EU GDPR DATA PROCESSING ADDENDUM INSTRUCTIONS

WHO SHOULD EXECUTE THIS DPA?

If you have determined that you qualify as a data controller under the GDPR, and need a data processing addendum (DPA) in place with vendors that process personal data on your behalf, we want to help make things easy for you.

Our GDPR compliant DPA is attached and ready for your signature in accordance with the instructions below.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Annexes 1, and 2 (including Appendices 1 to 5).

2. This DPA has been pre-signed on behalf of Gnosis Data Analysis PC (doing business as JADBio, hereinafter – JADBio). In addition, the Standard Contractual Clauses in Annex 2 (including Appendices 1 to 5) have been pre-signed by JADBio as the data importer.

3. To complete this DPA, Customer must complete the information in the signature boxes and **sign on Pages 7, 19, 21 and 24.**

4. Send the completed and signed DPA to JADBio by email, indicating the Customer's Legal Name (as set out on the applicable JADBio Agreement or invoice, if applicable), to **dpo@jadbio.com**.

Upon receipt of the validly completed DPA by JADBio at this email address, this DPA will become legally binding.

EU GDPR

DATA PROCESSING ADDENDUM

(*Version October 2021*)

This Data Processing Addendum **("DPA")**, forms part of the JADBio Terms and Conditions (available at https://jadbio.com/terms-and-conditions/), or other written or electronic agreement, by and between Gnosis Data Analysis PC ("**JADBio**") and the undersigned customer of JADBio ("**Customer**") for certain security services (collectively, the "**Service**") provided by JADBio (the "**Main Agreement**"). All capitalized terms not defined herein shall have the meanings set forth in the Main Agreement. Each of Customer and JADBio may be referred to herein as a "**party**" and together as the "**parties**."

In connection with the Service, the parties anticipate that JADBio may process outside of the European Economic Area ("**EEA**") and United Kingdom, and Switzerland, certain Personal Data in respect of which the Customer or any Affiliate of Customer may be a data controller or data processor, as applicable, under applicable EU Data Protection Laws.

The parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by EU Data Protection Laws.

HOW TO EXECUTE THIS DPA:

1. This DPA consists of two parts: the main body of the DPA, and Annexes 1, and 2 (including Appendices 1 to 5).

2. This DPA has been pre-signed on behalf of Gnosis Data Analysis PC (doing business as JADBio, hereinafter – JADBio). In addition, the Standard Contractual Clauses in Annex 2 (including Appendices 1 to 5) have been pre-signed by JADBio as the data importer.

3. To complete this DPA, Customer must complete the information in the signature boxes and sign on Pages 7, 19, 21 and 24.

4. Send the completed and signed DPA to JADBio by email, indicating the Customer's Legal Name (as set out on the applicable JADBio Order Form or invoice, if applicable), to **dpo@jadbio.com**.

Upon receipt of the validly completed DPA by JADBio at this email address, this DPA will become legally binding.

HOW THIS DPA APPLIES

This DPA is an addendum to and forms part of the Main Agreement. The Customer entity signing this DPA must be the same as the Customer entity party to the Main Agreement.

If the Customer entity signing this DPA is not a party to the Main Agreement directly with JADBio, but is instead a customer indirectly via an authorized reseller of JADBio services, this DPA is not valid and is not legally binding. Such an entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

DATA PROCESSING TERMS

In the course of providing the Service to Customer pursuant to the Main Agreement, JADBio may Process Personal Data on behalf of Customer. JADBio agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to JADBio or collected and processed by or for Customer using JADBio's Services.

The parties agree that the obligations under this DPA that are specific to the GDPR shall not apply until the GDPR has come into full force and effect.

1. Definitions

1.1 The following definitions are used in this DPA:

a. "**Adequate Country**" means a country or territory that is recognized under General Data Protection Regulation (EU) 2016/679 as providing adequate protection for Personal Data;

b. "**Affiliate**" means, with respect to a party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists);

c. "**EU Data Protection Laws**" means all laws and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom, and Switzerland, applicable to the processing of Personal Data under the Main Agreement, including (where applicable) the General Data Protection Regulation (Regulation (EU) 2016/679;

d. "**GDPR**" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 25 May 2018 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data);

e. "**Personal Data**" means all data which is defined as '*personal data'* under General Data Protection Regulation (EU) 2016/679 and to which General Data Protection Regulation (EU) 2016/679 apply and which is provided by the Customer to JADBio, and accessed, stored or otherwise processed by JADBio as a data processor as part of its provision of the Service to Customer;

f. "**Verified Technical Resource**" means a category, in accordance with Article 13(1)(e) of the GDPR, of technical contractors verified by JADBio to be able to technically adhere to the security provisions of this DPA and the GDPR, have entered an agreement with JADBio at least as restrictive as this DPA; and may provide services to JADBio when requested.

g. "**processing**", "**data controller**", "**data subject**", "**supervisory authority**" and "**data processor**" shall have the meanings ascribed to them in General Data Protection Regulation (EU) 2016/679.

1.2 An entity "**Controls**" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

2. Status of the parties

2.1 The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Annex 1.

2.2 Each party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with General Data Protection Regulation (EU) 2016/679. As between the parties, the Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data.

2.3 In respect of the parties' rights and obligations under this DPA regarding the Personal Data, the parties hereby acknowledge and agree that the Customer is the data controller or processor, and JADBio is the data processor or sub-processor, as applicable, and accordingly JADBio agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA. The Customer agrees that, regarding the Personal Data received from JADBio, the Customer is the data processor and JADBio the data controller and the Customer agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA and that it has all the obligations described in article 3 below.

2.4 If Customer is a data processor, Customer warrants to JADBio that Customer's instructions and actions with respect to the Personal Data, including its appointment of JADBio as another processor and concluding the standard contractual clauses (Annex 2), have been authorized by the relevant controller.

2.5 Where and to the extent that JADBio processes data which is defined as 'personal data' under EU Data Protection Laws as a data controller as set out in the JADBio Privacy Policy available at https://jadbio.com/privacy-policy/, JADBio will comply with applicable General Data Protection Regulation (EU) 2016/679 in respect of that processing

2.6 Each party shall appoint a Data Privacy Officer within its organization authorized to respond from time to time to enquiries regarding Personal Data, the parties shall make the Data Privacy Officer known to the other party, and the Data Privacy Officer shall deal with such enquiries promptly.

3. JADBio obligations

3.1 With respect to all Personal Data, JADBio warrants that it shall:

(a) only process Personal Data in order to provide the Service, and shall act only in accordance with: (i) this DPA, (ii) the Customer's written instructions as set forth in the Main Agreement and this DPA, and (iii) as required by applicable laws;

(b) upon becoming aware, inform the Customer if, in JADBio's opinion, any instructions provided by the Customer under clause 3.1(a) are in conflict with the GDPR;

(c) implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Annex 3;

(d) take reasonable steps to ensure that only authorized personnel have access to such Personal Data and that any persons whom it authorizes to have access to the Personal Data are under obligations of confidentiality;

(e) without undue delay after becoming aware, notify the Customer of any 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 by JADBio, its sub-processors, or any other identified or unidentified third party (a "**Security Breach**");

(f) promptly provide the Customer with reasonable cooperation and assistance in respect of a Security Breach and all reasonable information in JADBio's possession concerning such Security Breach insofar as it affects the Customer, including, to the extent then known, the following:

(i) the possible cause and consequences for the Data Subjects of the Security Breach;

(ii) the categories of Personal Data involved;

(iii) a summary of the possible consequences for the relevant data subjects;

(iv) a summary of the unauthorized recipients of the Personal Data; and

(v) the measures taken by JADBio to mitigate any damage;

(g) not make any public announcement about a Security Breach (a "**Breach Notice**") without the prior written consent of the Customer, unless required by applicable law;

(h) promptly notify the Customer if it receives a request from a data subject of Customer to access, rectify or erase that individual's Personal Data, or if a data subject objects to the processing of, or makes a data portability request in respect of, such Personal Data (each a "**Data Subject Request**"). JADBio shall not respond to a Data Subject Request without the Customer's prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees. To the extent that the Customer does not have the ability to address a Data Subject Request, then upon Customer's request JADBio shall provide

reasonable assistance to the Customer to facilitate such Data Subject Request to the extent able and in line with applicable law. To the extent the Customer does not respond, JADBio may respond to the Data Subject Request in any manner it deems appropriate. Customer shall cover all costs incurred by JADBio in connection with its provision of such assistance or response;

(i) other than to the extent required to comply with applicable law, following termination or expiry of the Main Agreement or completion of the Service, JADBio will delete all Personal Data (including copies thereof) processed pursuant to this DPA, according to its retention policy;

(j) taking into account the nature of processing and the information available to JADBio, provide such assistance to the Customer as the Customer reasonably requests in relation to JADBio's obligations under General Data Protection Regulation (EU) 2016/679 with respect to:

(i) data protection impact assessments (as such term is defined in the GDPR);

(ii) notifications to the supervisory authority under General Data Protection Regulation (EU) 2016/679 and/or communications to data subjects by the Customer in response to any Security Breach; and

(iii) the Customer's compliance with its obligations under the GDPR with respect to the security of processing;

provided that the Customer shall cover all costs incurred by JADBio in connection with its provision of such assistance.

4. Sub-processing

4.1 The Customer grants a general authorization: (a) to JADBio to appoint any Affiliate as sub-processors, and (b) to JADBio and any Affiliate to appoint any Verified Technical Resource to act as third party data center operators, and outsourced marketing, business, engineering and customer support providers as sub-processors to support the performance of the Service.

4.2 JADBio will only use a Verified Technical Resource as sub-processors of any Personal Data. If JADBio is reasonably able to provide the Service to the Customer in accordance with the Main Agreement without using the sub-processor and decides in its discretion to do so, then the Customer will have no further rights under this clause 4.2 in respect of the proposed use of the sub-processor. If JADBio requires use of a sub-processor at its discretion and Customer does not want JADBio to use a Verified Technical Resource as a sub-processor, Customer may provide written notification of any objections to JADBio. Within ninety (90) days from the Customer's notification of objections, the Customer may within thirty (30) days following the end of the ninety (90) day period referred to above, terminate the applicable Order Form without refund. If the Customer does not provide a timely objection to the use of a Verified Technical Resource in accordance with this clause 4.2, the Customer will be deemed to have consented to the use of any Verified Technical Resource as a sub-processor and waived its right to object. JADBio may use a new or replacement Verified Technical Resource as a sub-processor whilst the objection procedure in this clause 4.2 is in process.

4.3 JADBio will ensure that any sub-processor it engages to provide an aspect of the Service on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Personal Data than those imposed on JADBio in this DPA (the "**Relevant Terms**"). JADBio shall procure the performance by such sub-processor of the Relevant Terms and shall be liable to the Customer for any breach by such person of any of the Relevant Terms.

5. Audit and records

5.1 JADBio shall, in accordance with General Data Protection Regulation (EU) 2016/679, make available to the Customer such information in JADBio's possession or control as the Customer may reasonably request with a view to demonstrating JADBio's compliance with the obligations of data processors under General Data Protection Regulation (EU) 2016/679 in relation to its processing of Personal Data.

5.2 The Customer may exercise its right of audit under General Data Protection Regulation (EU) 2016/679 in relation to Personal Data, through JADBio providing:

(a) an audit report not older than **eighteen (18) months**, prepared by an independent external auditor demonstrating that JADBio's technical and organizational measures are sufficient and in accordance with an accepted industry audit standard;

b) additional information in JADBio's possession or control to an EU supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by JADBio under this DPA; and

c) Customer shall cover all costs incurred by JADBio in connection with any such audit.

6. Data transfers

6.1 To the extent any processing of Personal Data by JADBio takes place in any country outside the EEA (except if in an Adequate Country), the parties agree that the standard contractual clauses approved by the EU authorities under General Data Protection Regulation (EU) 2016/679 and set out in Annex 2 will apply in respect of that processing, and JADBio will comply with the obligations of the 'data importer' in the standard contractual clauses and the Customer will comply with the obligations of the 'data exporter'.

6.2 The Customer acknowledges and accepts that the provision of the Service under the Main Agreement may require the processing of Personal Data by sub-processors in countries outside the EEA.

6.3 If, in the performance of this DPA, JADBio transfers any Personal Data to a Verified Technical Sub-processor located outside of the EEA (without prejudice to clause 4), JADBio shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:

(a) the requirement for JADBio to execute or procure that the Verified Technical Sub-processor execute to the benefit of the Customer standard contractual clauses approved by the EU authorities under General Data Protection Regulation (EU) 2016/679 and set out in Annex 2;

(b) the requirement for the Verified Technical Sub-processor to be certified under the EU-U.S. Privacy Shield Framework; or

(c) the existence of any other specifically approved safeguard for data transfers (as recognized under General Data Protection Regulation (EU) 2016/679) and/or a European Commission finding of adequacy.

6.4 The following terms shall apply to the standard contractual clauses set out in Annex 2:

(a) The Customer may exercise its right of audit under clause 5.1(f) of the standard contractual clauses as set out in, and subject to the requirements of, clause 5.2 of this DPA; and

(b) JADBio may appoint Verified Technical Sub-processors as set out, and subject to the requirements of, clauses 4 and 6.3 of this DPA.

7. General

7.1 This DPA is without prejudice to the rights and obligations of the parties under the Main Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Main Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

7.2 JADBio's liability under or in connection with this DPA (including under the standard contractual clauses set out in Annex 3) is subject to the limitations on liability contained in the Main Agreement.

7.3 This DPA does not confer any third-party beneficiary rights, it is intended for the benefit of the parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

7.4 This DPA and any action related thereto shall be governed by and construed in accordance with the laws of - Greece, without giving effect to any conflicts of laws principles. The parties consent to the personal jurisdiction of, and venue in, the courts of Greece.

7.5 This DPA is the final, complete and exclusive agreement of the parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorized signatory of each party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorized and has legal capacity to execute and deliver this DPA. Each party represents and warrants to the other that the execution and delivery of this DPA and the performance of such party's obligations hereunder, have been duly authorized and that this DPA is a valid and legally binding agreement on each such party, enforceable in accordance with its terms.

IN WITNESS WHEREOF, the parties have each caused this DPA to be signed and delivered by its duly authorized representative.

CUSTOMER: _____		**Gnosis Data Analysis PC**	
SIGNATURE		**SIGNATURE**	Ioannis Tsamardinos
NAME		**NAME**	Ioannis Tsamardinos
TITLE		**TITLE**	CEO
ADDRESS		**ADDRESS**	N.Plastira 100, Vasilika Vouton, 70013, Heraklion, Crete, Greece
DATE		**DATE**	Nov 19, 2021

Annex 1

Details of the Personal Data and processing activities

(a) The personal data comprises: in relation to our Customers and their customers sign-up information (name, email, organization, role, IP), payment information (name, address, city), encrypted sensitive data (genetic or biometric data).

(b) The duration of the processing will be: until the earliest of (i) expiry/termination of the Main Agreement, or (ii) the date upon which processing is no longer necessary for the purposes of either party performing its obligations under the Main Agreement (to the extent applicable);

(c) The processing will comprise: Processing necessary to provide the Service to Customer, pursuant to the Main Agreement ;

(d) The purpose(s) of the processing is/ are: necessary for the provision of the Service;

(e) Personal data may concern the following data subjects:

- Prospective customers, customers, resellers, referrers, business partners, and vendors of the Customer (who are natural persons);
- Employees or contact persons of the Customer's prospective customers, customers, resellers, referrers, sub-processors, business partners, and vendors (who are natural persons);
- Employees, agents, advisors, and freelancers of the Customer (who are natural persons); and/or
- Natural persons authorized by the Customer to use the Service.

(f) Special category of the personal data: genetic or biometric data for Customer`s own research purposes.
(g) Storage location: the gathered data of the data subjects is transferred and stored for the above-mentioned purposes at the Amazon Web Services` data centers located at: Ireland

Annex 2

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Appendix 1.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Appendix 1.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Appendix 1.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

12.1 (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Appendix 1.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Appendix 1.A.

(b) Once it has completed the Appendix and signed Appendix 1.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Appendix 1.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Appendix 1.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Appendix 2 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Appendix 1.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least

implement the technical and organizational measures specified in Appendix 2. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Appendix 1.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least sixty (60) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least sixty (60) days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller

with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body (11) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Appendix 1.C, shall act as competent supervisory authority.

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

which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Appendix 1.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Appendix 1.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third

country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under

the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Greece.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Greece.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

This agreement has been entered into on the date shown at the beginning of the first page of this agreement.

CUSTOMER (DATA EXPORTER): _____		**Gnosis Data Analysis PC (DATA IMPORTER)**	
SIGNATURE		**SIGNATURE**	Ioannis Tsamardinos
NAME		**NAME**	Ioannis Tsamardinos
TITLE		**TITLE**	CEO
ADDRESS		**ADDRESS**	N.Plastira 100, Vasilika Vouton, 70013, Heraklion, Crete, Greece
DATE		**DATE**	Nov 19, 2021

Appendix 1

to the Standard Contractual Clauses

A. **LIST OF PARTIES**

Data exporter(s): The data exporter is (please specify briefly your activities relevant to the transfer):

The (i) legal entity that has created an account with Gnosis Data Analysis PC ("**JADBio**") for provision of the Service, and executed the Clauses as a data exporter and, (ii) all affiliates of such entity established within the EEA, which have purchased services from JADBio or its Affiliates.

Data importer(s): The data importer is (please specify briefly activities relevant to the transfer):

JADBio, that processes Personal Data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and JADBio.

B. **DESCRIPTION OF TRANSFER**

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

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

The data exporter may submit Personal Data to Gnosis Data Analysis PC and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospective customers, customers, resellers, referrers, business partners, and vendors of the data exporter (who are natural persons);
- Employees or contact persons of the data exporter's prospective customers, customers, resellers, referrers, subcontractors, business partners, and vendors (who are natural persons);
- Employees, agents, advisors, and freelancers of the data exporter (who are natural persons); and/or
- Natural persons authorized by the data exporter to use the services provided by JADBio to the data exporter.

Categories of personal data transferred

The personal data transferred concern the following categories of data:

The data exporter may submit Personal Data to JADBio and its Affiliates, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to, the following categories of Personal Data:

- sign-up information (name, email, organization, role, IP), payment information (name, address, city), encrypted sensitive data (genetic or biometric data).

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

The personal data transferred concern the following special categories of data: Genetic or biometric data

The data exporter should not provide or submit any special categories of data to JADBio and its Affiliates.

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

The data is transferred on a continuous basis.

Nature of the processing

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

The objective of the processing of Personal Data by JADBio is to provide the Service, pursuant to the Main Agreement.

Purpose(s) of the data transfer and further processing

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

The objective of the processing of Personal Data by JADBio is to provide the Service, pursuant to the Main Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

C. **COMPETENT SUPERVISORY AUTHORITY**

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

The Hellenic Data Protection Authority is a competent supervisory authority.

CUSTOMER: _____		**Gnosis Data Analysis PC**	
SIGNATURE		**SIGNATURE**	Ioannis Tsamardinos
NAME		**NAME**	Ioannis Tsamardinos
TITLE		**TITLE**	CEO
ADDRESS		**ADDRESS**	N.Plastira 100, Vasilika Vouton, 70013, Heraklion, Crete, Greece
DATE		**DATE**	Nov 19, 2021

Appendix 2

to the Standard Contractual Clauses

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

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA:

Security Measures

A. Data importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards.

B. More specifically, data importer/sub-processor's security program shall include:

Access Control of Processing Areas

Data importer/sub-processor implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- establishing security areas;
- protection and restriction of access paths;
- establishing access authorizations for employees and third parties, including the respective documentation;
- all access to the data center where personal data are hosted is logged, monitored, and tracked; and
- the data center where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Data importer/sub-processor implements suitable measures to prevent their data processing systems from being used by unauthorized persons, including:

- use of adequate encryption technologies;
- identification of the terminal and/or the terminal user to the data importer/sub-processor and processing systems;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- all access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that personal data cannot be read, copied or modified or removed without authorization. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;

- monitoring capability in respect of individuals who delete, add or modify the personal data;
- release of data only to authorized persons, including allocation of differentiated access rights and roles;
- use of adequate encryption technologies; and
- control of files, controlled and documented destruction of data.

Availability Control

Data importer/sub-processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data importer/sub-processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- certain highly confidential employee data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system; and
- providing user alert upon incomplete transfer of data (end to end check); and
- as far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Data importer/sub-processor implements suitable input control measures, including:

- an authorization policy for the input, reading, alteration and deletion of data;
- authentication of the authorized personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilization of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time; and
- proof established within data importer/sub-processor’s organization of the input authorization; and
- electronic recording of entries.

Separation of Processing for different Purposes

Data importer/sub-processor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- modules within the data importer/sub-processor’s database separate which data is used for which purpose, i.e. by functionality and function;

- at the database level, data is stored in different normalized tables, separated per module, per Controller Customer or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data importer/sub-processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/sub-processor shall take reasonable steps to ensure that persons employed by it and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Appendix 2.

Monitoring

Data importer/sub-processor shall implement suitable measures to monitor access restrictions to data importer/sub-processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/sub-processor and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.

CUSTOMER: _____		**Gnosis Data Analysis PC**	
SIGNATURE		**SIGNATURE**	Ioannis Tsamardinos
NAME		**NAME**	Ioannis Tsamardinos
TITLE		**TITLE**	CEO
ADDRESS		**ADDRESS**	N.Plastira 100, Vasilika Vouton, 70013, Heraklion, Crete, Greece
DATE		**DATE**	Nov 19, 2021

Appendix 3

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

The processor uses the following sub-processors during the cooperation with the controller:

Third Party Sub-Processor	Purpose	Applicable Service	Data Center Sub-Processor Location
Amazon Web Services Inc., 410 Terry Avenue North, Seattle, WA 98109-5210, USA.	Infrastructure services	JADBio`s infrastructure is built on AWS resources.	Ireland

Appendix 4

Data exporter's instructions:

The Processor agrees to process the Personal Data in compliance with European and national legislation, its knowledge of which is confirmed by signing this deed. In particular, by this Agreement, Controller appoints JADBio to process the Personal Data of the Controller:

(i) solely in compliance with the applicable legislation;

(ii) solely in order to provide the Services and any related technical support;

(iii) solely if necessary for the proper satisfaction of the obligations accepted pursuant to the Terms and Conditions for the Service and, in all cases, in full compliance with the instructions given;

(iv) as documented in the Terms and Conditions, including this Agreement; and

(v) as further documented in any written instructions given by the Controller to JADBio as additional instructions pursuant to this Agreement.

Appendix 5

Data importer has assessed the data protection laws, regulations and practices in the jurisdictions where it processes data exporter's personal data, namely: EEA ("Processing Jurisdictions").

Data importer has determined that laws and practices in the Processing Jurisdictions applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, do not prevent the data importer from fulfilling its obligations under these Clauses, having taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

The main reasons for this assessment are to comply with the applicable Data Protection laws and regulations.