and according to the instructions of the Customer.

7.2 The Processor shall design the in-house organization in his area of responsibility in such a way that it meets the special requirements of data protection. The Processor shall take technical and organizational measures to especially adequately safeguard the Customer's data against misuse and loss that meet the requirements of the relevant data protection regulations. Upon request, the Processor must show proof of these measures to the Customer and, if necessary, to the Supervisory Authority. This proof particularly includes the implementation of the measures resulting from Article 32 GDPR/national law. The technical and organizational measures of the Processor will at least ensure the measures listed in Art. 32 (1) GDPR.

7.3 The technical and organizational measures are subject to technical progress and further development. In that regard, the Processor is permitted to implement

alternative, demonstrably adequate measures and the Processor is obliged to do so in case security assessments show that changes are necessary to retain the level of protection. It must be ensured that the contractually agreed level of protection is met. Significant changes must be documented. A description of these technical and organizational measures is given in **Appendix 1** to this DPA.

7.4 The Processor himself maintains a record of processing activities within the meaning of Article 30 GDPR/national law. On request, the Processor shall provide the Customer with the information required for the overview pursuant to Article 30 GDPR/national law. Furthermore, the Processor shall make the record available to the supervisory authority upon request.

7.5 The Processor shall assist the Customer with any necessary data protection impact assessment by providing all information available to him. In the event prior consultation of the competent authority is required, the Processor shall also support the Customer in this respect.

7.6 If required by applicable law the Processor shall appoint a data protection officer. If the data protection officer changes, the Customer must be informed immediately in writing. The Processor guarantees that the requirements with regard to the data protection officer and the data protection officer's activities are fulfilled in accordance with Article 38 GDPR/national law. If the Processor does not have an appointed data protection officer, the Processor shall appoint a contact person for the Customer.

7.7 The Processor shall inform the Customer immediately in case of violations of regulations regarding the protection of the Customer's Personal Data or the stipulations made in the DPA committed by the Processor or the persons employed by the Processor within the scope of this Agreement. The Processor shall take the necessary measures to safeguard the data and to mitigate possible adverse consequences for the persons concerned and shall immediately discuss them with the Customer. The Processor assists the Customer in fulfilling the Customer's duty to inform the relevant Supervisory Authority or the Data Subject about any infringement of the protection of Personal Data pursuant to Article 33, 34 GDPR.

7.8 Insofar as a Data Subject should contact the Processor directly for the purpose of exercising their rights according to Chapter III of the GDPR or the relevant provisions of the FADP (including, but not limited to, Articles 25-32 FADP), the Processor shall immediately forward this request to the Customer. The Processor assists the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR and the FADP, as applicable.

7.9 Transferred data carriers as well as all copies or reproductions made thereof remain the property of the Customer. The Processor must keep these safe so that they are not accessible to third parties. The Processor is obliged to provide the Customer with

information at any time as far as the Customer's data and documents are concerned.

7.10 If the Customer is obligated by data protection laws to give information to a Data Subject concerning the collection, processing or use of data on that person, the Processor shall assist the Customer in providing this information, provided the Customer has requested the Processor to do so in writing.

7.11 The Processor shall inform the Customer immediately about any controls and measures taken by the supervisory authorities or if a supervisory authority investigates the Processor.

7.12 The Processor shall inform the Customer immediately if, in the Processor's opinion, an instruction issued by the Customer violates statutory provisions. The Processor is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the Customer.

7.13 If the data of the Customer are endangered by assignment or seizure, a bankruptcy or settlement procedure, or by other events or measures of third parties, the Processor shall inform the Customer immediately. The Processor shall immediately inform all those responsible in this context that the sovereignty and the ownership of the data are exclusively with the Customer as Controller as defined by the GDPR/national law.

7.14 The Processor shall not use the data provided for any purpose other than the performance of the DPA and shall not use any means of processing that have not been previously approved by the Customer.

7.15 The Processor shall not store data that is subject to special secrecy on systems that are beyond the control of the Customer or that are not subject to seizure protection.

7.16 If the Processor is required by law of the Union or Member States to process the data in other ways, the Processor shall inform the Customer of these legal requirements prior to processing.

7.17 The fulfillment of the aforementioned obligations shall be verified by the Processor, as well as documented and proven to the Customer in a suitable manner upon request.

7.18 The Processor assists the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor.

8. Obligations of the Customer

8.1 The Customer is within his area of responsibility responsible for the assessment of the admissibility of the data processing and for the protection of the rights of the persons concerned. The Customer shall ensure within his area of responsibility that the legally required conditions (such as by obtaining consent for the processing of the data) are maintained so that the Processor can provide the agreed services without violating the law.

8.2 The Customer is within his area of responsibility responsible for a with applicable data protection law compliant processing of Personal Data while using the services of

Alphacruncher.

8.3 The Customer is responsible for the information obligations resulting from Article 33, 34 GDPR/national law to the supervisory authority or those affected by an infringement of the protection of Personal Data.

8.4 The Customer shall stipulate the procedure for the return of provided data media and/or deletion of the stored data after completion of the order by contract or by instruction.

9. Inspection Rights of the Customer

9.1 The Customer has the right to inspect the compliance with the provisions laid down in this agreement as well the technical and organizational measures specified in **Appendix 1** or have them inspected by a commissioned inspector.

For this purpose, the Customer may for instance:

- consider privacy-related certifications or privacy seals and marks,
- obtain self-disclosure in writing from the Processor,
- receive an attestation by an expert,
- have a competent third Party, who is not a competitor of the Processor, verify compliance with regulations after timely registration - except in emergency cases, e. g. a data breach - during normal business hours without disturbing business operations or,
- verify compliance with regulations after timely registration (except in emergency cases, e. g. a data breach) during normal business hours without disturbing business operations.

9.2 If, in the context of this agreement the Processor or the Processor's employees have breached the provisions for the protection of the Customer's Personal Data or the stipulations made in this agreement, an appropriate inspection can also be conducted without timely registration. A disruption of the operations of the Processor should be avoided as much as possible.

9.3 The execution of the order verification by means of regular inspections with regard to the execution or fulfillment of this agreement, in particular compliance and possibly necessary adaptation of regulations and measures for the execution of the order shall be supported by the Processor. In particular, the Processor undertakes to provide the Customer, upon written request, with all information necessary to carry out an inspection within a reasonable period of time.

10. Correction and Limitation on Processing, Deletion and Return of Data Media

10.1 During the current commissioning, the Processor corrects, deletes or blocks the contractual data only based on instructions from the Customer.

10.2 If destruction of data carriers and other materials is to be carried out during the ongoing commissioning, the Processor shall carry out such destruction in a manner demonstrably compliant with the data protection regulations and based solely on the

respective individual instruction by the Customer. This does not apply if a corresponding provision has already been made in the Service Agreement.

10.3 In certain cases which are explicitly defined by the Customer storage or handover to the Customer shall be carried out.

10.4 Upon completion of the provision of processing services, the Processor shall, at the discretion of the Customer, either securely and permanently delete or return all Personal Data to the Customer. This obligation shall not apply to the extent the Processor is subject to a statutory obligation to store the Personal Data under applicable Swiss law. The Processor shall inform the Customer of any such legal storage obligations, where legally permitted. These obligations to return or delete data shall also apply to all information containing business or trade secrets of the Customer. Proof of deletion shall be provided to the Customer upon request.

10.5 Documentation serving as proof of orderly and proper data processing must be kept by the Processor according to the respective retention periods beyond the expiration of the DPA. The Processor can hand them over to the Customer for his relief at the end of this agreement.

10.6 The Customer may at any time, i.e. during the term of the agreement as well as after the termination of the agreement, request the correction, deletion, processing restriction (blocking), and publication of data by the Processor as long as the Processor has the ability to comply with this request.

10.7 The Processor shall correct, delete or block the contractual data if instructed by the Customer. The Processor is responsible for the destruction of data media and other materials in accordance with data protection based on a specific order by the Customer, unless otherwise agreed in individual cases. In special cases to be determined by the Customer, the data shall be stored or transferred. Insofar as a Data Subject should contact the Processor directly for the purpose of rectification or deletion of their data, the Processor shall immediately forward this request to the Customer.

10.8 Should the Customer not be able to take back the data, the Customer shall inform the Processor in writing in good time. The Processor is then entitled to delete Personal Data on behalf of the Customer.

11. Subcontractors

11.1 The Processor is only entitled to engage sub-contractors with the explicit prior consent of the Customer. The Customer gives its explicit consent to the engagement of the following Subcontractors:

Infrastructure			
Service provider	**Data collected or shared**	**Purpose**	**Place of processing**
Amazon Web Services, Inc. (Privacy policy)	Contact details Data from your contracts Data that identifies you	This is a web hosting provider: we use it to store contracts and other data you generate by using the service securely in the cloud.	EU
Microsoft Corporation (Privacy policy)	Data that identifies you	Microsoft Azure Services	EU
Analytics			
Google Analytics (Privacy policy)	Contact details Data on how you use Covered Services Data that identifies you Cookies	This is a web analytics service: we use it to track your use of the Covered Services, and prepare reports on user activity.	US
Integrations (by your request)			
Auth0, Inc. (Privacy policy)	Data that identifies you Data on how you use Covered Services Contact details Cookies	This enables users to authenticate.	US
SWITCH (Privacy policy)	Data that identifies you Data on how you use Covered Services Contact details Cookies	This enables users to authenticate via their university login.	CH

eudGAIN interfederation service[1] ([Privacy policy])	Data that identifies you Data on how you use Covered Services Contact details Cookies	This enables users to authenticate via their university login.	EU
Comms			
HubSpot Germany GmbH ([Privacy policy])	Contact details	We use this service for sending, storing and tracking emails.	EU and US
Payments			
Stripe, Inc. ([Privacy policy])	Contact details Financial information Cookies	This service processes payments for us.	EU and US

11.2 If the Customer wishes to use an Alphacruncher application that requires the processing of Personal Data in the US or another third country, the customer will be informed of the processing location before the processing of the Personal Data begins.

11.3 Notwithstanding the obligation in Sec. 11.1 the Processor must engage any Subcontractors in accordance with the provisions of this DPA and thereby ensure that the Customer is also able to exercise his rights under this agreement (in particular his inspection and verification rights) directly with the Subcontractors. The Processor shall provide proof to the Customer on request concerning the conclusion of the aforementioned agreements with his Subcontractors.

11.4 The contractor is authorized, within the scope of its contractual obligations, to establish further Subcontractor relationships. Before establishing additional Subcontractor relationships, the contractor informs the Customer in written form with a notice period of six weeks. The Customer can only object to the change for significant reasons. The objection must be made within 14 calendar days and explicitly state all significant reasons. A significant reason on the part of the Costumer exists, in particular, if the Subcontractor is not based in a country that is a member of the EU/EEA or for which the Commission has issued an adequacy decision pursuant

[1] Customer personal data will be protected according to the GÉANT Data Protection Code of Conduct for Service Providers, a common standard for the research and higher education sector to protect privacy.

to Article 45 GDPR , or which is included in the list of countries ensuring an adequate level of data protection published by the Swiss Federal Council under the FADP.

12. Liability

The provisions set forth in the Service Agreement shall apply.

13. Final Provisions

13.1 In the event of any controversy or inconsistency between the Service Agreement and this DPA this DPA shall prevail.

13.2 The objection of the right of retention is excluded with regards to data processed for the Customer and the associated data carriers.

13.3 The written form is required for ancillary agreements.

13.4 Should individual parts of this agreement be ineffective, this does not affect the validity of the Agreement.

13.5 The processing of Personal Data shall be governed by FADP/national law and, where applicable, additionally by GDPR. The place of jurisdiction is as specified in the Service Agreement.

Appendix 1

Implementation of technical and organizational measures

1. Confidentiality (Article 32 (1) GDPR/national law)

1.1 Entry Control

No unauthorized access to data processing systems.

1.1.1 Do you have an access control system with magnetic or chip cards? - Yes.

1.1.2 Is the allocation of keys in your company regulated? - Yes.

1.1.3 Do you have an access control system with magnetic or chip cards? - Yes.

1.1.4 Do you have a gatekeeper or factory security? - Yes.

1.1.5 Are alarm and video systems used? – Yes.

1.2 Access Control

No unauthorized system usage.

1.2.1 Do you have requirements for the passwords e.g. security, length, special characters, regular change? – Yes.

1.2.2 Does your company use two-factor authentication, e.g. hardware token + password/PIN? – Yes.

1.2.3 Do you use automatic blocking mechanisms such as screen savers? – Yes.

1.2.4 Are all accessible storage media containing personal data encrypted? – Yes.

1.3 Access Control

No unauthorized reading, copying, modification or removal within the system.

1.3.1 Is there an authorization concept in your company established with differentiated profiles, roles, transactions and objects? – Yes.

1.3.2 If the need-to-know principle (need-based) is adhered to in the allocation of access rights? – Yes.

1.3.3 Can the access rights be evaluated? – No.

1.3.4 Are the individual accesses logged, be it knowledge, modification or deletion? – Yes.

1.4 Separation Control

Separate processing of data collected for different purposes.

1.4.1 Are Personal Data collected for different purposes also processed separately? – Yes.

1.4.2 Is your authorization system multi-client capable? – Yes.

1.4.3 Do you have a test and production system, e.g. sandboxing? – Yes.

1.5 Pseudonymization (Article 32 (1) GDPR, Article 25 (1) GDPR/ national law)

1.5.1 Processing of Personal Data in such a way that the data can no longer be assigned to a specific Data Subject without the need for additional information, provided that such additional information is kept separate and subject to appropriate technical and

organizational measures;

2. Integrity (Article 32 (1) GDPR/ national law)

2.1 Relay Control

No unauthorized reading, copying, modification or removal during electronic transmission or transport.

2.1.1 Is every electronic data transmission of Personal Data encrypted? – No.

2.2 Entry Control

Determining whether and by whom Personal Data has been entered, altered or removed in data processing systems.

2.2.1 Are all data entries, changes and deletions logged and evaluated? – Yes.

2.2.2 Do you have an administrator log? – Yes.

2.2.3 Are document management systems used? – Yes.

3. Availability and Capacity (Article 32 (1) GDPR/ national law)

3.1 Availability Control

3.1.1 Protection against accidental or willful destruction or loss.

3.1.2 Do you have a backup strategy (online/offline; on-site/off-site)? – Yes.

3.1.3 Does your company have an uninterruptible power supply (UPS)? – Yes.

3.1.4 Do you use virus protection and firewalls? – Yes.

3.1.5 Are an emergency plan and corresponding reporting channels in place? – No.

3.1.6 Is rapid recoverability (Article 32 (1) (c) GDPR/national law) ensured? – Yes.

4. Procedure for Periodic Review, Assessment and Evaluation (Article 32 (1) of the GDPR/ national law, Article 25 (1) of the GDPR/ national law)

4.1 Order control

No order processing within the meaning of Article 28 GDPR without corresponding instructions from the Customer.

4.1.1 Is a formalized order management system used? – Yes.

4.2 Data privacy management

4.2.1 Is accountability (proof that the legal requirements for data protection are met) met? – Yes.

4.2.2 Is the timeliness and effectiveness of the measures, taking into account the state of the art, ensured by a data protection management system? – Yes.

4.3 Incident response management

4.3.1 Are technical and organizational measures/processes in place to ensure that actual or suspected security incidents (e.g. attacks on the IT infrastructure, malfunctions,

vulnerabilities) can be detected and eliminated? – Yes.

4.4 Privacy-friendly default settings (Article 25 (2) GDPR/ national law)

4.4.1 Are suitable technical and organizational measures taken to ensure that, in terms of quantity, scope, storage period and accessibility, processing is only carried out for the respective specific processing purpose through default settings? – Yes.

5. Data Storage

The Processor ensures that the hosting of the Customer Data will be separated from the Usage Data.